البنى الجبرية

قسم الاحصاء

السنة الثانية

تنويـــــه

نرجو من القارئ الكريم الانتباه إلى أنه في هذا الكتاب استُخدِمَ:

- الرمز Y بدلاً من الرمز المألوف $\cup$ (الاجتماع).
- الرمز I بدلاً من الرمز المألوف $\cap$ (التقاطع).

منشورات جامعة دمشق
كلية العلوم

البنى الجبرية

الدكتور
يوسف الوادي
الأستاذ المساعد في قسم الرياضيات

الدكتور
عبد اللطيف هنانو
المدرس في قسم الرياضيات

جامعة دمشق

١٤٣٢ - ١٤٣٣ هـ
٢٠١١ - ٢٠١٢ م

الفهـــرس

الموضـــوع	الصفحـة
- الفهـــرس	٥
- المقـــدمة	١٢
الفصل الأول : مبادئ نظرية المجموعات	
١ — ١ - مقدمـــة	١٥
١ — ٢ - مبدأ الثنوية	١٦
١ — ٣ - طرائق إثبات صحة مطابقة	١٨
١ — ٤ - التغطية والتجزئة	٢١
١ — ٥ - العلاقات الثنائية في المجموعة	٢٢
١ — ٥ — ١ تعاريف	٢٢
١ — ٥ — ٢ صفات العلاقات الثنائية في مجموعة	٢٣
١ — ٥ — ٣ علاقة التكافؤ	٢٤
١ — ٥ — ٤ علاقة الترتيب	٣١
١ — ٦ - الشبكات	٣٤
١ — ٧ - قدرة مجموعة	٣٥
١ — ٨ - المجموعات القابلة للعد	٤٠
تمـــرينات محلولة	٤١
تمـــرينات (١)	٤٥

الموضـــــوع	الصفحـــة

الفصل الثاني :التطبيقات The Mappings

٢ — ١ - مقدمـــة	٤٩
٢ — ٢ - المخططات التبديلية للتطبيقات	٥١
٢ — ٣ - بعض التطبيقات الشهيرة	٥٩
تمـــرينات محلولة	٦٥
تمـــرينات (٢)	٦٨

الفصل الثالث : مجموعة الأعداد الطبيعية

٣ — ١ - مقدمـــة	٧١
٣ — ٢ - وصف مجموعة الأعداد الطبيعية	٧١
٣ — ٣ - عملية الجمع في **N**	٧٣
٣ — ٤ - عملية الضرب في **N**	٧٧
٣ — ٥ - قابلية القسمة في **N**	٨٢
٣ — ٦ - القاسم المشترك الأكبر والمضاعف المشترك الأصغر في **N**	٨٥
٣ — ٧ - الأعداد الأولية	٨٦
تمـــرينات محلولة	٩٠
تمـــرينات (٣)	٩٧

الفصل الرابع : مجموعة الأعداد الصحيحة

٤ — ١ - بناء مجموعة الأعداد الصحيحة	٩٩
٤ — ٢ - عمليتا الجمع والضرب في **Z**	١٠٠

الموضـــوع	الصفحـة

٤ — ٣ — الشكل المألوف لمجموعة الأعداد الصحيحة	١٠١
٤ — ٤ — قابلية القسمة في Z	١٠٣
٤ — ٥ — القاسم المشترك الأكبر لعددين صحيحين	١٠٤
٤ — ٦ — الأعداد الصحيحة غير القابلة للتحليل	١٠٨
تمـــرينات محلولة	١١٠
تمـــرينات (٤)	١١٣

الفصل الخامس : نظرية الزمر

٥ — ١ — مقدمة	١١٥
٥ — ٢ — تعريفات	١١٥
٥ — ٣ — بعض خواص الزمرة	١٢٤
٥ — ٤ — القوى ذات الأسس الصحيحة في الزمر	١٢٥
٥ — ٥ — مرتبة عنصر في زمرة	١٣٠
٥ — ٦ — المرافقات اليسارية والمرافقات اليمينية لزمرة جزئية	١٣١
٥ — ٧ — زمرة خارج القسمة	١٣٦
٥ — ٨ — الزمرة المولدة بمجموعة — الزمرة الدوارة	١٣٧
٥ — ٩ — التشاكلات الزمرية	١٤٠
تمـــرينات محلولة	١٥٣
تمـــرينات (٥)	١٥٩

الموضـــوع	الصفحـة

الفصل السادس : نظرية الحلقات ، الحقول

٦ — ١ — تعريف	١٦١
٦ — ٢ — خواص الحلقة	١٦٢
٦ — ٣ — الحلقة التامة — المنطقة التكاملية	١٦٤
٦ — ٤ — العناصر القلوبة في الحلقة	١٦٦
٦ — ٥ — الحقل	١٦٧
٦ — ٦ — مميز الحلقة	١٦٨
٦ — ٧ — الحلقة الجزئية — الحقل الجزئي	١٧٠
٦ — ٨ — المثاليات في الحلقة	١٧١
٦ — ٩ — الحلقات الجزئية المولدة بمجموعة ، المثاليات المولدة بمجموعة	١٧٣
٦ — ١٠ — العمليات على المثاليات	١٧٥
٦ — ١١ — التشاكلات الحلقية	١٧٧
٦ — ١٢ — حلقة خارج القسمة	١٨١
٦ — ١٣ — المثاليات الأولية والأعظمية في الحلقات التبديلية	١٨٤
٦ — ١٤ — حلقة المثاليات الرئيسة	١٨٥
٦ — ١٥ — القواسم والعناصر المتشاركة في الحلقة التبديلية	١٨٦
٦ — ١٦ — حلقة التحليل الوحيد	١٨٩
٦ — ١٧ — الحلقة الإقليدية	١٩٤
٦ — ١٨ — القاسم المشترك الأكبر في المنطقة التكاملية	١٩٦

الموضـــوع	الصفحـة

٦ — ١٩ - الحقول الأولية في حقل	١٩٨
٦ — ٢٠ - حلقة الكسور	٢٠١
٦ — ٢١ - الجداء المباشر للحلقات	٢٠٤
تمـــرينات محلولة	٢٠٦
تمـــرينات (٦)	٢١٤
الفصل السابع : حقل الأعـــداد العقدية	
٧ — ١ - بناء حقل الأعداد العقدية	٢١٧
٧ — ٢ - الشكل المألوف للأعداد العقدية	٢١٧
٧ - ٣ - مرافقات عدد عقدي	٢١٩
٧ — ٤ - طويلة عدد عقدي	٢٢٠
٧ — ٥ - المعنى الهندسي لعدد عقدي — الشكل المثلثي لعـــدد عقدي	٢٢٠
٧ — ٦ - الشكل الأسي للعـــدد العقدي	٢٢٢
٧ — ٧ - بعض المعادلات الشهيرة في C	٢٢٥
تمـــرينات محلولة	٢٢٧
تمـــرينات (٧)	٢٢٩
الفصل الثامن : حلقـــة الحـــدوديات (كثيرات الحدود)	
٨ — ١ — بناء حلقة الحـــدوديات	٢٣١
٨ — ٢ - الشكل المألوف للحـــدودية	٢٣٢
٨ — ٣ - درجة الحـــدودية	٢٣٤

الموضـــوع	الصفحـة

٨ — ٤ — قابلية القسمة في F[X]	٢٣٦
٨ — ٥ — مشتق الحـدودية	٢٤٦
تمـرينات محلولة	٢٥٣
تمـرينات (٨)	٢٥٨
الفصل التاسع : الفضاءات الشعاعية على حلقة تبديلية واحدية المودولات (المقاسات)	
٩ — ١ — المقاس	٢٦١
٩ — ٢ — المقاسات الجزئية	٢٦٣
٩ — ٣ — مقاس خارج القسمة	٢٦٧
٩ — ٤ — التشاكلات المقاسية	٢٦٨
تمـرينات محلولة	٢٧٥
تمـرينات (٩)	٢٧٩
الفصل العاشر : تمـديد الحقول ، الحقول المنتهية	
١٠ — ١ — مقدمـة	٢٨١
١٠ — ٢ — تمـديد الحقل	٢٨١
١٠ — ٣ — العناصر الجبرية والعناصر المتسامية	٢٨٥
١٠ — ٤ — التمـديد البسيط	٢٩٠
١٠ — ٥ — تطبيقات تمديد الحقول في الإنشاءات الهندسية	٢٩٥
تمـرينات محلولة	٢٩٩
تمـرينات (١٠)	٣٠٢

الموضـــــوع	الصفحـــة

الفصل الحادي عشر : مبادئ نظريـــة الجبـــور

١١ — ١ - تعاريف	٣٠٥
١١ — ٢ - الجـــبر الجزئـــي	٣٠٦
١١ — ٣ - المثاليات في الجـــبر	٣٠٦
١١ — ٤ - جـــبر القسمة	٣٠٧
١١ — ٥ - التشاكلات الجـــبرية	٣٠٩
١١ — ٦ - تشاكل الاشتقاق	٣١٢
١١ — ٧ - جـــبر لـــي **Algebra Lie**	٣١٣
١١ — ٨ - جـــبر لـــي التبادلي	٣١٥
تمـــرينات محلولة	٣١٦
تمـــرينات (١١)	٣٢٠
المصطلحات العلمية	٣٢٢
المراجع العلمية	٣٢٨
اللجنة العلمية	٣٢٩

المقدمة

يعد الجبر أحد الفروع الرئيسة الهامة من الرياضيات البحتة لما له من دورٍ مهمٍ في تطوير الرياضيات التي تشكل أساس تطوير كثير من العلوم مثل التحليل والاحتمالات والإحصاء والهندسة بجميع فروعها ، حيث كان للجبر فضل كبير في تطوير علوم الإحصاء والاحتمالات .

لقد عَرضنا في هذا الكتاب المفاهيم الأساسيَّة في الجبر المجرد التي تلبي حاجات الطالب لدراسة علوم الإحصاء ، ولقد عَمدنا عرض هذه المفاهيم بلغةٍ مبسطة لتصبح سهلة الفهم للطالب ، وأتبعنا كل فصل بعدد من التمارين المحلولة لتغطية هذه المفاهيم ولترسيخها وتعميقها في ذهن الطالب .

وتضمن هذا الكتاب مفردات المنهاج المقررة في أحد عشر فصلاً على النحو التالي :

الفصل الأول : مبادئ نظرية المجموعات، وتتضمن جبر المجموعات والعلاقات الثنائية (علاقة التكافؤ - علاقة الترتيب) وأسرة المجموعات .

الفصل الثاني : التطبيقات وتتضمن خواص الصورة المباشرة والصورة العكسية والمخططات التبديلية للتطبيقات وبعض التطبيقات المشهورة .

الفصل الثالث : مجموعة الأعداد الطبيعيةN ، وتتضمن موضوعات بيانو وعملية الجمع والضرب فيN وخواصها .

الفصل الرابع : مجموعة الأعداد الصحيحة Z ، وتتضمن بناء مجموعة الأعداد الصحيحة وعملية الجمع والضرب في Z وخواصها .

الفصل الخامس : نظرية الزمر وتتضمن الزمر الدوارة وزمرة القسمة ومبرهنات التماثل الزمري و الـ P زمرة .

الفصـــل السادس : نظرية الحلقات والحقول، وتتضمن المثاليات والعمليات عليها ، حلقة القسمة ، حلقة المثاليات الرئيســة ، حلقة التحليل الوحيد ، الحلقة الإقليدية ، حلقة الكسور .

الفصـــل السابع : حقل الأعـــداد العقديـــة، ويتضمن الشكل الديكـــارتي والشكل المثلثي والشكل القطبي لعدد عقدي وخواصها .

الفصل الثامن : حلقة الحد وديات (كثيرات الحدود) .

الفصل التاسع : الفضاءات الشعاعية على حلقة تبديلية (المقاسات) .

الفصل العاشر : ويدرس تمـــديد الحقـــول والحقـــول المنتهية .

الفصل الحادي عشر : ويعالج نظريـــة الجـــبور ، جـــبر لـــي Lie Algebra .

وأخـــيراً ، نـــأمل أن نكون قد وفقنا في صياغة مفردات هذا الكتاب ، كما نرجو أن يكون هذا الكتاب مساهمة متواضعة في إثراء المكتبة العربية بالكتب العلمية العربية .

المؤلفان

الدكتور : يوسف الوادي

الدكتور : عبد اللطيف هنانو

الفصل الأول

مبادئ نظرية المجموعات

١-١- مقدمة :

تعد نظرية المجموعات الركيزة الأساسية في علم الجبر المجرد ، الذي بدوره يشكل المنطلق الرئيس في تطور علوم الجبر بشكل خاص والعلوم التطبيقية بشكل عام ، حيث تعتمد هذه العلوم - في كثير من الأحيان - على المجموعات والعمليات عليها والتي تؤلف ما يسمى بجبر المجموعات .

إن جبر المجموعات هو قوانين العمليات :

الاجتماع Y ، التقاطع I ، المتمم/ . بالإضافة إلى نتائج تلك القوانين

إذا كان A , B , C ثلاث مجموعات من مجموعة شاملة نسبياً M ، فإن :

$$1-\begin{cases} A \,Y\, A = A \\ A \,I\, A = A \end{cases}$$

$$2-\begin{cases} A \,Y\, B = B \,Y\, A \\ A \,I\, B = B \,I\, A \end{cases}$$

$$3-\begin{cases} A \,Y\, (B \,Y\, C) = (A \,Y\, B) \,Y\, C \\ A \,I\, (B \,I\, C) = (A \,I\, B) \,I\, C \end{cases}$$

$$4-\begin{cases} A \,Y\, (B \,I\, C) = (A \,Y\, B) \,I\, (A \,Y\, C) \\ A \,I\, (B \,Y\, C) = (A \,I\, B) \,Y\, (A \,I\, C) \end{cases}$$

$$5-\begin{cases} A \,Y\, M = M \quad ; \quad A \,Y\, \phi = A \\ A \,I\, M = A \quad ; \quad A \,I\, \phi = \phi \end{cases}$$

$$6-\begin{cases}(A')'=A\\ M'=\phi \quad ; \quad \phi'=M\end{cases}$$

$$7-\begin{cases}(A\,\mathrm{Y}\,B)'=A'\,\mathrm{I}\,B'\\ (A\,\mathrm{I}\,B)'=A'\,\mathrm{Y}\,B'\end{cases}$$

نلاحظ من هذه القوانين أنها صيغت من أجل العمليات Y ، I ، / فقط على الرغم من وجود عمليات أخرى على المجموعات مثل Δ "الفرق التناظري" و - "الفرق". ويبرر ذلك أنه يمكن التعبير عن العمليتين Δ ، - بدلالة العمليات Y ، I ، / وفق العلاقتين :

$$A-B=A\,\mathrm{I}\,B'$$
$$A\Delta B=(A-B)\,\mathrm{Y}\,(B-A)=(A\,\mathrm{I}\,B')\,\mathrm{Y}\,(B\,\mathrm{I}\,A')$$

١ – ٢ مبدأ الثنويَّة (Dual Principle):

وجدنا في الفقرة السابقة أن كلاً من العمليتين (–) , (Δ) يمكن التعبير عنهما بدلالة العمليات Y ، I ، / وبالتالي كل عبارة (تركيب) على المجموعات يمكن كتابتها بدلالة Y ، I ، / فقط .

تعريف (١): لتكن M مجموعة شاملة نسبياً ولتكن $P(M)$ مجموعة أجزاء M. نسمي كل مجموعة جزئية من $P(M)$ أسرة مجموعات من المجموعة M ، ونسمي كل مجموعة ناتجة من الأسرة Γ بوساطة العمليات Y ، I ، / تركيب من Γ ونرمز له بـ $T(\Gamma)$

مثال :

إذا كانت $M = \{1,2,3\}$ مجموعة شاملة نسبياً فإن كلاً من :

$$\Gamma_1 = \{\{1\}, \{1,2\}\}$$
$$\Gamma_2 = \{\phi, \{1\}, \{3\}\}$$
$$\Gamma_3 = \{\phi, M\}$$

أسرة مجموعات من المجموعة M . وأن :

$T_1 = \{1\} \text{ I } \{1,2\}'$ تركيب من الأسرة Γ_1

$T_2 = \{1\}'$ تركيب من الأسرة Γ_2

$T_3 = \{1\} \text{ Y } \{3\}$ تركيب من الأسرة Γ_2 وليس تركيباً من Γ_1

لاحظ أن $\phi \notin \Gamma_1$ بينما $\phi \in \Gamma_2$

تعريف (٢) : لتكن Γ أسرة مجموعات من المجموعة M وليكن T تركيباً من الأسرة Γ . نعرّف ثنويّة التركيب $\dot{Q}$ من Γ الذي ينتج من T باستبدال :

- الاجتماع Y بالتقاطع I .
- التقاطع I بالاجتماع Y .
- المجموعة الخالية ϕ بالمجموعة الشاملة نسبياً M .
- المجموعة الشاملة نسبياً M بالمجموعة الخالية ϕ .

أمثلة :

١. اكتب ثنويّة التركيب :

$$T = (A \text{ Y } B') \text{ I } A$$

<u>الحل</u> : إن ثنويّة التركيب T هو التركيب :

$$Q = (A \text{ I } B') \text{ Y } A$$

٢. اكتب ثنويّة التركيب :

$$T = A - (B \mathrm{I}\ C)$$

الحل : نعبّر عن التركيب T بدلالة العمليات Y ، I ، / فنجد

أن : $T = A \mathrm{I}\ (B \mathrm{I}\ C)'$

وبالتالي يكون ثنوية التركيب المعطى هو التركيب $Q = A\,Y(B\,Y\,C)'$

- **نص مبدأ الثنويّة :**

ليكن T_1, T_2 تركيبين من أسرة مجموعات Γ وليكن Q_1, Q_2 التركيبين الثنويين للتركيبين T_1, T_2 على الترتيب عندئذٍ :

إذا كان $T_1 \equiv T_2$ مطابقة صحيحة فإن $Q_1 \equiv Q_2$ تكون صحيحة .

١ - ٣ طرائق إثبات صحة مطابقة في المجموعات :

ليكن T_1, T_2 تركيبين من أسرة مجموعات ما Γ . لمناقشة صحة المطابقة T_1, T_2 هناك عدة طرائق يمكن اعتمادها و من أهمها :

- **الطريقة الأولى :** تعتمد على طريقة العناصر (الطريقة الكلاسيكية) -

الطريقة الثانية : تعتمد على استخدام جبر المجموعات .

- **الطريقة الثالثة :** تعتمد على مبدأ الثنويّة .

- **الطريقة الرابعة :** تعتمد على استخدام جدول الحقيقة .

والأمثلة النموذجية الآتية توضح كيفيّة تطبيق كلٍ من هذه الطرائق .

مثال (١) : بفرض A, B مجموعتين من مجموعة شاملة M . برهن أن :

$$(A \mathrm{I}\ B)\,Y\,(A \mathrm{I}\ B') = A$$

الحل : الأسلوب الأول (الطريقة الكلاسيكية) :

$$\forall x \in (A \cap B) \cup (A \cap B') \Leftrightarrow x \in (A \cap B) \text{ أو } x \in (A \cap B')$$

$$\Leftrightarrow (x \in A, x \in B) \text{ أو } (x \in A, x \in B')$$

$$\Leftrightarrow x \in A, (x \in B, \text{ أو } x \in B')$$

$$\Leftrightarrow x \in A, x \in B \cup B'$$

$$\Leftrightarrow x \in A, x \in M$$

$$\Leftrightarrow x \in A$$

وبالتالي : $(A \cap B) \cup (A \cap B') = A$

الأسلوب الثاني : (طريقة جبر المجموعات) .

$$(A \cap B) \cup (A \cap B') = A \cap (B \cup B')$$

$$= A \cap M$$

$$= A$$

الأسلوب الثالث : (طريقة جدول الحقيقة) .

ليكن x عنصراً كيفياً من المجموعة الشاملة نسبياً M ، نضع في الجدول القيمة 1 عندما ينتمي العنصر x إلى المجموعة المكتوبة في أعلى العمود ، ونضع القيمة 0 عندما لا ينتمي العنصر x إلى المجموعة المكتوبة في أعلى العمود . وإذا رمّزنا الطرف الأول بـ T_1 والطرف الثاني بـ T_2 فيكون $T_1 \equiv T_2$ فقط عندما تتطابق قيم الحقيقة للعمود T_1 مع القيم الحقيقة المقابلة لها في العمود T_2.

في مثالنا يكون الجدول التالي :

A	B	B'	$A \cap B$	$A \cap B'$	$(A \cap B) \cup (A \cap B')$
1	1	0	1	0	1
1	0	1	0	1	1
0	1	0	0	0	0
0	0	1	0	0	0

بمقارنة العمودين الأول والأخير نجد أن : $(A \cap B) \cup (A \cap B') = A$

مثال (٢) : بفرض A,B مجموعتين ما من مجموعة شاملة نسبياً M .

أثبت صحة القضيتين : $(A \cup B)' = A' \cap B'$ (I).

$(A \cap B)' = A' \cup B'$ (II).

الحل : لإثبات (I) نعتمد على جدول الحقيقة :

A	B	$A \cup B$	$(A \cup B)'$	A'	B'	$A' \cap B'$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

من العمودين الرابع والأخير نجد أن القضية (I) صحيحة .

إثبات (II) :

حسب مبدأ الثنويّة تكون (II) صحيحة (لأن (II) هي ثنويّة المطابقة (I)).

مثال (٣) : بفرض A , B, C ثلاث مجموعات من مجموعة شـــاملة نسبياً M

أثبت أن : $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$

الحل : لنعتمد طريقة جدول الحقيقة ولذلك نكتب جدول الحقيقة :

A	B	C	$B \Delta C$	$A \cap (B \Delta C)$	$A \cap B$	$A \cap C$	$(A \cap B) \Delta (A \cap C)$
1	1	1	0	0	1	1	0
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

من العمودين الخامس و الأخير نجد أن :

$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$$

١ – ٤ – التغطيّة والتجزئة :

وجدنا في الفقرة السابقة أن أسرة المجموعـــات هي عبارة عن مجموعةٍ ، عناصرها مجموعات وأن لأسرة المجموعات الشكل :

$$\Gamma = \{A_1 , A_2 , \dots , A_n , \dots\}$$

والتي نكتبها بالشكل المختصر :

$$\Gamma = \{A_i \ ; \ i \in I\} \quad \text{حيث} \quad I = \{1 , 2 , \dots , n , \dots\}$$

ونقول عن الأســرة $\Gamma = \{A_i \ ; \ i \in I\}$ إنهـــا غـــير منتهية عندما تكون المجموعـــة I غير منتهيّة ، أما إذا كانت المجموعة I منتهية فإننا نقول عن الأسرة Γ إنها أسرة منتهيّة .

أما في الحالـــة التي تكون فيها $I = \phi$ فنقول عن الأسرة Γ عندئذٍ إنها أسرة خالية .

تعاريف :

لنكن $\Gamma = \{A_i \ ; \ i \in I\}$ أسرة مجموعات ما :

١- نعرّف اجتماع الأسرة Γ ونرمز لـــه بـــ $\bigcup_{i \in I} A_i$ بأنـــه المجموعـــة :

$$\bigcup_{i \in I} A_i = \{x \in A_i \ ; \ \forall i \in I\}$$

$$= \{x : \exists i_0 \in I \ : \ x \in A_{i_0}\}$$

٢- نعرّف تقاطع الأسرة Γ ونرمـــز لـــه بـــ $\bigcap_{i \in I} A_i$ بأنـــه المجموعـــة :

$$\bigcap_{i \in I} A_i = \{x \ ; \forall i \in I \ : \ x \in A_{i_0}\}$$

وتجـــدر الإشارة هنا أنـــه من أجل الأسرة الخـــالية يكون $\bigcup_{i \in I} A_i = \phi$

ويكون تقاطع الأسرة الخالية :

$$\bigcap_{i\in I} A_i = (\bigcup_{i\in I} A_i)' = (\phi)' = M$$

٣- نقول عن الأسرة $\Gamma = \{A_i \ ; \ i \in I\}$ إنها تغطية لمجموعة X عندما يتحقق الشرط : $X \subseteq \bigcup_{i\in I} A_i$

٤ - نقول عن الأسرة $\Gamma = \{A_i \ ; \ i \in I\}$ إنها تجزئة لمجموعة X عندما تتحقق الشروط :

1. $\forall A_i \in \Gamma \ : \ A_i \neq \phi$
2. $\forall i, j \in I \ : \ A_i \cap A_j = \phi$ أو $A_i = A_j$
3. $\bigcup_{i\in I} A_i = X$

ملاحظة : نلاحظ من التعرفين الأخيرين أن كل تجزئة لمجموعة X تكون تغطيّة لها ، لكن العكس غير صحيح .

أمثلة : إذا كانت $X = \{a,b,c\}$ فإن :

١ - الأسرة : $\Gamma_1 = \{\{a\},\{b\},\{c\}\}$ تشكل تجزئة للمجموعة X وبالتالي فهي تغطية لـ X

٢ - الأسرة : $\Gamma_2 = \{\phi,\{a\},\{b,c\}\}$ لا تشكل تجزئة للمجموعة X لأن $\phi \in \Gamma_2$ ، لكن Γ_2 تشكل تغطية لـ X

٣ - الأسرة : $\Gamma_3 = \{X\}$ تشكل تجزئة للمجموعة X وبالتالي فهي تغطية لـ X .

١ - ٥ - العلاقات الثنائية : (Binary Relations)

١ - ٥ - ١ تعاريف :

تعريف (١) : لتكن A , B مجموعتين ما ولتكن G مجموعة جزئية

من الجداء الديكارتي $A\times B$. عندئذ نقول عن المجموعة G إنها بيان في المجموعة $A\times B$ ، وإذا كان $(a,b)\in G$ فإننا نقول إن العنصر b يرتبط بالعنصر a وفق البيان G

تعريف (٢) : ليكن G بياناً في المجموعة $A\times B$. نقول عن الثلاثية $R(A,B,G)$ إنها علاقة ثنائية بين عناصر المجموعة A وعناصر المجموعة B ، إذا كان $a\in A$, $b\in B$

فإننا نقول إن a مرتبط بـ b ونكتب aRb عندما $(a,b)\in G$ أي : $(a,b)\in G \Leftrightarrow aRb$

وفي حالة خاصة : إذا كان $A=B$ نقول عن العلاقة الثنائية R إنها علاقة ثنائية في المجموعة A .

تعريف (٣) : نعرّف العلاقة العكسية للعلاقة الثنائية $R(A,B,G)$ بأنها العلاقة الثنائية $R^{-1}(B,A,G^{-1})$ حيث $G^{-1}\subseteq B\times A$

ويعرّف كما يلي :

$$G^{-1}=\{(b,a):(b,a)\in B\times A;(a,b)\in G\}$$

أي أن :

$$(b,a)\in G^{-1} \Leftrightarrow bR^{-1}a \Leftrightarrow aRb \Leftrightarrow (a,b)\in G$$

وبسهولة يمكن للقارئ إثبات أن :

$$(G^{-1})^{-1}=G \quad ; \quad (R^{-1})^{-1}=R$$

١ – ٥ – ٢ صفات العلاقة الثنائية في مجموعة :

إذا كانت R علاقة ثنائية في مجموعة غير خالية A فإن العلاقة R يمكن أن تتمتع بالصفات التالية :

١. **الانعكاسية** : نقول عن العلاقة الثنائية R إنها انعكاسية عندما يتحقق الشرط :

$$\forall x \in A \ : \ xRx$$

٢. **التناظرية** : نقول عن العلاقة الثنائية R إنها تناظرية عندما يتحقق الشرط :

$$\forall x, y \in A \ : \ xRy \ \Rightarrow \ yRx$$

٣. **تخالفيّة** : نقول عن العلاقة الثنائية R إنها تخالفيّة عندما يتحقق الشرط :

$$\forall x, y \in A \ : \ (xRy) \wedge (yRx) \ \Rightarrow \ x = y$$

٤. **متعدية** : نقول عن العلاقة الثنائية R إنها متعدية عندما يتحقق الشرط :

$$\forall x, y, z \in A \ : \ (xRy) \wedge (yRz) \ \Rightarrow \ xRz$$

١ـ٥ ـ ٣ علاقة التكافؤ : (Equivalence Relation)

تعريف (١) : نقول عن العلاقة الثنائية R المعرفة في المجموعة غير الخالية A إنها علاقة تكافؤ عندما تكن R انعكاسية و تناظرية ومتعدية .

تعريف (٢) : إذا كانت R علاقة تكافؤ في مجموعة A ، وإذا كان $a \in A$ فإننا نعرّف صف تكافؤ العنصر a ونرمز له بـ $[a]$ بأنه مجموعة العناصر :

$$[a] = \{x \in A ; xRa\}$$

وندعو العنصر a ممثلاً لصف التكافؤ $[a]$ ونرمّز مجموعة صفوف التكافؤ للمجموعة A وفق R بالرمز A/R أي :

$$A / R = \{[x] \; ; \; x \in A\}$$

مبرهنة : إذا كانت R علاقة تكافؤ في مجموعة A ، وإذا كان $a,b \in A$

فإن : $b \in [a] \Leftrightarrow [a] = [b]$

الإثبات : ($\Leftarrow$) واضح وذلك حسب تعريف صف التكافؤ .

($\Rightarrow$) لنفرض أن $b \in [a]$ ولنبرهن على أن $[a] = [b]$.

من جهة أولى :

$$\left.\begin{array}{l} \forall x \in [a] \Rightarrow xRa \\ b \in [a] \Rightarrow bRa \Rightarrow aRb \end{array}\right\} \Rightarrow xRb \Rightarrow x \in [b]$$

أي أن : $[a] \subseteq [b] \qquad (\mathrm{I})$

ومن جهة أخرى :

$$\left.\begin{array}{l} \forall y \in [b] \Rightarrow yRb \\ b \in [a] \Rightarrow bRa \end{array}\right\} \Rightarrow yRa \Rightarrow y \in [a]$$

أي أن :

$$[b] \subseteq [a] \qquad (\mathrm{II})$$

من (I) و (II) نجد أن : $[a] = [b]$

مبرهنة : أية علاقة تكافؤ في مجموعة غير خالية تعيّن تجزئة لهذه المجموعة ، وبالعكس كل تجزئة لمجموعة غير خالية تعرف في هذه المجموعة علاقة تكافؤ .

الإثبات : أولاً : لتكن R علاقة تكافؤ في مجموعة غير خالية A . إن A/R (مجموعة صفوف التكافؤ لعناصر المجموعة A وفق R) تشكل تجزئة للمجموعة A وذلك للأسباب التالية :

I. أياً كان $x \in A$ فإن x ينتمي إلى صف تكافؤ . أي :

$$\forall [x] \in A/R \Rightarrow [x] \neq \phi$$

II. أياً كان $[x],[y] \in A/R$ فإما $[x]=[y]$ أو $[x] \cap [y] = \phi$ وذلك

لأنه إذا كان $[x] \cap [y] \neq \phi$

فإنه يوجد عنصر مثل a من المجموعة A بحيث يكون $a \in [x] \cap [y]$

وبالتالي يكون :

$$a \in [x] \quad \wedge \quad a \in [y]$$

وحسب المبرهنة السابقة سيكون :

$$[a]=[x] \wedge [a]=[y]$$

ومنه : $[x]=[y]$

III. بما أن كل عنصر من المجموعة A ينتمي إلى صف تكافئه ، فإن :

$$\bigcup_{x \in A} [x] = A$$

من I و II و III نجد أن الأسرة $\Gamma = \{[x]; x \in A\}$ قد حققت الشروط الثلاثة للتجزئة إذن مجموعة صفوف التكافؤ تشكل تجزئة للمجموعة A .

ثانياً :

لتكن $\Gamma = \{ A_i \ ; \ i \in I \}$ تجزئة لمجموعة غير خالية A . لنعرّف في المجموعة A علاقة ثنائية R كما يلي :

$$\forall a,b \in A : \{ aRb \Leftrightarrow \exists \ j \in I : a \in A_j \wedge b \in A_j \}$$

عندئذ يكون لدينا ما يلي :

(i). أياً كان العنصر $x \in A$ فإن :

$$x \in A \Rightarrow x \in \bigcup_{i \in I} A_i \Rightarrow \exists \ j \in I : a \in A_j \wedge b \in A_j$$

أي أن العلاقة R انعكاسية .

(ii). أياً كان العنصران $x,y \in A$ بحيث xRy فإن :

$$xRy \Rightarrow \exists j \in I \ : \ x \in A_j \ \wedge \ y \in A_j$$

هذا يعني أن yRx . أي أن العلاقة R تناظرية .

(iii). أياً كانت العناصر $x,y,z \in A$ بحيث $(xRy) \wedge (yRz)$ فإن :

$$xR\,y \Rightarrow \exists j \in I \ : \ x \in A_j \ \wedge \ y \in A_j$$

$$yR\,z \Rightarrow \exists k \in I \ : \ y \in A_k \ \wedge \ z \in A_k$$

وبالتالي نجد أن : $y \in A_k \cap A_j$

وبما أن : A_j ، A_k صفا تجزئة

فإن : $A_k = A_j$ ومنه $x \in A_j \wedge z \in A_j$ وهذا يعني أن xRz

أي أن العلاقة R متعدية .

إذاً العلاقة R المعرفة أعلاه هي انعكاسية وتناظرية ومتعدية فهي علاقة تكافؤ في A .

تمرين مشهور :ليكن n عدداً صحيحاً موجباً ، ولتكن R علاقة ثنائية معرفة في Z (مجموعة الأعداد الصحيحة) كما يلي :

$aRb \Leftrightarrow$ [يقبل العدد $(a-b)$ القسمة على n في Z] .

حيث $a,b \in Z$. المطلوب :

١. برهن أن العلاقة الثنائية R هي علاقة تكافؤ في Z.

٢. أوجد المجموعة Z/R .

الحل :

١. إن العلاقة الثنائية R هي علاقة تكافؤ في Z وذلك للأسباب الآتية :

أ – أياً كان $x \in Z$ فإن $x - x = 0$ وبالتالي $x - x$ يقبل القسمة على n في Z ومنه xRx . أي أن R انعكاسية .

ب – إذا كان $x,y \in Z$ بحيث xRy فإن $x - y$ يقبل القسمة على

n في Z وبالتالي $x-y$ يقبل القسمة على n في Z .

ومنه yRx . أي أن R تناظرية .

جـ – إذا كان $x,y,z \in Z$ بحيث $(xRy) \wedge (yRz)$ فإننا نجد

$$xRy \Leftrightarrow \exists n_1 \in Z : x - y = n.n_1$$
$$yRz \Leftrightarrow \exists n_2 \in Z : y - z = n.n_2$$

وبالتالي :

$$(x - y) + (y - z) = n.n_1 + n.n_2$$

أي: $x - z = n.(n_1 + n_2) \quad ; \quad (n_1 + n_2) \in Z$

ومنه xRz أي أن R متعدية .

إذاً العلاقة الثنائية R انعكاسية وتناظرية ومتعدية فهي علاقة تكافؤ.

١. إيجاد المجموعة Z/R :

$$\forall a \in Z : \quad [a] = \{x \in Z \ : \ aRx\}$$
$$= \{x \in Z : x - a = n.n_0 \ ; \ n_0 \in Z\}$$
$$= \{x \in Z : x = a + n.n_0 \ ; \ n_0 \in Z\}$$

وبهذا يكفي أن يكون $a \in \{0,1,...,n-1\}$ لتعين مجموعة صفوف التكافؤ Z/R . ومنه :

$$Z/R = \{[0],[1],...,[n-1]\}$$

فمثلاً من أجل $n = 7$ نحصل على مجموعة صفوف التكافؤ :

$$[0] = \{...,-14,-7,0,7,14,...\}$$
$$[1] = \{...,-13,-6,1,8,15,...\}$$
$$[2] = \{...,-12,-5,2,9,16,...\}$$
$$[3] = \{...,-11,-4,3,10,17,...\}$$
$$[4] = \{...,-10,-3,4,11,18,...\}$$
$$[5] = \{...,-9,-2,5,12,19,...\}$$
$$[6] = \{...,-8,-1,6,13,20,...\}$$
$$[7] = \{...,-7,0,7,14,21,...\} = [0].$$

وبشكل عام سنرمّز المجموعة Z/R بالرمز Z/nZ ويكون فيها:

$$[n]=[0] \;;\; [n+1]=[1] \;;\ldots;\; [n+r]=[r] \;;\; 0 < r < n$$

إن علاقة التكافؤ السابقة تدعى التطابق بالمقياس n في Z ونكتب عادة $a \equiv b(\bmod n)$ بدلاً من aRb .

كما أن لهذه العلاقة دوراً هاماً في كثير من العلوم الرياضية بشكل عـــام وفي التحليل التوافقي بشكل خاص.

هذا ويكون :

$$\begin{aligned} a \equiv b(\bmod\ n) &\Leftrightarrow \exists k \in Z : b-a = kn \\ &\Leftrightarrow \exists k \in Z : b = a+kn \end{aligned}$$

فمثلاً :

$7 \equiv 2 \pmod 5$.

$13 \equiv 6 \pmod 7$.

$111222 \equiv 0 \pmod 3$.

نتائـــــج :

ليكن n عدداً صحيحاً بحيث $n > 1$. وليكن $a,b,c,d \in Z$ بحيث

$$a \equiv b \pmod n \quad \wedge \quad c \equiv d \pmod n$$

فإن :

١ . $(a+c) \equiv (b+d) \pmod n$

٢ . $(a-c) \equiv (b-d) \pmod n$

٣ . $(a.c) \equiv (b-d) \pmod n$

٤ . إذا كان $c \neq 0$ و $d \neq 0$ وكان c قاسماً لـــ a وكان d قاسماً لـــ b فليس من الضروري أن يكون $a/c \equiv b/d(\bmod n)$

الـــبرهان :

بما أن : $a \equiv b \pmod n \quad \wedge \quad c \equiv d \pmod n$

فإنه يوجد $k_1, k_2 \in Z$ بحيث :

$$a = b + n k_1 \quad \wedge \quad c = d + n k_2$$

١ . إن : $k_1 + k_2 \in Z \quad ; \quad a + c = (b + d) + n(k_1 + k_2)$

وبالتالي :

$$a + c \equiv (b + d) \pmod{n}$$

٢ . إن : $k_1 - k_2 \in Z \quad ; \quad a - c = (b - d) + n(k_1 - k_2)$

وبالتالي : $a - c \equiv (b - d) \pmod{n}$

٣ . إن : $a.c = (b + n k_1).(d + n k_2)$

$$= (b.d) + n(b k_2 + d k_1 + n k_1 \cdot k_2) \quad ; \quad b k_2 + d k_1 + n k_1 \cdot k_2 \in Z$$

وبالتالي :

$$a.c \equiv (b.d) \pmod{n}$$

٤ . لإثبات هذه القضية يكفي أن نضرب مثالاً . لنأخذ :

$$a = 28 \quad ; \quad b = 4 \quad ; \quad c = -4 \quad ; \quad d = 2 \quad ; \quad n = 6$$

فنجد أن :

$28 \equiv 4 \pmod{6}$ أي $a \equiv b \pmod{n}$

$4 \equiv 2 \pmod{6}$ اي $c \equiv d \pmod{n}$

لكن $-7 \not\equiv 2 \pmod{6}$ أي $a/c \not\equiv b/d \pmod{n}$

معادلة التوافق الخطي :

تعريف : إن معادلة التوافق الخطي من الشكل : $ax \equiv b \pmod{n}$

حيث a, b, n أعداد صحيحة ثابتة و $n > 1$ ، x متغير يأخذ قيمة في Z.

إذا كان $x_1 \in Z$ حلاً للمعادلة التوافق الخطي $ax \equiv b \pmod{n}$

فإن كل عنصر من عناصر صف التكافؤ $[x_1]$ يكون حلاً للمعادلة

المذكـــورة . وهـــذا يفيدنا في البحـــث عن مجموعـــة حلول المعادلـــة $ax \equiv b \pmod{n}$ حيث نجرب إعطاء المتحـــول x جميع قيم المجموعـــة $\{0,1,2,\ldots,n-1\}$ ثم نأخـــذ اجتماع صفوف التكافـــؤ التي يمثلها قيم x الـــتي حققت المعادلـــة فنحصل على مجموعـــة الحلـــول المطلوبـــة والأمثلة التالية توضح ذلك :

مثال (١) : عيّن في Z مجموعة حلول المعادلة : $6x \equiv 3 \pmod{5}$.

الحـــل : نجعل x يأخذ قيمة من المجموعة $\{0,1,2,3,4\}$ فنجد ان $x = 3$ هي القيمة الوحيدة التي تحقق المعادلة وبالتالي مجموعة حلول المعادلة المذكورة هي $[3]$

مثال (٢) : عيّن في Z مجموعـــة حلول المعادلـــة : $8x \equiv 2 \pmod{6}$

الحـــل : نجعل x يأخذ قيمة من المجموعـــة $\{0,1,2,3,4,5\}$ فنجد أن كـــلاً من القيمتين $x = 4$ و $x = 1$ تحققان المعادلـــة وبالتـــالي مجموعـــة حلول المعادلـــة هـــي $[1] \cup [4]$.

مثال (٣) : عيّن في Z مجموعـــة حلول المعادلـــة : $6x \equiv 5 \pmod{3}$

الحـــل : نجعل x يأخذ قيمة من المجموعـــة $\{0,1,2\}$ فنجـــد أن أياً من هـــذه القيم لا تحقق المعادلـــة وبالتالي مجموعـــة الحلول هـــي ϕ .

١ – ٥ – ٤ علاقة الترتيب : (Ordered Relation)

تعاريف :

١ – نقول عن العلاقة الثنائية R في مجموعة غـــير خالية A إنها علاقـــة ترتيب عندما تكون R انعكاسية، تخالفية ومتعدية ونرمز لها بـــ $\leq$.

٢ – إذا كانت المجموعة A مزودة بعلاقة ترتيب $\leq$ فنقول عن A إنهـــا مرتبة وفق علاقة الترتيب $\leq$ ونكتب $(A,\leq)$.

٣ – إذا كانت $(A,\leq)$ مجموعة مرتبة وكان $a,b \in A$ فتقول عن a,b إنهما متقارنان إذا كان : $a \leq b \quad \vee \quad b \leq a$

٤ – إذا كانت $(A,\leq)$ مجموعة مرتبة ، فنقول عن $(A,\leq)$ إنها مرتبة كلياً إذا كان كل عنصرين من A متقارنين ، ونقول عن $(A,\leq)$ إنها مرتبة جزئياً إذا وجد في A عنصران غير متقارنين .

أمثلـــــــــة :

١ – إن العلاقة $\leq$ المألوفة على الأعداد هي علاقة ترتيب كلي .

٢ – إن العلاقة $\subseteq$ الاحتواء المألوفة على المجموعات هي علاقة ترتيب جزئي .

٣ إن العلاقة $\leq$ المعرفة في $Z - \{0\}$ كما يلي :

$$x \leq y \Leftrightarrow \exists n \in Z \quad ; \quad y = nx$$

هي علاقة ترتيب جزئي – نترك ذلك كتمرين للقارئ–

مبرهنة : لتكن $\leq$ علاقـــة ترتيب في مجموعـــة A ، وليكن بيانها G. عندئـــذٍ

$$G \cup G^{-1} = A^2 \quad \Leftrightarrow \quad (\leq \text{ علاقة ترتيب كلي})$$

الإثبات : $(\Rightarrow)$: لنفرض أولاً أن $\leq$ هي علاقة ترتيب كلي في A ولنبرهن على أن $G \cup G^{-1} = A^2$.

من جهة أولى واضح أن $G \cup G^{-1} = A^2$. (I)

من جهة ثانية : بما أن $\leq$ علاقة ترتيب كلي في A فمن أجل أي عنصر $(x,y) \in A^2$ يكون : $x \leq y \quad \vee \quad y \leq x$

إذا كان $x \leq y$ فإن $(x,y) \in G$ وبالتالي $(x,y) \in G \cup G^{-1}$

وإذا كان $y \leq x$ فإن $(y,x) \in G$ ومنه $(x,y) \in G^{-1}$ وبالتالي :

$(x,y) \in G \cup G^{-1}$ ومنه $A^2 \subseteq G \cup G^{-1}$. (II)

من (I) و (II) نجد أن : $G \cup G^{-1} = A^2$.

($\Leftarrow$) : لنفرض الآن أن $G \cup G^{-1} = A^2$ ولنبرهن على أن العلاقة $\leq$ هي علاقة ترتيب كلي . ليكن $x, y \in A$ عندئذٍ $(x,y) \in A^2$ وحسب الفرض يكون : $(x,y) \in G \cup G^{-1}$ ومنه :

$$\begin{aligned} & (y,x) \in G \quad \vee \quad (x,y) \in G^{-1} \\ \Rightarrow \quad & (y,x) \in G \quad \vee \quad (y,x) \in G \\ \Rightarrow \quad & x \leq y \quad \vee \quad y \leq x \end{aligned}$$

أي أن كل عنصرين من A يكونان متقارنين ، وبالتالي $\leq$ علاقة ترتيب كلي

بعض العناصر الخاصة في مجموعة مرتبة :

لتكن $(A, \leq)$ مجموعة مرتبة ولتكن X مجموعة جزئية غير خالية من A .

* نقول عن العنصر $a \in A$ إنه عنصر راجح على X إذا تحقق :

$$\forall x \in X \quad : \quad x \leq a$$

* نقول عن العنصر $b \in A$ إنه عنصر قاصر عن X إذا تحقق :

$$\forall x \in X \quad : \quad b \leq x$$

* نقول عن العنصر $c \in A$ إنه أكبر عنصر في X إذا تحقق :

$$\forall x \in X \quad : \quad (x \leq c) \quad \wedge \quad (c \in X)$$

ونرمز لهذا العنصر – إن وجد – بالرمز max A .

* نقول عن العنصر $d \in A$ إنه أصغر عنصر في X إذا تحقق :

$$\forall x \in X \quad : \quad (d \leq x) \quad \wedge \quad (d \in X)$$

ونرمز لهذا العنصر – إن وجد – بالرمز min A .

* نقول عن العنصر $\alpha \in A$ إنه الحد الأعلى لـ X إذا كان α أصغر العناصر الراجحة على X . ونرمز لهذا العنصر – إن وجد – بالرمز sup A.

* نقول عن العنصر $\beta \in A$ إنه الحد الأدنى لـ X إذا كان β أكبر

العناصر القاصر عن X . ونرمز لهذا العنصر – إن وجد – بالرمز $\inf A$.

* نقول عن العنصر $\mu \in X$ إنه عنصر أعظمي في X إذا تحقق :

$$\forall x \in X \quad : \quad \mu \leq x \quad \Rightarrow \quad \mu = x$$

* نقول عن العنصر $m \in X$ إنه عنصر أصغري في X إذا تحقق :

$$\forall x \in X \quad : \quad x \leq m \quad \Rightarrow \quad m = x$$

أمثـــــلة :

١ . لتكن $A = \{\{1\},\{2\},\{3\},\{1,4\}\}$ ، ولتكن $(A,\subseteq)$ المجموعـــة المرتبة وفق علاقة الاحتواء المألوفة عندئذٍ نجد أن :

كلاً من المجموعـــات : $\{2\},\{3\},\{1,4\}$ هي عنصر أعظمي في $(A,\subseteq)$

وأن كلاً من المجموعات : $\{1\},\{2\},\{3\}$ هي عنصر أصغري في $(A,\subseteq)$

وأن المجموعة $\{1\}$ ليست بعنصر أعظمي وأن المجموعة $\{1,4\}$ ليست بعنصر أصغري

٢ . في المجموعة المرتبة $(\{1\}, \leq)$ المرتبة وفق علاقة الترتيب $\leq$ المألوفة يكون العدد 1 عنصراً راجحاً وعنصراً أصغرياً وأعظمياً .

١ — ٦ – الشبكات : (Lattices)

لتكن L مجموعة غير خالية مرتبة وفق علاقة ترتيب $\leq$.

١ . نقول عن المجموعة المرتبة $(L, \leq)$ أنها شبكة إذا تحقق الشرط:

أياً كان $H = \{a,b\} \subseteq L$ فإنه يوجد في L عنصران α, β بحيث يكون :

$$\sup H = \alpha \quad , \quad \beta = \inf H$$

٢ . نقول عن المجموعة المرتبة $(L, \leq)$ إنها شبكة تامة إذا تحقق الشرط :

" أياً كانت المجموعة $\phi \neq L \subseteq H$ فإنه يوجد في L عنصران α, β

بحيث يكون :

$$\alpha = \sup H \quad \text{و} \quad \beta = \inf H$$

٣ . نقول عن المجموعة الجزئية P من الشبكة $(L,\leq)$ إنها شبكة جزئية من L إذا وفقط إذا تحقق الشرط :

" أياً كان $a,b \in P$ فإن العنصرين $\{a,b\}$ sup ، $\{a,b\}$ inf الموجودين في L ينتميان إلى P ".

أمثـــــــلة :

١ . إذا كانت A مجموعـــة ما ، فإن $P(A)$ مجموعة أجزاء A المرتبة وفق علاقة الاحتواء تكون شبكة تامة .

٢ . كل مجموعة منتهية ومرتبة كلياً تكون شبكة تامة .

٣ . إن المجموعة $N-\{0\}$ (مجموعة الأعداد الطبيعية المغايرة للصفر) المرتبة وفق علاقة الترتيب $\leq$ المعرفة كما يلي :

$$a \leq b \quad \Leftrightarrow \quad \exists \ k \in N \ : \ b = k.a$$

هي شبكة وذلك إذا أخذنا

$\{a,b\}$ sup = المضاعف المشترك الأصغر لـــ a,b .

$\{a,b\}$ inf = القاســـم المشترك الأكبر لـــ a,b .

١ – ٧ – قـــدرة مجموعة :

تمهـــــيد : لتكن $\Gamma = \{A_i ; i \in I\}$ أسرة مجموعات غير خالية ولنعرف على Γ العلاقة الثنائية $\sim$ كما يلي :

$$A \sim B \ : \ \forall A,B \in \Gamma \quad \Leftrightarrow \quad f : A \to B$$

يوجد تطبيق تقابل مثل

إن العلاقة الثنائية $\sim$ المعرفة أعلاه هي علاقة تكافؤ لأن :

١ . أياً كانت $\phi \neq A \in \Gamma$ فإن التطبيق المطابق $I_A : A \to A$ هو تقابل فالعلاقة الثنائية ~ انعكاسية .

٢ . أياً كانت $A, B \in \Gamma$ بحيث $A \sim B$ فإنه يوجد تقابل $f : A \to B$ وبالتالي يوجد التطبيق العكسي $f^{-1} : B \to A$ الذي هو تقابل أيضاً فالعلاقة الثنائية ~ تناظرية .

٣ . أياً كانت $A, B, C \in \Gamma$ بحيث $(A \sim B) \wedge (B \sim A)$ فإن

يوجد تقابل مثل $f : A \to B \quad \Leftrightarrow \quad A \sim B$

يوجد تقابل مثل $g : B \to C \quad \Leftrightarrow \quad B \sim C$

وبالتالي التركيب $g \circ f : A \to C$ تقابل فالعلاقة الثنائية ~ متعدية

تعريف (١) :

إذا كانت A, B مجموعتين ما . نقول إن قدرة المجموعة A تساوي قدرة المجموعة B ونكتب : $card\ A = card\ B$ عندما وفقط عندما يوجد تقابل مثل $f : A \to B$

اي :

$$card\ A = card\ B \quad \Leftrightarrow \quad \text{يوجد تقابل } f : A \to B$$
$$\Leftrightarrow \quad A \sim B$$

تعريف (٢) : نعرّف قدرة المجموعة المنتهية بأنه عدد عناصرها .

أمثلة :

$$card\ \{1, 2, \ldots, n\} = n$$
$$card\ \phi = 0$$
$$card\ \{\phi\} = 1$$

ملاحظة هامة : استنادا إلى التعريفين السابقين نلاحظ أن المجموعتين المنتهيتين تكونان متكافئتين عندما ، يكون عدد عناصر إحداهما يساوي

عدد عناصر الأخرى .

وبالتالي لا يمكن أن تكون المجموعة المنتهية مكافئة لمجموعة جزئية محتواة تماماً فيها ، لكن هذا الأمر يمكن أن يتحقق من أجل المجموعات غير المنتهية . فمثلاً :

لنأخذ Z مجموعة الأعداد الصحيحة ولنأخذ $2Z$ مجموعة الأعداد الصحيحة الزوجية .

إن $2Z \subset Z$ كما أن التطبيق : $f : Z \to 2Z$

المعرّف كما يلي :

$$f(z) = 2z \qquad \forall z \in Z$$

هو تقابل -تأكد من ذلك- وبالتالي : $Z \sim 2Z$ رغم أن $2Z \subset Z$

تمرين مشهور :

إن قدرة أي مجال حقيقي $I \subseteq R$ مغلق تساوي قدرة أي مجال حقيقي مفتوح وتساوي قدرة أي مجال حقيقي نصف مفتوح .

الحل : بإيجاز :

١ . إن العلاقة : $f :]-\frac{\pi}{2}, \frac{\pi}{2}[\to R$

$$f(x) = tgx \qquad \forall x \in]-\frac{\pi}{2}, \frac{\pi}{2}[$$

هي تقابل وبالتالي : $]-\frac{\pi}{2}, \frac{\pi}{2}[\sim R$

٢ . ليكن $a \in R$ ولنأخذ العلاقة : $f :]0,1[\to]a, \infty[$

$$f(x) = a + \frac{x}{1-x} \qquad \forall x \in]0,1[$$

فنجد أن f تقابل وبالتالي : $]0,1[\sim]a, \infty[$

٣ . ليكن $a \in R$ ولنأخذ العلاقة : $f:[0,1[\to[a,\infty[$

$$f(x)=a+\frac{x}{1-x}$$

فنجد أن f تقابل وبالتالي : $[0,1[\sim[a,\infty[$

٤ . ليكن $b \in R$ ولنأخذ العلاقة :

$$f:]-1,0[\to]-\infty,b[$$

$$f(x)=b+\frac{x}{1+x} \qquad \forall x\in]-1,0[$$

فنجد أن f تقابل وبالتالي : $]-1,0[\sim]-\infty,b[$

٥ . ليكن $b \in R$ ولنأخذ العلاقة : $f:]-1,0] \to]-\infty,b]$

$$f(x)=b+\frac{x}{1+x} \qquad \forall x\in]-1,0]$$

فنجد أن f تقابل وبالتالي : $]-1,0]\sim]-\infty,b]$

٦ . ليكن $a,b,c,d \in R$ بحيث $a<b \ , \ c<d$ لنأخذ العلاقة :

$$f:[a,b]\to[c,d]$$

$$f(x)=c+\frac{x-a}{b-a}(d-c) \qquad \forall x\in[a,b]$$

فنجد أن f تقابل وبالتالي : $[a,b]\sim[c,d]$

بعض خواص قدرات المجموعات المنتهية :

١ . إذا كانت A مجموعة منتهية وكانت $B\subseteq A$ فإن $cardB \le cardA$

٢ . إذا كانت A مجموعة منتهية وكان $f:A\to B$ تطبيقاً فإن :

أ - $card\,(\vec{f}(A)) \le card\ A$

ب - $card\,(\vec{f}(A)) = card\ A \iff f$ متباين.

٣ . إذا كان $f:A\to B$ تطبيقاً متبايناً وإذا كانت المجموعة $f(A)$ منتهية

فإن المجموعة A تكون منتهية ويكون $cardA = card(f(A))$

٤ . إذا كانت $f : A \to B$ تطبيقاً غامراً وإذا كانت A مجموعة منتهية فإن المجموعة B تكون منتهية زد على ذلك :

أ - $card\ B \le card\ A$

ب - $card\ B = card\ A \Leftrightarrow f$ تقابل

٥ . إذا كان $f : A \to B$ تطبيقاً ما وكانت A,B مجموعتين منتهيتين فإن :

f متباين $\Leftrightarrow$ f غامر $\Leftrightarrow$ f تقابل .

٦ . إذا كانت A,B مجموعتين منتهيتين ومنفصلتين فإن :

card (A Y B) = card A + card B

٧ . إذا كانت A,B مجموعتين منتهيتين فإن المجموعة $A \times B$ منتهية وإن :

$$card\ (A \times B) = card\ A\ .\ card\ B$$

٨ . إذا كانت A مجموعة منتهية فإن P(A) مجموعة أجزاء A تكون منتهية ويكون :

$$card\ (P(A)) = 2^{card\ A}$$

٩ . إذا كانت A مجموعة منتهية وكان $card\ A = n$ فإن المجموعة $P_k(A)$ مجموعة أجزاء A التي عدد عناصر كل منها K ، تكون منتهية وإن :

$$card\ P_k(A) = C_n^k = \begin{cases} 0 & ; \quad n < k \\ \dfrac{n!}{k!(n-k)!} & ; \quad 0 \le k \le n \end{cases}$$

١٠ . إذا كانت A مجموعة منتهية بحيث $cardA = n \ge 1$ فإن المجموعة $S(A)$ ، مجموعة التقابلات في A ، تكون منتهية

ويكون : $cardS(A) = n!$

١ – ٨ – المجموعات القابلة للعـــد :

تعريف : لتكن A مجموعـــة غـــير منتهية . نقول عن المجموعـــة A إنـــها قابـــلة للعـــد إذا كان

$$card\ A = card\ N - \{0\}$$

بعبارة أخرى مكافئة : نقول عن المجموعـــة غير المنتهية A إنهـــا قابلة للعـــــد إذا وجد تقابل مثل

$$f : N - \{0\} \to A$$

نتائـــج :

(١) – أية مجموعة مكافئة لمجموعة قابلة للعد تكون قابلة للعد .

(٢) – إن كل مجموعتين قابلتين للعد متكافئتان .

البرهـــــان :

(١). لتكن A مجموعة قابلة للعد ، ولتكن $B \sim A$. وبما أن A قابلة للعد

فإن : $card\ A = card\ N - \{0\}$

وبما أن $B \sim A$ فإن : $card\ B = card\ A$

وبالتالي : $card\ B = card\ N - \{0\}$

أي أن المجموعة B قابلة للعـــد .

(٢). لتكن A, B مجموعتين قابلتين للعد . عندئذ :

$$(card\ A = card\ N - \{0\}) \quad \wedge \quad (card\ B = card\ N - \{0\})$$

وبالتالي : $card\ A = card\ B$ أي $A \sim B$.

تمرينات محلولـــة

التمرين الأول : لتكن A,B مجموعتين من مجموعـــة شاملة نسبياً M . والمطلوب :

برهن صحة القضية : $(A\Delta B)' = A\Delta B'$

الحل : نكتب جدول الحقيقة :

A	B	$A\Delta B$	$(A\Delta B)'$	B'	$A\Delta B'$
1	1	0	1	0	1
1	0	1	0	1	0
0	1	1	0	0	0
0	0	0	1	1	1

بمقارنة العمودين الرابع و الأخير نجد تطابق قيم الحقيقة وبالتالي القضية :

$(A\Delta B)' = A\Delta B'$ صحيحة .

التمرين الثاني : لتكن N مجموعة الأعداد الطبيعية،ولنعرف في المجموعة N × N العلاقة الثنائية R كما يلي : $(a_1,b_1)\,R\,(a_2,b_2) \Leftrightarrow a_1+b_2=b_1+a_2$

وذلك أياً كان $(a_1,b_1),(a_2,b_2)\in N\times N$

برهن أن العلاقـــة الثنائية R علاقة تكافؤ في N × N ، ثم عين مجموعة صفوف التكافـــؤ N^2/R .

الحـــل:

١ . أياً كان $(a,b)\in N^2$ فإن $a+b=b+a$ وبالتالي $(a,b)R(a,b)$

فالعلاقـــة R انعكاسية .

٢ . أياً كان $(a_1,b_1),(a_2,b_2)\in N^2$ وكان $(a_1,b_1)R(a_2,b_2)$

فإن $a_2+b_1=b_2+a_1 \Leftrightarrow a_1+b_2=b_1+a_2$

أي أن $(a_2,b_2)R(a_1,b_1)$ فالعلاقة R تناظرية .

٣ . أياً كان $(a_1,b_1),(a_2,b_2),(a_3,b_3) \in N^2$ وكان

$$(a_1,b_1)R(a_2,b_2) \quad \wedge \quad (a_2,b_2)R(a_3,b_3)$$

فإن :

$$(a_1,b_1)R(a_2,b_2) \Leftrightarrow a_1+b_2=b_1+a_2$$

$$(a_2,b_2)R(a_3,b_3) \Leftrightarrow a_2+b_3=b_2+a_3$$

ومنه :

$$(a_1+b_2)+(a_2+b_3)=(b_1+a_3)+(b_2+a_3)$$

وبالتالي :

$$a_1+b_3=b_1+a_3$$

أي أن : $(a_1,b_1)R(a_3,b_3)$ فالعلاقة R متعدية .

إيجاد N^2/R :

$$\forall (a,b) \in N^2 \quad : \quad [(a,b)] = \{(x,y) \in N^2 : (x,y)R(a,b)\} = \{(x,y) \in N^2 : x+b=y+a\}$$

فمثلاً :

$$[(0,1)] = \{(0,1),(1,2),(2,3),...\} = \{(x,x+1); x \in N\}$$

$$[(2,5)] = \{(2,5),(0,3),(1,4),...\} = \{(x,x+3); x \subset N\}$$

التمرين الثالث :

لتكن $\Gamma = \{A_i ; i \in I\}$ أسرة غير خالية من المجموعات غـــير الخالية .

ولنعرّف العلاقة الثنائية $\leq$ على مجموعـــة قدرات المجموعات A_i كما يلي :

$card\ A_1 \leq card\ A_2 \Leftrightarrow [\ \varphi : A_1 \to A_2$ يوجد تطبيق متباين مثل $]$

وذلك أياً كانت $A_1, A_2 \in \Gamma$. برهن أن العلاقة الثنائية $\leq$ علاقة ترتيب .

الحـــل : ١ . أياً كانت $A \in \Gamma$ فإنه يوجد التطبيق المطابق $I_A : A \to A$ الذي هو متباين وبالتالي :

$cardA \le cardA$ فالعلاقة $\le$ انعكاسية .

٢ . أياً كانت $A,B \in \Gamma$ وكان :

$$(cardA \le cardB) \quad \wedge \quad (cardB \le cardA)$$

[يوجد تطبيق متباين مثل $\varphi : A \to B$] $\Leftrightarrow$ $cardA \le cardB$

[يوجد تطبيق متباين مثل $\psi : B \to C$] $\Leftrightarrow$ $cardB \le cardC$

وبالتالي التركيب $\psi o \varphi : A \to C$ يكون متبايناً وبالتالي :

$cardA \le cardC$ فالعلاقة $\le$ متعديّة .

إذا $\le$ انعكاسية ، تخالفية و متعدية فهي علاقة ترتيب .

التمرين الرابع:

لتكن $A = \{1,2,3\}$ ولتكن $\Gamma = \{\{1\},\{2\},\{1,2\},\{3\}\}$ أسرة مجموعات مرتبة وفق علاقة الاحتواء $\subseteq$.

والمطلوب : ١ – هل Γ تشكل تجزئة للمجموعة A ؟ علل إجابتك.

٢ – بيّن فيما إذا كانت Γ تغطية للمجموعة A . علل إجابتك.

٣ – عين العناصر الأصغريّة في Γ والعناصر الأعظمية في. Γ

الحـــل :

١ – إن الأسرة Γ لا تشكل تجزئة للمجموعة A لأن :

$$\{1\}, \{1,2\} \in \Gamma \quad \wedge \quad \{1\} \cap \{1,2\} = \{1\} \ne \phi$$

٢ – إن الأسرة Γ تشكل تغطية للمجموعة A لأن :

$$\bigcup_{i=1}^{3} A_i = \{1\} \cup \{2\} \cup \{1,2\} \cup \{3\} = \{1,2,3\} = A$$

أي أن الشرط : $\bigcup_{i \in I} A_i \supseteq A$ محقق .

٣ – حسب تعريف كل من العنصر الأصغر والعنصر الأكبر في مجموعة

مرتبة يكون :

العناصر الأصغرية : $\{3\}$, $\{2\}$, $\{1\}$

العناصر الأعظمية : $\{3\}$, $\{1,2\}$

تمرينات (١)

التمرين الأول :

بفرض A,B,C ثلاث مجموعات من مجموعة شاملة نسبياً M .

ناقش صحة القضايا التالية :

1. $(A \cap B) \subset A \cup B$.
2. $A \Delta B = B \Delta A$.
3. $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.
4. $\begin{cases} A \cap (A \cup B) = A \\ A \cup (A \cap B) = A \end{cases}$
5. $(A \subseteq B) \Leftrightarrow (B' \subseteq A')$.
6. $(A \cup B = B) \Leftrightarrow (A \subseteq B) \Leftrightarrow (A \cap B = A)$.
7. $A - (B \cap C) = (A - B) \cup (A - C)$.
8. $A - (B \cup C) = (A - B) \cap (A - C)$.
9. $(B \subseteq A) \Rightarrow B \cup (A - B) = A$.
10. $A \cap (B - C) = (A \cap B) - (A \cap C)$.
11. $(A \cup B) - C = (A - C) \cup (B - C)$.
12. $A - (B \cup C) = (A - B) - C$.
13. $(A \cap B) - C = (A - C) \cap (B - C)$.
14. $A - (B - C) = (A - B) \cup (A \cap C)$.

التمرين الثاني :

بفرض A,B مجموعتين ما من مجموعة شاملة نسبياً M . برهن أنه إذا كان $A \cap B = A \cap C$ فليس من الضروري أن يكون $B = C$. ضع شرطاً لازماً وكافياً لكي يكون : $A \cap B = A \cap C \Rightarrow B = C$

التمرين الثالث :

لتكن المجموعة $X = \{1,2,3\}$.عيّن أي من الأسرة التالية تشكل تغطية للمجموعة X وأي منها تشكل تجزئة لها . علل إجابتك .

$$\Gamma_1 = \{\{1\},\{2,3\},\{4\}\}$$
$$\Gamma_2 = \{\phi, X\}$$
$$\Gamma_3 = \{\{1,2,3,4,5\}\}$$
$$\Gamma_4 = \{\{0,1,2,3\}\}$$

التمرين الرابع :

نعرف في المجموعة R^2 (R مجموعة الأعداد الحقيقية) العلاقة الثنائية $\leq$ كما يلي :

$$(a_1,b_1) \leq (a_2,b_2) \Leftrightarrow (a_1 \leq a_2) \wedge (b_1 \leq b_2)$$

حيث $(a_1,b_1),(a_2,b_2) \in R^2$

والمطلوب :

١. برهن أن $(R^2 , \leq)$ مجموعة مرتبة .

٢. برهن أن مجموعة العناصر الأعظمية للمجموعة :

$$X = \{(x,y) \in R^2 ; x^2 + y^2 = 1\}$$

هي المجموعة :

$$\{(x,y) \in R^2 ; x^2 + y^2 = 1 \wedge x \geq 0 \wedge y \geq 0\}$$

٣. برهن أن مجموعة العناصر الأعظمية للمجموعة :

$$B = \{(x,y) \in R^2 ; x^2 + y^2 < 1\}$$

هي المجموعة الخالية .

التمرين الخامس :

لتكن $A = N - \{0,1\}$. ولنعرف في A العلاقة الثنائية $\leq$ كما يلي :

$$(\forall a,b \in A) \ : \ a \leq b \quad \Leftrightarrow \quad \exists n \in N - \{0\} \quad : \quad b = n.a$$

والمطلوب :

١. أثبت أن العلاقة الثنائية $\leq$ هي علاقة ترتيب في A .

٢. برهن أن مجموعة العناصر الأصغرية في$(\leq , A)$ تتألف من الأعداد الأولية

٣. برهن أن مجموعة العناصر الأعظمية في $(\leq , A)$ هي المجموع الخالية

التمرين السادس :

نعرف في R مجموعة الأعداد الحقيقية العلاقة الثنائية R كما يلي :

$$\forall a,b \in \mathrm{R} \quad : \quad aRb \Leftrightarrow \exists n \in Z \quad : \quad a - b = 2\pi n$$

المطلوب :

١. أثبت أن العلاقة الثنائية R هي علاقة تكافؤ في A .

٢. أوجد مجموعة صفوف التكافؤ A/R .

التمرين الثامن :

لتكن A مجموعة غير خالية وليكن C عنصراً مثبتاً من مجموعة الأجزاء $P(A)$

نعرف في المجموعة $P(A)$ العلاقة الثنائية R كما يلي :

$$\forall X,Y \in P(A) \quad : \quad XRY \Leftrightarrow [C \cap X = C \cap Y]$$

والمطلوب :

١. أثبت أن العلاقة الثنائية R هي علاقة تكافؤ في P(A) .

٢. أوجد مجموعة صفوف التكافؤ $P(A)/R$.

الفصل الثاني

التطبيقـــــات

The Mappings

٢ – ١ مقدمـــــــة :

نعلم أن التطبيق هو علاقة ثنائية منطلقها مجموعة A ومستقرها مجموعـــة B . بحيث كل عنصر من المنطلق A مرتبط بعنصر وحيد من المستقر B ونرمّز ، عادة ، التطبيق f كما يلي :

$$f : A \to B$$
$$x \,\alpha\, f(x) = y \qquad \forall x \in A$$

تعبّر القضية $f(x) = y$ عن علاقـــة الربط بين عناصر المنطلق بعناصر المستقر والتي تدعى قاعدة ربط التطبيق f .

وبذلك فإن الشرط الذي يجب أن تحققه علاقة ثنائية مثل $f : A \to B$. كي تكون تطبيقاً هو :

$$f(a_1) \neq f(a_2) \quad \Rightarrow \quad a_1 \neq a_2 \qquad (\forall a_1, a_2 \in A)$$

وهذا الشرط يكافئ الشرط :

$$a_1 = a_2 \quad \Rightarrow \quad f(a_1) = f(a_2) \quad (\forall a_1, a_2 \in A)$$

ويكون التطبيق f متبايناً إذا تحقق الشرط التالي :

$$a_1 \neq a_2 \quad \Rightarrow \quad f(a_1) \neq f(a_2) \quad (\forall a_1, a_2 \in A)$$

وهذا الشرط يكافئ الشرط :

$$f(a_1) = f(a_2) \quad \Rightarrow \quad a_1 = a_2 \qquad (\forall a_1, a_2 \in A)$$

ويكون التطبيق f غامراً إذا تحقق الشرط التالي :

$$\forall b \in B \quad : \quad \exists a \in A \quad : \quad f(a) = b$$

ويكون التطبيق f تقابلاً إذا كان f متبايناً و غامراً .

كما أنه إذا كان $f : A \to B$ ، $g : B \to C$ تطبيقين ما فإن التركيب $g \circ f$ هو تطبيق معرفاً بـــ : $g \circ f : A \to C$

$$(g \circ f)(x) = g(f(x)) \qquad \forall x \in A$$

ومن المعروف أن علاقـــة التركيب O عملية ليست تبديلية،تجميعية وتحقق القضايا التالية : (التي نترك إثبات صحتها كتمرين) .

1. (f متباين) $\wedge$ (g متباين) $\Rightarrow$ ($g \circ f$ متباين).
2. (f غامر) $\wedge$ (g غامر) $\Rightarrow$ ($g \circ f$ غامر).
3. (f تقابل) $\wedge$ (g تقابل) $\Rightarrow$ ($g \circ f$ تقابل).
4. ($g \circ f$ متباين) $\to$ (f متباين).
5. ($g \circ f$ غامر) $\Rightarrow$ (g غامر).
6. ($g \circ f$ تقابل) $\Rightarrow$ (f متباين) $\wedge$ (g غامر).

وهنا نذكّر بأنه إذا كان $f : A \to B$ تقابلاً فإن التطبيق العكسي f^{-1} موجود ووحيد ويحقق : $f \circ f^{-1} = I_B \quad \wedge \quad f^{-1} \circ f = I_A$

حيث I_A التطبيق المطابق في A .

حيث I_B التطبيق المطابق في B .

وأخـــيراً نذكّـــر بمفهومي الصورة المباشرة والصورة العكسية لمجموعـــة وفـــق تطبيق .

ليكن $f : A \to B$ تطبيقاً ما ولتكن $A_1 \subseteq A$ ، $B_1 \subseteq B$ تُعرف الصورة المباشرة لـــ A_1 وفـــق التطبيق f ونرمـــز لـــها بـــ $\vec{f}(A_1)$ بأنهـــا المجموعـــة :

$$\overrightarrow{f}(A_1) = \{f(x); x \in A_1\}$$

ونرمّز الصورة المباشرة للمنطلق A بالرمز $I_m f$ أي $\overrightarrow{f}(A) = I_m f$

ونعرف الصورة العكسية لـــ B_1 وفق التطبيق f ونرمز لها بـــ $\overleftarrow{f}(B_1)$

بأنها المجموعة : $\overleftarrow{f}(B_1) = \{x \in A : f(x) \in B_1\}$

واستنادا إلى هذين التعريفين يمكن للقارئ - بســـهولة - التحقق من القضايـــا التالية :

بفرض $f : A \to B$ تطبيقاً ما ، A_1, A_2 مجموعتان جزئيتان من A و B_1, B_2 مجموعتان جزئيتان من B فإن :

1. $\overrightarrow{f}(A_1 \cup A_2) = \overrightarrow{f}(A_1) \cup \overrightarrow{f}(A_2)$
2. $\overrightarrow{f}(A_1 \cap A_2) \subseteq \overrightarrow{f}(A_1) \cap \overrightarrow{f}(A_2)$
3. $A_1 \subseteq A_2 \Rightarrow \overrightarrow{f}(A_1) \subseteq \overrightarrow{f}(A_2)$
4. $\overleftarrow{f}(B_1 \cup B_2) = \overleftarrow{f}(B_1) \cup \overleftarrow{f}(B_2)$
5. $\overleftarrow{f}(B_1 \cap B_2) = \overleftarrow{f}(B_1) \cap \overleftarrow{f}(B_2)$
6. $B_1 \subseteq B_2 \Rightarrow \overleftarrow{f}(B_1) \subseteq \overleftarrow{f}(B_2)$
7. $\overleftarrow{f}(\overrightarrow{f}(A_1)) \supseteq A_1$

وتتحقق المساواة إذا كان f متبايناً .

8. $\overrightarrow{f}(\overleftarrow{f}(B_1)) \subseteq B_1$

وتتحقق المساواة إذا كان f غامراً .

9. $\overrightarrow{f}(A - A_1) \supseteq \overrightarrow{f}(A) - \overrightarrow{f}(A_1)$
10. $\overleftarrow{f}(B - B_1) = A - \overleftarrow{f}(B_1)$.

٢ – ٢ المخططات التبديلية للتطبيقات :(Commutative Diagrams)

سندرس في هـــذه الفقـــرة ما يســـمى بالمخططات التبديلية للتطبيقات

وسنناقش المسألتين الآتيتين :

المسألة الأولى : إذا كانت A,B,C ثلاث مجموعات غير خالية ، وكان $f:A\to B$ ، $g:A\to C$ تطبيقين (لاحظ أن لهما مجموعة المنطلق A نفسها).

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "g"'] & B \\ C \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

فما هي الشروط الواجب توافرها لوجود تطبيق مثل $h:C\to B$ بحيث يكون $h\circ g=f$.

في حال وجود مثل هذا التطبيق h نقول إن المخطط السابق أصبح تبديلياً

المسألة الثانية : إذا كانت A,B,C ثلاث مجموعات غير خالية ، وكان $f:B\to A$ و $g:C\to A$ تطبيقين (لاحظ أن لهما مجموعة المستقر A نفسها) .

$$\begin{tikzcd} B \arrow[d, "F"'] & \\ A & C \arrow[l, "g"] \arrow[ul, dashed, "h"'] \end{tikzcd}$$

فما هي الشروط الواجب توافرها لوجـــود تطبيق مثل $h: C \to B$ بحيث يكون :

$$f \circ h = g$$

في حالة وجـــود مثل هذا التطبيق h نقول إن المخطط السابق أصبح تبديلياً.

إن الإجابـــة عن هاتين المسالتين تكمن في المبرهنتين الآتيتين :

المبرهنة الأولى :

لتكـــن A, B, C ثـــلاث مجموعـــات غـــير خـــالية ، وليكـــن :

$$f: A \to B \quad , \quad g: A \to C$$

تطبيقين . عندئـــذٍ تكون القضيتان التاليتان متكافئتين :

(I) - يوجـــد تطبيق مثل $h: B \to C$ بحيث يكون $h \circ f = g$.

(II)- إذا كان $a_1, a_2 \in A$ بحيث $f(a_1) = f(a_2)$ فإن

$$g(a_1) = g(a_2)$$

الإثبـــات :

(I) $\Rightarrow$ (II) : لنفرض أن (I) محققـــة ولنبرهن على صحـــة (II).

إذا كان $a_1, a_2 \in A$ بحيث $f(a_1) = f(a_2)$ فإن :

$$g(a_1) = (h \circ f)(a_1) = h(f(a_1)) = h(f(a_2)) = (h \circ f)(a_2) = g(a_2)$$

(II) $\Rightarrow$ (I) : لنفرض أن (II) محققـــة ولنبرهن على صحـــة (I).

لنأخـــذ العلاقـــة : $\varphi: \operatorname{Im} f \to C$

المعرفـــة كما يلي :

$$\varphi(f(x)) = g(x) \qquad \forall x \in A$$

إن العلاقـــة φ هي تطبيق لأنـــه :

بفرض $a_1, a_2 \in A$ وبفرض $f(a_1) = f(a_2)$ فإن $g(a_1) = g(a_2)$

لنأخـــذ الآن العلاقـــة : $h : B \to C$

المعرفـــة كما يلي :

$$h(b) = \begin{cases} \varphi(b) & (\text{عندمـــا } b \in \operatorname{Im} f) \\ c_0 \in C & (\text{عندمـــا } b \notin \operatorname{Im} f) \end{cases}$$

حيث c_0 عنصر مثبت من المجموعة C لأجل جميع العناصر $b \notin \operatorname{Im} f$

واضح أن العلاقة h هي تطبيق .وعندئذٍ يكون للتطبيقين g ، $h o f$

المنطلق نفسه وهو المجموعة A والمستقر نفسه وهو المجموعة C .

ومن جهة أخرى :

$$\forall x \in A : \quad (h o f)(x) = h(f(x)) = \varphi(f(x)) = g(x)$$

وبالتالي : $h o f = g$

المبرهنة الثالثة :

لتكن A, B, C ثلاث مجموعات غير خالية ، وليكن

$f : B \to A$ ، $g : C \to A$

تطبيقين . عندئذٍ القضيتان التاليتان تكونان متكافئتين :

(I´) - يوجد تطبيق مثل $h : C \to B$ بحيث يكون $f o h = g$.

(II´) - $\operatorname{Im} g \subseteq \operatorname{Im} f$.

الإثبـــــات :

(I´) $\Rightarrow$ (II´) : لنفرض أن (I´) محققة ولنبرهن على صحة (II´).

$$\forall a \in I_m g \quad \Rightarrow \quad \exists c \in C \quad : \quad a = g(c)$$

وبما أن $f \circ h = g$ (فرضاً) فإن :

$$a = g(c) = (f \circ h)(c) = f(h(c)) \in \operatorname{Im} f.$$

إذاً : $\operatorname{Im} g \subseteq \operatorname{Im} f$

(I) ⇐ (II) : لنفرض أن (II) محققة ولنبرهن على صحة (I) .

بما أن $\operatorname{Im} g \subseteq \operatorname{Im} f$ فإنه من أجل أي عنصر $c \in C$ يوجد عنصر واحد – على الأقل – مثل $b \in B$ بحيث يكون $g(c) = f(b)$.

من أجل كل عنصر $c \in C$ نثبت عنصراً واحداً فقط $b_c \in B$.

بحيث يكون : $g(c) = f(b_c)$ فنحصل على العلاقة : $h : C \to B$ المعرفة كما يلي :

$$h(c) = b_c \qquad \forall c \in C$$

من الواضح أن h هي تطبيق .وعندئـــذٍ يكون للتطبيقين g ، $f \circ h$ المنطلق نفسه وهو المجموعـــة C والمستقر نفسه وهـــو المجموعـــة A .

ومن جهة أخرى :

$$\forall c \in C \quad : \quad (f \circ h)(c) = f(h(c)) = f(b_c) = g(c)$$

وبالتالي : $f \circ h = g$

تعريف (١) : إذا كانت A, B مجموعتين غير خاليتين وكان $f : A \to B$ تطبيقاً نقول عن التطبيق f إنه منتظم يساري (أو أن f قابل للاختصار من اليسار) إذا تحقق الشرط التالي :

" أياً كانت المجموعة غير الخالية C وأياً كان التطبيقان :

$$\psi : C \to A \quad ، \quad \varphi : C \to A$$

بحيث $f \circ \varphi = f \circ \psi$ فإن $\varphi = \psi$ "

تعريف (٢) : إذا كانت A, B مجموعتين غير خاليتين وكان $f : A \to B$ تطبيقاً .

نقول عن التطبيق f إنـــه منتظم يميني (أو أن f قابـــل للاختصار من اليمين) إذا تحقق الشرط التالي :

• أياً كانت المجموعـــة غـــير الخالية C وأياً كان التطبيقان :

$$\psi : B \to C \quad , \quad \varphi : B \to C$$

بحيث $\varphi o f = \psi o f$ فـــإن $\varphi = \psi$ •

مبرهنة : لتكن A, B مجموعتين غـــير خاليتين ، وليكن $f : A \to B$ تطبيقاً ما . عندئـــذٍ القضايا التالية تكون متكافئة :

(١). التطبيق f متباين .

(٢). يوجد تطبيق مثل $g : B \to A$ بحيث يكون $g o f = I_A$.

(٣). التطبيق f قابل للاختصار من اليسار .

الإثبـــــات :

(٢) $\Leftrightarrow$ (١) : ينتج مباشرة من المبرهنة الأولى وذلك بأن نأخـــذ

$$C = A \quad \text{و} \quad g = I_A \ .$$

(٣) $\Rightarrow$ (٢) : لنفرض أن (٢) محققة ولنبرهن على صحة (٣) .

لتكن C مجموعة غير خالية وليكن $\varphi : C \to A$ ، $\psi : C \to A$ تطبيقين بحيث يكون : $f o\varphi = f o\psi$ عندئـــذٍ :

$$\begin{aligned} f o\varphi = f o\psi \quad &\Rightarrow \quad g o(f o\varphi) = g o(f o\psi) \Rightarrow \\ &\Rightarrow \quad (g o f) o\varphi - (g o f) o\psi \Rightarrow \\ &\Rightarrow \quad I_A o\varphi = I_A o\psi \Rightarrow \\ &\Rightarrow \quad \varphi = \psi \end{aligned}$$

إذاً : f قابل للاختصار من اليسار .

(١) $\Rightarrow$ (٣) : لنفرض أن (٣) محققة ولنبرهن على صحة (١) .

نفرض جدلاً أن التطبيق f ليس متبايناً .

عندئذٍ يوجد $a_1, a_2 \in A$ بحيث يكون :

$$f(a_1) = f(a_2) \quad \wedge \quad a_1 \neq a_2$$

لتكن C مجموعة غير خالية ولنأخذ التطبيقين ψ, φ كما يلي :

$$\varphi : C \to A$$
$$\varphi(x) = a_1 \qquad \forall x \in C$$
$$\psi : C \to A$$
$$\psi(x) = a_2 \qquad \forall x \in C$$

فنجد ، من جهة أولى أن : $\varphi \neq \psi$. ونجد من جهة ثانية أن:

$$\forall x \in C \quad : \quad f(\varphi(x)) = f(a_1) = f(a_2) = f(\psi(x))$$

وهذا يعني أن :

$$f \circ \varphi = f \circ \psi$$

وبما أن f قابل للاختصار من اليسار فإنه يكون $\varphi = \psi$

وهذا يناقض كون $\varphi \neq \psi$ إذاً f متباين .

مبرهنة :

لتكن A, B مجموعتين غير خاليتين ، وليكن $f : A \to B$ تطبيقاً.

عندئذٍ القضايا التالية تكون متكافئة :

(١). التطبيق f غامر .

(٢). يوجد تطبيق مثل $g : B \to A$ بحيث يكون $f \circ g = I_B$.

(٣). التطبيق f قابل للاختصار من اليمين .

الإثبـــات :

(٢) $\Leftrightarrow$ (١) : ينتج مباشرة من المبرهنة الثانية .

(٣) $\Rightarrow$ (٢) : لنفرض أن (٢) محققة ولنبرهن على صحـــة (٣) .

لتكن C مجموعة غير خالية وليكن $\varphi : B \to C$ ، $\psi : B \to C$

تطبيقين بحيث يكون : $\varphi \circ f = \psi \circ f$

عندئـــذ :

$$\begin{aligned} \varphi \circ f = \psi \circ f \quad &\Rightarrow \quad (\varphi \circ f) \circ g = (\psi \circ f) \circ g \Rightarrow \\ &\Rightarrow \quad \varphi \circ (f \circ g) = \psi \circ (f \circ g) \Rightarrow \\ &\Rightarrow \quad \varphi \circ I_B = \psi \circ I_B \Rightarrow \\ &\Rightarrow \quad \varphi = \psi \end{aligned}$$

إذاً : f قابل للاختصار من اليمين .

(١) $\Leftarrow$ (٣) : لنفرض أن (٣) محققة ولنبرهـــن على صحـــة (١) .

لنفرض جدلاً أن التطبيق f ليس غامراً .

عندئذٍ يوجـــد في المجموعة B عنصر واحد على الأقل مثل b بحيث

$f(a) \neq b$ لأجل جميع العناصر a من المجموعة A .

لنأخذ المجموعـــة $C=\{1,2,3\}$ ولنأخذ التطبيق $\varphi : B \to C$

المعرف كما يلي : $(\forall x \in B)$:

$$\varphi(x) = \begin{cases} 1 & ; \quad x = b \\ 2 & ; \quad x \neq b \end{cases}$$

ولنأخذ التطبيق $\psi : B \to C$ المعرف كما يلي : $(\forall x \in B)$:

$$\psi(x) = \begin{cases} 3 & ; \quad x = b \\ 2 & ; \quad x \neq b \end{cases}$$

فنجد أن $\varphi \circ f = \psi \circ f$ لكن $\varphi \neq \psi$ وهذا يناقض (٣) إذاً f غامر

٢ – ٣ بعض التطبيقات المشهورة :

سنعرض في هذه الفقرة بعض التطبيقات المشهورة التي لها دور كبير في كثير من الموضوعات الرياضية .

١ – **التطبيق الثابت** : نقول عن التطبيق $f : A \to B$ إنـــه ثابت إذا كان :

$$f(a_1) = f(a_2) \qquad \forall a_1, a_2 \in A$$

وبعبارة مكافئة : نقول عن التطبيق $f : A \to B$ إنه ثابت إذا وجـــد عنصر $b \in B$ بحيث يكون :

$$\operatorname{Im} f = \overrightarrow{f}(A) = \{b\}$$

٢ – **المقصور** : ليكن $f : A \to B$ تطبيقاً ما ، وليكن $A_1 \subseteq A$. نعرف مقصور التطبيق f على المجموعة الجزئية A_1 (ونرمز له بـــ f_{A_1}) بأنه التطبيق :

$$f_{A_1} : A_1 \to B$$

المعرف كما يلي :

$$f_{A_1}(x) = f(x) \qquad \forall x \in A_1$$

٣ – **التباين القانوني** : لتكن A_1 مجموعـــة جزئية من المجموعة A . نعرف التباين القانوني للمجموعة A_1 في المجموعة A (ونرمز له بـــ J_{A_1}) بأنه مقصور التطبيق المطابق $I_A : A \to A$ على المجموعة A_1 .

أي أن التباين القانوني للمجموعة A_1 في المجموعة A هو التطبيق :

$$J_{A_1} : A_1 \to A$$

المعرف كما يلي :

$$J_{A_1}(x) = x \qquad \forall x \in A_1$$

هذا ويسمى تطبيق التباين القانوني – أحياناً – الاحتواء القانوني .

٤ – **الممدود** : ليكن $f : A \to B$ تطبيقاً ما ، ولتكن D مجموعة بحيث $A \subseteq D$. نعرّف ممدود التطبيق f إلى المجموعة D بأنه التطبيق $g : D \to B$ المعرف كما يلي :

$$g(x) = f(x) \qquad \forall x \in A$$

لاحظ أن $g_A = f$.

٥ – **المتتالية** : لتكن A مجموعة غير خالية ولتكن N مجموعة الأعداد الطبيعية . نعرف المتتالية من عناصر المجموعة A بأنها أي تطبيق

مثل : $a : N \to A$

المعرف كما يلي :

$$a(n) = a_n \qquad \forall n \in N$$

نلاحظ أن العناصر الآتية (التي تسمى حدود هذه المتتالية):

$$a_0, a_1, \dots, a_n, \dots$$

تعيّن تماماً التطبيق a ولذلك يرمز – عادة – لهذه المتتالية بالرمز (a_n) أو بالرمز $\{a_n\}$. إذا كانت المجموعة A مجموعة عددية (حقيقية ، عقدية) فإن المتتالية $\{a_n\}$ تكون عددية (حقيقية ، عقدية) .

٦ – التطبيق المميز لمجموعة : لتكن A مجموعة غير خالية ، ولتكن $X \subseteq A$ نعرّف التطبيق المميز للمجموعة X (ونرمز له بـ X_X) بأنه التطبيق

$$X_X : A \to \{0,1\}$$

والمعرف كما يلي :

$$X_X(x) = \begin{cases} 1 & ; \quad x \in X \\ 0 & ; \quad x \notin X \end{cases}$$

٧ – المصفوفة : لتكن A مجموعة غير خالية ، ولتكن :

$$T = \{1,2,\dots,m\}$$

$$S = \{1,2,\dots,n\}$$

ندعـــو كل تطبيق مثل :

$$a : T \times S \to A$$

والمعرف كما يلي :

$$a(i,j) = a_{ij} \qquad \forall (i,j) \in T \times S$$

بمصفوفة على A من المرتبة $m \times n$.

ونلاحظ أن العناصر :

$$a_{11}, a_{12}, \dots, a_{1n};$$

$$a_{21}, a_{22}, \dots, a_{2n};$$

$$\dots\dots\dots\dots\dots\dots$$

$$a_{m1}, a_{m2}, \dots, a_{mn}$$

تعيّن تماماً التطبيق a وبالتالي يرمز – عادة – لهذه المصفوفة بالرمـــز (a_{ij}) . إذا رتبنا العناصر السابقـــة ضمن قوسين حصلنا على الشكل النموذجي للمصفوفـــة :

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

وتجـــدر الإشـــارة هنا إلى أن للمصفوفـــة دوراً كبيراً ومهماً في موضوعات الجبر الخطي .

٨ – التباديل من الدرجة n : نعرف التبديل من الدرجة n بأنه كل تقابل في مجموعة

عدد عناصرهـــا n ، ويمـــكن أن نعـــد هـــذه المجموعـــة هي $\{1,2,...,n\}$

وبذلك يكون التبديل من الدرجة n هو كل التقابل :

$$S:\{1,2,...,n\}\to\{1,2,...,n\}$$

$$S(i)=i_j \qquad \forall i\in\{1,2,...,n\}$$

حيث : $j\in\{1,2,...,n\}$

ويمكننا أن نعـــبر عن التقابل S بالشكل :

$$\begin{array}{cccc} 1 & 2 & \dots & n \\ \downarrow & \downarrow & & \downarrow \\ i_1 & i_2 & & i_n \end{array}$$

حيث $\{i_1\,,\,i_2,...,i_n\}=\{1,2,...,n\}$ وبـــذلك يمكن أن نعبر عن التبديل من الدرجـــة n بالشكل النموذجي التالي :

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

نرمز لمجموعة التباديل من الدرجة n بالرمـــز S_n . فمثلاً من أجل $n=3$ نحصل على مجموعـــة التباديل من الدرجـــة 3 :

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

٩ – قوانين التشكيل : لتكن A مجموعة غير خالية . نعرف قانون التشكيل الداخلي في A بأنـــه كل تطبيق من الشكل :

$$f:A\times A\to A$$

$$(x,y)\,\alpha\;\; f(x,y)$$

وعادة يُرمّز القانون التشكيل الداخلي بالرمز (+) وندعوه قانون الجمع أو بالرمز (.) وندعوه قانون الضرب .

ففي الكتابـــة الجمعية (+) نكتب $x+y$ بدلاً من $f(x,y)$ فنكتب قانون الجمع بالشكل :

$$+ : A \times A \to A$$
$$+(x,y) = x+y \qquad \forall \ (x,y) \in A^2$$

وفي الكتابـــة الضربية (.) نكتب $x \cdot y$ أو (xy) بدلاً من $f(x,y)$ فنكتب قانـــون الضرب بالشكل :

$$\bullet : A \times A \to A$$
$$\bullet(x,y) = xy \qquad \forall \ (x,y) \in A^2$$

لتكن A, M مجموعتين غـــير خاليتين . نعرف قانـــون التشكيل الخارجـــي اليساري في A الذي مجموعـــة مؤثـــرا تـــه M بانـــه كل تطبيق :

$$\bullet : M \times A \to A$$
$$\bullet(\alpha,x) = \alpha \bullet x \qquad \vee \ (x,\alpha) \in M \times A$$

ونعرف قانون التشكيل الخارجي اليميني في A الذي بمجموعة مؤثرا ته M بأنه كل تطبيق :

$$\bullet : A \times M \to A$$
$$\bullet(x,\alpha) = x \bullet \alpha \qquad \forall \ (x,\alpha) \in A \times M$$

ونذكر أن لهذين القانونين الخارجيين اليساري واليميني الصفات ذاتها ولذلك سنتعامل فقط مع قانون التشكيل الخارجي اليساري .

فيما يلي سنذكر قانون تشكيل خارجي ونقصد بذلك قانون تشكيل خارجي يساري .

وتجدر الإشارة هنا أن دراسة البنى الجبريـــة تعتمد على دراسة صفات قوانين

التشكيل المكونة لهذه البنية . هذا وسنعتبر أن القارئ ملم بالصفات الأساسية التي يمكن أن تتصف بها قوانين التشكيل مثل الصفات :

التبديلية ، التجميعية ، وجود العنصر المحايد ، وجود العنصر الماص ، نظير (مقلوب) عنصر بالنسبة لقانون تشكيل داخلي ، قابلية التوزيع ... إلخ

تمرينات محلولـــة

التمرين الأول :

لتكن A مجموعـــة غير خـــالية ولتكن R علاقـــة تكافـــؤ في المجموعة A .

برهن أنه يوجد تطبيق غامر بين المجموعـــة A وبين صفوف التكافؤ A/R

الحـــل : لنأخـــذ العلاقـــة :

$$\pi : A \to A/R$$

المعرفـــة كما يلي :

$$\pi(a) = [a] \qquad \forall a \in A$$

فنجـــد أن العلاقـــة π تطبيق لأن :

$$\forall a_1, a_2 \in A \ , \ a_1 = a_2 \quad \Rightarrow \quad [a_1] = [a_2] \quad \Rightarrow \quad \pi(a_1) = \pi(a_2)$$

كما أن التطبيق π غامـــر لأن :

$$\forall [a] \in A/R \quad \Rightarrow \quad \exists \quad a \in A \quad : \quad \pi(a) = [a]$$

وتجـــدر الإشارة هنا أن هـــذا التطبيق الغامـــر يـــدعى بالغمر القانوني .

التمرين الثاني :

لتكن A مجموعـــة غير خالية وليكن $f : A \to A$ تطبيقاً بحيث $f \circ f = f$

برهـــن صحـــة القضيتين الآتيتين :

$$(\mathrm{I}) . (f \text{ متباين}) \quad \Rightarrow \quad (f \text{ مطابق في } A)$$

$$(\mathrm{II}) . (f \text{ غامر}) \quad \Rightarrow \quad (f \text{ مطابق في } A)$$

الحـــل : ١. إثبات القضية (I) :

بمـــا أن $f \circ f = f$ فإنـــه من أجل أي عنصر $x \in A$ يكون :

$$(f \circ f)(x) = f(x)$$

وبالتالي :

$$f(f(x)) = f(x)$$

وبما أن f متباين فإن :

$$f(x) = x \qquad \Rightarrow \qquad x \in A$$

أي أن :

$$f : A \to A$$
$$f(x) = x \qquad \Rightarrow \qquad x \in A$$

هذا ما يبرهن أن f هو المطابق في A .

٢. إثبات القضية (II) .

بما أن التطبيق f غامر فإنه أياً كان $y \in A$ فإنه يوجد عنصر $x \in A$ بحيث يكون $y = f(x)$

ولدينا $f \circ f = f$ وبالتالي من أجل أي عنصر $x \in A$ يكون :

$$(f \circ f)(x) = f(x)$$

ولكن $y = f(x)$ بالتالي :

$$f(y) = y \qquad \forall \qquad y \in A$$

أي أن :

$$f : A \to A$$
$$f(y) = y \qquad \forall \qquad y \in A$$

هذا ما يبرهن أن f هو المطابق في A .

التمرين الثالث :

لتكن A مجموعة غير خالية مزودة بقانون تشكيل داخلي + .

برهن على صحة النص الآتي : " إذا كان + تجميعياً وكان للعنصر $a \in A$ نظيراً a' في A بالنسبة لـ + فإن هذا النظير يكون وحيداً وأن $(a')' = a$

الحـــل :

نفرض وجـــود نظيرين a',a'' للعنصر a في A بالنسبة لـــ + . عندئـــذٍ

يكون : $a+a'=a'+a=e \quad \wedge \quad (a+a''=a''+a=e)$

حيث e العنصر المحايـــد في A بالنسبة لـــ + .

وبالتالي يكون :

$$a'=a'+e \qquad (\text{تعريف المحايد})$$

$$=u'+(u+u'') \qquad (u \text{ نظير } u'')$$

$$=(a'+a)+a'' \qquad (+ \text{ تجميعي})$$

$$=e+a'' \qquad (a \text{ نظير } a')$$

$$=a'' \qquad (\text{تعريف المحايد})$$

أي أن النظير وحيد .

ومن جهة أخرى : إن كلاً من $a,(a')'$ نظيران للعنصر a' بالنسبة لـــ +

وبالتالي : $(a')'=a$

تمرينات (٢)

التمرين الأول :

لتكن A,B,C ثلاث مجموعات غير خالية وليكن $f : A \to B$ ، $g : B \to C$ تطبيقين ما . برهن صحة القضايا الآتية :

1. (f متباين) $\wedge$ (g متباين) $\Rightarrow$ ($g o f$ متباين)
2. (f غامر) $\wedge$ (g غامر) $\Rightarrow$ ($g o f$ غامر)
3. (f تقابل) $\wedge$ (g تقابل) $\Rightarrow$ ($g o f$ تقابل)
4. ($g o f$ متباين) $\Rightarrow$ (f متباين)
5. ($g o f$ غامر) $\Rightarrow$ (g غامر)
6. ($g o f$ تقابل) $\Rightarrow$ (f متباين) $\wedge$ (g غامر)

التمرين الثاني :

لتكن A,B مجموعتين غير خاليتين وليكن $f : A \to B$ تطبيقاً ما A_1, A_2 مجموعتين جزئيتين من المجموعة A ، B_1, B_2 مجموعتين جزئيتين من المجموعة B . برهن صحة القضايا الآتية :

1. $(A_1 \subseteq A_2) \Rightarrow (\vec{f}(A_1) \subseteq \vec{f}(A_2))$
2. $\vec{f}(A_1 \cup A_2) = \vec{f}(A_1) \cup \vec{f}(A_2)$
3. $\vec{f}(A_1 \cap A_2) \subseteq \vec{f}(A_1) \cap \vec{f}(A_2)$
4. $(B_1 \subseteq B_2) \Rightarrow \vec{f}(B_1) \subseteq \vec{f}(B_2)$
5. $\vec{f}(B_1 \cup B_2) = \vec{f}(B_1) \cup \vec{f}(B_2)$
6. $\vec{f}(B_1 \cap B_2) = \vec{f}(B_1) \cap \vec{f}(B_2)$
7. $\vec{f}(\vec{f}(A_1)) \supseteq A_1$

وتتحقق المساواة إذا كان f متبايناً .

8. $\vec{f}(\vec{f}(B_1)) \subseteq B_1$

وتتحقق المساواة إذا كان f غامراً .

9. $\vec{f}(A - A_1) \supseteq \vec{f}(A) - \vec{f}(A_1)$

10. $\vec{f}(B - B_1) = A - \vec{f}(B_1)$

التمرين الثالث :

لتكن A,B مجمـــوعتين غير خـــاليتين ولتكن $f : A \to B$ تطبيقاً .

ولنأخذ التطبيق :

$$\varphi : P(A) \to P(B)$$

المعرف كما يلي :

$$\varphi(X) = \vec{f}(X) \qquad \forall \quad X \in P(A)$$

(حيث $P(B), P(A)$ مجموعة أجزاء كل من المجموعتين A,B على الترتيب).

برهن على أنـــه إذا كان f تقابلاً فـــإن φ يكون تقابـــلاً .

الفصل الثالث

مجموعة الأعداد الطبيعية

The Set Of Natural Numbers

٣ – ١ مقدمـــــة :

تعـد مجموعـة الأعـداد الطبيعية N أماً لمجموعـة الأعـداد :

Z – مجموعة الأعداد الصحيحة .

Q – مجموعة الأعداد العادية .

R – مجموعة الأعداد الحقيقية.

C – مجموعة الأعداد العقدية .

حيث إنه يمكن توليد هذه المجموعات انطلاقاً من مجموعة الأعداد الطبيعية N (سنرى ذلك في الفصل الرابع) ولذلك سنوضح طبيعة هذه المجموعة وسندرس بالتفصيل مفاهيم عمليتي الجمع والضرب في N بالإضافة إلى القوة في N .

٣ – ٢ وصف مجموعة الأعداد الطبيعية :

وضع العالم الإيطالي بيانو Giuserppe Peano (1932 – 1858) موضوعات تحـدد وصفاً تاماً لمجموعـة الأعـداد الطبيعية N وهذه الموضوعات هي :

الموضوعة (١) : يوجد في N عنصر نرمز له بـ 0

الموضوعة (٢) : لكل عنصر $n \in N$ يوجد في N عنصر يليه مباشرة نرمزه n' .

الموضوعة (٣) : لأجل كل عنصر $n \in N$ يكون $n' \neq 0$.

الموضوعة (٤) : إذا كان $m,n \in N$ بحيث $m = n$ فإن $m' = n'$

الموضوعة (٥) : إذا كانت S مجموعـــة جزئية من N بحيث تحقق :

I . $0 \in S$

II . إذا كان $k \in S$ فإن $k' \in S$ فعندئذٍ $S = N$

نلاحظ من الموضوعة (١) أن $N \neq \phi$. أما الموضوعة (٢) فتبين أن المجموعة N مجموعة غير منتهية لأن :

$$0 \in N \Rightarrow 0' \in N \Rightarrow (0')' \in N,...$$

ويُصطلح أن :

$$0' = 1 \quad ; \quad 1' = (0')' = 2 \quad ; \quad 2' = (1')' = ((0')')' = 3 \quad ;...$$

وبهذا تأخذ مجموعة الأعداد الطبيعية الشكل المألوف وهو :

$$N = \{0,1,2,3,...\}$$

ونصطلح على أن $N - \{0\} = N^*$

أما الموضوعة (٥) فتسمى موضوعة الاستقراء الرياضي التي تستخدم في كثير من الأحيان في إثبات القضايا الرياضية التي تتبع لمتغير طبيعي n فإذا كانت P_n قضية رياضية تتبع لمتحول طبيعي n ، لإثبات صحـــة القضية P_n من أجل كل $n \in N$ ، يكفي إثبات صحة P_n من أجل $n = 0$ ثم نفرض أن القضية P_n صحيحة من أجل $k \in N$ ثم نثبت أن P_n صحيحة من أجل $k' \in N$.

سنعتمد على هذه الموضوعة في إثبات عـــدد من القضايا المتعلقة بـــ N في هـــذا الفصل .

٣ – ٣ عملية الجمع في N :

تعريف عملية الجمع في N :

تُعرف عمليـــة الجمـــع في N بأنهـــا قانـــون التشكيل الـــداخلي :

$$+ : N \times N \to N$$

المعرفـــة كما يلي :

$$+(n,m) = n + m \qquad \forall \quad (n,m) \in N \times N$$

والمحقق للشرطين الآتيين :

$$(\mathrm{i}).\ \forall n \in N \quad : \quad n + 0 = n$$

$$(\mathrm{ii}).\ \forall n,m \in N \quad : \quad n + m' = (n+m)'$$

ويسمى $n+m$ ناتـــج جمـــع n و m .

نتائـــــــج :

1. $\forall n \in N \quad : \quad n' = n + 1$
2. $\forall n,m \in N \quad : \quad n + (m+1) = (n+m) + 1$
3. $\forall n,m \in N \quad : \quad n + m \in N$

البرهـــــان :

1. $\forall n \in N \quad : \quad n' = (n+0)' = n + 0' = n + 1$
2. $\forall n,m \in N \quad : \quad n + (m+1) = n + m' = (n+m)' = (n+m) + 1$
3. أياً كان العـــدد الطبيعي $n \in N$. لنعتمد موضوعة الاستقراء الرياضي على $m \in N$ لإثبات أن $n + m \in N$

من أجل $m = 0$ يكون :

$$n + 0 = n \in N$$

نفرض أن $n + k \in N$

ولنبرهن على أن $n+k' \in N$

أي $n+(k+1) \in N$

إن :

$n+(k+1)=(n+k)+1$ حسب النتيجة (٢) السابقة

$=(n+k)'$ حسب النتيجة (١) السابقة

وبما أن $n+k \in N$ فإن $(n+k)' \in N$ حسب الموضوعة (٢)

وبالتالي $n+(k+1) \in N$

خواص عملية الجمع في N :

مبرهنة (١) : العنصر 0 عنصر محايد في N بالنسبة لـ + أي :

$$\forall n \in N \quad : \quad n+0=n=0+n$$

الإثبات : حسب تعريف عملية الجمع في N يكون :

$$\forall n \in N \quad : \quad n+0=n$$

ولنثبت أن : $\forall n \in N \quad : \quad 0+n=n$

وذلك حسب موضوعة الاستقراء الرياضي .

من أجل $n=0$ يكون :

$0+0=0$ (حسب الشرط الأول من تعريف عملية الجمع)

وهذا يعني أن القضية $0+n=n$ صحيحة من أجل $n=0$.

نفرض أن $0+k=k$ ولنبرهن على أن $0+(k+1)=k+1$.

إن :

$$0+(k+1)=(0+k)+1=k+1$$

إذاً :

$$\forall n \in N \quad : \quad 0+n=n$$

مبرهنة (٢) :

عملية الجمـــع في N عملية تجميعية أي :

$$\forall n,m,t \in N \quad : \quad (n+m)+t=m+(n+t)$$

أياً كانت $n,m \in N$ ولنبرهن على صحة المـــبرهنة حســـب موضوعـــة الاستقراء الرياضي على $t \in N$.

من أجل $t=0$ يكون :

$$(n+m)+0=n+m=n+(m+0)$$

وهـــذا يعني أن القضية $(n+m)+t=n+(m+t)$ محققـــة من أجل $t=0$ ومن أجل أي $n,m \in N$

نفرض أن القضية محققـــة من أجل $k \in N$ أي

$$(n+m)+k=n+(m+k)$$

ولنـــبرهن صحتها من أجل $k+1$.

إن :

$$\begin{aligned}(n+m)+(k+1) &= [(n+m)+k]+1 \\ &= [n+(m+k)]+1 \\ &= n+[(m+k)+1] \\ &= n+[m+(k+1)]\end{aligned}$$

إذاً :

$$\forall n,m,t \in N \quad : \quad (n+m)+t=n+(m+t)$$

تمهيدية : $\forall n \in N \quad : \quad n+1=1+n$

الإثبات :

لنعتمد موضوعـــة الاستقراء الرياضي لإثبات صحة هـــذه القضية.

من أجل $n=0$ يكون :

$$0+1=1=1+0$$

فالقضية $n+1=1+n$ محققة من أجل $n=0$.

نفرض أن القضية محققة من أجل k أي $k+1=1+k$

ولنبرهن صحة القضية من أجل $k+1$.

إن :

$$1+(k+1)=(1+k)+1=(k+1)+1$$

أي أن القضية محققة من أجل $k+1$

إذاً :

$$\forall n \in N \quad : \quad n+1=1+n$$

مبرهنة (٣) :

عملية الجمـــع في N عملية تبديلية أي :

$$\forall n,m \in N \quad : \quad n+m=m+n$$

الإثبات :

أيـــاً كان $m \in N$. لنعتمد موضوعـــة الاســـتقراء الرياضي على n

من أجل $n=0$ يكون :

$$0+m=m=m+0$$

فالمبرهنة صحيحة من أجل $m \in N$ و $n=0$.

نفرض أن المبرهنة صحيحة من أجل k أي $k+m=m+k$ ولنبرهـــن صحتها من أجل $k+1$.

إن :

$$(k+1)+m=k+(1+m)=k+(m+1)=(k+m)+1$$
$$=(m+k)+1=m+(k+1)$$

أي القضية صحيحة من أجل $k+1$

إذاً : $\forall n,m\in N \quad : \quad n+m=m+n$

نتائـــــج :

1. $\forall \quad n,m,t\in N \quad : \quad m+t=n+t \quad \Rightarrow \quad m=n$
2. $\forall \quad n\in N^{*} \quad : \quad \exists \quad n_1\in N \quad : \quad n=n_1+1$
3. $\forall \quad n\in N^{*} \quad \wedge \quad m\in N \quad : \quad n+m\in N^{*}$
4. $(n,m\in N)\wedge(m\neq 0 \ \vee \ n\neq 0) \quad : \quad n+m\neq 0$

البرهان : يترك للقارئ كتمرين .

٣ - ٤ عملية الضرب في N :

تعريف عملية الضرب في N :

تُعرف عمليـــة الضرب في N بأنهـــا قانـــون التشكيل الداخـــلي :

$$\bullet : N\times N\rightarrow N$$

المعرفة كما يلي :

$$\bullet(n,m)=n.m \qquad \forall \quad (n,m)\in N\times N$$

والمحقق للشرطين الآتيين :

(i) $\forall n\in N \quad : \quad n.0=0$

(ii) $\forall n,m\in N \quad : \quad n.m'=n.m+n$

ويسمى $n.m$ ناتج ضرب n بـــ m

نتائج وملاحظـــات :

١. نلاحظ من التعريف أن العـــدد 0 عنصر ماص من اليمين في N بالنســـبة لـــ • .

٢. إن العـــدد ١ عنصر محايـــد من اليمين بالنسبة لـــ • لأن :

$$\forall n \in N \quad : \quad n.1 = n.0' = n.0 + n = 0 + n = n$$

خواص عملية الضرب في N :

مبرهنة (١) : العنصر 0 هو العنصر الماص في N بالنســـبة لـــ (•) أي :

$$\forall n \in N \quad : \quad n.0 = 0.n = 0$$

الإثبات : حسب تعريف عملية الضرب في N يكون :

$$\forall n \in N \quad : \quad n.0 = 0$$

ولنثبت أن :

$$\forall n \in N \quad : \quad 0.n = 0$$

وذلك حسب موضوعة الاستقراء الرياضي

من أجل $n = 0$ يكون :

$0.0=0$ (حسب الشرط الأول من تعريف عملية الضرب)

وهـــذا يعني أن القضية $0.n = 0$ صحيحة من أجل $n = 0$.

نفرض أن $0.k = 0$ ولنـــبرهن على أن $0 . (k+1) = 0$

إن :

$$0.(k+1) = 0.k' = 0.k + 0 = 0 + 0 = 0$$

إذاً :

$$\forall n \in N \quad : \quad n.0 = 0$$

مبرهنة (٢) :

العنصر ١ هـو العنصر المحايـد في N بالنسـبة لـ (•) أي :

$$\forall n \in N \quad : \quad n.1 = 1.n = n$$

الإثبات : حسب تعريف عملية الضرب في N يكون :

$$\forall n \in N \quad : \quad n.1 = n.0' = n.0 + n = 0 + n = n$$

ولنثبت أن :

$$\forall n \in N \quad : \quad 1.n = n$$

وذلك حسب موضوعة الاستقراء الرياضي .

من أجل $n = 0$ يكون :

$1.0 = 0$ (حسب الشرط الأول من تعريف عملية الضرب في N)

وهـذا يعني أن القضية $1.n = n$ صحيحة من أجل $n = 0$.

بفرض أن $1.k = k$ ولنبرهن على أن $1.(k+1) = k+1$

إن :

$$1.(k+1) = 1.k' = 1.k + 1 = k + 1$$

إذاً :

$$\forall n \in N \quad : \quad 1.n = n$$

وبالتالي :

$$\forall n \in N \quad : \quad n.1 = 1.n = n$$

مبرهنة (٣) :

عمليـة الضـرب توزيعيـة من اليمـين عـلى الجمـع في N أي :

$$\forall n, m, t \in N \quad : \quad (n+m).t = n.t + m.t$$

الإثبـــات :

أياً كان $n,m \in N$. نعتمد موضوعة الاستقراء الرياضي على t لإثبات صحة المبرهنة. من أجل $t = 0$ يكون :

$$(n+m).0 = 0 = 0+0 = n.0 + m.0$$

وهذا يعني أن القضية $(n+m).t = n.t + m.t$ صحيحة من أجل أي $n,m \in N$ و $t = 0$.

نفرض أن :

$$(n+m).k = n.k + m.k$$

ولنبرهن على أن :

$$(n+m).(k+1) = n.(k+1) + m.(k+1)$$

إن :

$$\begin{aligned}(n+m).(k+1) &= (n+m).k' = (n+m).k + (n+m)\\ &= n.k + m.k + (n+m)\\ &= (n.k+n) + (m.k+m)\\ &= n.k' + m.k'\\ &= n.(k+1) + m.(k+1)\end{aligned}$$

إذاً :

$$\forall n,m,t \in N \quad : \quad (n+m).t = n.t + m.t$$

مبرهنة (٤) :

عملـــية الضـــرب في N عملـــية تبـــديلية أي :

$$\forall n,m \in N \quad : \quad n.m = m.n$$

الإثبـــات : أياً كان $m \in N$. لنعتمد موضوعة الاستقراء الرياضي على n

لإثبات صحة المبرهنة .

من أجل $n = 0$ يكون :

$$0 \,.m = 0 = m.0$$

وهـــذا يعـــني أن القضية $n.m = m.n$ صحيحـــة من أجـــل أي $m \in N$ و $n = 0$.

نفرض أن $k.m = m.k$

ولنبرهن على أن $(k+1).m = m.(k+1)$

إن : $(k+1).m = k.m + 1.m = m.k + m = m.(k+1)$

إذاً :

$$\forall n, m \in N \quad : \quad n.m = m.n$$

مبرهنة (٥) :

عملية الضرب في N عملية تجميعيـــة أي :

$$\forall n, m, t \in N \quad : \quad (n.m).t = n.(m.t)$$

الإثبـــات :

أياً كان $n, m \in N$ لنعتمد موضوعة الاستقراء الرياضي على t لإثبات صحـــة المـــبرهنة .

من أجل $t = 0$ يكون :

$$(n.m).0 = 0 = n.0 = n.(m.0)$$

وهـــذا يعني أن القضية $(n.m).t = n.(m.t)$ صحيحـــة من أجـــل أي $n, m \in N$ و $t = 0$.

نفرض أن : $(n.m).k = n.(m.k)$

ولنبرهن على أن : $(n.m).(k+1) = n.[m.(k+1)]$

إن :

$$\begin{aligned}(n.m).(k+1) &= (n.m).k + n.m \\ &= n.(m.k) + n.m \\ &= n.(m.k+m) \\ &= n.[m.(k+1)]\end{aligned}$$

إذاً :

$$\forall n,m,t \in N \quad : \quad (n.m).t = n.(m.t)$$

نتائـــــج :

من المبرهنات الخمس السابقة نستنتج أن :

١. عملية الضرب توزيعية على عملية الجمع في N .

٢. إذا كان $n,m \in N$ فإن :

$$[(n=0) \vee (m=0)] \quad \Leftrightarrow \quad n.m = 0$$

٣. إذا كان $n,m \in N$ فإن :

$$[(n \neq 0) \wedge (m \neq 0)] \quad \Leftrightarrow \quad n.m \neq 0$$

٤. إذا كان $n,m \in N$ فإن :

$$[(n.t = m.t)] \wedge [(t \neq 0)] \quad \Leftrightarrow \quad n = m$$

٣ – ٥ قابلية القسمة في N :

تعريف : ليكن $n,m \in N$ بحيث $m \neq 0$. نقول إن m قاسم لـــ n (ونكتب $m|n$) في N إذا وجد عدد $q \in N$ بحيث يكون

$$n = m.q$$

أي أن :

$$m|n \quad \Leftrightarrow \quad \exists \ q \in N \ : \ n = m.q$$

مبرهنـــة : (خوارزمية القسمة في N)

إذا كان $n,m \in N$ بحيث $m \neq 0$ فإنـــه يوجد $q,r \in N$ وحيدان بحيث يكون :

$$n = m.q + r \quad ; \quad 0 \leq r \leq m$$

الإثبـــات : إثبات الوجـــود : ليكن $m \in N^*$. ولنعتمد موضوعـــة الاستقراء الرياضي على n لإثبات صحة القضية :

$$\forall n \in N \ : \ \exists \ q,r \in N \ : \ n = m.q + r \ ; \ 0 \leq r \leq m \quad (\mathrm{I})$$

من أجل $n = 0$ يوجد في N العددان: $r = 0$, $q = 0$ بحيث يكون

$$0 = m.0 + 0 \quad ; \quad 0 \leq 0 < m$$

أي أن القضية (I) صحيحة من أجل $m \in N^*$ و $n = 0$.

نفرض أن القضية (I) صحيحة من أجل $k \in N$ أي :

$$\exists \ q_1, r_1 \in N \ : \ k = m.q_1 + r_1 \quad ; \quad 0 \leq r_1 < m$$

ولنبرهن على صحة (I) من أجل $k+1$.

إذا كان : $k = m.q_1 + r_1$.

فإن : $k + 1 = m.q_1 + r_1 + 1$.

وبالتالي يكون :

إذا كان $r_1 + 1 < m$ فإنه يوجد في N العددان

$$q = q_1 \quad و \quad r = r_1 + 1$$

بحيث يكون :

$$k+1=m.q+r \quad ; \quad 0<r<m$$

أما إذا كان $r_1+1=m$ فإنه يوجد في N العددان

$$q=q_1+1 \quad و \quad r=0$$

بحيث يكون :

$$k+1=m.q+r \quad ; \quad 0=r<m$$

إذاً :

$$\forall n,m\in N \quad \wedge \quad (m\neq 0):\exists q,r\in N: n=m.q+r \quad ; \quad 0\leq r<m$$

إثبات الوحدانية :

لنفرض أنه من أجل $n\in N$ و $m\in N^*$ يوجد $q,q',r,r'\in N$

بحيث يكون :

$$m.q+r=m.q'+r' \quad ; \quad 0\leq r<m \quad \wedge \quad 0\leq r'<m \qquad (\text{II})$$

ولنفرض أن $r\leq r'$ وهـــذا لا يفقد عموميّة المسألة .

من (II) ينتج أن :

$$r'-r=m(q-q') \qquad (\text{III})$$

وهـــذا يعني أن m قاسم لـــ $r'-r$ في N وهذا يتحقق فقط إذا كان $r'-r=0$ (وذلك لأن $r<m$ و $r'<m$) .

بالتبديل في (III) ينتج أن $q-q'=0$

إذاً :

$$(q'=q)\wedge(r'=r)$$

٣ – ٦ القاسم المشترك الأكبر والمضاعف المشترك الأصغر في N :

تعريف (١) :نعرف القاسم المشترك الأكـــبر للعددين $n,m \in N^*$ بأنه العدد الطبيعي المغاير للصفر d والمحقق للشرطين الآتيين :

١ – $(d|n) \wedge (d|m)$

٢ – إذا كان $d' \in N^*$ بحيث $(d'|n) \wedge (d'|m)$ فإن $d'|d$

تعريف (٢) : نعرف المضاعف المشـــترك الأصغر للعددين $n,m \in N^*$ بأنه العدد الطبيعي المغاير للصفر c والمحقق للشرطين الآتيين :

١َ – $(m|c) \wedge (n|c)$

٢َ – إذا كان $c' \in N^*$ بحيث $(m|c') \wedge (n|c')$ فإن $c|c'$

مبرهنة :

إذا كانت $n,m \in N^*$ فإن القاسم المشترك الأعظم d للعددين n,m موجود ووحيد .

الإثبات : إذا كان $n = m$ فإن $d = n = m$ وهو وحيد .

لنفرض أن $n \neq m$ ولنفرض أن $m < n$ وهذا لا يفقد عمومية المسألة

حسب خوارزمية القسمة في N يوجد $q_1, r_1 \in N$ بحيث :

$$n = m.q_1 + r_1 \quad ; \quad 0 \le r_1 < m$$

فإذا كان r_1 لا يقسم m فيوجد $q_2, r_2 \in N$ بحيث :

$$m = q_2 . r_2 + r_2 \quad ; \quad 0 \le r_2 < r_1$$

وهكذا ... فنحصل على مجموعة غير خالية : $\{m, r_1, r_2, ...\}$ حيث :

$$..... < r_2 < r_1 < m$$

ومنه يوجد في هذه المجموعة عنصر أصغر وليكن r_k بحيث يكون قاسماً

لـ r_{k-1} وهذا نحصل على العلاقات :

1. $n = m.q_1 + r_1 \quad ; \quad 0 \le r_1 < m$
2. $m = q_2 \cdot r_1 + r_2 \quad ; \quad 0 \le r_2 < r_1$
3. $r_1 = q_2 \cdot r_2 + r_3 \quad ; \quad 0 \le r_3 < r_2$

....

4. $r_{k-2} = q_k \cdot r_{k-1} + r_k \quad ; \quad 0 \le r_{k-1} < r_{k-2}$
5. $r_{k-1} = q_{k+1} \cdot r_k$

إن r_k هو القاسم المشترك الأكبر للعددين n, m وذلك لأنه :

من جهة أولى : من العلاقة (٥) نجد أن $r_k | r_{k-1}$

وحسب العلاقة (٤) يكون $r_k | r_{k-2}$

وحسب العلاقة (٣) يكون $r_k | r_{k-3}$. وهكذا .....

وحسب العلاقة (٢) يكون $r_k | m$

وحسب العلاقة (١) يكون $r_k | n$

أي : $(r_k | n) \wedge (r_k | m)$.

ومن جهة أخرى : إذا كان $d \in N^*$ بحيث : $(d | n) \wedge (d | m)$.

من العلاقة (١) يكون $r_1 = n - m.q_1$ وبالتالي يكون $d | r_1$.

ومن العلاقة (٢) يكون $d | r_2$. وهكذا .....

ومن العلاقة الأخيرة يكون $d | r_k$.

٣ — ٧ الأعـــداد الأوليـــة :

تعريف : نقول عن العدد الطبيعي p إنه أولي إذا تحقق الشرطان التاليان:

١. $p \in N - \{0,1\}$.

٢. $\forall n \in N : n | p \Rightarrow (n = 1) \vee (n = p)$.

مبرهنة : إذا كان $n \in N - \{0,1\}$ فإن العدد n يكتب كجداء لإعـــداد أولية وهـــذا الجـــداء وحيد بغض النظر عن ترتيب المضاريب .

الإثبات : لنعتمد موضوعة الاستقراء الرياضي .

من أجل $n = 2$ فـــإن $2 = 2$ أي أن نص المبرهنة صحيح (وجـــود ووحدانية) لأجل $n = 2$.

إذا كان $2 < n$ عـــدداً أولياً فـــإن n يتحلل وبشكل وحيد إلى جداء أعـــداد أوليـــة $n = n$.

لنفترض الآن أن $2 < n$ ليس أولياً .

ونفترض أن المبرهنة صحيحة (وجود ووحدانية) من أجل جميع الأعداد الطبيعية x المحققة للشرط $2 \le x < n$.

أي أن كل عـــدد طبيعي x بحيث $2 \le x < n$ يتحلل بشكل وحيد إلى جـــداء أعـــداد أوليـــة .

بما أن n ليس أولياً فيوجد $n_1 \in N - \{0,1\}$ قاسماً لـــ n وبالتالي يوجد $n_2 \in N - \{0,1\}$ بحيث يكون :

$$(n = n_1 . n_2) \wedge (2 \le n_1 < n) \wedge (2 \le n_2 < n)$$

وحسب طبيعة الأعداد x فإن كلاً من العددين n_1, n_2 يتحلل بشكل وحيد إلى جداء أعداد أولية وبالتالي n يتحلل إلى جداء أعداد أولية .

لنفرض أن $2 < n$ وليس أولياً وليكن :

$$n = p_1 . p_2 .... p_r = p'_1 . p'_2 .... p'_s \qquad (*)$$

حيث p_i, p'_j أعداد أولية $(i = 1,2,....,r)$, $(j = 1,2,....,s)$

ولنبرهن على أن :

$r = s$.(I)

$p_i = p'_i$. (II) $\forall i = 1,2,\ldots,r$ بترقيم مناسب .

بما أن الطرف الأيسر في (*) يقبل القسمة على p_1 فإن الطرف الأيمن في (*) أيضاً يقبل القسمة على p_1 .

وبالتالي أحد المضاريب $p'_1 . p'_2 \ldots p'_s$ يقبل القسمة على p_1 وبالتالي بعد إعادة الترقيم للأعداد $p'_1, p'_2, \ldots, p'_s$ سيكون $p_1 | p'_1$ وبما أن كلاً من p_1, p'_1 أولي فإن $p_1 = p'_1$ وبالتالي بعد اختصار طرفي (*) على $p_1 = p'_1$ نحصل على :

$$p_2 . p_3 \ldots\ldots p_r = p'_2 . p'_3 \ldots\ldots p'_s$$

وبما أن n ليس أولياً فإن $r > 1$.

عندئذٍ بفرض $n_1 = p_2 . p_3 \ldots\ldots p_r$ يكون $2 \le n_1 < n$

وبالتالي فالتحليل لـ n_1 يكون وحيداً (حسب الفرض الاستقرائي)

ومنه يكون $r - 1 = s - 1$ أي $r = s$ و $p_i = p'_i$ $(i = 2,\ldots,r)$

وذلك بعد ترقيم ملائم .

ومنه : (I) . $r = s$.

(II) . $p_i = p'_i$ $(i = 2,\ldots,r)$ بترقيم مناسب .

مبرهنة : مجموعة الأعداد الأولية مجموعة غير منتهية .

الإثبات :

لنفرض جدلاً أن مجموعة الأعداد الأولية مجموعة منتهية ولتكن $\{P_1, P_2, \ldots, p_n\}$ وليكن p_n هو أكبر الأعداد الأولية .

ولنأخذ الجـــداء : $P = P_1 . P_2 ..... p_n$

فنجـــد أن العـــدد $p+1$ لا يقبل القسمة على أي عـــدد من الأعداد $P_1, P_2, ..., p_n$ لأن باقي القسمة دوماً هو ١ .

وبالتالي تكون لدينا إحدى الحالتين :

I . العـــدد $p+1$ أولي ، وهذا يناقض كون p_n هو أكبر الأعـــداد الأوليـــــة .

II . أن العـــدد $p+1$ هو جداء لأعـــداد أولية وهذا يناقض اختيار الجـــداء p .

إذاً الفرض الجدلي خاطئ وبالتالي مجموعـــة الأعـــداد الأولية غير منتهية.

لاحظ أن كلاً من الأعداد :

11014491 , 10014493 , 10014497 , 294319 , 299477

هي أعـــــداد أوليـــــة .

تمرينات محلولـــــــة

التمريـــن الأول:

بفرض أن $n \in N$ برهـــن صحـــة القضيتين الآتيتين :

(I) $1 \le 2^n$

(II) $n < 2^n$

الحـــل: لنعتمـــد على موضوعـــة الاستقراء الريـــاضي .

(I) . من أجل $n = 0$ يكون :

$1 \le 2^0 = 1$ أي أن القضية (I) صحيحة من أجل $n = 0$.

نفرض صحـــة القضية (I) من أجل k أي أن : $1 \le 2^k$ ولنبرهن على صحـــة (I) من أجل $k+1$

بما أن : $1 \le 2^k$ وبالتالي يكون $2 \cdot 1 \le 2 \cdot 2^k$ ومنه $2 \le 2^{k+1}$

ومنه $1 \le 2^{k+1}$. أي أن القضية (I) صحيحة من أجل $k+1$

إذاً :

$$\forall n \in N \quad : \quad 1 \le 2^n$$

(II) . من أجل $n = 0$ يكون:

$0 \le 2^0 = 1$ أي أن القضية (II) صحيحة من أجل $n = 0$.

نفرض صحة القضية (II) من أجل k أي أن : $k \le 2^k$ ولنبرهن على صحـــة (II) من أجل $k+1$

بمـــا أن $k \le 2^k$ وبالتالي يكون $k+1 < 2^k+1$. وحسب (I) يكون

$k+1<2^{k+1}$ وبالتالي $k+1<2^k+2^k=2.2^k$

أي أن القضية (II) صحيحة من أجل $k+1$.

إذاً :

$$\forall n \in N \quad : \quad n<2^n$$

التمرين الثـــاني :

برهـــن صحـــة القضيـــة الآتيـــة :

$$\forall n \in N \quad : \quad 10^n \equiv 1 \pmod 9$$

الحـــل : من أجل $n=0$ يكون $1 \equiv 1 \pmod 9$ أي أن القضية المفروضة صحيحة من أجل $n=0$.

لنفرض أن القضية صحيحة من أجل $n=k$ أي أن :

$$10^k \equiv 1 \pmod 9$$

ولنبرهن على صحة القضية من أجل $n=k+1$.

لدينا : $10^k \equiv 1 \pmod 9$

ولدينا : $10 \equiv 1 \pmod 9$

وبالتالي :

$$10^k.10 = 1.1 \pmod 9$$

ومنه :

$$10^{k+1} \equiv 1 \pmod 9$$

أي أن القضية صحيحة من أجل $n=k+1$.

إذاً :

$$\forall n \in N \quad : \quad 10^n \equiv 1 \pmod n$$

التمرين الثالث :

نعرف القـــوة في N^* بأنهـــا التطبيق : $f : N^* \times N \to N^*$

المعرف كما يلي :

$$f(n,m) = n^m \qquad \forall (n,m) \in N^* \times N$$

والمحقق للشرطين الآتيين :

(١). أياً كان $n \in N^*$ فإن $n^0 = 1$.

(٢). أياً كان $m \in N^*$ وأياً كان $n \in N$ فإن $m^{n+1} = m^n.m$.

بفرض $n,t \in N$ و $m,d \in N^*$. برهن صحة القضايا :

1) $1^n = 1$

2) $m^n \cdot m^t = m^{n+t}$

3) $(m^n)^t = m^{n.t}$

4) $(m.d)^t = m^t \cdot d^t$

الحـــل: (١). من أجل $n = 0$ يكون $1^0 = 1$ فالقضية صحيحـــة من أجل $n = 0$.

بفرض أن القضية صحيحة من أجل $n = k$ أي $1^k = 1$ وبالتالي :

$$1^{k+1} = (1^k).1 = 1.1 = 1$$

أي أن القضية (١) صحيحة من أجل $n = k+1$.

إذاً :

$$\forall n \in N \quad : \quad 1^n = 1$$

(٢). أياً كان $m \in N^*$, $n \in N$ فإنه من أجل $t = 0$ يكون :

$$m^n \cdot m^0 = m^n . 1 = m^n = m^{n+0}$$

أي أن القضية (٢) صحيحة من أجل $t = 0$.

نفرض أن القضية (٢) صحيحة من أجل $t = k$ أي أن :

$$m^n \cdot m^k = m^{n+k}$$

وبالتالي يكون :

$$\begin{aligned} m^n \cdot m^{k+1} &= m^n . (m^k . m) = (m^n \cdot m^k) . m \\ &= m^{n+k} . m = m^{(n+k)+1} \\ &= m^{n+(k+1)} \end{aligned}$$

أي أن القضية (٢) صحيحة من أجل $t = k + 1$

إذاً :

$$\forall m \in N^* \quad , \quad \forall n, t \in N \quad : \quad m^n \cdot m^t = m^{n+t}$$

(٣). أياً كان $m \in N^*$, $n \in N$ فإنه :

من أجل $t = 0$ يكون :

$$(m^n)^0 = 1 = m^0 = m^{n.0}$$

أي أن القضية (٣) صحيحة من أجل $t = 0$.

نفرض أن القضية (٣) صحيحة من أجل $t = k$ أي أن :

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

وبالتالي يكون :

$$\begin{aligned} (m^n)^{k+1} &= (m^n)^k . (m^n) \\ &= m^{n.k} \cdot m^n \\ &= m^{n.k+n} \\ &= m^{n.(k+1)} \end{aligned}$$

أي أن القضية (٣) صحيحة من أجل $t = k+1$.

إذاً :

$$\forall m \in N^* \quad , \quad \forall n,t \in N \quad : \quad (m^n)^t = m^{n.t}$$

(٤). أياً كان $m,d \in N^*$ فإنه :

من أجل $t = 0$ يكون :

$$(m.d)^0 = 1 = 1.1 = m^0.d^0$$

أي أن القضية (٤) صحيحة من أجل $t = 0$.

نفرض أن القضية (٤) صحيحة من أجل $t = k$ أي أن :

$$(m.d)^k = m^k.d^k$$

وبالتالي يكون :

$$\begin{aligned}(m.d)^{k+1} &= (m.d)^k.(m.d) \\ &= m^k d^k.(m.d) \\ &= (m^k.m).(d^k.d) \\ &= m^{k+1}.d^{k+1}\end{aligned}$$

أي أن القضية (٤) صحيحة من أجل $t = k+1$.

إذاً :

$$\forall m,d \in N^* \quad , \quad t \in N \quad : \quad (m.d)^t = m^t.d^t$$

التمرين الرابع :

اعتمد على تعريف كل من عمليتي جمع وضرب الأعداد الطبيعية وخواصها لإثبات القضية : $\forall n \in N^* \quad : \quad n.2 = n + n$

الحل: من أجل $n = 1$ يكون :

$$n.2 = 1.2 = 1.(1)' = 1.1 + 1 = 1 + 1 = n + n$$

فالقضية صحيحة من أجل $n = 1$.

نفرض أن القضية صحيحة من أجل $n = k$ أي أن : $k.2 = k + k$

ولنبرهن صحة القضية من أجل $n = k + 1$.

إن :

$$(k+1).2 = (k+1).(1)' = (k+1).1 + (k+1) = (k+1) + (k+1)$$

أي أن القضية صحيحة من أجل $n = k + 1$.

إذاً :

$$\forall n \in N^* \quad : \quad n.2 = n \cdot n$$

التمرين الخـــامس :

برهن أنه إذا كان مجموع أرقام العـــدد الطبيعي n يقبل القسمة على ٩ فإن العدد n يقبل القسمة على ٩ .

الحـــل :

أياً كان العـــدد الطبيعي فإنه يكتب على الشكل :

$$n = \alpha_0 + 10 \cdot \alpha_1 + 10^2 \cdot \alpha_2 + \ldots + 10^k \cdot \alpha_k \qquad (*)$$

حيث $\alpha_0, \alpha_1, \ldots, \alpha_k$ أرقام العدد n .

بما أن :

$$\alpha_i \equiv \alpha_i \pmod 9 \quad \wedge \quad 10^i \equiv 1 \pmod 9$$

وذلك أياً كان $i = 1, 2, \ldots, k$

وبالتالي يكون :

$$10^i \cdot \alpha_i \equiv \alpha_i \pmod 9 \qquad \forall i = 1, 2, \ldots, k$$

وبالتالي يمكن كتابة المساواة (*) وفق $(\bmod 9)$ كما يلي :

$$n \equiv (\alpha_0 + \alpha_1 + \ldots + \alpha_k) \qquad (\bmod 9)$$

وهذا ما يثبت أن العـــدد ٩ يقسم n .

تمرينات (٣)

التمرين الأول :

بفرض $n,m \in N$. برهـــن على صحـــة القضيتين الآتيتين :

1. $(n.m')' = n.m + n'$.
2. $(n'.m')' = n' + n.m + m'$.

التمرين الثاني :

بفرض $n,m \in N$. برهـــن على صحـــة القضيتين الآتيتين :

1. $(n + m')' = n' + m'$.
2. $n' + m' = (n + m)' + 1$.

التمرين الثالث :

اعتمـــد على تعريف كل من عمليتي جمـــع وضرب الأعـــداد الطبيعية وخواصهما لإثبات صحة القضية الآتية :

$$\forall n \in N^* \quad : \quad n.3 = (n + n) + n$$

حيث $3 = 2'$

التمرين الرابع :

نُعرف في مجموعـــة الأعـــداد الطبيعية N العلاقة الثنائية $\leq$ كما يلي :

$$\forall n,m \in N \quad : \quad n \leq m \quad \Leftrightarrow \quad \exists k \in N^* \quad : \quad m = n + k$$

والمطـــــلوب :

١. برهن أن العلاقة الثنائية $\leq$ المعرفة في N هي علاقة ترتيب .

٢. بفرض أن $n,m,t \in N$ فبرهن على صحة القضية الآتية :

$$t \neq 0 \Rightarrow [n.t \leq m.t \Rightarrow n \leq m]$$

(إن العلاقة الثنائية $\leq$ المعرفة على N هي علاقة الترتيب المألوفة) .

التمرين الخامس :

إذا كان p عـــدداً أوليـــاً فبرهـــن أن الجداء $n = 1.2.3.....(p-1)$ لا يقبل القسمة على p .

التمرين السادس :

بفرض $n,m \in N$. برهن صحـــة الاقتضـــاء :

$$n.m = 1 \Rightarrow (n = 1) \wedge (m = 1)$$

الفصل الرابع

مجموعة الأعداد الصحيحة

The Set Of Integers

٤ - ١ بناء مجموعة الأعداد الصحيحة :

ذكرنا في الفصل السابق أن مجموعة الأعداد الطبيعية N هي أم المجموعات العددية الأساسية .وسنبيّن في هذا البند كيفية بناء مجموعة الأعداد الصحيحة انطلاقاً من مجموعة الأعداد الطبيعية N .

نعرف في المجموعة $N \times N$ العلاقة الثنائية R كما يلي :

$$\forall (a_1,b_1),(a_2,b_2) \in N \times N : \quad (a_1,b_1)R(a_2,b_2) \Leftrightarrow a_1 + b_2 = b_1 + a_2$$

إن هذه العلاقة الثنائية R هي علاقة تكافؤ (راجع التمرين الثاني المحلول في الفصل الأول) .

وبالتالي لكل عنصر $(a,b) \in N^2$ صف تكافؤ وفق R ونرمز له $[a,b]$ نسمي مجموعة صفوف التكافؤ N^2/R مجموعة الأعداد الصحيحة ونرمز لها بالرمز Z .

أي أن : أيّ عدد صحيح Z هو صف تكافؤ مثل $[a,b]$.

وإذا كان $Z_1 = [a_1,b_1]$ ، $Z_2 = [a_2,b_2]$ عددين صحيحين فإن :

$$\begin{aligned} Z_1 = Z_2 &\Leftrightarrow [a_1,b_1] = [a_2,b_2] \\ &\Leftrightarrow (a_1,b_1)R(a_2,b_2) \\ &\Leftrightarrow a_1 + b_2 = b_1 + a_2 \end{aligned}$$

ومنه أياً كان $n \in N$ فإن :

$$[a+n, b+n] = [a,b] \quad ; \quad \forall [a,b] \in Z$$

٤ – ٢ عمليتا الجمـــع والضرب في Z :

تعريف (١) :تعرّف عملية الجمع في Z بأنها القانون التشكيل الداخلي $+$

$$+ : Z \times Z \to Z$$

المعرفة كما يلي :

$$+([a_1,b_1]+[a_2,b_2]) = [a_1,b_1]+[a_2,b_2] = [a_1+a_2, b_1+b_2]$$

وذلك أياً كان $[a_1,b_1],[a_2,b_2] \in Z$

تعريف (٢):تُعرف عملية الضرب في Z بأنها القانون التشكيل الداخلي $\bullet$

$$\bullet : Z \times Z \to Z$$

المعرف كما يلي :

$$\bullet([a_1,b_1],[a_2,b_2]) = [a_1,b_1]\bullet[a_2,b_2]$$
$$= [a_1a_2+b_1b_2 \quad , \quad a_1b_2+b_1a_2]$$

وذلك أياً كان $[a_1,b_1],[a_2,b_2] \in Z$

خواص عمليتي الجمع والضرب في Z :

ليكن $[a,b],[c,d],[e,f] \in Z \quad , \quad [0,0] \neq [\alpha,\beta] \in Z$.

عندئذٍ يمكن – بسهولة – إثبات صحة القضايا الآتية :

١. كل من عمليتي الجمـــع والضرب في Z هي عملية تبديـــلية . أي :

$$[a,b]+[c,d] = [c,d]+[a,b]$$
$$[a,b]\bullet[c,d] = [c,d]\bullet[a,b]$$

٢. كل من عمليتي الجمـــع والضرب في Z هي عملية تجميعية . أي :

$$([a,b]+[c,d])+[e,f] = [a,b]+([c,d]+[e,f])$$
$$([a,b]\bullet[c,d])\bullet[e,f] = [a,b]\bullet([c,d]\bullet[e,f])$$

٣. عملية الضرب توزيعية على عملية الجمـــع في Z . أي :

$$[a,b]\cdot([c,d]+[e,f])=[a,b]\cdot[c,d]+[a,b]\cdot[e,f]$$
$$([c,d]+[e,f])\cdot[a,b]=[c,d]\cdot[a,b]+[e,f]\cdot[a,b]$$

٤. العدد الصحيح $[0,0]$ عنصر محايد في Z بالنسبة لعملية الجمع . أي

$$\forall[x,y]\in Z \quad : \quad [x,y]+[0,0]=[0,0]+[x,y]=[x,y]$$

٥. العدد الصحيح $[1,0]$ عنصر محايد في Z بالنسبة لعملية الضرب .أي

$$\forall[x,y]\in Z \quad : \quad [x,y]\cdot[1,0]=[1,0]\cdot[x,y]=[x,y]$$

٦. لكل عـــدد صحيح $[x,y]$ نظير في Z بالنسبة لعملية الجمـــع وهو العـــدد الصحيح $[x,y]$ أي :

$$[x,y]+[y,x]=[y,x]+[x,y]=[0,0]$$

(نرمّز نظير العـــدد الصحيح $[x,y]$ بالنسبة لعملية الجمـــع بالرمز $-[x,y]$ أي : $-[x,y]=[y,x]$) .

نتيجة : نستنتج من الخواص السابقة أن $(Z,+,.)$ حلقة واحـــدية تبديلية .

٤ – ٣ الشكل المألوف لمجموعة الأعداد الصحيحة :

لنأخـــذ العلاقـــة :

$$\varphi : N \to Z$$

المعرفة كما يلي :

$$\varphi(a)=[a,0] \quad ; \quad \forall a\in N$$

فنجد ما يلي :

١. التطبيق φ تطبيق متباين :

$$\forall a,b\in N \quad : \quad a=b \Leftrightarrow a+0=b+0 \Leftrightarrow [a,0]=[b,0]$$
$$\Leftrightarrow \varphi(a)=\varphi(b)$$

٢. التطبيق φ يتمتع بالصفات الآتية :

(i)ـ φ يحافظ على عملية الجمع أي : $\varphi(a+b)=\varphi(a)+\varphi(b)$

(ii)ـ φ يحافظ عل عملية الضرب أي : $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$

(iii)ـ $\varphi(0)=[0,0]$ و $\varphi(1)=[1,0]$ أياً كان $a,b\in N$

في الحقيقة :

(i) $\varphi(a+b)=[a+b,0]=[a,0]+[b,0]=\varphi(a)+\varphi(b)$

(ii) $\varphi(a\cdot b)=[a\cdot b,0]=[a,0]\cdot[b,0]=\varphi(a)\cdot\varphi(b)$

(iii) $\varphi(1)=[1,0]$, $\varphi(0)=[0,0]$

إن وجود التطبيق المتباين φ والمحافظ على العمليات يسمح لنا بأن نطابق بين منطلق φ وبين مجموعة المستقر الفعلي $I_m\varphi$ وذلك بأن نطابق بين كل عنصر $a\in N$ بصورته وفق φ أي :

$$\forall a\in N \quad : \quad \varphi(a)=[a,0]=a$$

ونستنتج مباشرة أن :

1. $[1,0]=1$
2. $[0,0]=0$
3. $[0,a]=-[a,0]=-a \qquad \forall a\in N$

وبالتالي أياً كان العدد الصحيح $[a,b]$ فإن :

$$[a,b]=[a,0]+[0,b]=[a,0]+(-[b,0])=a-b$$

نسمي الأعداد الصحيحة ذات الشكل $[a,0]$ حيث $a\subset N^*$ بالأعداد الصحيحة الموجبة ونرمّزها بـــ Z^+ .

ونسمي الأعداد الصحيحة ذات الشكل $[0,b]$ حيث $b\in N^*$ بالأعداد

الصحيحة السالبة ونرمّزها بـــ Z^- .

مما سبق يمكن التعبير عن المجموعتين Z^+ ، Z^- كما يلي :

$$Z^+ = \{[a,0] = a \quad ; \quad a \in N^*\} = \{a \quad ; a \in N^*\} = \{1,2,3,...\}$$

$$Z^- = \{[0,b] \quad ; \quad b \in N^*\} = \{-[b,0] \quad ; \quad b \in N^*\}$$
$$= \{-b \quad ; \quad b \in N^*\}$$
$$= \{-1,-2,-3,...\}$$

لاحظ أن الأسرة $\Gamma = \{\{0\}, Z^-, Z^+\}$ تجزئة لمجموعة الأعداد الصحيحة Z . نصطلح أن : $Z^* = Z - \{0\}$.

وهـــذا نحصل على الشكل المألوف لمجموعـــة الأعـــداد الصحيحـــة :

$$Z = \{...,-2,-1,0,1,2,...\}$$

٤ – ٤ قابلية القسمة في Z :

تعاريف :

تعريف (١) : ليكن $z \in Z$. نعرف القيمـــة المطلقـــة للعـــدد z ونرمز لها بـــ $|z|$ كما يلي :

$$|z| = \begin{cases} z & ; \ (0 < z \ \text{عندما}) \\ 0 & ; \ (z = 0 \ \text{عندما}) \\ -z & ; \ (z < 0 \ \text{عندما}) \end{cases}$$

تعريف (٢) : ليكن $a,b \in Z$ بحيث $b \neq 0$. نقول عن b إنه قاسم لـــ a في Z (ونكتب $b|a$) إذا وجد عـــدد صحيح $q \in Z$ من أجله يكون $a = q \cdot b$.

أي :

$$b|a \quad \Leftrightarrow \quad \exists q \in Z \quad : \quad a = q \cdot b$$

وتبقى خوارزمية القسمة صحيحة في Z .

أي :

$$\forall a,b \in Z \quad ; \quad b \neq 0 \quad : \quad \exists q \cdot r \in Z : a = q \cdot b + r \ ; \ 0 \leq r < |b|$$

٤ ـ ٥ القاسم المشترك الأكبر لعددين صحيحين :

تعريف: نعرف القاسم المشترك الأكبر للعددين $a,b \in Z$ ونرمز له بـ $d(a,b)$ بأنه العدد الصحيح $d \in Z^+$ والمحقق للشرطين الآتيين :

١. $(d|a) \wedge (d|b)$.

٢. إذا كان $d' \in Z^+$ بحيث $(d'|a) \wedge (d'|b)$ فإن $d'|d$.

مبرهنة :

أياً كان $a,b \in Z^*$ فإن :

(d ق.م.أ للعددين $|a|,|b|$ في N) $\Leftrightarrow$ (d ق.م.أ للعددين $a,b \in Z^*$ في Z)

أي :

$$d(a,b) \text{ في } Z \quad \Leftrightarrow \quad d(|a|,|b|) \text{ في } N$$

الإثبات :

($\Leftarrow$) لنفرض أن d قاسم مشترك أكبر للعددين $|a|,|b|$ فإن $d > 0$ وأن

$$(d||a|) \wedge (d||b|)$$

وبالتالي :

$$(d|a) \wedge (d|b)$$

من جهة ثانية . إذا كان $d' \in Z^*$ بحيث $(d'|a) \wedge (d'|b)$.

فإن العـــدد الطبيعي $|d'|$ قاســـم مشـــترك للعـــددين الطبيعيين $|a|,|b|$

وبالتالي $|d'|\|d$ ومنـــه $d'|d$ إذاً d قاســـم مشترك أكبر للعددين a,b

في Z أي : $d(a,b)$ في Z

$(\Rightarrow)$: لنفرض أن d قاسم مشترك أكبر للعـــددين a,b فإن $d > 0$

أي $d \in N^*$ وأن : $(d|a) \wedge (d|b)$

من جهة ثانية : إذا كان $c \in N^*$ بحيث $(c||a|) \wedge (c||b|)$ فإن $c \in Z^*$

وأن $(c|a) \wedge (c|b)$ وبالتالي $c|d$.

إذاً d قاسم مشترك أكـــبر للعـــددين $|a|,|b|$ في N .

أي $d(|a|,|b|)$ في N .

نتيجـــة :

حســـب خوارزمية القسمة في Z ومن تعريف القاسم المشترك الأكـــبر

للعـــددين $a,b \in Z^*$ نحصل على النتيجة التالية :

إذا كان d القاسم المشترك الأكبر للعـــددين $a,b \in Z^*$ فإنـــه يوجـــد

$\alpha,\beta \in Z$ بحيث يكون : $d = \alpha \cdot a + \beta \cdot b$

وإن العـــددين α,β ليسا وحيدين .

خوارزميّـــة إقليـــدس المعممة :

إن خوارزميّة إقليدس المعممة توضح كيفية إيجاد القاسم المشترك الأكبر d

للعددين $a,b \in Z^*$ (وهو القاسم المشترك الأكبر للعددين $|a|,|b|$)

كمـــا توضـــح كيفيّة تعيين العـــددين $\alpha,\beta \in Z$ بحيث يكـــون

$d = \alpha \cdot a + \beta \cdot b$ وتتلخص هـــذه الخـــوارزمية بما يأتي :

إذا كان $0 < b < a$ فإنــه يوجــد $q_i, r_i \in Z$ $(i = 1,2,\dots,n)$

بحيث :

$$a = q_1 \cdot b + r_1 \quad ; \quad 0 \le r_1 < b$$
$$b = q_2 \cdot r_1 + r_2 \quad ; \quad 0 \le r_2 < r_1$$
$$r_1 = q_3 \cdot r_2 + r_3 \quad ; \quad 0 \le r_3 < r_2$$
$$\dots \quad \dots\dots \quad \dots\dots \quad \dots\dots \quad \dots\dots \quad \dots\dots$$
$$r_{n-2} = q_n \cdot r_{n-1} + r_n \quad ; \quad 0 \le r_n < r_{n-1}$$
$$r_n = q_{n+1} \cdot r_n$$

إن $d(a,b) = r_n$.

ولتعيين α, β نعرف المتتاليتين $(\alpha_n),(\beta_n)$ كما يلي :

$$\alpha_0 = 1 \quad ; \quad \alpha_1 = 0 \quad ; \quad \alpha_{k+1} = \alpha_{k-1} - q_k \cdot \alpha_k$$
$$\beta_0 = 0 \quad ; \quad \beta_1 = 1 \quad ; \quad \beta_{k+1} = \beta_{k-1} - q_k \cdot \beta_k$$

حيث $k = 2,3,\dots,n-1$

فيكون : $d = r_n = \alpha_n \cdot a + \beta_n \cdot b$

ويمكن ترتيب خطوات هذه الخوارزمية في الجدول التالي :

k	r_k	q_k	α_k	β_k
0	a	-	1	0
1	b	q_1	0	1
2	r_1	q_2	α_2	β_2
.....	.....	.....	.....	.....
n	r_{n-1}	q_n	α_n	β_n
$n+1$	r_n	q_{n+1}	α_{n+1}	β_{n+1}
$n+2$	0			

والمثال التالي يوضح هـــذه الخـــوارزميـــة .

مثـــال :أوجـــد d القاسم المشترك الأكبر للعددين $b=666$, $a=936$

ثم عيّن العددين $\alpha,\beta \in Z$ بحيث يكون : $d=\alpha\cdot a+\beta\cdot b$

k	r_k	q_k	α_k	β_k
0	936	–	1	0
1	666	1	0	1
2	270	2	1	-1
3	126	2	-2	3
4	18	5	5	-7
5	0			

من الجدول نجد أن : $d=18$, $\alpha_n=5$, $\beta=-7$ وبالتالي

$$d=18=5.936+(-7).666$$

ملاحظة :إن العددين α,β لا يتعينان بشكل وحيد .

فمثلاً إذا كان $a=116$ و $b=20$ فنجد بسهولة أن $d=4$ وهو وحيد

وأن :

$$d=4=(-1)\cdot 116+6.20 \quad ; \quad \alpha=-1 \quad , \quad \beta=6$$

كما أن :

$$d=4=4.116+(-23)\cdot 20 \quad ; \quad \alpha=4 \quad , \quad \beta=-23$$

تعريف :نقول عن العددين $a,b\in Z^*$ إنهما أوليان فيما بينهما (أولياً نسبياً)

إذا كان $d(a,b)=1$.

نتيجـــة :أياً كان $a,b\in Z^*$ فإن :

$$(a,b \text{ أوليان فيما بينهما}) \Leftrightarrow \exists\ \alpha,\beta\in Z \ : \ 1=\alpha\cdot a+\beta\cdot b$$

تدعى المساواة $\alpha \cdot a + \beta \cdot b = 1$ علاقة بيزو .

فمثلاً : العددان $b = 12$, $a = 25$ أوليان فيما بينهما وأن :

$$d(a,b) = 1 = 1.25 + (-2) \cdot 12$$

٤ – ٦ الأعداد الصحيحة غير القابلة للتحليل :

تعريف: نقول عن العـــدد الصحيح P إنه غير قابل للتحليل في Z عندما وفقط عندما يتحقق الشرطان الآتيان :

١. $P \in Z - \{-1,0,1\}$

٢. إذا كان n قاسماً لـــ P فإن $n \in \{\pm 1, \pm p\}$

وبعبارة مكافئة :

(العدد الصحيح P غير قابل للتحليل في Z) $\Leftrightarrow$ العدد $|p|$ أولي .

مبرهنة : إذا كان P عدداً غير قابل للتحليل في Z ، وكان $a \in Z$ فإن :

P غير قاسم لـــ a $\Leftrightarrow$ $d(a,p) = 1$

الإثبات : ($\Leftarrow$) لنفرض أن P غير قاسم لـــ a . ولنفرض أن $d(a,p) = d$

فيكون : $(d|P) \wedge d \neq \pm P$

لكن P غير قابل للتحليل في Z وبالتالي سيكون $d = \pm 1$ وبما أن $d > 0$

فإن $d = 1$ إذاً : $d(a,p) = 1$

($\Rightarrow$) : لنفرض أن $d(a,p) = 1$. ولنفرض جدلاً أن $p|a$

وبالتالي $d(a,p) = |p|$

وبما أن P غير قابل للتحليل في Z فإن $|p| > 1$

وبالتالي سيكون $d(a,p) > 1$ وهذا يناقض الفرض .

وبالتالي P لا يقسم a .

مبرهنة :

إذا كان P عدداً صحيحاً غير قابل للتحليل في Z ، $a,b \in Z^*$

وإذا كان $p|(a \cdot b)$ فإن $(p|a) \vee (p|b)$.

الإثبات :إذا كان P غير قاسم لـــ a فإن $d(a,p)=1$ (حسب المبرهنة السابقة)

وبما أن $p|(a \cdot b)$ فإن $p|b$.

تمرينات محلولـــــة

التمرين الأول :

بفرض $m \in N^*$, $a,b,c \in Z$. إذا كان $c \cdot a \equiv c \cdot b \pmod{m}$

وإذا كان $d(c,m) = d$ و كان $m = d \cdot n$ ، فـبرهن أن :

$$a \equiv b \pmod{n}$$

الحـــل :بما أن $d = d(c,m)$ فإن :

$$m = d \cdot n \quad \wedge \quad c = d \cdot t \quad ; \quad t \in Z$$

وبما أن $c \cdot a \equiv c \cdot b \pmod{m}$ فإن يوجـد $k \in Z$ بحيث يكون :

$$c \cdot a - c \cdot b = k \cdot m$$

$$\Rightarrow \quad (d \cdot t) \cdot a - (d \cdot t) \cdot b = k \cdot (d \cdot n)$$

$$\Rightarrow \quad (d \cdot t) \cdot (a - b) = d \cdot k \cdot n$$

$$(d \neq 0) \quad \Rightarrow \quad t \cdot (a - b) = k \cdot n$$

وهذا يبين أن n يقسم الجداء $t \cdot (a - b)$

وحسب تعريف القاسم المشترك الأكبر فإن t,n أوليان فيما بينهما وبالتالي

n يقسم $(a - b)$ وبالتالي :

$$a \equiv b \pmod{n}$$

التمرين الثاني :

بفرض أن $a,b,c \in Z^*$. برهن أن :

1. $d(a,b) = 1 \quad \wedge \quad d(a,c) = 1 \quad \Rightarrow \quad d(a,b,c) = 1$
2. $a | (b \cdot c) \quad \wedge \quad d(a,b) = 1 \quad \Rightarrow \quad a | c$

الحـــل :

$$1.\quad d(a,b)=1 \quad\Rightarrow\quad \exists \alpha_1,\beta_1\in Z \quad : \quad \alpha_1\cdot a+\beta_1\cdot b=1$$

$$d(a,c)=1 \quad\Rightarrow\quad \exists \alpha_2,\beta_2\in Z \quad : \quad \alpha_2\cdot a+\beta_2\cdot c=1$$

ومنه :

$$(\alpha_1\cdot a+\beta_1\cdot b)\cdot(\alpha_2\cdot a+\beta_2\cdot c)=1$$

$$\Rightarrow (\alpha_1\cdot a\cdot\alpha_2+\alpha_1\cdot c\cdot\beta_2+\alpha_2\cdot b\cdot\beta_1)\cdot a+(\beta_1\cdot\beta_2)\cdot(b\cdot c)=1$$

بفرض أن :

$$\alpha_1\cdot a\cdot\alpha_2+\alpha_1\cdot c\cdot\beta_2+\alpha_2\cdot b\cdot\beta_1=\alpha \quad , \quad \beta_1\cdot\beta_2=\beta$$

يكون :

$$\alpha\cdot a+\beta\cdot(b\cdot c)=1 \quad ; \quad \alpha,\beta\in Z$$

إذاً :

$$d(a,b,c)=1$$

$$2.\quad d(a,b)=1 \quad\Rightarrow\quad \exists \alpha,\beta\in Z \quad : \quad \alpha\cdot a+\beta\cdot b=1$$

وبالتالي :

$$(\alpha\cdot a+\beta\cdot b)\cdot c=1\cdot c$$

$$\Rightarrow \quad (\alpha\cdot c)\cdot a+\beta\cdot(b\cdot c)=c \qquad (*)$$

لكن $a|(b\cdot c)$ وبالتـــالي a يقســـم الطرف الأيســـر من العلاقـــة (*)

وبالتالي a يقسم الطرف الأيمن للعلاقة (*) .

إذاً : $a|c$.

التمرين الثالث :

ليكن $n,m\in Z^*$ وليكن $d(n,m)=1$ و ليكن $x_1,x_2\in Z$ برهـــن أنه يوجـــد $x\in Z$ بحيث يكون :

$$x \equiv x_1 \pmod{n} \quad \wedge \quad x \equiv x_2 \pmod{m}$$

الحـــل :

$$d(n,m)=1 \quad \Rightarrow \quad \exists \alpha, \beta \in Z \quad : \quad \alpha \cdot n + \beta \cdot m = 1$$

ولنأخـــذ العـــدد الصحيـــح $x = x_2 \cdot \alpha \cdot n + x_1 \cdot \beta \cdot m$ فنجـــد أن :

$$\begin{aligned} x - x_1 &= x_2 \cdot \alpha \cdot n + x_1 \cdot (\beta \cdot m - 1) \\ &= x_2 \cdot \alpha \cdot n + x_1 \cdot (-\alpha \cdot n) \\ &= (x_2 \cdot \alpha - x_1 \cdot \alpha) \cdot n \end{aligned}$$

و هـــذا ما يبين أن $x \equiv x_1 (\bmod n)$

وبطريقة مماثلة يُبرهن ن $x \equiv x_2 (\bmod m)$.

تمرينات (٤)

التمرين الأول :

ليكن $[a,b],[c,d],[e,f] \in Z$, $[0,0] \neq [\alpha,\beta] \in Z$.

برهـــن صحـــة القضايا الآتيـــة :

1. $\begin{cases} [a,b]+[c,d]=[c,d]+[a,b] \\ [a,b]\cdot[c,d]=[c,d]\cdot[a,b] \end{cases}$

2. $\begin{cases} ([a,b]+[c,d])+[e,f]=[a,b]+([c,d]+[e,f]) \\ ([a,b]\cdot[c,d])\cdot[e,f]=[a,b]\cdot([c,d]\cdot[e,f]) \end{cases}$

3. $\begin{cases} [a,b]\cdot([c,d]+[e,f])=[a,b]\cdot[c,d]+[a,b]\cdot[e,f] \\ ([c,d]+[e,f])\cdot[a,b]=[c,d]\cdot[a,b]+[e,f]\cdot[a,b] \end{cases}$

4. $\forall [x,y]\in Z:[x,y]+[0,0]=[0,0]+[x,y]=[x,y]$

5. $\forall [x,y] \in Z : [x,y]\cdot[1,0]=[1,0]\cdot[x,y]=[x,y]$

6. $\forall [x,y] \in Z : [x,y]+[y,x]=[y,x]+[x,y]=[0,0]$

التمرين الثاني :

أوجد القاسم المشترك الأكبر d لكل زوج (a,b) من الأزواج في الأعداد الصحيحة الآتية ، وعيّن عددين $\alpha,\beta \in Z$ بحيث : $d=\alpha\cdot a+\beta\cdot b$

1). $a=1137$; $b=419$

2). $a=5313$; $b=2047$

3). $a=60809$; $b=58483$

التمرين الثالث : ليكن $n \in N$. أثبت صحـــة التكافـــؤ :

$n-2 \notin 5Z \Leftrightarrow$ (العددان $2n+1$, n^3+n أوليان فيما بينهما)

التمرين الرابع :

برهن أن أي عدد صحيح $z \in Z-\{0,\pm 1\}$ يتحلل إلى جـــداء أعداد غير قابلة للتحليل ، وهـــذا التحليل وحيد بغض النظر عن تـــرتيب المضاريب وعن المضروبين ± 1 .

الفصل الخامس

نظرية الزمر

٥ – ١ مقدمـــة :

إذا كان $(+),(\cdot)$ قانوني تشكيل داخليين معرفين على مجموعة غير خالية G فإن كلاً من $(G,+)$ ، $(G,\cdot)$ ، $(G,+,\cdot)$ بنية جبريـــة .

نسمي قانون التشكيل الداخلي $(+)$ بالجمـــع فإذا كان a,b عنصرين من المجموعـــة G فإن تشكيل العنصرين a,b وفق $(+)$ هو $a+b$ وندعوه بمجموع العنصرين a,b .

كما نسمي قانون التشكيل الداخـــلي $(\cdot)$ بالضرب فإذا كان a,b عنصرين من المجموعة G فإن تشكيل العنصرين a,b وفق $(\cdot)$ هو $a\cdot b$ وندعوه بجـــداء العنصرين a,b .

سنستخدم في هذا الفصل – في كثير من الأحيان – قانـــون الضرب

٥ – ٢ تعريفات :

تعريف (١) : نقول عن البنية $(G,\cdot)$ إنها نصف زمـــرة إذا كان الضرب المعرف على G تجميعياً . أي أن :

$$\forall a,b,c \in G : a\cdot(b\cdot c) = (a\cdot b)\cdot c$$

ونقول عن نصف الزمـــرة $(G,\cdot)$ أنهـــا تبديلية إذا كان قانـــون الضرب المعرف على G تبديلياً . أي أن : $\forall a,b \in G : a\cdot b = b\cdot a$

ونقول عن نصف الزمـــرة $(G,\cdot)$ أنها واحـــدية إذا وجـــد في G عنصر محايد بالنسبة لقانون الضرب المعرف على G (نرمز له بـــ e) أي أن :

$$\forall a \in G : a \cdot e = e \cdot a = a$$

تعريف (٢) :نقول عن البنية $(G,\cdot)$ إنها زمـــرة ، إذا وفقط إذا ، تحققت الشروط الآتية :

(١). قانون الضرب المعرف على G تجميعياً أي أن :

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

(٢). يوجـــد في G عنصر محايـــد بالنسبة لقانـــون الضـــرب (نرمز له بـــ e) أي أن :

$$\forall a \in G : \quad a \cdot e = e \cdot a = a$$

(٣). أياً كان العنصر $a \in G$ فإنـــه يوجـــد في G مقلوب لـــ a بالنسبة للقانون $(\cdot)$ نرمز له بـــ a^{-1} . أي أن :

$$\forall a \in G : \quad a \cdot a^{-1} = a^{-1} \cdot a = e$$

بعبارة مكافئة :

$(G,\cdot)$ زمـــرة عندما وفقط عندما يتحقق الشرطان التاليان :

I . $(G,\cdot)$ نصف زمـــرة واحـــدية .

II . لكل عنصر من G مقلوب في G بالنسبة لـــ $(\cdot)$.

ونقول عن الزمـــرة $(G,\cdot)$ إنها تبديلية إذا كان قانون الضرب تبديلياً .

ونقول عن الزمـــرة $(G,\cdot)$ إنها منتهية إذا كانت المجموعة G منتهية. أما إذا كانت المجموعة G غير منتهية فإننا نقول عن الزمـــرة $(G,\cdot)$ إنها غير منتهية

تعريف (٣):

نعرف مرتبة الزمرة $(G,\cdot)$ بأنه $cardG$ ونرمز له بالرمز $(G:1)$ أي :

$$(G:1) = cardG$$

تعريف (٤):

لتكن $(G,\cdot)$ زمرة ما ولتكن $\phi \neq H \subseteq G$. نقول عن H إنها زمرة جزئية من الزمرة G إذا كانت $(H,\cdot)$ زمرة بالنسبة لقانون الضرب المعرفة على G .

مبرهنة :

إذا كانت $(G,\cdot)$ زمرة ما وكانت $\phi \neq H \subseteq G$ فإن القضايا الثلاث الآتية متكافئة :

١. H زمرة جزئية .

٢. $\forall a,b \in H: \quad (a \cdot b \in H) \wedge (a^{-1} \in H)$

٣. $\forall a,b \in H: \quad a \cdot b^{-1} \in H$

الإثبـــات : يترك كتمرين لسهولته .

أمثـــلة :

(١) الزمـــرة العـــددية :

١. إن كلاً من C,R,Q,Z المزودة بعملية الجمع المألوفة على الأعداد زمرة غير منتهية . المحايد في كلٍ منها $e=0$ ونظير أي عنصر x هـــو $x' = -x$.

٢. إن كلاً من C^*,R^*,Q^* المزودة بعملية الضرب المألوفة على

الأعداد . زمرة تبديلية غير منتهية . المحايد في كلٍ منها $e=1$ ومقلوب أي عنصر x هـــو x^{-1} .

٣. إن المجموعة $H=\{1,-1\}$ زمرة جزئية منتهية (وبالتالي زمرة منتهية) من الزمرة $(R^*,\cdot)$. كما أن المجموعة $H=(i,-1,-i,1\}$ زمرة جزئية منتهية $((H:1)=4)$ من الزمرة $(C^*,\cdot)$ (حيث $i^2=-1$) .

(٢) الزمـــرة R^n :

لتكن R مجموعة الأعداد الحقيقية ، وليكن n عدداً صحيحاً موجباً. نعرف على الجـــداء الديكارتي $R^n=R\times R\times\ldots\times R$ قانـــون التشكيل الداخلي + كما يلي :

$$\forall(a_1,a_2,\ldots,a_n),(b_1,b_2,\ldots,b_n)\in R^n:$$

$$(a_1,a_2,\ldots a_n)+(b_1,b_2,\ldots,b_n)=(a_1+b_1,a_2+b_2,\ldots,a_n+b_n)$$

فنجـــد أن $(R^n,+)$ زمـــرة تبديلية غـــير منتهية ، المحايـــد فيها هـــو $e=(0,0,\ldots,0)$ ونظير العنصر $(a_1,a_2,\ldots,a_n)$ هـــو العنصر :

$$-(a_1,a_2,\ldots,a_n)=(-a_1,-a_2,\ldots,-a_n)$$

(٣) زمـــرة صفوف التكافـــؤ بالمقاس n (Z/nZ) :

١- ليكن Z مجموعة الأعداد الصحيحة ، وليكن n عـــدداً صحيحاً موجباً . نعلم أن مجموعة صفوف التكافؤ في المجموعة Z بالمقاس n هي المجموعـــة :

$$Z/nZ=\{[0],[1],\ldots,[n-1]\}$$

لنعرف على هذه المجموعة قانون التشكيل الداخلي + كما يلي :

$$\forall [a],[b] \in Z/nZ \quad : \quad [a]+[b]=[a+b]$$

فنجـــد أن $(Z/nZ,+)$ زمرة تبديلية منتهية . المحايـــد فيها هـــو العنصر $e=[0]$ ونظير العنصر $[a]$ هو العنصر $-[x]=[n-x]$ وأن $(Z/nZ:1)=card \quad Z/nZ=n$.

٢- ليكن P عدداً أولياً ولنعرف على المجموعة :

$$G=Z/pZ-\{[0]\}=\{[1],[2],...,[p-1]\}$$

قانون التشكيل الداخلي . كما يلي :

$$\forall [a],[b] \in G \quad : \quad [a]\cdot[b]=[a\cdot b]$$

فنجد أن $(G,\cdot)$ زمرة تبديلية منتهية . المحايد فيها هو $e=[1]$ ومقلوب العنصر $[a]$ هـــو العنصر $[x]\in G$ بحيث $[x]\cdot[a]=[1]$ و أن :

$$(Z/pZ:1)=card(Z/pZ)=P-1$$

ملاحظة :

إن العلاقة $[x]\cdot[a]=[1]$ تكافئ العلاقة $x\cdot a=1(\bmod n)$ التي تعين لنا مقلوب العنصر $[a]$. فمثلاً من أجل $p=5$ يكون :

$$Z/5Z-\{[0]\}=\{[1],[2],[3],[4]\}$$

وإن :

$$[1]^{-1}=[1] \quad , \quad [2]^{-1}=[3] \quad , \quad [3]^{-1}=[2] \quad , \quad [4]^{-1}=[4]$$

(٤) الزمـــرة Z_n :

١- ليكن n عدداً صحيحاً موجباً . ولنعرف على المجموعة :

$Z_n=\{0,1,2,...,n-1\}$ قانون التشكيل الداخلي + كما يلي :

$$\forall\, a,b \in Z_n \;:\; a+b=\begin{cases} a+b & ; \quad (a+b<n) \\ a+b-n & ; \quad (a+b\geq n) \end{cases}$$

فنجد أن $(Z_n,+)$ زمرة تبديلية منتهية . المحايد فيها هو $e=0$

ونظير العنصر $x \in Z_n$ هو العنصر $-x = n - x$ كما أن :

$$(Z_n : 1) = card \quad Z_n = n$$

٢- ليكن p عدداً أولياً . ولنعرف على المجموعة :

$$Z_p - \{0\} = \{1,2,\ldots,P-1\}$$

قانون التشكيل الداخلي $\bullet$ كما يلي :

$$\forall a,b \in Z_p - \{0\} : a \cdot b = r \quad ; \quad r = x \cdot y - p \cdot q \quad ; \quad p,q \in Z \wedge 0 < r < p$$

فنجد أن $(Z_p - \{0\},\bullet)$ زمرة تبديلية منتهية ، المحايد فيها هو $e=1$

ومقلوب العنصر a هو العنصر $x \in Z_p - \{0\}$ بحيث يكون :

$$x \cdot a = 1 \quad (\mathrm{mod}\, n)$$

فمثلاً من أجل $p=5$ يكون :

$$Z_7 - \{0\} = \{1,2,3,4\}$$

وإنّ :

$$1^{-1} = 1 \quad , \quad 2^{-1} = 3 \quad , \quad 3^{-1} = 2 \quad , \quad 4^{-1} = 4$$

(٥) زمـــرة المصفوفات :

وجدنا في الفصل الثاني أن الشكل النموذجي للمصفوفة من المرتبة $n \times m$ على حقل F هو :

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix}$$

والتي نكتبها بالشكل المختزل (a_{ij}) ورمزنا لمجموعة المصفوفات من

المـرتبة $n\times m$ على الحقل F بالرمـز $M_{n\times m}(F)$. لنعرّف على المجموعـة $M_{n\times m}(F)$ قانون التشكيل الداخلي + كما يلي :

$$\forall \quad A=(a_{ij}),B=(b_{ij})\in M_{n\times m}(F): A+B=(a_{ij}+b_{ij})$$

فمثلاً :

$$\begin{pmatrix}1&0&-1&3\\0&2&0&-1\\1&1&-1&0\end{pmatrix}+\begin{pmatrix}-1&1&1&-1\\2&-1&1&0\\0&0&-1&2\end{pmatrix}=\begin{pmatrix}0&1&0&2\\2&1&1&-1\\1&1&-2&2\end{pmatrix}$$

فنجد أن $(M_{n\times m}(F),+)$ زمرة تبديلية غير منتهية . المحايد فيها هـو العنصر $e=O_{n\times m}=(a_{ij});a_{ij}=0 \quad \forall i,j$

وأن نظير العنصر $A=(a_{ij})\in M_{n\times m}(F)$ هو العنصر :

$$-A=(-a_{ij})$$

ملاحظة :سندرس في مقرر الجبر (٢) عملية الضرب على المصفوفات وعندئذٍ سنتعرف على زمرة المصفوفات المربعة بالنسبة لعملية $\bullet$ (ضرب المصفوفات)

(٦). زمرة التباديل (الزمرة المتناظرة) S_n :

لتكن S_n مجموعة التباديل من الدرجة n (راجع الفصل الثاني – التطبيقات الخاصة) ولنعرف على S_n قانون التشكيل الداخلي $\bullet$ الذي هو عملية تركيب التطبيقات والذي سندعوه جداء التباديل فنجد أن $(S_n,\bullet)$ زمرة منتهية غير تبديلية . المحايد فيها هو العنصر :

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

ولكل عنصر $\tau\in S_n$ مقلوب τ^{-1} هو التطبيق العكسي لـــ τ وأن :

$$(S_3:1)=card\ S_n=n!$$

فمثلاً من أجل $n=3$ تكون :

$$S_n=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\right.$$
$$\left.\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}$$

وإذا كان

$$\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad,\quad\sigma=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

فإن :

$$\tau\cdot\sigma=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

وإن :

$$\tau^{-1}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^{-1}=\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$\sigma^{-1}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}^{-1}=\begin{pmatrix}1&3&2\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

كما وأن :

$$(S_3:1)=card\,S_3=3!=6$$

نقول عن التبديل $\tau\in S_n$ أنه دورة من المرتبة m $(2\le m)$ إذا وفقط إذا وجدت مجموعة :

$$A=\{i_1,i_2,\dots,i_m\}\subseteq\{1,2,\dots,n\}$$

عناصرها مختلفة مثنى مثنى $(cardA=m)$ بحيث يتحقق :

1. $\forall j \in \{1,2,\ldots,n\} - \{i_1, i_2, \ldots, n\} : \tau(j) = j$
2. $\forall k \in \{1,2,\ldots,m-1\} : \tau(i_p) = i_{p+1}$
3. $\tau(i_m) = i_1$

ونرمز لهذا التبديل (الدورة) بالرمز $(i_1, i_2, \ldots, i_m)$.

إذا كانت الدورة $\tau \in S_n$ من المرتبة ٢ فندعوها مناقلة .

وإذا كانت :

$$(i_1, i_2, \ldots, i_m) \quad , \quad (j_1, j_2, \ldots, j_k)$$

دورتين . نقول عنهما إنهما مستقلتان إذا كان :

$$\{i_1, i_2, \ldots, i_m\} \cap \{j_1, j_2, \ldots, j_k\} = \phi$$

فمثلاً :

التبديل :

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ 2 & 3 & \ldots & 1 \end{pmatrix} = (1 \quad 2 \quad \ldots \quad n) \in S_n$$

دورة من المرتبة n .

أمـــا التبديل :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (2 \quad 3) \in S_4$$

مناقلة .

ملاحظة : كل تبديل يساوي جـــداء عـــدد منته من الدورات المستقلة مثنى مثنى (بغض النظر عن ترتيب هذه المضاريب).

فمثلاً : التبديل :

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \end{pmatrix} \in S_8$$

يساوي جـــداء الدورتين :

$$(1\ \ 3\ \ 5\ \ 7)\cdot(2\ \ 4\ \ 6\ \ 8)$$

٥ ـ ٣ بعض خواص الزمـــرة :

بفرض $(G,\circ)$ زمـــرة ما ، فإن :

١. العنصر المحايد في G موجود ووحيد .

٢. لكل عنصر من G مقلوب وحيد في G .

٣. أياً كان $a,b \in G$ فإن :

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

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

٤. أياً كان $a \in G$ فإن :

$$\left(a^{-1}\right)^{-1} = a$$

٥. أياً كان $a_1, a_2, \ldots, a_n \in G$ فإن :

$$(a_1, a_2, \ldots, a_n)^{-1} = a_n^{-1}, \ldots, a_2^{-1}, a_1^{-1}$$

٦. أياً كان $a,b \in G$ فإن للمعادلة $a\cdot x = b$ حلاً وحيداً في G هو : $x = a^{-1}\cdot b$ كما أن للمعادلة $y\cdot a = b$ حلاً وحيداً في G هو $y = b\cdot a^{-1}$.

٧. إذا كانت $\{H_i \ ; \ i \in I\}$ أسرة منتهية من الزمرة الجزئية من الزمرة G فإن $\mathop{\mathrm{I}}\limits_{i\in I} H_i$ زمرة جزئية من الزمرة G .

٨. إذا كان e المحايـــد في الزمـــرة G فإن $\{e\}$ زمـــرة جزئية من الزمرة G .

٥ – ٤ القوى ذات الأسس الصحيحة في الزمرة :

تعريف : ليكن a عنصراً من الزمرة $(G,\bullet)$ المحايد فيها e وليكن n عدداً صحيحاً . نعرف القوة a^n بأنه عنصر من G معرف كما يلي :

$$a^n = \begin{cases} e & ; \quad (n=0) \\ a\,.\,a\,.\mathrm{K}\,.\,a = a^n & ; \quad (n=0) \\ a^{-1}.a^{-1}.....a^{-1} = (a^{-1})^{-n} & ; \quad (n<0) \end{cases}$$

ملاحظة :يؤول مفهوم القوى في الزمرة $(G,\bullet)$ إلى مفهوم المضاعف في الزمرة الجمعية $(G,+)$. فـــإذا كان a عنصراً من الزمرة الجمعية $(G,+)$ وإذا كان n عدداً صحيحاً فإننا نعرف المضاعف $n.a$ بأنه عنصر من الزمرة G معرف كما يلي :

$$n.a = \begin{cases} e & ; \quad (\text{عندما } n=0) \\ a+a+...+a = n.a & ; \quad (\text{عندما } n>0) \\ (-a)+(-a)+...+(-a) = (-n).(-a) & ; \quad (\text{عندما } n<0) \end{cases}$$

نتيجة (١):

إذا كان a عنصراً من الزمرة $(G,\bullet)$ وإذا كان n عـــدداً صحيحاً موجباً فإن :

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

البرهان : حسب التعريف يكون :

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

ومنه :

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

نتيجة (٢):

إذا كان a,b عنصريـــن من زمـــرة $(G,\circ)$ بحيث $a \cdot b = b \cdot a$

وإذا كان n عـــدداً صحيحاً فإن :

$$(a \cdot b)^n = a^n \cdot b^n$$

البرهان : من أجل $n = 0$ يكون :

$$(a.b)^n = (a.b)^0 = e = e \cdot e = a^0 \cdot b^0 = a^n \cdot b^n$$

من أجل $n > 0$ يكون :

$$(a.b)^n = (a \cdot b) \cdot (a \cdot b) \cdot \ldots (a \cdot b) = (a \cdot a \cdot \ldots \cdot a) \cdot (b \cdot b \cdot \ldots \cdot b) = a^n \cdot b^n$$

من أجل $n < 0$ يكون :

$$(a.b)^n = \left[(a.b)^{-1}\right]^{-n} = \left[(b.a)^{-1}\right]^{-n} = (a^{-1}.b^{-1})^{-n}$$
$$= (a^{-1})^{-n} \cdot (b^{-1})^{-n} = a^n \cdot b^n$$

مبرهنة : إذا كان a عنصراً من زمرة $(G,\circ)$ وكان e المحايد في G وإذا كان $n,m \in Z$ فإن :

(1). $e^n = e$

(2). $a^n \cdot a^m = a^{n+m} = a^m \cdot a^n$

(3). $(a^n)^m = a^{n.m} = (a^m)^n$

الاثبات :

(١). من أجل $n = 0$ يكون $e^0 = e$ وبالتالي $e^n = e$.

من أجل $n > 0$ يكون : $e^n = e \cdot e \cdot \ldots \cdot e = e$

من أجل $n<0$ يكون :

$$e^n=(e^{-1})^{-n}=(e)^{-n}=e$$

إذاً أياً كان $n\in Z$ فإن $e^n=e$

(٢). • أولاً : إذا كان $n=0$ وأياً كان $m\in Z$ فإن :

$$a^n\cdot a^m=a^0\cdot a^m=e\cdot a^m=a^m=a^{0+m}=a^{n+m}$$

• ثانياً : إذا كان $m=0$ وأياً كان $n\in Z$ فإن :

$$a^n\cdot a^m=a^n\cdot a^0=a^n\cdot e=a^n=a^{n+0}=a^{n+m}$$

• ثالثاً : إذا كان $(m\neq 0)\wedge(n\neq 0)$ فإننا نكون أمام الحالات الآتية:

(أ) $(n>0)\wedge(m>0)$

(ب) $(n<0)\wedge(m<0)$

(جـ) $(n>0)\wedge(m<0)$

(د) $(n<0)\wedge(m>0)$

الحالة (أ) : إذا كان $(n>0)\wedge(m>0)$ فإن :

$$a^n\cdot a^m=(\underbrace{a\cdot a\cdots a}_{n})\cdot(\underbrace{a\cdot a\cdots a}_{m})=(\underbrace{a\cdot a\cdots a}_{n+m})=a^{n+m}$$

الحالة (ب) : إذا كان $(n<0)\wedge(m<0)$ فإنه يوجد $t,r\in Z^+$ بحيث

$$m=-t\wedge n=-r\quad;\quad r+t=-(n+m)$$

وبالتالي يكون :

$$a^n\cdot a^m=a^{-r}\cdot a^{-t}=(a^{-1})^r\cdot(a^{-1})^t=(a^{-1})^{r+t}$$
$$=(a^{-1})^{-(n+t)}=a^{n+m}$$

الحالة (جـ) : إذا كان $(n>0)\wedge(m<0)$ فإنه يوجد $t\in Z^+$ بحيث $m=-t$ وهنا نميز الحالات الآتية :

(*) إذا كان $n > t$ فإنه يوجد $s \in Z^+$ بحيث $n = s + t$ وبالتالي يكون

$$a^n \cdot a^m = a^{s+t} \cdot a^{-t} = (a^s \cdot a^t) \cdot (a^{-1})^t = a^s \cdot [a^t \cdot (a^{-1})^t]$$
$$= a^s \cdot (a^{-1}.a)^t = a^s \cdot e^t = a^s = a^{n-t} = a^{n+m}$$

(**) إذا كان $n < t$ فإنه يوجد $r \in Z^+$ بحيث $t = n + r$ وبالتالي يكون

$$a^n \cdot a^m = a^n \cdot a^{-t} = a^n \cdot a^{-(n+r)} = a^n \cdot (a^{-1})^{n+r}$$
$$= a^n \cdot [(a^{-1})^n \cdot (a^{-1})^r] = [a^n \cdot (a^{-1})^n] \cdot (a^{-1})^r$$
$$= (a.a^{-1})^n \cdot a^{-r} = e^n \cdot a^{-r} = e \cdot a^{-r}$$
$$= a^{-t} = a^{n-t} = a^{n+m}$$

(***) إذا كان $n = t$ فإن :

$$a^n \cdot a^m = a^n \cdot a^{-t} = a^n \cdot (a^{-1})^t = a^n \cdot (a^{-1})^n$$
$$= (a.a^{-1})^n = e^n = e = a^0 = a^{n-t} = a^{n+m}$$

الحالة (د) : إذا كان $(n < 0) \wedge (m > 0)$ فأسلوب مشابه للحالة (جـ)

نجد أن :

$$a^n \cdot a^m = a^{n+m}$$

إذاً :

$$\forall n, m \in Z, \forall a \in G : a^n \cdot a^m = a^{n+m} = a^{m+n} = a^m \cdot a^n$$

(٣) • أولاً : إذا كان $n = 0$ وأياً كان $m \in Z$ فإن :

$$(a^n)^m = (a^0)^m = e^m = e = a^0 = a^{0 \cdot m} = a^{n \cdot m}$$

• ثانياً : إذا كان $m = 0$ وأياً كان $n \in Z$ فإن :

$$(a^n)^m = (a^n)^0 = a^0 = a^{n.0} = a^{n \cdot m}$$

• ثالثاً : إذا كان $(m \neq 0) \wedge (n \neq 0)$ فإننا نكون أمام الحالات الآتية :

(أ) $(n > 0) \wedge (m > 0)$

(ب) $(n < 0) \wedge (m < 0)$

(جـ) $(n > 0) \wedge (m < 0)$

(د) $(n < 0) \wedge (m > 0)$

الحالة (أ): إذا كان $(n > 0) \wedge (m > 0)$ فإن :

$$(a^n)^m = \underbrace{a^n \cdot a^n \cdot \ldots \cdot a^n}_{m} = (a \cdot a \cdot \ldots \cdot a) \cdot \ldots \cdot (a \cdot a \cdot \ldots \cdot a) = a^{n.m}$$

الحالة (ب): إذا كان $(n < 0) \wedge (m < 0)$ فإنه يوجد $t, r \in Z^+$ بحيث :

$$m = -t \wedge n = -r \quad : \quad r \cdot t = n \cdot m$$

وبالتالي يكون :

$$(a^n)^m = (a^{-r})^{-t} = [(a^{-r})^{-1}]^t = [((a^{-1})^{-1})^r]^t = (a^r)^t$$

$$= a^{r.t} = a^{n.m}$$

الحالة (جـ): إذا كان $(n > 0) \wedge (m < 0)$ فإنه يوجد $t \in Z^+$ بحيث

$m = -t$ وبالتالي يكون :

$$(a^n)^m = (a^n)^{-t} = [(a^n)^{-1}]^t = [(a^{-1})^n]^t = (a^{-1})^{n.t}$$

$$= a^{-(n.t)} = a^{n.(-t)} = a^{n.m}$$

الحالة (د): إذا كان $(n < 0) \wedge (m > 0)$ فإنه يوجد $r \in Z^+$ بحيث

$n = -r$ وبالتالي يكون :

$$(a^n)^m = (a^{-r})^m = [(a^{-1})^r]^m = (a^{-1})^{r.m} = a^{-(r.m)}$$

$$= a^{(-r).m} = a^{n.m}$$

إذاً :

$$\forall n,m \in Z, \forall a \in G : (a^n)^m = a^{n.m} = a^{m.n} = (a^m)^n$$

ملاحظة :إذا اعتمدنا الزمرة الجمعية $(G,+)$ فإن نص المبرهنة السابقة يصبح:

إذا كان a عنصراً من الزمرة $(G,+)$ وكان e المحايد في G وإذا كان $n,m \in Z$ فإن :

1. $n \cdot e = e$
2. $(n \cdot a) + (m \cdot a) = (n+m) \cdot a = (m \cdot a) + (n \cdot a)$
3. $n \cdot (m \cdot a) = (n \cdot m) \cdot a = m \cdot (n \cdot a)$

٥ ـ ٥ مرتبة عنصر في زمـــرة :

تعريف(١) : ليكن a عنصراً من زمرة $(G,\circ)$ المحايد فيها e . نقول عن العنصر a أنه ذو مرتبة محدودة في الزمرة G إذا وفقط إذا وجد عدد صحيح موجب مثل k من أجله $a^k = e$.

نسمي أصغر عـــدد صحيـــح مـــوجب n الذي من أجله يكون $a^n = e$ بمرتبـــة العنصر a في الزمـــرة G ونـــرمز لذلك بالـــرمز $O(a) = n$

وإذا كان a ذا مرتبـــة مـــحدودة فنعبر عن ذلك بالـــرمز $O(a) < \infty$

تعريف(٢) :ليكن b عنصراً من الزمرة $(G,\circ)$ المحايد فيها e . نقول عن العنصر b أنه ذو مرتبة غير محـــدودة في الزمـــرة G ونكتب $O(b) = \infty$ إذا كان $b^m \neq e$ لأجل أي عـــدد صحيـــح موجب m

بعبارة أخرى :

$O(b) = \infty \Leftrightarrow$ القوة الوحيدة للعنصر b التي تساوي e في الزمرة G هـــي b^0 .

أمثلة:

١. في الزمرة $(R^*,\circ)$ العنصر (2) ذو مرتبة غير محدودة ، بينما العنصر (-1) يكون ذا مرتبة محدودة في هذه الزمرة ويكون $O(-1)=2$.

٢. في الزمرة $(S_3,\circ)$ العنصر $a=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ ذو مرتبة محدودة وأن $O(a)=3$.

نتيجة : ليكن a عنصراً من زمرة $(G,\circ)$ وليكن $O(a)=n$ و إذا كان m عدداً صحيحاً موجباً من أجله $a^m=e$ فإن $n|m$.

البرهان : من أجل العددين الصحيحين n,m يوجد $q,r\in Z$ بحيث يكون :

$$m=q\cdot n+r \quad ; \quad 0\le r<n$$

ومنه :

$$e=a^m=a^{q.n+r}=(a^n)^q\cdot a^r=e^q\cdot a^r=e\cdot a^r=a^r$$

إن $r=0$ لأنه في الحالة المعاكسة يكون :

$$a^r=e \quad ; \quad r\in Z \quad \wedge \quad 0<r<n$$

وهذا يخالف كون $O(a)=n$.

إذن :

$m=q\cdot n$ أي n يقسم m وبالتالي $n|m$.

٥ – ٦ المرافقات اليسارية والمرافقات اليمينية لزمرة جزئية :

تعريف(١) : لتكن H زمرة جزئية من زمرة $(G,\circ)$ ، وليكن $x\in G$.

نعرف المرافقة اليسارية لـ H في G المعينة بالعنصر x .ونرمز لها بـ Hx بأنها المجموعة : $Hx=\{h\cdot x \quad ; \quad h\in H\}$

كما نعرف المرافقة اليمينية لـ H في G المعينة بالعنصر x . ونرمز لها بـ xH بأنها المجموعة :

$$xH = \{x \cdot h \quad ; \quad h \in H\}$$

نتائج :

إذا كانت H زمرة جزئية من زمرة $(G,\circ)$ وكان $x \in G$ فإن :

١- $\phi \neq Hx \subseteq G \quad , \quad \phi \neq xH \subseteq G$

٢- H مرافقة يسارية ويمينية في آن واحد في G .

٣- إذا كان $x \in H$ فإن المرافقة اليسارية Hx (أو اليمينية xH لـ H) تكون زمرة جزئية في G .

٤- $cardH = card(xH) \quad , \quad cardH = card(Hx)$

البرهان :

١ - من جهة أولى ، واضح أن $Hx \subseteq G \quad \wedge \quad xH \subseteq G$

ومن جهة ثانية :

$$x = e \cdot x \in Hx \quad \wedge \quad x = x \cdot e \in xH$$

أي : $\phi \neq Hx \quad \wedge \quad \phi \neq xH$

إذن : $\phi \neq Hx \subseteq G \quad \wedge \quad \phi \neq xH \subseteq G$

٢ - إن $e \cdot H = H = H \cdot e$ وبالتالي H هي مرافقة يسارية ويمينية في آن واحد لنفسها في G معينة بالعنصر e .

٣- إذا كان $x \in H$ فإن :

$$Hx = H \cdot e = H$$
$$xH = e \cdot H = H$$

أي أن كلاً من Hx , xH تتطابق مع H وبالتالي كلٌّ من Hx و xH هي زمرة جزئية من الزمرة G .

٤ – لنأخذ العلاقة :

$$\varphi : H \to Hx$$

المعرفة كما يلي :

$$\varphi(h) = h \cdot x \qquad \forall h \in H$$

فنجد أن φ تطبيق متباين لأن :

$$\forall h_1, h_2 \in H : \quad h_1 = h_2 \Leftrightarrow h_1 \cdot x = h_2 \cdot x \Leftrightarrow \varphi(h_1) = \varphi(h_2)$$

كما أن التطبيق φ غامر لأن :

$$\forall hx \in Hx : \quad \exists h \in H : \quad \varphi(h) = h \cdot x$$

إذاً φ تقابل وبالتالي $H \sim Hx$

أي : $cardH = card(Hx)$

وبالمثل يُبرهن أن :

$$cardH = card(xH)$$

مبرهنة (١):

إذا كانت H زمرة جزئية من زمرة G فإن أسرة المرافقات اليمينية لـ H في G تشكل تجزئة لـ G .

الاثبات : لتكن :

$$M_r = \{xH \quad ; \quad x \in G\}$$

أسرة المرافقات اليمينية لـ H في G . إن M_r تشكل تجزئة لـ G وذلك للأسباب الآتية :

١- أياً كان $xH \in M_r$ فإن $xH \neq \phi$ لأن :

$$x = x \cdot e \in xH$$

٢- أياً كان $xH, yH \in M_r$ فإنه إذا كان $xH \cap yH \neq \phi$ فإنه يوجد $a \in G$ بحيث : $a \in xH \cap yH$

$$\Rightarrow \quad a \in xH \quad \wedge \quad a \in yH$$

$$\Rightarrow \quad \exists h_1, h_2 \in H : \quad a = x \cdot h_1 \quad \wedge \quad a = y \cdot h_2$$

$$\Rightarrow \quad x \cdot h_1 = y \cdot h_2$$

$$\Rightarrow \quad x = y \cdot h_2 \cdot h_1^{-1} \quad \wedge \quad y = x \cdot h_1 \cdot h_2^{-1}$$

ليكن الآن $b \in xH$ عندها يوجد $h \in H$ بحيث يكون $b = x \cdot h$

وبالتالي : $b = (y \cdot h_2 \cdot h_1^{-1}) \cdot h$

أي : $b = y \cdot (h_2 \cdot h_1^{-1} \cdot h)$

ومنه $b \in yH$

إذاً : $xH \subseteq yH$

وبطريقة مشابهة نبرهن $yH \subseteq xH$.

وبالتالي يكون : $xH = yH$.

٣- $G = \bigcup_{x \in G} xH$

مبرهنة (٢):

إذا كانت H زمرة جزئية من زمرة G فإن أسرة المرافقات اليسارية لـ H في G تشكل تجزئة لـ G .

الإثبات : يتم بطريقة مماثلة لإثبات المبرهنة (١) .

تعريف(٢): لتكن H زمرة جزئية من زمرة $(G,\bullet)$. نعرف دليل الزمرة الجزئية H في الزمرة G ونرمز له بـــ $(G:H)$ بأنه قدرة الأسرة M_r

أي : $(G:H) = card\, M_r$

مبرهنة (٣):

إذا كانت $(G,\bullet)$ زمرة منتهية وكانت H زمرة جزئية من G فإن

$$(G:1) = (G:H)\cdot(H:1)$$

الإثبات : لتكن $(G,\bullet)$ زمرة منتهية وليكن $(G:1) = cardG = n$. عندئذٍ M_r تكون منتهية وليكن $(G:H) = card\, M_r = k$. بما أن M_r تشكل تجزئة لـــ G فإن :

$$G = \mathop{\mathrm{Y}}_{i=1}^{k} x_i H \quad ; \quad x_i \in G$$

وبالتالي :

$$cardG = card(\mathop{\mathrm{Y}}_{i=1}^{k} x_i H)$$

لكن :

$$card\, x_i H = cardH \qquad \forall x_i \in G$$

وبالتالي يكون :

$$cardG = k\cdot cardH$$

أي أن :

$$(G:1) = (G:H)\cdot(H:1)$$

نتيجة : إذا كانت H زمـــرة جزئية من زمـــرة منتهية G وكان :

$$(G:1) = cardG = n \quad , \quad (H:1) = cardH = m$$

فإن m يقسم n .

تعريف(٣): لتكن $(G,\bullet)$ زمرة ما . نقول عن الزمرة الجزئية H من G إنها ناظميّة في G إذا تحقق الشرط :

$$\forall x \in G \quad : \quad xH = Hx \qquad (*)$$

وإذا كانت H زمرة جزئية ناظمية في زمرة G .

فإننا نعبّر عن ذلك بالرمز $H < G$.

ملاحظة (١) : كل زمرة جزئية من زمرة تبديلية تكون ناظميّة .

ملاحظة (٢) : إن الشرط (*) يكافئ الشرط :

$$\forall a \in G, \forall h \in H : a \cdot h \cdot a^{-1} \in H$$

٥ – ٧ زمرة خارج القسمة :

لتكن $(G,\bullet)$ زمرة ما ولتكن H زمرة جزئية ناظميّة في G ولنأخذ المجموعة : $G/H = \{xH \quad ; \quad x \in G\}$

إن $G/H \neq \phi$ لأن :

$$H = e \cdot H \in G/H$$

لاحظ أن : $G/H = M_r = M_\lambda$ لأن $H < G$

نعرف على المجموعة غير الخالية G/H قانون التشكيل الداخلي $(\bullet)$ كما يلي :

$$\forall aH, bH \in G/H \quad : \quad (aH)\cdot(bH) = (a \cdot b)H$$

فنجد أن البنية $(G/H,\bullet)$ زمرة – تأكد من ذلك – المحايد فيها هو $H = eH$ (حيث e المحايد في الزمرة G) وأن مقلوب العنصر $xH \in G/H$ هو $x^{-1}H \in G/H$ تسمى هذه الزمرة بزمرة خارج القسمة الزمرة G على الزمرة الجزئية H .

ملاحظة (١):إذا كانت H زمرة جزئية من زمرة تبديلية فإن زمرة القسمة G/H تكون تبديلية .

ملاحظة (٢): بما أن $G/H = M_r$ فإن $(G/H:1) = card\, M_r$ ، لكن $(G:H) = card\, M_r$ وبالتالي $(G:H) = (G/H:1)$

وبذلك يمكن صياغة مبرهنة لاغرانج كما يلي :

إذا كانت H زمرة جزئية ناظمية في زمرة منتهية G فإن :

$$(G:1) = (G/H:1)\cdot(H:1)$$

٥ – ٨ الزمرة المولدة بمجموعة – الزمرة الدوارة :

تعريف(١):لتكن S مجموعة غير خالية من زمرة G . إن تقاطع كل الزمر الجزئية من الزمرة G والتي كل منها تحوي المجموعة S يكون زمرة جزئية من الزمرة G وتحوي S : نسميها الزمرة الجزئية المولدة بالمجموعة S ونرمز لها بالرمز $<S>$.

بعبارة مكافئة : الزمرة $<S>$ هي أصغر زمرة جزئية من الزمرة G ، تحوي S

تعريف(٢):إذا كانت S مجموعة جزئية منتهية غير خالية من زمرة G فإننا نقول عن الزمرة $<S>$ إنها زمرة منتهية التوليد .

ويبرهن على أنه إذا كانت $S = \{a_1, a_2, \dots, a_k\}$ مجموعة جزئية منتهية غير خالية من زمرة G فإن الزمرة المولدة بـــ S هي الزمرة :

$$<S> = \{x \in G : x = a_1^{n_1}\cdot a_2^{n_2}\cdot\ldots a_k^{n_k} \quad ; a_1, a_2, \dots, a_k \in S \quad ; \quad n_1, n_2, \dots, n_k \in Z \quad ; \quad k \in Z^+\}$$

وفي حالة خاصة إذا كانت $S = \{a\}$ مجموعة جزئية من زمرة G فإن الزمرة

المولدة بالمجموعة S ندعوها زمرة دوارة مولدة بالعنصر a ونرمز لها $<a>$

ويكون : $<a> = \{a^z \quad ; \quad z \in Z\}$

أمثلة :

١- إن الزمرة $(S_3,\circ)$ مولدة بالمجموعة $S=\{a,b\}$ حيث :

$$a=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} \quad ; \quad b=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

ويكون :

$$S_3 = <a,b> = \{e=a^3, a, a^2, b, a\cdot b, a^2.b\}$$

٢- إن الزمرة $G=\{i,-1,-i,1\}$ (بالنسبة لعملية الضرب المألوفة على الأعداد) . هي زمرة دوارة مولدة بالعنصر i ويكون :

$$G = <i> = \{i, i^2, i^3, i^4=1\}$$

مبرهنة :

إذا كان a عنصراً من زمرة $(G,\circ)$ وإذا كان $O(a)=n$ فإن :

$$<a> = \{a, a^2, \dots, a^{n-1}, a^n=e\}$$

الإثبات : أياً كان $a^z \in <a>$ (حيث $z \in Z$) فإنه من أجل العددين z,n يوجد $q,r \in Z$ بحيث يكون :

$$z = q\cdot n + r \quad ; \quad 0 \le r < n$$

ومنه :

$$a^z = a^{q.n+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = e \cdot a^r = a^r$$

فإذا كان $r=0$ فإن : $a^z = a^r = a^0 = e = a^n$

أما إذا كان $r \neq 0$ فإن :

$$a^z = a^r \quad ; \quad r \in \{1,2,\dots,n-1\}$$

ولكي يتم الإثبات يجب أن نثبت أن القوى : $a\ ,a^2,\dots,a^{n-1},a^n = e$ مختلفة مثنى مثنى .

لنفرض جدلاً أن $a^t = a^s$ حيث $1 \leq s < t \leq n$ وبالتالي :

$$a^{t-s} = e \quad \wedge \quad 0 < t-s < n$$

وهذا يناقض كون $O(a) = n$.

ملاحظة (١): إذا كان a عنصراً من زمـــرة G وكان $O(a) = \infty$ فإن الزمـــرة المولدة بالعنصر a تكون غير منتهية نرمّزها بـــ $< a >_\infty$ وهذه الزمـــرة تتألف من جميع قوى العنصر a ذات الأسس الصحيحة أي :

$$< a >_\infty = \{a^z \quad ; \quad z \in Z\}$$

نتيجة (١):

كل زمـــرة دوارة هـــي زمـــرة تبديليـــة .

البرهان : لتكن $< a >$ زمرة دوارة مولدة بالعنصر a . أياً كان $x, y \in < a >$ فإن :

$$x = a^{z_1} \quad , \quad y = a^{z_2} \quad ; \quad z_1, z_2 \in Z$$

وبالتالي يكون :

$$x \cdot y = a^{z_1} \cdot a^{z_2} = a^{z_1+z_2} = a^{z_2+z_1} = a^{z_2} \cdot a^{z_1} = y \cdot x$$

نتيجة (٢):

زمـــرة خارج القسمة لزمـــرة دوارة هـــي زمـــرة دوارة .

البرهان :

لتكن $G=<a>$ زمرة دوارة مولدة بالعنصر a ولتكن H زمرة جزئية من G فيكون $H<G$ لأن G تبديلية أياً كان $x\in G$ فإن $x=a^z; z\in Z$ وبالتالي أياً كان $xH\in G/H$ فإن :

$$xH=a^z\cdot H=(aH)^z \quad ; \quad z\in Z$$

أي أن الزمـــرة G/H مولدة بالعنصر aH .

٥ ـ ٩ التشاكلات الزمرية :

تعاريف : لتكن $(G,\circ)$ ، $(G',\circ)$ زمرتين ما . وليكن e المحايد في الزمـــرة G ، e' المحايد في الزمرة G' .

١ـ نعرف التشاكل الزمري بأنه كل تطبيق $f:G\to G'$ يحقق الشرط :

$$\forall a,b\in G: f(a\cdot b)=f(a)\cdot f(b) \qquad (*)$$

٢ـ نعرف التماثل الزمري بأنه كل تقابل $f:G\to G'$ ويحقق الشرط (*) وفي هـــذه الحالة نقول عن الزمرتين G ، G' إنهما متماثلتان ونكتب

$$G\cong G'$$

٣ـ إذا كان $f:G\to G'$ تشاكلاً زمرياً . نعرف نواة f ونرمز لها بالرمز $\ker f$ بأنها المجموعة :

$$\ker f=\{x\in G: f(x)=e'\}=\overleftarrow{f}(\{e'\})=\overleftarrow{f}(e')$$

مبرهنة : إذا كان $f:G\to G'$ تشاكلاً زمرياً وكان e المحايد في G ، e' المحايد في G' فإن :

١. $f(e)=e'$

٢. أياً كان $a\in G$ فإن : $f(a^{-1})=[f(a)]^{-1}$

٣. $\ker f$ زمرة جزئية ناظمية في G .

٤. إذا كانت H زمرة جزئية من الزمـــرة G فإن $\overleftarrow{f}(H)$ زمـــرة جزئية من الزمـــرة G' .

٥. إذا كانت K زمرة جزئية من الزمـــرة G' فإن $\overleftarrow{f}(K)$ زمـــرة جزئية من الزمـــرة G .

٦. $\operatorname{Im} f=\overrightarrow{f}(G)$ زمـــرة جزئية من الزمـــرة G' .

٧. f متبايـــن $\Leftrightarrow$ $\ker f=\{e\}$.

الإثبات :

١. إن :

$e\cdot e=e$ $\quad$ e المحايـــد في G .

$\Rightarrow f(e\cdot e)=f(e)$ $\quad$ f تطبيق .

$\Rightarrow f(e)\cdot f(e)=f(e)$ $\quad$ f تشاكل زمري .

$\Rightarrow f(e)\cdot f(e)=f(e)\cdot e'$ $\quad$ e' المحايـــد في G' .

$\Rightarrow f(e)=e'$ $\quad$ قانون الاختصار من اليسار في G'

٢. أياً كان $a\in G$ فإن :

$a\cdot a^{-1}=a^{-1}\cdot a=e$ $\quad$ تعريف المقلوب في G .

$\Rightarrow f(a\cdot a^{-1})=f(a^{-1}\cdot a)=f(e)$ $\quad$ f تطبيق .

$\Rightarrow f(a)\cdot f(a^{-1})=f(a^{-1})\cdot f(a)=e'$ $\quad$ f تشاكل زمري حسب (١) .

$\Rightarrow [f(a)]^{-1}=f(a^{-1})$ $\quad$ تعريف المقلوب في G' .

٣. لنثبت أولاً أن $\ker f$ زمرة جزئية من الزمرة G .

من جهة أولى :

$$\left.\begin{array}{l} f(e)=e' \text{ لأن } e\in \ker f \\ \ker f\subseteq G \text{ " تعريفاً " .} \end{array}\right\} \Rightarrow \phi\neq \ker f\subseteq G$$

من جهة ثانية : أياً كان $a,b\in \ker f$ فإن :

$f(a\cdot b^{-1})=f(a)\cdot f(b^{-1})$ $\quad$ f تشاكل زمري

$=f(a)\cdot[f(b)]^{-1}$ $\quad$ حسب (٢)

$=e'\cdot(e')^{-1}$ $\quad$ لأن $a,b\in \ker f$

$=e'$ $\quad$ e' المحايد في G' .

أي أن $a\cdot b^{-1}\in \ker f$

إذاً $\ker f$ زمرة جزئية من الزمرة G .

لنثبت أن الزمرة الجزئية $\ker f$ ناظمية في G . أياً كان $h\in \ker f$ و $a\in G$ فإن :

$f(a\cdot h\cdot a^{-1})=f(a)\cdot f(h)\cdot f(a^{-1})$ $\quad$ f تشاكل زمري .

$=f(a)\cdot e'\cdot[f(a)]^{-1}$ $\quad$ حسب (٢) $h\in \ker f$.

$=e'$ $\quad$ تعريف المقلوب في G' .

هذا يبين أن $a\cdot h\cdot a^{-1}\in \ker f$ أي أن $\ker f$ ناظمية في G .

٤. من جهة أولى :

$e\in H\subseteq G$ وبالتالي $f(e)\in \vec{f}(H)\subseteq G'$

أي أن $\phi\neq \vec{f}(H)\subseteq G'$

من جهة ثانية : أياً كان $y_1,y_2\in \vec{f}(H)$ فإنه يوجد $x_1,x_2\in H$ بحيث

$$y_1 = f(x_1) \quad \wedge \quad y_2 = f(x_2)$$

وبالتالي يكون :

$$y_1 \cdot y_2^{-1} = f(x_1) \cdot [f(x_2)]^{-1}$$

$= f(x_1) \cdot f(x_2^{-1})$ حسب (٢)

$= f(x_1 \cdot x_2^{-1})$ f تشاكل زمري .

وبما أن $x_1, x_2 \in H$ وأن H زمرة جزئية من G فإن $x_1 \cdot x_2^{-1} \in H$

وبالتالي $f(x_1 \cdot x_2^{-1}) \in \overrightarrow{f}(H)$ أي أن $y_1 \cdot y_2^{-1} \in \overrightarrow{f}(H)$.

إذاً $\overrightarrow{f}(H)$ زمرة جزئية من الزمرة G' .

٥. من جهة أولى : $f(e) = e' \in K \subseteq G'$

وبالتالي : $e \in \overleftarrow{f}(K) \subseteq G$

أي أن : $\phi \neq \overleftarrow{f}(K) \subseteq G$.

من جهة ثانية : أياً كان $x_1, x_2 \in \overleftarrow{f}(K)$ فإن $f(x_1), f(x_2) \in K$

وبالتالي يكون :

$f(x_1 \cdot x_2^{-1}) = f(x_1) \cdot f(x_2^{-1})$ f تشاكل زمري .

$= f(x_1) \cdot [f(x_2)]^{-1}$ حسب (٢)

وبما أن $f(x_1), f(x_2) \in K$ وأن K زمرة جزئية من G'

فإن $f(x_1) \cdot [f(x_2)]^{-1} \in K$

وبالتالي : $x_1 \cdot x_2^{-1} \in \overleftarrow{f}(K)$

إذاً $\overleftarrow{f}(K)$ زمرة جزئية من الزمرة G .

٦. بما أن G زمرة جزئية من نفسها فإنه حسب (٤) يكون $\operatorname{Im} f = \overrightarrow{f}(G)$ زمرة جزئية من الزمرة G' .

٧. $(\Leftarrow)$: نفرض أولاً أن f متباين ولنبرهن على أن $\ker f = \{e\}$

من الواضح أن :

$$\{e\} \subseteq \ker f \qquad (\mathrm{I})$$

من ناحية أخرى . أياً كان $a \in \ker f$ فإن :

$$f(a) = e' \qquad (\text{تعريف النواة})$$

$$= f(e) \qquad (\text{حسب } (1))$$

وبما أن f متباين فإن $a = e$ وبالتالي :

$$\ker f \subseteq \{e\} \qquad (\mathrm{II})$$

من (I) و (II) نجد أن $\ker f = \{e\}$

$(\Rightarrow)$: لنفرض الآن أن $\ker f = \{e\}$ ولنبرهن على أن f متباين .

لذلك نفرض أن :

$$f(x_1) = f(x_2) \quad ; \quad x_1, x_2 \in G$$

$$\Rightarrow f(x_1) \cdot [f(x_2)]^{-1} = e' \qquad (G' \text{ زمرة})$$

$$\Rightarrow f(x_1 \cdot x_2^{-1}) = e' \qquad (\text{حسب } (2) \text{ ، } f \text{ تشاكل زمري})$$

$$\Rightarrow x_1 \cdot x_2^{-1} \in \ker f \qquad (\text{تعريف النواة})$$

بما أن $\ker f = \{e\}$ فإن $x_1 \cdot x_2^{-1} = e$ ومنه $x_1 = x_2$. أي أن f متباين

مبرهنة :

إذا كان $f : G \to G'$ تشاكلاً زمرياً وكانت H زمـــرة جزئية من G K زمرة جزئية من G' فإن :

1. $H < G \Rightarrow \vec{f}(H) < \vec{f}(G)$
2. $K < G' \Rightarrow \overleftarrow{f}(K) < G$

الإثبات :

١. أيـاً كـان $y \in \vec{f}(H)$ وأيـاً كـان $b \in \vec{f}(G)$ فإنـه يوجد

$$a \in G \text{ و } x \in H$$

بحيث يكون :

$$y = f(x) \quad \wedge \quad b = f(a)$$

وبالتالي يكون :

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

وبما أن $H < G$ فإن $a \cdot x \cdot a^{-1} \in H$ وبالتالي $f(a \cdot x \cdot a^{-1}) \in \vec{f}(H)$

ومنه :

$$b \cdot y \cdot b^{-1} \in \vec{f}(H)$$

وهذا ما يثبت أن $\vec{f}(H) < \vec{f}(G)$.

٢. أياً كان $x \in \overleftarrow{f}(K)$ وأياً كان $a \in G$ فإن:

$$f(x) \in K \quad \wedge \quad f(a) \in G'$$

وبما أن $K < G$ فإن :

$$f(a) \cdot f(x) \cdot (f(a))^{-1} \in K$$

ومنه :

$$a \cdot x \cdot a^{-1} \in \overleftarrow{f}(K)$$

وهذا ما يثبت أن $\overleftarrow{f}(K) < G$

مبرهنة :

إذا كان $f : G \to G'$ تشـاكلاً زمـرياً فـإن : $G / \ker f \cong \operatorname{Im} f$

الإثبات : لنأخذ العلاقة :

$$\varphi : G/\ker f \to \operatorname{Im} f$$

المعرفة كما يلي :

$$\varphi(x \cdot \ker f) = f(x) \qquad \forall x \cdot \ker f \in G/\ker f$$

فنجد أن φ تطبيق متباين

لأنه أياً كان $x_1 \cdot \ker f, x_2 \cdot \ker f \in G/\ker f$ فإن :

$$\begin{aligned} x_1 \cdot \ker f = x_2 \cdot \ker f &\Leftrightarrow x_1 \cdot x_2^{-1} \in \ker f \\ &\Leftrightarrow f(x_1 \cdot x_2^{-1}) = e' \\ &\Leftrightarrow f(x_1) \cdot f(x_2^{-1}) = e' \\ &\Leftrightarrow f(x_1) \cdot (f(x_2))^{-1} = e' \\ &\Leftrightarrow f(x_1) = f(x_2) \\ &\Leftrightarrow \varphi(x_1 \cdot \ker f) = \varphi(x_2 \cdot \ker f) \end{aligned}$$

كما أن φ غامر لأنه أياً كان $y = f(x) \in \operatorname{Im} f$ فإنه يوجد $x \in G$

بحيث يكون $\varphi(x \cdot \ker f) = f(x)$.

كما أن φ تشاكل زمري لأنه أياً كان $x_1 \cdot \ker f, x_2 \cdot \ker f \in G/\ker f$

فإن :

$$\begin{aligned} \varphi(x_1 \cdot \ker f \cdot x_2 \cdot \ker f) &= \varphi[(x_1 \cdot x_2) \cdot \ker f] \\ &= f(x_1 \cdot x_2) \\ &= f(x_1) \cdot f(x_2) \\ &= \varphi(x_1 \cdot \ker f) \cdot \varphi(x_2 \cdot \ker f) \end{aligned}$$

مما سبق نجد أن φ تماثل زمري وبالتالي : $G/\ker f \cong \operatorname{Im} f$.

نتيجة :

في المبرهنة السابقة إذا كان f غامراً فإن $\operatorname{Im} f = G'$ وعندئـــذٍ يكون

$$G/\ker f \cong G'$$

مبرهنة : إذا كانت H,K زمرتين جزئيتين ناظميتين من زمرة G وكان $K \subseteq H$ فإن :

$$(G/K)/(H/K) \cong G/H$$

الإثبات : لنأخذ العلاقة

$$f : G/K \to G/H$$

المعرفة كما يلي :

$$f(x,K) = x \cdot H \qquad \forall x \cdot K \in G/K$$

فنجد أن العلاقة f تطبيق لأنه أياً كان $x_1 \cdot K, x_2 \cdot K \in G/K$ فإن :

$$\begin{aligned} x_1 \cdot K = x_2 \cdot K &\Rightarrow x_1 = x_2 \cdot k \quad ; \quad k \in K \\ &\Rightarrow x_1 = x_2 \cdot k \quad ; \quad k \in H \\ &\Rightarrow x_1 \cdot H = x_2 \cdot H \\ &\Rightarrow f(x_1 \cdot K) = f(x_2 \cdot K) \end{aligned}$$

كما أن f تشاكل زمري لأنه أياً كان $x_1 \cdot K, x_2 \cdot K \in G/K$ فإن:

$$\begin{aligned} f(x_1 K \cdot x_2 K) &= f(x_1 \cdot x_2 K) \\ &= x_1 x_2 \cdot H \\ &= (x_1 H) \cdot (x_2 H) \\ &= f(x_1 K) \cdot f(x_2 K) \end{aligned}$$

كما أن f غامر نواته :

$$\ker f = \{xK \in G/K \quad : \quad f(xK) = H\}$$
$$= \{xK \in G/K \quad : \quad xH = H\}$$
$$= \{xK \in G/K \quad : \quad x \in H\} = H/K$$

وحسب المبرهنة السابقة يكون :

$$(G/K)/(H/K) \cong G/H$$

الزمـــر القابلة للحـــل :

تعريف : نقول عن الزمـــرة G إنها قابلة للحل عندما وفقط عندما توجـــد سلسلة منتهية من الزمـــر الجزئية من G مثل :

$$\{e\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = G$$

بحيث يكون :

$$G_i < G_{i+1} \qquad \forall i = 0,1,\dots,n-1$$

G_{i+1}/G_i تبديلية $\qquad \forall i = 0,1,\dots,n-1$

مبرهنة :

إذا كانت H زمـــرة جزئية من زمـــرة G وكان $K < G$ فإن :

1. (G قابلة للحل) $\Rightarrow$ (H قابلة للحل)
2. (G قابلة للحل) $\Rightarrow$ (G/K قابلة للحل)
3. (K قابلة للحل) $\wedge$ (G/K قابلة للحل) $\Rightarrow$ (G قابلة للحل)

الإثبات :

١. بما أن G قابلة للحل فإنه توجد سلسلة منتهية من الزمر الجزئية من G مثل :

$$\{e\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = G \qquad (*)$$

بحيث يكون :

I. $G_i < G_{i+1} \qquad \forall i = 0,1,\ldots,n-1$

II. تبديلية $G_{i+1}/G_i \qquad \forall i = 0,1,\ldots,n-1$

لنأخذ الأسرة المنتهية

$$H_i = G_i \cap H \qquad i = 0,1,\ldots,n-1$$

(والتي هي زمرة جزئية من الزمرة H) .

عندئذٍ نحصل على السلسلة :

$$\{e\} = H_0 \subseteq H_1 \subseteq \ldots \subseteq H_n = H$$

وأن $H_i < H_{i+1} \qquad (i = 0,1,\ldots,n-1)$ كما أن :

$$H_{i+1}/H_i = (G_{i+1} \cap H)/G_i \cap H$$

$$= (G_{i+1} \cap H)/G_i \cap (G_{i+1} \cap H) \subseteq G_{i+1}/G_i$$

أي أن :

$$H_{i+1}/H_i \subseteq G_{i+1}/G_i \qquad \forall i = 0,1,\ldots,n-1$$

وبما أن $G_{i+1}/G_i \quad (i = 0,1,\ldots,n-1)$ تبديلية فإن:

$H_{i+1}/H_i \quad \forall i = 0,1,\ldots,n-1$ تبديلية .

إذن H قابلة للحل .

٢. بما أن G قابلة للحل فتوجد السلسلة (*) والمحققة للشرطين (I) ، (II)

وبالتالي توجد أسرة منتهية :

$$G_i K/K \qquad i = 0,1,\ldots,n$$

والتي هي زمرة جزئية من زمرة القسمة G/K .

عندئذٍ نحصل على السلسلة :

$$\{K\} = G_0 K/K \subseteq G_1 K/K \subseteq \ldots \subseteq G_n K/K = G/K$$

وأن :

$$G_iK/K < G_{i+1}K/K \qquad i = 0,1,\dots,n-1$$

كما أن :

$$\begin{aligned}(G_{i+1}K/K)/(G_iK/K) &\cong G_{i+1}K/G_iK = G_{i+1}(G_iK)/G_iK \\ &\cong G_{i+1}/G_{i+1}\cap(G_iK) \\ &\cong (G_{i+1}/G_i)/[G_{i+1}\cap(G_iK)/G_i]\end{aligned}$$

أي أن :

$$(G_{i+1}K/K)/(G_iK/K) \cong (G_{i+1}/G_i)/[G_{i+1}\cap(G_iK)/G_i]$$

حيث $i = 0,1,\dots,n-1$

وبما أن $(i = 0,1,\dots,n-1)$ G_{i+1}/G_i تبديلية فإن :

$(G_{i+1}/G_i)/[(G_{i+1}\cap G_iK)/G_i]$ $\quad i = 0,1,\dots,n-1$ تبديلية .

وبالتالي :

$(G_{i+1}K/K)/(G_iK/K)$ $\quad i = 0,1,\dots,n-1$ تبديلية .

إذاً G/K قابلة للحل .

٣. بما أن K قابلة للحل و G/K قابلة للحل فإنه توجد سلسلتان :

$$\{e\} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = K$$

$$K/K = G_0/K \subseteq G_1/K \subseteq \dots \subseteq G_m/K = G/K$$

بحيث يكون :

$K_{i+1}/K_i \quad \wedge \quad K_i < K_{i+1} \qquad i = 0,1,\dots,n-1$ تبديلية .

$(G_{i+1}/K)/G_i/K \wedge G_i/K < G_{i+1}/K \quad i = 0,1,\dots,m-1$ تبديلية .

عندئذٍ توجد سلسلة من الزمر الجزئية من G :

$$\{e\} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = K = G_0 \subseteq G_1 \subseteq \dots \subseteq G_m = G$$

بحيث :

$$K_i < K_{i+1} \qquad i = 0,1,\dots,n-1$$

$$G_i < G_{i+1} \qquad i = 0,1,\dots,m-1$$

وأن :

$K_{i+1}/K_i \qquad i = 0,1,\dots,n-1$ تبديلية .

وأن :

$G_{i+1}/G_i \qquad i = 0,1,\dots,m-1$ تبديلية . لأن :

$$G_{i+1}/G_i \cong (G_{i+1}/K)/(G_i/K) \qquad i = 0,1,\dots,m-1$$

إذاً G قابلة للحل .

الـ P – زمـــرة ، الزمر السيلوفية .

تعريف (١): نقول عن الزمرة G إنها P – زمرة إذا كانت G منتهية و كان P أولي ; $(G:1) = P^n \quad ; n \in N$

أمثلة :

١. كل زمرة من المرتبة 8 تكون 2 – زمرة .

٢. الزمرة $\{e\}$ هي P – زمرة .

مبرهنة :

إذا كانت $G \neq \{e\}$ P – زمرة فإنه يوجـــد فيها عنصر ذو مرتبة مساوية P

الإثبات :

بما أن G P – زمرة فإن $(G:1) = P^n$ حيث $n > 0$ وبالتالي يوجـــد $e \neq a \in G$ بحيث :

$$O(a) = P^m \quad ; \quad 1 \le m \le n$$

أي أن :

$$a^{P^m} = e$$

وبالتالي :

$$a^{P^{m-1}} = a^{-1} \cdot a^{P^m} = a^{-1} \in G$$

أي يوجد $x = a^{m-1} \in G$ وأن $O(x) = P$.

تعريف (٢):لتكن G زمرة منتهية وليكن $(G:1) = P^{\alpha} \cdot r$ حيث P أولي ، $\alpha, r \in N$ وأن P لا يقسم r . نقول عن الزمرة الجزئية H من الزمرة G أنها زمرة جزئية السيلوفية في G إذا كان $(H:1) = P^{\alpha}$.

ملاحظة :كل زمـــرة جزئية سيلوفية من زمـــرة G هي P - زمـــرة .

لتكن G زمرة بحيث $(G:1) = P^{\alpha} \cdot r$ بحيث P عدد أولي لا يقسم r .

عندئذٍ يمكن إثبات صحة القضايا التالية :

١. توجد زمرة جزئية سيلوفية في G .

٢. كل P - زمرة جزئية من G هي زمرة جزئية سيلوفية في G .

٣. إذا كان m عدد الزمر الجزئية السيلوفية في G فإن :

$$m = 1 \pmod{P}$$

تمرينات محلولـــة

التمرين الأول :

لتكن H زمرة جزئية من زمرة $(G,\circ)$ ، نعرف على المجموعـــة G العلاقة الثنائية R كما يلي :

$$aRb \quad \Leftrightarrow \quad a\cdot b^{-1}\in H \qquad (\forall a,b\in G)$$

والمطلوب :

١. برهن أن R علاقة تكافؤ في G .

٢. أثبت أن مجموعة صفوف التكافؤ لعناصر G وفق R هي M_λ مجموعة المرافقات اليسارية لـــ H في G .

الحـــل:

(١).

١. أياً كان $a\in G$ فإن :

$$a\cdot a^{-1}=e\in H$$

وبالتالي R انعكاسية .

٢. أياً كان $a,b\in G$ بحيث aRb فإن $a\cdot b^{-1}\in H$ وبالتالي $(a\cdot b^{-1})^{-1}\in H$ وبالتالي $b\cdot a^{-1}\in H$ أي bRa وبالتالي R تناظرية .

٣. أياً كان $a,b,c\in G$ بحيث $(aRb)\wedge(bRc)$ فإن :

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

$$bRc\Rightarrow b\cdot c^{-1}\in H$$

وبالتالي $(a\cdot b^{-1})\cdot(b\cdot c^{-1})\in H$ ومنه $a\cdot(b^{-1}\cdot b)\cdot c^{-1}\in H$

وبالتالي $a \cdot c^{-1} \in H$ أي aRc

وبالتالي R متعدية .

إذاً العلاقـــة الثنائية R انعكاسية ، تناظرية ومتعدية فهي علاقـــة تكافـــؤ .

.(٢)

$$\forall a \in G \quad : \quad [a] = \{x \in G \quad : \quad xRa\}$$
$$= \{x \in G \quad : \quad x \cdot a^{-1} \in H\}$$
$$= \{x \subset G \quad : \quad x = h \cdot a \quad ; \quad h \in H\}$$
$$= H \cdot a$$

وهذا ما يبيّن أن مجموعة صفوف التكافؤ هي المجموعة :

$$M_\lambda = \{[a] \quad ; \quad a \in G\}$$
$$= \{H \cdot a \quad ; \quad a \in G\}$$

التمرين الثاني :

لتكن H زمرة جزئية من زمرة $(G,\cdot)$ ولتكن :

$M_r = \{x \cdot H; x \in G\}$ مجموعة المرافقات اليمينية للزمرة الجزئية H في الزمرة G

$M_\lambda = \{H \cdot x; x \in G\}$ مجموعة المرافقات اليسارية للزمرة الجزئية H في الزمرة G

أثبت أن :

$$card\, M_r = card\, M_\lambda$$

الحـــل: لنأخذ العلاقة :

$$f : M_r \to M_\lambda$$

المعرفة كما يلي :

$$f(x \cdot H) = H \cdot x^{-1} \qquad (\forall x \cdot H \in M_r)$$

فنجد أن f تطبيق متباين لأن :

$$\forall x_1\cdot H, x_2\cdot H \in M_r : x_1\cdot H = x_2\cdot H \Leftrightarrow (x_1\cdot H)^{-1} = (x_2\cdot H)^{-1}$$
$$\Leftrightarrow H\cdot x_1^{-1} = H\cdot x_2^{-1}$$
$$\Leftrightarrow f(x_1\cdot H) = f(x_2\cdot H)$$

كما أن التطبيق f غامر لأنه أياً كان العنصر $H\cdot x^{-1}$ من M_λ فإنه يوجد $x\in G$ وبالتالي $x\cdot H\in M_r$ ويكون $f(x\cdot H) = H\cdot x^{-1}$

إذاً f تقابل وبالتالي $M_r \sim M_\lambda$ أي أن $card\, M_r = card\, M_\lambda$.

التمرين الثالث :

لتكن $(G,\circ)$ زمرة ما ولنأخذ التطبيق :

$$f : G \to G$$

المعرف كما يلي :

$$f(x) = x^{-1} \qquad (\forall x\in G)$$

أثبت صحة التكافؤ :

الزمـــرة G تبديلية $\Leftrightarrow$ f تشاكل زمـــري

الحـــل : $(\Leftarrow)$:أياً كان $a,b\in G$ فإن :

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

$$= (b\cdot a)^{-1}$$ الزمرة G تبديلية .

$$= a^{-1}\cdot b^{-1}$$ خواص المقلوب .

$$= f(a)\cdot f(b)$$ تعرف f .

أي :

$$\forall a,b\in G \quad : \quad f(a\cdot b) = f(a)\cdot f(b)$$

وبالتالي f تشاكل زمري .

$(\Rightarrow)$: أياً كان $a,b \in G$ فإن :

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

$(a\cdot b)^{-1} = a^{-1}\cdot b^{-1}$ f تشاكل زمري .

$(a\cdot b)^{-1} = (b\cdot a)^{-1}$ خواص المقلوب .

$a\cdot b = b\cdot a$ المقلوب وحيد في الزمرة .

إذاً الزمـــرة G تبديلية .

التمرين الرابع :

لتكن $(G,\circ)$ زمرة مولدة بالمجموعة المنتهية $S = \{a_1, a_2, \ldots, a_r\}$ وليكن $f : G \to G'$ تماثلاً زمرياً . أثبت أن الزمرة G' مولدة بالمجموعة المنتهية $S' = \{f(a_1), f(a_2), \ldots, f(a_r)\}$.

الحـــل :

بما أن f تماثل فإنه أياً كان $y \in G'$ فإنه يوجد $x \in G$ بحيث $y = f(x)$

وبما أن G زمرة مولدة بالمجموعة S فإن :

$$x = a_1^{n_1}\cdot a_2^{n_2}\cdot \ldots \cdot a_r^{n_r} \quad ; \quad n_1, n_2, \ldots, n_r \in Z$$

وبالتالي يكون :

$$\begin{aligned} y &= f(a_1^{n_1}\cdot a_2^{n_2}\cdot \ldots \cdot a_r^{n_r}) \\ &= f(a_1^{n_1})\cdot f(a_2^{n_2})\cdot \ldots \cdot f(a_r^{n_r}) \\ &= [f(a_1)]^{n_1}\cdot [f(a_2)]^{n_2}\cdot \ldots \cdot [f(a_r)]^{n_r} \end{aligned}$$

وهذا ما يثبت أن الزمرة G' مولدة بالمجموعة المنتهية

$$S' = \{f(a_1), f(a_2), \ldots, f(a_r)\}$$

التمرين الخامس :

لتكن $G=<a>_\infty$ زمـــرة دوارة غـــير منتهية مولدة بالعنصر a ولتكن $(Z,+)$ زمرة الأعداد الصحيحة بالنسبة لعملية الجمع المألوفة .

أثبت أن الزمرة $(G,\circ)$ تماثل الزمر الجمعية $(Z,+)$.

الحـــل :لنأخذ العلاقة : $f:G\to Z$

المعرفة كما يلي :

$$f(a^z)=z \qquad \forall a^z\in G$$

فنجد أن f تطبيق متباين لأن :

$$\forall a^{z_1},a^{z_2}\in G: a^{z_1}=a^{z_2}\Leftrightarrow z_1=z_2\Leftrightarrow f(a^{z_1})=f(a^{z_2})$$

كما أن التطبيق f غامر لأنه أياً كان $z\in Z$ فإنه يوجد $a^z\in G$ بحيث يكون : $f(a^z)=z$

كما أن f تشاكل زمري لأنه أياً كان $a^{z_1},a^{z_2}\in G$ فإن :

$$f(a^{z_1}\cdot a^{z_2})=f(a^{z_1+z_2})=z_1+z_2=f(a^{z_1})+f(a^{z_2})$$

مما سبق نجد أن f تماثل زمري وبالتالي $<a>_\infty\cong Z$.

التمرين السادس :

لتكن $G=<a>_n$ زمـــرة دوارة منتهية من المرتبة n ومولـــدة بالعنصر a ولنكن $(Z/nZ,+)$ زمرة صفوف التكافؤ $(\bmod n)$.

أثبت أن الزمرة $(G,\circ)$ تماثل الزمرة الجمعية Z/nZ .

الحـــل :لنأخذ العلاقة :

$$f:G\to Z/nZ$$

المعرفة كما يلي : $f(a^r)=[r] \qquad \forall a^r\in G$

فنجد أن f تطبيق متباين لأن :

$$\forall a^{r_1}, a^{r_2} \in G \quad : \quad a^{r_1} = a^{r_2} \Leftrightarrow a^{r_1 - r_2} = e$$

$$\Leftrightarrow r_1 - r_2 = 0 \pmod{n}$$

$$\Leftrightarrow r_1 = r_2 \pmod{n}$$

$$\Leftrightarrow [r_1] = [r_2]$$

$$\Leftrightarrow f(a^{r_1}) = f(a^{r_2})$$

كما أن التطبيق f غامر لأنه أياً كان $[r] \in Z/nZ$ فإنه يوجد $a^r \in G$

بحيث يكون $f(a^r) = [r]$

كما أن f تشاكل زمري لأنه أياً كان $a^{r_1}, a^{r_2} \in G$ فإن :

$$f(a^{r_1}, a^{r_2}) = f(a^{r_1 + r_2})$$

$$= [r_1 + r_2]$$

$$= [r_1] + [r_2]$$

$$= f(a^{r_1}) + f(a^{r_2})$$

مما سبق نستنتج أن f تماثل زمري أي أن :

$$<a>_n \cong Z/nZ$$

تمرينات (٥)

التمرين الأول :

لتكن $(G,\circ)$ زمرة ، نعرف مركز الزمرة G ونرمز له بـ $Z(G)$ بأنه المجموعة : $Z(G)=\{x\in G \quad : \quad xy=yx \quad \forall y\in G\}$.

والمطلوب :

١. أثبت أن $Z(G)$ زمرة جزئية ناظمية في الزمرة G .

٢. إذا كانت H زمرة جزئية من الزمرة $Z(G)$ فأثبت أن H زمرة جزئية ناظمية في الزمرة G .

التمرين الثاني :

لتكن $(G,\circ)$ زمرة ولتكن S مجموعة جزئية غير خالية من G . نعرف مناظم المجموعة S في الزمرة G ونرمز له بالرمز $N_G(S)$ بأنه المجموعة :

$$N_G(S)=\{x\in G \quad : \quad x\ S\ x^{-1}=S\}$$

إذا كانت H,K زمرتين جزئيتين من الزمرة G وكان H زمرة جزئية ناظمية في الزمرة K . فبرهن أن $K\subseteq N_G(H)$.

التمرين الثالث :

لتكن $(G,\circ)$ زمرة ما ، المحايد فيها e . برهن أنه إذا كان $O(a)=2$ من أجل كل عنصر $e\neq a\in G$ فإن الزمرة G تبديلية .

التمرين الرابع :

لتكن $(G,\circ)$ زمرة ما ، المحايد فيها e . برهن أنه إذا كان $a^2=e$ من أجل كل عنصر $a\in G$ فإن الزمرة G تبديلية .

التمرين الخامس :

لتكن $(G,\circ)$ زمـــرة ما ، برهـــن أنه إذا كان

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

فإن الزمـــرة G تبديلية .

التمرين السادس :

ليكن $f:G\to G$ تشاكلاً زمرياً ولنأخذ المجموعة :

$$H=\{a\in G \quad : \quad f(a)=a\}$$

برهن أن H زمـــرة جزئية من الزمـــرة G .

التمرين السابع :

ليكن $f:G\to G'$ تشاكلاً زمرياً . برهن صحة القضيتين الآتيتين :

I. إذا كانت الزمرة G تبديلية فإن $\operatorname{Im} f$ زمرة تبديلية .

II. إذا كانت الزمرة G دوارة فإن $\operatorname{Im} f$ زمرة دوارة .

التمرين الثامن :

لتكن $G=\langle a\rangle_{15}$ زمـــرة دوارة منتهية من المرتبة $(G:1)=15$ مولـــدة بالعنصر a ، ولتكن H زمرة جزئية من G بحيث يكون $H=\langle a^3\rangle$.

عيّن عناصر الزمرة G/H .

الفصل السادس

نظرية الحلقات ، الحقول

٦ – ١ تعريف :

لتكن R مجموعة غير خالية مزودة بقانوني تشكيل داخليين $+$ ، $\cdot$ نقول عن البنية $(R,+,\cdot)$ إنها حلقة إذا تحققت الشروط الآتية :

i – البنية $(R,+)$ زمـــرة تبديلية .

ii – البنية $(R,\cdot)$ نصف زمـــرة واحديـــة .

iii – القانون $(\cdot)$ توزيعي على القانون $(+)$ أي :

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

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

وإذا كان القانون $(\cdot)$ تبديلياً كانت الحلقة R تبديلية .

نرمز للمحايد في الزمـــرة الجمعية $(R,+)$ بالرمز 0_R (أو اختصاراً 0 إن لم يؤد هذا الاختصار إلى أي التباس) وندعوه صفر الحلقة R ، كما ونرمز للمحايـــد في البنية $(R,\cdot)$ بالرمز 1_R (أو اختصاراً 1 إن لم يـــؤد هـــذا الاختصار إلى أي التباس) وندعوه واحـــد الحلقة R .

أمثلة:

١. إن كلاً من Z ، Q ، R ، C بالنسبة لعمليتي جمع الأعـــداد و ضربها هي حلقة واحـــدية تبديلية .

٢. إن $M_2(R)$ (مجموعة المصفوفات الحقيقية المربعة من المرتبة 2) بالنسبة لعمليتي جمع المصفوفات وضربها هي حلقة غير تبديلية .

$$0_R = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad ; \quad 1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

٣. إن Z/nZ (مجموعة صفوف التكافؤ بالمقاس n) بالنسبة لعمليتي جمع صفوف التكافؤ وضربها هي حلقة تبديلية .

$$0_R = [0] \quad ; \quad 1_R = [1]$$

٤. إن Z_n (راجع المثال (٤) في الفقرة ٥ – ٢) بالنسبة لعمليتي جمع وضرب عناصر Z_n هي حلقة تبديلية .

$$0_R = 0 \quad \wedge \quad 1_R = 1$$

٥. لتكن A مجموعة غير خالية ولتكن $P(A)$ مجموعة أجزاء A . إن $(P(A),\Delta,\mathrm{I})$ حلقة واحدية تبديلية (تدعى هذه الحلقة بالحلقة البوليانيّة) .

$$0_R = \phi \quad \wedge \quad 1_R = A$$

٦ – ٢ خواص الحلقة :

إذا كانت $(R,+,\cdot)$ حلقة وكانت $a,b,c \in R$ فإن :

1. $a \cdot 0 = 0 \cdot a = 0$
2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
3. $(-a) \cdot (-b) = a \cdot b$
4. $\begin{cases} a \cdot (b-c) = a \cdot b - a \cdot c \\ (b-c) \cdot a = b \cdot a - c \cdot a \end{cases}$
5. $\forall a \in R \quad , \quad \forall m,n \in Z \quad , \quad t,s \in Z^+$

$$(a^t)^s = a^{t\cdot s}$$
$$a^t \cdot a^s = a^{t+s}$$
$$n\cdot(m\cdot a) = (n\cdot m)\cdot a$$
$$(n\cdot a)+(m\cdot a) = (n+m)\cdot a$$

مبرهنة : إذا كانت $(R,+,\cdot)$ حلقة تبديلية وإذا كانت $n \in N-\{0\}$ فإن :

$$\forall a,b \in R \quad : \quad (a+b)^n = a^n + \sum_{i=1}^{n-1} C_n^i a^{n-i} b^i + b^n \qquad (*)$$

حيث :

$$C_n^p = \frac{n!}{p!(n-p)!}$$

الإثبات : لنعتمد موضوعة الاستقراء الرياضي على المتحول الطبيعي n .

من أجل $n=1$ يكون :

$$(a+b)^1 = a+b$$

فالمبرهنة صحيحة .

نفرض أن $(*)$ صحيحة من أجل $n=k$ أي أن :

$$(a+b)^k = a^k + \sum_{i=1}^{k-1} C_k^i\, b^{b-i}\cdot b^i + b^k \qquad (*)'$$

ولنبرهن أن $(*)$ صحيحة من أجل $n=b+1$. إن :

$$\begin{aligned}(u+b)^{k+1} &= (a+b)^k\cdot(a+b)\\ &= (a^k + \sum_{i=1}^{k-1} C_k^i a^{k-i}\cdot b^i + b^k)\cdot(a+b)\\ &= a^{k+1} + a^k\cdot b + \sum_{i=1}^{k-1} C_k^i\, a^{k-i+1}\, b^i + \sum_{i=1}^{k-1} C_k^i\, a^{k-i}\, b^{i+1}\\ &\quad + b^k\cdot a + b^{k+1}\end{aligned}$$

لكن :

$$\sum_{i=1}^{k-1} C_k^i\, a^{k-i+1}\cdot b^i = k\, a^k\cdot b + \sum_{i=2}^{k-1} C_k^i\, a^{k-i+1}\cdot b^i$$

$$\sum_{i=1}^{k-1} C_k^i\, a^{k-i}\cdot b^{i+1} = n\cdot a b^k + \sum_{i=2}^{k-1} C_k^i\, a^{k-i+1}\cdot b^i$$

وبالتالي :

$$(a+b)^{k+1} = a^{k+1} + b^{k+1} + (k+1)\,a^k\cdot b + (n-1)\cdot a\cdot b^k + \\ + \sum_{i=2}^{k-1}(C_k^i + C_k^{i-1})\cdot a^{k-i+1}\cdot b^i$$

لكن :

$$C_k^i + C_k^{i-1} = C_{k+1}^i \qquad ; \qquad C_{k+1}^i = C_{k+1}^k = n+1$$

وبالتالي يكون :

$$(a+b)^{k+1} = a^{k+1} + \sum_{i-1}^{k} C_{k+1}^i\cdot a^{k+1-i}\cdot b^i + b^{k+1}$$

وبذلك يتم الإثبات .

ملاحظة : تبقى المبرهنة السابقة صحيحة من أجل أية حلقة R يتحقق فيها

$$a\cdot b = b\cdot a$$

٦ – ٣ الحلقة التامة – المنطقة التكاملية :

تعريف (١) :لتكن $(R,+,\cdot)$ حلقة ما . نقول عن العنصر $0 \neq a \in R$ إنه قاسم للصفر من اليسار في R إذا وجد $0 \neq b \in R$ بحيث يكون : $a\cdot b = 0$

وفي هذه الحالة نقول – أيضاً – إن b قاسم للصفر من اليمين في R .

تعريف (٢) :نعرف الحلقة التامة بأنها حلقة واحدية $1 \neq 0$ ولا تحوي قواسم للصفر .

تعريف (٣) :نعرف المنطقة التكاملية بأنها حلقة تامة تبديلية .

أمثلة :

١. إن الحلقة $(M_2(R),+,\cdot)$ ليست تامة لأنها تحوي قواسم للصفر ، لاحظ أن :

$$0 \neq a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad ; \quad 0 \neq b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

لكن :

$$a \cdot b = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

٢. إن الحلقة $(Z/6Z,+,\cdot)$ ليست تامة لأنها تحـــوي قواسم للصفر ، لاحظ أن :

$$0 \neq a = [2] \quad ; \quad 0 \neq b = [3]$$

لكن :

$$a \cdot b = [2] \cdot [3] = [6] = [0]$$

وبشكل عام الحلقة Z/nZ ليست تامة عندما يكون n مركباً . أما إذا كان $n = p$ عـــدداً أولياً فإن الحلقـــة Z/pZ تكون تامـــة .

٣. الحلقة $(\mathbb{Z},+,\cdot)$ حلقـــة تامـــة تبديلية فهـــي منطقـــة تكامليـــة .

خاصة هامة :

إذا كانت $(R,+,\cdot)$ حلقـــة تامـــة فـــإن :

$$\forall a,b,c \in R \quad : \quad (a \cdot c = b \cdot c) \wedge (c \neq 0) \Rightarrow a = b$$

في الحقيقـــة : إذا كان

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

فـــإن :

$$(a - b) \cdot c = 0$$

وبما أن الحلقـــة R تامـــة (أي لا تحـــوي قواسم للصفر) وبما أن $c \neq 0$

فـــإن $a-b=0$ وبالتالي $a=b$

لاحظ أن الاقتضاء السابق غير صحيح في الحلقات التي تحوي قواسم للصفر .

٦ – ٤ العناصر القلوبة في الحلقة :

تعريف : لتكن $(R,+,\cdot)$ حلقـــة . نقول عن العنصر $a \in R$ إنه قلوب إذا وجـــد $a' \in R$ بحيث :

$$a \cdot a' = a' \cdot a = 1$$

ندعو a' مقلوب a ونرمز له بـــ a^{-1} ونرمز لمجموعة العناصر القلوبة في الحلقة R بالرمز $U(R)$ ويُبرهن أن $U(R)$ هي زمرة بالنسبة للقانون $(\cdot)$

أمثلة :

١. في الحلقة $(Z,+,\cdot)$ يكون :

$$U(Z) = \{-1,1\}$$

٢. في الحلقة $(Q,+,\cdot)$ يكون :

$$U(Q) = Q - \{0\} = Q^*$$

٣. في الحلقة $(M_2(R),+,\cdot)$ يكون :

$$U(M_2(R)) = \{A \in M_2(R) \quad ; \quad \det A \neq 0\}$$

٤. في الحلقة $(Z/nZ,+,\cdot)$ يكون :

$$U(Z \mid nz) = \{[x] \in Z \mid nZ \quad : \quad d(x,n) = 1\}$$

وفي حالة خاصة إذا كان $n = p$ عدداً أولياً فإن :

$$U(Z/pZ) = Z/pZ - \{[0]\}$$

٦ – ٥ الحقـــل :

تعريف : لتكن F مجموعة غير خالية مزودة بقانوني تشكيل داخليين $(+),(\cdot)$ نقول عن البنية $(F,+,\cdot)$ إنها حقـــل إذا تحقق الشرطان :

١. البنية $(F,+,\cdot)$ حلقة واحدية تبديلية $1_F \neq 0_F$.

٢. $U(F) = F - \{0\}$.

أمثلة :

١. إن كلاً من Q ، R ، C حقل وذلك بالنسبة لعمليتي جمع الأعـــداد وضربها .

٢. إذا كان p عدداً أولياً فإن Z/pZ حقـــل .

ملاحظة هامة : لا توجد في الحقل قواسم للصفر .

في الحقيقة إذا كان F حقلاً وكان $a,b \in F$ بحيث $a \cdot b = 0$ فإنـــه إما $a = 0$ أو $b = 0$ لأنه إذا كان $a \neq 0$ و $b \neq 0$ فإن $a^{-1}, b^{-1} \in F$ ويكون :

$$1_F = b^{-1} \cdot a^{-1} \cdot a \cdot b = b^{-1} \cdot a^{-1} \cdot 0_F = 0_F$$

وهذا غير ممكن في الحقل .

مبرهنة :

إذا كان n عدداً صحيحاً بحيث $n > 1$ فإن الحلقة التبديلية Z_n تكون حقلاً عندما وفقط عندما يكون العدد n أولياً .

الإثبات : لنفرض أولاً n غير أولي . عندئذٍ يوجد $r,s \in Z$ بحيث :

$$n = r \cdot s \quad \wedge \quad 1 < r < n \quad \wedge \quad 1 < s < n$$

ومنه : $(r + nZ)(s + nZ) = r \cdot s + nz = nz = 0$

حيث :

$$r+nZ \neq nZ \quad , \quad r\cdot s+nZ = nZ = 0$$

ومنه توجد في Z_n قواسم للصفر ، فلا يمكن أن تكون حقلاً .

لنفرض الآن أن n عـــدداً أولياً . وليكن $0 \neq k+nZ \in Z_n$. بما أن n,k أوليان فيما بينهما فيوجد $\alpha,\beta \in Z$ بحيث : $\alpha\cdot k+\beta\cdot n=1$

ومنه : $(k+nZ)(\alpha+nZ)=(1-\beta\cdot n)+nZ=1+nZ=1$

وهذا يعني أن العنصر $(\alpha+nZ)\in Z_n$ مقلوب العنصر $0\neq k+nZ\in Z_n$

أي كل عنصر مختلف عن الصفر من الحلقـــة Z_n مقلوب في Z_n أي أن Z_n حقـــل .

٦ – ٦ ممـــــيز الحلقـــــة :

تعريف : لتكن R حلقة ، إذا وجـــد عدد صحيح موجب m من أجلـــه:

$$m\cdot x=0 \qquad \forall x\in R$$

فإننا نقول عن الحلقـــة R إنها ذات ممـــيز غير معدوم ونسمي أصغر عـــدد صحيح موجب n من أجله :

$$n\cdot x=0 \qquad \forall x\in R$$

ممـــيز الحلقـــة R .

أما في حال عدم وجود مثل هذا العدد الصحيح m فنقول عن الحلقة R إنها ذات ممـــيز معدوم .

ملاحظة (١):

إذا كانت الحلقـــة R واحدها 1 فإن أصغر عدد صحيح موجب n يحقق $n\cdot 1=0$ نسميه ممـــيز الحلقـــة R .

ملاحظة (٢):

إن مميز الحقل F هو مميز F على اعتبارها حلقة .

نتائج وملاحظات :

١. إن مميز كل منطقة تكاملية هو إما صفر أو عدد أولي .

٢. إن مميز كل حقل هو إما صفرٌ أو عدد أولي .

٣. إن مميز الحلقة Z/nZ هو n .

٤. إذا كانت R منطقة تكاملية مميزها العدد الأولي p . فإن :

$$(a+b)^p = a^p + b^p \qquad \forall a,b \in R$$

وذلك بملاحظة أن :

$$(a+b)^p = a^p + \sum_{i=1}^{n-1} C_p^i \cdot a^{p-i} \cdot b^i + b^p$$

وبما أن p عدد أولي فإن :

$$d(p,k) = 1 \qquad ; \quad 2 \le k \le p-1$$

وبالتالي :

$$2 \cdot 3 \cdot \ldots \cdot k = k! \quad \mid (p-1)\ldots(p-k+1)$$

وبالتالي يوجد عدد صحيح m من أجله $c_p^i = m \cdot p$ وبالتالي ولكون أن مميز المنطقة التكاملية هو العدد الأولي p فإن :

$$\begin{aligned} C_p^i \cdot a^{p-i} \cdot b^i &= m \cdot p \cdot a^{p-i} \cdot b^i \\ &= m(p \cdot a^{p-i} \cdot b^i) \\ &= 0 \end{aligned}$$

وبالتالي :

$$(a+b)^p = a^p + b^p$$

ويمكن تعميم ذلك في المنطقة التكاملية R . فإذا كانت $a_1, a_2, \ldots, a_n$ عناصر من منطقة تكاملية مميزها العدد الأولي p فإن :

$$(a_1+a_2+\ldots+a_n)^p = a_1^p + a_2^p + \ldots + a_n^p$$

٦ ـ ٧ الحلقة الجزئية ـ الحقل الجزئي :

تعريف (١) : لتكن $(R,+,\cdot)$ حلقة ولتكن $\phi \neq A \subseteq R$. نقول عن A إنها حلقة جزئية من الحلقة R عندما وفقط عندما يتحقق الشرطان الآتيان :

1. $\forall a,b \in A \quad : \quad a-b \in A$
2. $\forall a,b \in A \quad : \quad a \cdot b \in A$

أي أن A حلقة جزئية من R عندما وفقط عندما يتحقق الشرطان الآتيان :

١ ـ $(A,+)$ زمرة جزئية من الزمرة $(R,+)$.

٢ ـ A مغلقة بالنسبة للقانون $(\cdot)$.

تعريف (٢) : ليكن $(F,+,\cdot)$ حقلاً ولتكن $\phi \neq A \subseteq F$. نقول عن A إنها حقل جزئي من الحقل F عندما وفقط عندما يتحقق الشرطان الآتيان :

١ ـ $(A,+)$ زمرة جزئية من الزمرة $(F,+)$.

٢ ـ $(A-\{0\},\cdot)$ زمرة جزئية من الزمرة $(F-\{0\},\cdot)$.

أمثلة :

١ ـ إن المجموعة $2Z$ حلقة جزئية من الحلقة $(Z,+,\cdot)$.

٢ ـ إن Q حقل جزئي من الحقل R .

٣ ـ إن المجموعة :

$$A=\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \quad ; \quad a\in R\right\}$$

حلقة جزئية من الحلقة $M_2(R)$.

٤- إذا كانت R حلقة وكان 0 صفرها فإن $\{0\}$ حلقة جزئية من الحلقة R

٥- تقاطع عـــدد منتهٍ من الحلقات الجزئية من حلقةٍ R هو حلقة جزئية من الحلقة R .

٦- تقاطع عدد منتهٍ من الحقول الجزئية من حقل F هو حقل جزئي من الحقل F .

٦ - ٨ المثاليات في الحلقـــة :

تعريف : لتكن $(R,+,\cdot)$ حلقة ، ولتكن $\phi \neq I \subseteq R$.

- نقول عن I إنه مثالي يساري في الحلقة R إذا وفقط إذا تحقق الشرطان:

1. $\forall x,y\in I \quad : \quad x-y\in I$
2. $\forall x\in I \quad , \quad \forall a\in R \quad : \quad a\cdot x\in I$

- نقول عن I إنه مثالي يميني في الحلقة R إذا وفقط إذا تحقق الشرطان:

1. $\forall x,y\in I \quad : \quad x-y\in I$
2. $\forall x\in I \quad , \quad \forall a\in R \quad : \quad x\cdot a\in I$

- نقول عن I إنه مثالي في الحلقة R إذا وفقط إذا كان I مثالياً يسارياً ويمينياً بآن واحد في الحلقة R .

ملاحظة : إذا كانت الحلقة R تبديلية فإن القضايا التالية تكون متكافئة :

1. I مثالي يساري في R .
2. I مثالي يميني في R
3. I مثالي في R .

أمثلة :

١. إن المجموعة :

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

مثالي يساري في الحلقة $(M_2(R),+,\cdot)$ لكن I ليس مثالياً يمينياً في $M_2(R)$ – تأكد من ذلك – .

٢. إن المجموعة : $I=\{nZ \quad ; \quad n\in N^*\}$

مثالي في الحلقة $(Z,+,\cdot)$.

نتائـــج وملاحظـــات :

١. كل مثالي يساري (يميني) في الحلقة R يكون حلقة جزئية من R .

٢. كل حلقة R هي مثالية في نفسها .

٣. إذا كانت R حلقة ما فإن $\{0_R\}$ مثالي في R .

٤. تقاطع عدد منته من المثاليات (اليسارية ، اليمينية) في حلقة R هو مثالي (يساري ، يميني) في R .

٥. إذا انتمى عنصر قلوب من حلقة R إلى مثالي (يساري ، يميني) فيها فإن المثالي يتطابق مع الحلقة R .

<u>في الحقيقة</u> : إذا كان I مثالياً يسارياً في الحلقة R وكان x عنصراً قلوباً في R بحيث $x\in I$ فإن :

$$x^{-1}\cdot x=1\in I$$

وبالتالي يكون :

$$\forall a\in R \quad : \quad a=a\cdot 1\in I$$

أي أن $R \subseteq I$ وبما أن $I \subseteq R$ وبالتالي $R = I$.

أما إذا كان I مثالياً يمينياً فيبرهن $I = R$ بإسلوب مشابه .

٦. لا يوجد في الحقل سوى مثاليين فقط هما الحقل نفسه والمثالي الصفري .

في الحقيقة : إذا كان I مثالياً في حقلٍ F . فإذا كان $I \neq \{0_F\}$ فإنه يوجد $0 \neq x \in I \subseteq F$ وبالتالي $x^{-1} \in I$ وحسب النتيجة السابقة يكون $I = F$

٦ – ٩ الحلقات الجزئية المولدة بمجموعة ، المثاليات المولدة بمجموعة:

لتكن R حلقة ولتكن S مجموعة جزئية غير خالية من R .

١. إن تقاطع كل الحلقات الجزئية من R والتي كل منها تحوي المجموعة S يكون حلقة جزئية من الحلقة R وتحوي S نسميها الحلقة الجزئية من R والمولدة بالمجموعة S نرمز لها بـ $< S >$.

وإذا كانت S مجموعة منتهية غير خالية فنقول عن الحلقة $< S >$ إنها منتهية التوليد . ويبرهن على أنه إذا كانت $S = \{a_1, a_2, \ldots, a_n\}$ فإن :

$$< S > = \{x \in R : x = n_1 \cdot a_1 + n_2 \cdot a_2 + \ldots + n_k \cdot a_k ; n_1, n_2, \ldots, n_k \in Z\}$$

٢. إن تقاطع كل المثاليات (اليسارية ، اليمينية) في الحلقة R والتي كل منها تحوي المجموعة S يكون مثالياً (يسارياً ، يمينياً) في الحلقة R ويحوي S نسميه المثالي (اليساري ، اليميني) المولد بالمجموعة S ونرمز له بـ $< S >$ فإذا كانت $S = \{a_1, a_2, \ldots, a_k\}$ مجموعة منتهية فإن $< S >$ منتهي التوليد وعندئذ يكون :

- إذا كان $< S >$ مثالياً يسارياً فإن :

$$< S > = \sum_{i=1}^{k} x_i \cdot a_i \quad ; \quad x_i \in R \quad , \quad a_i \in S \quad i = 1, 2, \ldots, k$$

وبالتـــالي :

$$< S > = R \cdot S$$

•• إذا كان $< S >$ مثالياً يمينياً فإن :

$$< S > = \sum_{i=1}^{k} a_i \cdot x_i \quad ; \quad x_i \in R \quad , \quad a_i \in S \quad i = 1,2,\ldots,k$$

وبالتـــالي :

$$< S > = S \cdot R$$

••• إذا كان $< S >$ مثالياً فإن :

$$< S > = \sum_{i=1}^{k} x_i \cdot a_i \cdot y_i \quad ; \quad x_i, y_i \in R \quad , \quad a_i \in S \quad i = 1,2,\ldots,k$$

وبالتـــالي :

$$< S > = SRS$$

في حالة خاصة إذا كانت $S = \{a\}$ فإن :

$$R \cdot S = R \cdot a = \{x \cdot a \quad ; \quad x \in R\}$$

وندعـــو المثالي $R \cdot a$ مثالياً يسارياً رئيساً في الحلقـــة R مولداً بالعنصر a .

كما أن :

$$S \cdot R = a \cdot R = \{a \cdot x \quad ; \quad x \in R\}$$

وندعـــو المثالي $a \cdot R$ مثالياً يمينياً رئيساً في الحلقـــة R مولـــداً بالعنصر a

وأخـــيراً :

$$SRS = a \cdot R \cdot a = \{a \cdot x \cdot a \quad ; \quad x \in R\}$$

وندعـــو المثالي aRa مثالياً رئيساً في الحلقـــة R مولـــداً بالعنصر a .

ملاحظة :

إذا كانت الحلقـــة R تبديلية فإن :

$$R \cdot S = S \cdot R = S \cdot R \cdot S$$

أي أن كل مثالي I في الحلقـــة التبديلية هـــو يساري ويميني في آن واحد.

٦ – ١٠ العمليات على المثاليات :

إذا كان I,J مثاليين (يساريين ، يمينيين) في حلقـــة R فإن :

$$I \cap J = \{x \in R \quad ; \quad x \in I \wedge x \in J\}$$

وهو مثالي (يساري ، يميني) في الحلقة R . (تأكد من ذلك) .

وسندرس الآن عمليتي جمع المثاليات وعملية جـــذر المثالي لما لهاتين العمليتين من دور في تفسير بعض المفاهيم الرياضية .

١.عملية جمـــع المثاليـــات :

تعريف :

ليكن I,J مثاليين (يساريين ، يمينيين) في حلقـــة R نعرف مجموع I,J ونكتب $I+J$ بأنه المجموعـــة :

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

مبرهنة:

إذا كان I,J مثاليين (يساريين ، يمينيين) في حلقة R فإن $I+J$ مثـــالي (يساري ، يميني) في الحلقة R .

الإثبات :

ليكن I,J مثاليين يساريين في الحلقـــة R . عندئـــذ :

١. أياً كان $x_1, x_2 \in I+J$ فإن :

$$x_1 = a_1 + b_1 \quad ; \quad a_1 \in I \quad , \quad b_1 \in J$$

$$x_2 = a_2 + b_2 \quad ; \quad a_2 \in I \quad , \quad b_2 \in J$$

وبالتالي :

$$x_1 - x_2 = (a_1 + b_1) - (a_2 + b_2)$$
$$= (a_1 - a_2) - (b_1 - b_2) \quad ; \quad a_1 - a_2 \in I \quad , \quad b_1 - b_2 \in J$$

أي أن :

$$x_1 - x_2 \in I + J$$

٢. أياً كان $x \in I + J$ وأياً كان $\alpha \in R$ فإن :

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

وبالتالي :

$$\alpha \cdot x = \alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b \in I + J$$

إذن $I + J$ مثالي يساري في R .

أما إذا كان I, J مثاليين (يمينيين) فالإثبات يتم بإسلوب مشابه للحالة السابقة .

نتائـــج وملاحظـــات :

١. $I \subseteq I + J \quad ; \quad J \subseteq I + J$

لاحـــظ أن :

$$\forall x \in I \quad : \quad x = x + 0 \quad \in I + J$$
$$\forall y \in J \quad : \quad y = 0 + y \quad \in I + J$$

٢. إن $I + J$ أصغر مثالي (يساري ، يميني) يحوي المثاليين I, J .

٢. عمليـــة جذر المثالي في حلقـــة تبديلية :

تعريف :

ليكن I مثالي في حلقة تبديلية R . نعرف جذر المثالي I ونرمـــز

لـــه بالرمز $\sqrt{I}$ بأنه المجموعة :

$$\sqrt{I} = \{x \in R \quad ; \quad \exists n \in N^* \quad : \quad x^n \in I\}$$

مبرهنة :

إذا كان I مثالياً في حلقة تبديلية R فإن $\sqrt{I}$ مثالي في R .

الإثبات :

١. أياً كان $x, y \in \sqrt{I}$ فإنه يوجـــد $n, m \in N^*$ بحيث : $x^n, y^n \in I$

وحســـب مفهـــوم المنشور في الحلقـــات يكـــون $(x-y)^{n+m} \in I$

وبالتـــالي : $x - y \in \sqrt{I}$.

٢. أياً كان $x \in \sqrt{I}$ وأياً كان $a \in R$ فإنه يوجـــد $n \in N^*$ بحيث

$$a^n \in R \quad \wedge \quad x^n \in I$$

وبالتالي $a^n \cdot x^n \in I$ أي $(a \cdot x)^n \in I$ وبالتالي $a \cdot x \in \sqrt{I}$.

ملاحظة :

من التعريف السابق نلاحـــظ أن :

1. $I \subseteq \sqrt{I}$.
2. $\sqrt{\sqrt{I}} = \sqrt{I}$.
3. $\sqrt{I} + \sqrt{J} = \sqrt{I + J}$.

نترك برهان صحة القضايا الثلاث السابقة كتمرين للقارئ .

٦ – ١١ التشاكلات الحلقيـــة :

تعاريف : لتكن $(R,+,\cdot)$ ، $(R',+,\cdot)$ حلقتين ما .

١. نعرف التشاكل الحلقي بأنه تطبيق $f : R \to R'$ يحقق الشرطين التاليين :

$$(1). \quad \forall a,b \in R \quad : \quad f(a+b) = f(a) + f(b)$$

$$(2). \quad \forall a,b \in R \quad : \quad f(a \cdot b) = f(a) \cdot f(b)$$

وإذا كانت R واحـــدية فإن $f(1)=1$

٢.نعرف التماثل الحلقـــي بأنـــه تشاكل حلقـــي غامـــر ومتباين . إذا كان $f:R\to R'$ تماثلاً حلقياً فإننا نقول إن الحلقتين R',R متماثلتان ونكتب

$$R\cong R'$$

٣.إذا كان $f:R\to R'$ تشاكلاً حلقياً . نعرف نواة f ونرمز لهـــا بالرمز $\ker f$ بأنهـــا المجموعـــة :

$$\ker f=\{x\in R \quad : \quad f(x)=0_{R'}\}=\overline{f}(0_{R'})$$

ملاحظة :

إذا كان $f:R\to R'$ تشاكلاً حلقياً فإن f يكون تشاكلاً زمرياً من الزمـــرة $(R,+)$ في الزمـــرة $(R',+)$ وبالتالي يكون :

1. $f(0_R)=0_{R'}$
2. $\forall a\in R \quad : \quad f(-a)=-f(a)$
3. f متباين $\Leftrightarrow \ker f=\{0_R\}$

مبرهنة : إذا كـــان $f:R\to R'$ تشاكـــلاً حلقيـــاً فـــإن :

١. إذا كانت A حلقة جزئية من الحلقة R فإن $\overline{f}(A)$ حلقة جزئية من الحلقـــة R' .

٢.إذا كانت B حلقة جزئية من الحلقة R' فإن $\overline{f}(B)$ حلقـــة جزئيـــة من الحلقـــة R .

٣.إذا كان I مثالياً يسارياً (يمينياً) في الحلقـــة R' فإن $\overline{f}(I)$ مثالي يساري (يميني) في الحلقـــة R .

٤. $\ker f$ مثالي في الحلقـــة R .

الإثبات :

١. من جهة أولى :

بما أن A حلقة جزئية من الحلقة R فإن $(A,+)$ زمرة جزئية من الزمرة $(R,+)$ وبالتالي $(\vec{f}(A),+)$ زمرة جزئية من الزمرة $(R',+)$.

من جهة ثانية :

أياً كان $y_1, y_2 \in \vec{f}(A)$ فإنـــه يوجـــد $x_1, x_2 \in A$ بحيث

$$y_1 = f(x_1) \quad \wedge \quad y_2 = f(x_2)$$

وبالتالي يكون :

$$y_1 \cdot y_2 = f(x_1) \cdot f(x_2)$$

$$= f(x_1 \cdot x_2)$$

f تشاكل حلقي .

وبما أن $x_1, x_2 \in A$ وأن A حلقة جزئية من الحلقة R فإن $x_1, x_2 \in A$ وبالتالي يكون $f(x_1 \cdot x_2) \in \vec{f}(A)$ أي أن $y_1, y_2 \in \vec{f}(A)$.

إذاً $\vec{f}(A)$ حلقة جزئية من الحلقة R' .

٢. من جهة أولى :

بما أن B حلقة جزئية من الحلقة R' فإن $(B,+)$ زمرة جزئية من الزمرة $(R',+)$. وبالتالي $(\overleftarrow{f}(B),+)$ زمرة جزئية من الزمرة $(R,+)$.

من جهة ثانية :

أياً كان $x_1, x_2 \in \overleftarrow{f}(B)$ فإن $f(x_1) \cdot f(x_2) \in B$ وبالتالي $f(x_1 \cdot x_2) \in B$ أي $y_1, y_2 \in \vec{f}(A)$.

٣. من جهة أولى :

بمـــا أن I مثالي يساري في الحلقة R' فإن $(I,+)$ زمرة جزئية من الزمرة

$(R',+)$ وبالتالي $(\overleftarrow{f}(I),+)$ زمرة جزئية من الزمرة $(R,+)$.

من جهة ثانية :

أياً كان $x \in \overleftarrow{f}(I)$ وأياً كان $a \in R$ فإن $f(x) \in I$ و $f(a) \in R'$

وبالتالي يكون :

$$f(a \cdot x) = f(a) \cdot f(x)$$

وبما أن I مثالي يساري في الحلقة R' فإن $f(a) \cdot f(x) \in I$ وبالتالي

$f(a \cdot x) \in I$ أي أن $a \cdot x \in \overleftarrow{f}(I)$

إذاً $\overleftarrow{f}(I)$ مثالي يساري في الحلقة R

وبطريقة مشابهة نبرهن الحالة عندما يكون I مثالياً يمينياً .

٤. بما أن $\ker f = \overleftarrow{f}(0_{R'})$ وأن $\{0_{R'}\}$ مثالي في R' فحسب (٣) يكون $\ker f$ مثالي في الحلقـــة R .

ملاحظة:

بما أن كل حقل F يمكن اعتباره حلقـــة فإن تعريف التشاكل الحقلي هـــو نفسه تعريف التشاكل الحلقي . فإذا كان F, F' حقلين ما فإن :

١. يعرف التشاكل الحقلي بأنه تطبيق $f : F \to F'$ يحقق الشروط التالية :

1. $\forall a,b \in F \quad : \quad f(a+b) = f(a) + f(b)$
2. $\forall a,b \in F \quad : \quad f(a \cdot b) = f(a) \cdot f(b)$
3. $f(1_F) = 1_{F'}$

٢. يعرف التماثل الحقلي بأنه تشاكل حقلي غامر ومتباين . وإذا كان $f : F \to F'$ تماثـــلاً حقلياً فإننا نقـــول إن الحقلين F, F' متماثـــلان ونكتب $F \cong F'$

ملاحظة هامة :

أي تشاكل حقلي $f : F \to F'$ متباين دومـــاً .

في الحقيقة : بما أن $f(1_F) = 1_{F'}$ فإن $1_F \notin \ker f$ وبالتالي $\ker f \neq F$

وبما أن $\ker f$ مثالي في F وبما أن الحقل لا يحوي سوى المثاليين $\{0_F\}$

و F فإن $\ker f = \{0_F\}$ وهذا يبين أن f متباين .

٦ – ١٢ حلقة خارج القسمة :

بناء حلقة خارج القسمة :

لتكن $(R,+,\cdot)$ حلقة ما وليكن I مثالياً في R عندئذٍ $(I,\cdot)$ زمرة جزئية ناظمية من الزمرة $(R,+)$ [لاحظ أن الزمرة $(R,+)$ تبديلية] .

لنأخذ المجموعة :

$$R/I = \{x + I \quad ; \quad x \in R\}$$

واضح أن R/I غير خالية [لاحظ أن $0 + I \in R/I$] ، ولنعرف على R/I القانونيين الداخليين + ، . كما يلي :

أياً كان $(x+I),(y+I) \in R/I$ فإن :

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

فنجد أن :

١. البنية $(R/I,+)$ زمـــرة تبديلية .

٢. البنية $(R/I,\cdot)$ نصف زمـــرة واحـــدية .

٣. الضرب $(\cdot)$ توزيعي على الجمـــع $(+)$.

وبالتالي البنية $(R/I,+,\cdot)$ حلقة تدعى هذه الحلقـــة حلقـــة خارج قسمة

الحلقـــة R على المثـــالي I ، صفرها هـــو $0_R + I = I$ ، أمـــا واحدها فهـــو $1_R + I$.

ملاحظة (١) :إذا كانت الحلقـــة R تبديلية فإن الحلقـــة R/I تبديلية .

ملاحظة (٢) :إن التطبيق :

$$\pi : R \to R/I$$

المعرف كما يلي :

$$\pi(x) = x + I \qquad \forall x \in R$$

هو تشاكل حلقي غامر نواته $\ker \pi = I$ وذلك للأسباب الآتية :

1. $\forall a,b \in R \quad : \quad \pi(a+b) = (a+b) + I$
$$= (a+I) + (b+I)$$
$$= \pi(a) + \pi(b)$$
2. $\forall a,b \in R \quad : \quad \pi(a \cdot b) = (a \cdot b) + I$
$$= (a+I) \cdot (b+I)$$
$$= \pi(a) \cdot \pi(b)$$
3. $\pi(1_R) = 1_R + I$
$$= 1_{R/I}$$
4. $\forall x + I \in R/I \quad : \quad \exists x \in R : \pi(x) = x + I$
5. $\forall a \in \ker \pi \quad \Leftrightarrow \quad \pi(a) = I$
$$\Leftrightarrow \quad a + I = I$$
$$\Leftrightarrow \quad a \in I$$

ندعو التشاكل الحلقي π السابق تشاكل الغمر القانوني الحلقي .

مبرهنة :

إذا كان $f : R \to R'$ تشاكلاً حلقياً فإن : $R/\ker f \cong f(R)$

الإثبات :بما أن كل حلقة يمكن اعتبارها زمرة بالنسبة للقانون (+) فإن العلاقة :

$$\varphi : R/\ker f \to f(R)$$

المعرفة كما يلي :

$$\varphi(x+\ker f) = f(x) \qquad \forall x+\ker f \in R/\ker f$$

تكون تماثلاً زمرياً (حسب مبرهنة التشاكلات الزمرية) . كما أن :

$$\forall (a+\ker f),(b+\ker f) \in R/\ker f :$$

$$\begin{aligned}\varphi((a+\ker f)\cdot(b+\ker f)) &= \varphi(a.b+\ker f)\\ &= f(a\cdot b)\\ &= f(a)\cdot f(b)\\ &= \varphi(a+\ker f) = \varphi(b+\ker f)\end{aligned}$$

كما أن :

$$\begin{aligned}\varphi(1_R+\ker f) &= f(1_R)\\ &= 1_{R'}\end{aligned}$$

مما سبق نجد أن φ تماثل حلقي وبالتالي :

$$R/\ker f \simeq f(R)$$

ملاحظة (١) :

في المبرهنة السابقة إذا كان التشاكل f غامراً فإن $f(R) = R'$

وعندئذٍ يكون :

$$R/\ker f \cong R'$$

ملاحظة (٢) :إذا كانت R حلقة ما فإن :

1. $R \cong R/\{0_R\}$
2. $\{0_R\} \cong R/R$

٦ ـ ١٣ المثاليات الأولية والأعظمية في الحلقات التبديلية :

تعريف (١):ليكن I مثالياً في حلقة تبديلية R . نقول عن I إنه أولي عندما وفقط عندما يتحقق الشرطان الآتيان :

١. $I \neq R$

٢. أياً كان $x, y \in R$ بحيث $x \cdot y \in I$ فإن : $(x \in I) \vee (y \in I)$

تعريف (٢): ليكن M مثالياً من حلقة تبديلية R . نقول عن M إنه أعظمي عندما وفقط عندما يتحقق الشرطان الآتيان :

١. $M \neq A$

٢. لا يوجد في R أي مثالي J بحيث يكون $M \subset J \subset R$.

مبرهنة :

إذا كان I مثالياً في حلقة تبديلية R فإن :

R/I منطقة تكاملية $\Leftrightarrow$ المثالي I أولي .

الإثبات :

($\Leftarrow$): لتكن R/I منطقة تكاملية عندئذٍ :

١. $I \neq R$

٢. أياً كان $x, y \in R$ بحيث $x \cdot y \in I$ فإن :

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

وبما أن R/I منطقة تكاملية فإن :

$$(x+I) \in I \quad \vee \quad (y+I) \in I$$

أي أن : $x \in I \quad \vee \quad y \in I$

إذن المثالي I أولي .

($\Rightarrow$): ليكن المثالي I أولياً . عندئذٍ $I \neq R$ وبالتالي $1_R + I \neq I$ كما أنه أياً كان :

$$I \neq x+I \in R/I \quad \wedge \quad I \neq y+I \in R/I$$

فإن :

$$(x+I)\cdot(y+I) = x\cdot y + I \neq I$$

لأنه إذا كان $x\cdot y + I = I$ فإن $x\cdot y \in I$

وبما أن المثالي I أولي فإن $y \in I$ أو $x \in I$

أي $x+I = I \quad \vee \quad y+I = I$

وهذا مرفوض .

وبالتالي R/I حلقة تبديلية فيها $1_R + I \neq I$ ولا تحوي قواسم للصفر وبالتالي R/I منطقة تكاملية .

نتائج و ملاحظات :

١. كل مثالي أعظمي هو أولي والعكس غير صحيح .

٢. المثالي $\{0\}$ في الحلقة التبديلية R أولي $\Leftrightarrow$ R منطقة تكاملية .

٣. إذا كان I مثالياً في حلقة تبديلية R بحيث $I \neq R$ فإنه يوجد في R مثالي أعظمي M بحيث $I \subseteq M$.

٦ – ١٤ حلقة المثاليات الرئيسة :

تعريف : نقول عن الحلقة $(R,+,\circ)$ إنها حلقة المثاليات الرئيسة إذا كان $0_R \neq 1_R$ وكان كل مثالي فيها رئيساً .

أمثلة :

١. كل حقل هو حلقة مثاليات رئيسة .

٢. Z حلقة مثاليات رئيسة .

نتيجة :

إذا كانت R حلقة مثاليات رئيسة وكانت R منطقة تكاملية فإن كل مثالي أولي غير صفري في R هو مثالي أعظمي في R .

البرهان:

أياً كان $\{0\} \neq I = aR$ مثالياً أولياً في حلقة المثاليات الرئيسة R وليكن $J \subset I$ $(J \neq I)$ وليكن $J = b \cdot R$ مثالياً في R أي :

$bR \subset aR$ وبالتالي :

$$\exists r \in R \quad : \quad a = b \cdot r \qquad (1)$$

و بالتالي :

$$br \subset aR \quad \wedge \quad b \notin aR$$

وبالتالي $r \in aR$ ومنه $r = aZ$ (حيث $Z \in R$) .

نبدل في (1) فنجد : $a = baZ$ ، وبملاحظة أن R منطقة تكاملية فإن : $bZ = 1_R$ وبالتالي $bR = R$ أي $J = R$ وهذا يبين أن المثالي I أعظمي .

نتيجة :

إذا كان p عدداً أولياً فإن المثالي pZ يكون أولياً في الحلقة Z التي هي حلقة مثاليات رئيسة وبالتالي المثالي pZ أعظمي وبالتالي حلقة القسمة Z/pZ حقل .

٦ ـ ١٥ القواسم والعناصر المتشاركة في الحلقة التبديلية

تعريف (١) : لتكن R حلقة تبديلية وليكن $a \in R$ ، $0 \neq b \in R$.

نقول إن b قاسم لـ a في حلقة R ونكتب $b|a$ عندما

وفقط عندما يوجـــد $c \in R$ بحيث يكون $a = b \cdot c$ أي أن :

$$b|a \quad \Leftrightarrow \quad \exists c \in R \quad : \quad a = b \cdot c$$

نتائـــج وملاحظـــات :

١. $b \in U(R) \Leftrightarrow$ ($0 \neq b \in R$ قاسم لـــ 1_R)

٢. العنصر القلوب في R هـــو قاسم لأي عنصر من R .

تعريف (٢) : لتكن R حلقـــة تبديلية وليكن $a,b \in R - \{0\}$. نقـــول إن a متشارك مع b في R إذا وجـــد في R قلوب x بحيث $a = b \cdot x$ أي :

$$(\exists x \in U(R) \quad : \quad a = b \cdot x) \Leftrightarrow (\text{ } a \text{ متشارك مع } b \text{ في } R \text{ })$$

$$\Leftrightarrow (b|a) \quad \wedge \quad (a|b)$$

نتائـــج وملاحظـــات : (بفرض R حلقـــة تبديلية)

١. إذا كان $a,b \in R - \{0\}$ فإن القضايا التالية متكافئة .

i). a متشارك مع b في R .

ii). b متشارك مع b في R .

iii). a,b متشاركان في R .

٢. إذا كان $a,b \in R - \{0\}$ وكانت R منطقـــة تكامليـــة فإن القضايـــا التاليـــة متكافئـــة .

i). a,b متشاركان في R .

ii). $(b|a) \quad \wedge \quad (a|b)$.

iii). $aR = bR$.

٣. إذا كان $a,b \in U(R)$ فإن a,b متشاركان في R .

تعريف (٣) : لتكن R منطقة تكاملية وليكن $a \in R-\{0\}$. نقول عن a إنـــه بسيط في R عندما وفقط عندما يتحقق الشرطان التاليان :

١. $a \notin U(R)$.

٢. كل قاسم لـــ a في R هـــو إما عنصر قلوب في R أو متشاركاً مـــع a في R .

تعريف (٤) : لتكن R منطقة تكاملية وليكن $a \in R-\{0\}$.نقول عن a إنه أولي في R عندما وفقط عندما يتحقق الشرطان التاليان :

١. $a \notin U(R)$.

٢. أيـــاً كـــان $b,c \in R$ بحـــيث $a|b\cdot c$ فـــإن :

$$(a|b) \quad \vee \quad (a|c)$$

أمثلة :

١. العنصران $1,2$ غير متشاركين في الحلقة Z ، لكنهما متشاركان في الحلقة Q

٢. العنصر 2 أولـــي وبسيط في الحلقـــة Z .

مبرهنة :

إذا كانت R منطقـــة تكامليـــة وكان $0 \neq a \in R$ فإن القضيتين التاليتين متكافئتان :

I. a أولـــي في R .

II. المثالي aR أولـــي في R .

الإثبات :

$(I \Rightarrow II)$: بما أن a أولي في R فإن $0 \notin U(R)$ وبالتالي $aR \neq R$

ومن جهة ثانية أياً كان $x,y \in R$ بحيث $x \cdot y \in aR$ فإن $a|(x \cdot y)$

وعندئذٍ :

إمـــا $a|x$ وبالتالي يوجـــد $b \in R$ بحيث $x = a \cdot b$ وبالتالي $x \in aR$

أو $a|y$ وبالتالي يوجـــد $c \in R$ بحيث $y = a \cdot c$ وبالتالي $y \in aR$

إذن المثالـــي aR أولـــي في R .

$(II \Rightarrow I)$: بما أن aR أولـــي في R فإن $aR \neq R$ وبالتالي $a \notin U(R)$

ومن جهة ثانية أياً كان $b,c,d \in R$ بحيث $c \cdot d = a \cdot b$ فإن $c \cdot d \in aR$

وعندئذٍ :

إما $c \in aR$ وبالتالي يوجـــد $x \in R$ بحيث $c = a \cdot x$ ومنه $a|c$ في R

أو $d \in aR$ وبالتالي يوجـــد $y \in R$ بحيث $d = a \cdot y$ ومنه $a|d$ في R

إذن a أولـــي في R .

٦ – ١٦ حلقـــة التحليل الوحيد :

تعريف :نقول عن المنطقـــة التكامليـــة R إنهـــا حلقـــة تحليل وحيد .

عندما وفقط عندما يتحقق الشرطان التاليان :

I. أياً كان العنصر $x \in R - \{0\}$ فإن :

$$x = u \cdot a_1 \cdot a_2 \cdot \dots \cdot a_n \quad ; \quad n \geq 0$$

حيث :

$$u \in U(R) \quad \wedge \quad (\ a_i \text{ بسيط في } R \ ; \ i = 1,2,\dots,n \ )$$

II. إذا كان :

$$u \cdot a_1 \cdot a_2 \cdot \dots \cdot a_n = v \cdot b_1 \cdot b_2 \cdot \dots \cdot b_m \quad ; \quad n \geq 0 \ , \ m \geq 0$$

حيث :

$u,v \in U(R) \wedge$ (a_i, b_j بسيط في R ; $i=1,\dots,n; j=1,\dots,m$)

فإن : $n=m$ وأن a_i, b_i متشاركان وفق ترقيم مناسب لـ b_j

أمثلة :

١. الحلقة Z هي حلقة تحليل وحيد .

٢. كل حقل هو حلقة تحليل وحيد .

مبرهنة :

إذا كانت R منطقة تكاملية . فإن الشرط اللازم والكافي كي تكون R حلقة تحليل وحيد هو أن يتحقق الشرطان التاليان :

(١). أياً كان العنصر $x \in R-\{0\}$ فإن :

$$x = u \cdot a_1 \cdot a_2 \cdot \dots \cdot a_n \quad ; \quad n \geq 0$$

حيث :

$u \in U(R) \wedge$ (a_i بسيط في R $i=1,2,\dots,n$)

(٢). إذا كان x عنصراً بسيطاً في R فإن العنصر x أولي في R .

الإثبات :

لنفرض أولاً أن R حلقة تحليل وحيد فإن الشرط (١) محقق وذلك من تعريف حلقة التحليل الوحيد .

ليكن x عنصراً بسيطاً في R . عندئذ $x \neq 0_R$ وأن $x \notin U(R)$

ومن جهة أخرى أياً كان $c,d \in R$ بحيث $x|(c \cdot d)$ فإنه يوجد $y \in R$ بحيث يكون $x \cdot y = c \cdot d$.

وحسب الشرط (١) فإنه من أجل العناصر $y,c,d \in R$ يوجد

ويوجـــد $u,v,w \in U(R)$

y_i ; $i=1,2,\dots,n$ بسيطة في R

c_j ; $j=1,2,\dots,m$ بسيطة في R

d_k ; $k=1,2,\dots,\lambda$ بسيطة في R

بحيث :

$$y = u \cdot y_1 \cdot y_2 \cdot \dots \cdot y_n$$

$$c = v \cdot c_1 \cdot c_2 \cdot \dots \cdot c_m$$

$$d = w \cdot d_1 \cdot d_2 \cdot \dots \cdot d_\lambda$$

ومنه :

$$x \cdot (u \cdot y_1 \cdot y_2 \cdot \dots \cdot y_n) = (v \cdot c_1 \cdot c_2 \cdot \dots \cdot c_m) \cdot (w \cdot d_1 \cdot d_2 \cdot \dots \cdot d_\lambda)$$

ومنه :

$$u \cdot x y_1 \cdot y_2 \cdot \dots \cdot y_n - (v \cdot w) \cdot c_1 \cdot c_2 \cdot \dots \cdot c_m \cdot d_1 \cdot d_2 \cdot \dots \cdot d_\lambda$$

وبما أن R حلقة تحليل وحيد فحسب الشرط **II** يكون x مشاركاً مع أحد العناصر $(j=1,2,\dots,m)$; c_j أو مع أحد العناصر $(k=1,2,\dots,\lambda)$; d_k

وعندئذٍ نكون أمام حالتين :

الحالة الأولى : $x \mid c_j$ وبالتالي $x \mid c$

الحالة الثانية : $x \mid d_k$ وبالتالي $x \mid d$

أي أن x عنصر أولي في R

لنفرض الآن أن الشرطين (١) و (٢) محققان عندئذٍ لإثبات أن R حلقة تحليل وحيد يكفي أن نثبت تحقق الشرط **II** . لذلك لنفرض أن :

$$u \cdot a_1 \cdot a_2 \cdot \dots \cdot a_n = v \cdot b_1 \cdot b_2 \cdot \dots \cdot b_m \qquad (*)$$

حيث :

$$(n \geq 0 \quad , \quad m \geq 0) \quad \wedge \quad u,v \in U(R) \quad \wedge$$

$$(\ a_i, b_j \ \text{بسيطة في } R \quad ; \quad i = 1,2,\ldots,n \quad ; \quad j = 1,2,\ldots,m\ )$$

ولنبرهن على أن :

$$(\ a_i, b_i \ \text{متشاركان وفق ترقيم مناسب}\ ) \quad \wedge \quad (n = m)$$

لنعتمد موضوعة الاستقراء الرياضي على n .

مثال : إن Z حلقة إقليدية وذلك لوجود التطبيق :

$$\varphi : Z - \{0\} \to N$$

المعرف كما يلي :

$$\varphi(z) = |z| \quad ; \quad \forall z \in Z - \{0\}$$

والمحقق للشرطين (I) و (II) .

مبرهنة :

إذا كانت R حلقة إقليدية وكانت φ الدالة الإقليدية في R وكانت $a,b,c \in R - \{0\}$ فإن القضايا التالية محققة :

١. إذا كان a,b متشاركين في R فإن $\varphi(a) = \varphi(b)$.

٢. إذا كان $a|b$ وكان $\varphi(a) = \varphi(b)$ فإن a,b متشاركان في R .

٣. $c \in U(R) \quad \Leftrightarrow \quad \varphi(c) = \varphi(1_R)$

الإثبات :

١. إذا كان a,b متشاركين في R فإن :

$$(a|b) \quad \wedge \quad (b|a)$$

ومنه $\varphi(a) \leq \varphi(b) \quad \wedge \quad \varphi(b) \leq \varphi(a)$

وبالتالي :

$$\varphi(a) = \varphi(b)$$

٢. يكفي أن نثبت أن $b|a$. من أجل العنصرين a,b يوجد $q,r \in R$ بحيث يكون :

$$a = b \cdot q + r \quad ; \quad \varphi(r) < \varphi(b) \quad \vee \quad r = 0$$

إن $r = 0$ لأنه إذا كان $r \neq 0$ فإن $a|r$ وعندئذٍ يكون $\varphi(a) \leq \varphi(r)$ وهذا يناقض كون $\varphi(r) < \varphi(b) = \varphi(a)$.

إذن $r = 0$ وبالتالي $a = b \cdot q$ أي $b|a$.

(أصبح لدينا $(b|a) \wedge (a|b)$ وبالتالي a,b متشاركان في R).

٣. $(\Rightarrow)$:

لنفرض أن $c \in U(R)$ وبالتالي $c, 1_R$ متشاركان في R وحسب (١) يكون

$$\varphi(c) = \varphi(1_R)$$

من أجل $n = 0$ يكون :

$$u = v \cdot b_1 \cdot b_2 \cdot \ldots \cdot b_m$$

وعندئذٍ يكون $m = 0$ لأنه إذا كان $m > 0$ ولكون $u,v \in U(R)$ فإنه سيكون $b_j \in U(R) \quad j = 1,\ldots,m$ وهذا يناقض كون b_j بسيطة في R .

نفرض أن الشرط (II) محقق من أجل $n-1$. ولنبرهن صحة الشرط (II) من أجل n . حسب الشرط (٢) يكون a_n أولياً في R وبالتالي يكون a_n قاسماً للطرف الأيمن في (*) وبالتالي a_n قاسم لأحد المضاريب $v \cdot b_1 \cdot b_2 \cdot \ldots \cdot b_m$ فإذا كان $a_n | v$ فإن $a_n \in U(R)$ وهذا مرفوض ، وبالتالي $m > 0$ ولنفرض أن a_n قاسم لـ b_m وفق ترتيب مناسب للعناصر

b_j وبما أن b_m بسيط في R فإن b_m, a_n متشاركان في R وبالتالي يوجد

$w \in U(R)$ بحيث : $a_n = w \cdot b_m$

نبدل في (*) فنحصل على :

$$u \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} \cdot (w \cdot b_m) = v \cdot b_1 \cdot b_2 \cdot \ldots \cdot b_m$$

ومنـــه :

$$(u \cdot w) \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} = v \cdot b_1 \cdot b_2 \cdot \ldots \cdot b_{m-1}$$

وحسب الفرض الاستقرائي يكون :

(a_k, b_k) متشاركان في R من أجل $(k = 1,2,\ldots,n-1) \wedge (n-1 = m-1)$

وبملاحظة أن b_m, a_n متشاركان يكون

(a_i, b_i) متشاركان في R وفق ترقيم مناسب) $\wedge (n = m)$

٦ – ١٧ الحلقـــة الإقليـــديّة :

تعريف :نقول عن المنطقـــة التكاملية R إنهـــا حلقـــة إقليديـــة إذا وجـــد تطبيق مثل $\varphi : R - \{0\} \to N$ بحيث يتحقق الشرطان :

(I). أياً كان $a, b \in R - \{0\}$ وكان $a|b$ فإن :

$$\varphi(a) \le \varphi(b)$$

(حيث $\le$ علاقة الترتيب المألوفة في N).

(II). أياً كان $a, b \in R$ وكان $b \ne 0$ فإنه يوجد $q, r \in R$ بحيث :

$$a = b \cdot q + r \quad ; \quad \varphi(r) < \varphi(b) \quad \vee \quad r = 0_R$$

(يدعى التطبيق φ دالـــة إقليـــدية).

($\Leftarrow$): لنفرض أن $\varphi(c) = \varphi(1_R)$. بما أن $1_R|c$ فإنه حسب (٢) يكون

$1_R, c$ متشاركين في R وبالتالي يوجد $u \in U(R)$ بحيث يكون $c = 1_R \cdot u$ ومنـــه $c \in U(R)$.

مبرهنة :

إذا كانت R حلقـــة إقليدية فإن R حلقـــة مثاليات رئيسة .

الإثبات :

بما أن R حلقة إقليدية فإن R منطقة تكاملية . ولنبرهن على أن أي مثالي I في R هـــو مثالي رئيس .

إذا كان $I = \{0_R\}$ فإن I مثالي رئيس .

ليكن المثالي $I \neq \{0_R\}$ ولتكن φ الدالة الإقليدية ولنأخذ المجموعة :

$$S = \{\varphi(x) \quad ; \quad 0_R \neq x \in I\}$$

فنجد أن المجموعة $\phi \neq S \subseteq N$ وبالتالي يوجد في S عنصر أصغر مثل $\varphi(b)$ $(0_R \neq b \in I)$. أي :

$$\varphi(b) \leq \varphi(c) \qquad \forall 0_R \neq c \in I$$

ومنـــه $bR \subseteq I$

ومن جهة أخرى : أياً كان $a \in I$ فإنه من أجل $a, b \in R$ يوجد $q, r \in R$ بحيث يكون :

$$a = b \cdot q + r \quad ; \quad \varphi(r) < \varphi(b) \quad \vee \quad r = 0_R$$

إن $r = 0_R$ لأنه إذا كان $r \neq 0_R$ فإن

$$\varphi(r) < \varphi(b) \quad ; \quad 0_R \neq r = a - b \cdot q \in I$$

وهذا يناقض اختيار العنصر b . إذاً $r = 0_R$ وبالتالي $a = b \cdot q$ أي أن $a \in bR$ ومنـــه $I \subseteq bR$.

إذاً $I = bR$ أي المثالي I رئيس في R .

٦ – ١٨ القاسم المشترك الأكبر في المنطقة التكاملية :

تعريف : لتكن R منطقة تكاملية ولتكن $a_1, a_2, \ldots, a_n \in R - \{0\}$. نقول عن $d \in R - \{0\}$ إنه قاسم مشترك أكبر لـ $a_1, a_2, \ldots, a_n$ في R إذا تحقق الشرطان التاليان :

١. $d | a_i \quad \forall i = 1, 2, \ldots, n$

٢. إذا كان $d' \in R - \{0\}$ وكان $d' | a_i \quad (i = 1, 2, \ldots, n)$ فإن $d' | d$

فإذا كان d قاسماً مشتركاً أكبر للعناصر $a_1, a_2, \ldots, a_n$ فإننا نعبّر عن ذلك بالرمز $d(a_1, a_2, \ldots, a_n)$

نتيجة : إذا كان كل من d_1, d_2 قاسماً مشتركاً أكبر لـ $a_1, a_2, \ldots, a_n$ في منطقة تكاملية في R فإن :

$$d_2 = d_1 \cdot u \quad ; \quad u \in U(R)$$

البرهان : بما أن كل من d_1, d_2 قاسم مشترك أكبر لـ $a_1, a_2, \ldots, a_n$ فإن d_1, d_2 متشاركان في R وبالتالي :

$$\exists \quad u \in U(R) \quad : \quad d_2 = d_1 \cdot u$$

مبرهنة :

إذا كانت R حلقة مثاليات رئيسة وكانت R منطقة تكاملية وكانت $a_1, a_2, \ldots, a_n \in R - \{0\}$ فإن القضايا التالية تكون صحيحة :

I. يوجد في R قاسم مشترك أكبر للعناصر $a_1, a_2, \ldots, a_n$.

II. يكون العنصر $d \in R - \{0\}$ قاسماً مشتركاً أكبر للعناصر $a_1, a_2, \ldots, a_n$ في R عندما وفقط عندما يكون :

$$a_1 \cdot R + a_2 \cdot R + \ldots + a_n \cdot R = d \cdot R$$

الإثبات :

I. بما أن R حلقـــة مثاليات رئيسة فإن مجمـــوع المثاليات الرئيسة :

$$a_1 \cdot R + a_2 \cdot R + \ldots + a_n \cdot R$$

هو مثالي رئيس في R وليكن dR حيث $d \in R - \{0\}$ أي أن :

$$a_1 \cdot R + a_2 \cdot R + \ldots + a_n \cdot R = d \cdot R \qquad (*)$$

ومنه :

$$a_i \in dR \quad ; \quad i = 1,2,\ldots,n$$

وبالتالي :

$$d | a_i \qquad \forall i = 1,2,\ldots,n$$

وحسب (*) يوجد $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$ بحيث يكون :

$$d = a_1 \cdot \alpha_1 + a_2 \cdot \alpha_2 + \ldots + a_n \cdot \alpha_n = \sum_{i=1}^{n} a_i \alpha_i$$

لنفرض الآن أن $d' \in R - \{0\}$ وأن :

$$d' | a_i \qquad \forall i = 1,2,\ldots,n$$

وبالتالي يوجد $\beta_1, \beta_2, \ldots, \beta_n \in R$ بحيث يكون :

$$a_i = \beta_i \cdot d'$$

وبالتالي :

$$d = \sum_{i=1}^{n} \beta_i \cdot d' \cdot \alpha_i = d' \cdot \sum_{i=1}^{n} \beta_i \cdot \alpha_i$$

وهذا يبين أن $d' | d$ في R .

إذاً d قاسم مشترك أكبر للعناصر $a_1, a_2, \ldots, a_n$ في R .

II. لنفرض أولاً أن : $a_1 \cdot R + a_2 \cdot R + \ldots + a_n \cdot R = d \cdot R$

من خلال إثبات (I) نجد بسهولة أن d قاسم مشترك أكبر للعناصر $a_1, a_2, \ldots, a_n$ في R

لنفرض الآن أن d قاسم مشترك أكبر للعناصر $a_1, a_2, \ldots, a_n$ في R ولنفرض أن مجموع المثاليات الرئيسة $a_1R, a_2R, \ldots, a_nR$ هو المثالي الرئيس xR

أي أن : $a_1R + a_2R + \ldots + a_nR = xR$

وبالتالي d, x متشاركان في R وبالتالي يوجد $u \in U(R)$ بحيث $x = d \cdot u$ وبالتالي :

$$a_1R + a_2R + \ldots + a_nR = d \cdot u \cdot R = d \cdot R$$

نتيجة : من المبرهنة السابقة نستنتج مباشرة أن أي قاسم مشترك أكبر للعناصر $a_1, a_2, \ldots, a_n$ في R يكتب على الشكل :

$$a_1\beta_1 + a_2\beta_2 + \ldots + a_n\beta_n \quad ; \quad \beta_i \in R \quad ; \quad i = 1, 2, \ldots, n$$

أي إذا كان $d(a_1, a_2, \ldots, a_n) = d$ فإن :

$$\exists \quad \beta_1, \beta_2, \ldots, \beta_n \in R \quad : \quad d = a_1\beta_1 + a_2\beta_2 + \ldots + a_n\beta_n$$

٦ – ١٩ الحقول الأولية في حقل :

تعريف : نعرف الحقل الجزئي الأولي في حقل F بأنه تقاطع جميع الحقول الجزئية في F .

بعبارة مكافئة : الحقل الجزئي الأولي في حقل F هو الحقل الجزئي الأصغر (الوحيد) في F .

أمثلة :

١. إن الحقل Q هو حقل أولي لأن Q هو الحقل الجزئي الوحيد في Q .

٢. إن الحقل Z_p (p عدد أولي) هو حقل أولي لأن Z_p هو الحقل الجزئي

الوحيد في Z_p .

مبرهنة :

إذا كان P حقـلاً أوليـاً في حقـل F فـإن

$$(P \cong Q) \quad \vee \quad (P \cong Z_P)$$

(حيث p عدد أولي)

الإثبات :

بما أن P حقـلاً أولياً في حقـل F فـإن $1_F, 0_F \in P$. لنأخذ العلاقة

$$\varphi : Z \to P$$

المعرفة كما يلي :

$$\varphi(z) = z \cdot 1_F \quad \forall z \in Z$$

فنجد أن φ تشاكلاً حلقياً لأن :

$$\begin{aligned} \forall z_1, z_2 \in Z \quad : \quad \varphi(z_1 + z_2) &= (z_1 + z_2) \cdot 1_F \\ &= z_1 \cdot 1_F + z_2 \cdot 1_F \\ &= \varphi(z_1) + \varphi(z_2) \end{aligned}$$

$$\begin{aligned} \varphi(z_1 \cdot z_2) &= (z_1 \cdot z_2) \cdot 1_F \\ &= (z_1 \cdot 1_F) \cdot (z_2 \cdot 1_F) \\ &= \varphi(z_1) \cdot \varphi(z_2) \end{aligned}$$

$$\begin{aligned} \varphi(1) &= 1 \cdot 1_F \\ &= 1_F \\ &= 1_p \end{aligned}$$

كما أن :

$$\forall z \in \ker \varphi \quad : \quad \varphi(z) = 0_F \quad \Rightarrow \quad z \cdot 1_F = 0_F$$

وهنا نميز الحالتين :

الحالة الأولى : $(z \cdot 1_F = 0_F) \quad \wedge \quad (z \neq 0)$ عندئذٍ $(-z) \cdot 1_F = 0_F$

وبالتالي يوجد $p \in Z$ أصغر عدد صحيح موجب يحقق $p \cdot 1_F = 0_F$

وبالتالي $p \neq 1$ كما أن p أولي لأنه إذا كان p مركباً فإنه يوجد $1 < r < p \quad , \quad 1 < s < p$ بحيث يكون : $p = r \cdot s$ وبالتالي يكون :

$$\varphi(p) = p \cdot 1_F = 0_F$$

ومن جهة ثانية :

$$\varphi(p) = \varphi(r \cdot s) = \varphi(r) \cdot \varphi(s) = (r \cdot 1_F) \cdot (s \cdot 1_F)$$

وبالتالي :

$$(r \cdot 1_F) \cdot (s \cdot 1_F) = 0_F$$

ومنه :

$$(r \cdot 1_F = 0_F) \quad \vee \quad (s \cdot 1_F = 0_F)$$

وهذا يناقض اختيار العدد p . إذن p أولي وعندئذٍ يكون $\ker\varphi = pZ$

وحسب مبرهنة التشاكلات الحلقية يكون :

$$Z|pZ \cong \varphi(Z) \subseteq P$$

وبما أن $\varphi(Z)$ حقل جزئي من الحقل P وأن P حقل أولي فإن $\varphi(Z) = P$

وأن $Z|pZ = Z_p$ يكون $Z_p \cong P$.

الحالة الثانية : إذا كان $z \neq 0$ فإن $z \cdot 1_F \neq 0_F$ وعندئذٍ $\ker\varphi = \{0\}$

وبالتالي : $Z \cong \varphi(Z) \subseteq P$.

كما أن :

$$\forall n, m \in Z \quad ; \quad n \neq 0 \quad : \quad (m \cdot 1_F) \cdot (n \cdot 1_F)^{-1} = \frac{m \cdot 1_F}{n \cdot 1_F} \in P$$

ولكن :

$$\left\{\frac{m\cdot 1_F}{n\cdot 1_F} \quad ; \quad n,m\in Z \quad ;n\neq 0\right\}\cong Q$$

وهو حقل جزئي من الحقل الأولي P وبالتالي $P\cong Q$.

نتيجة : إذا كان P حقلاً جزئياً أولياً من حقل F عندئذٍ .

١. إذا كان $P\cong Q$ فإن الحقل F ذا مميز معدوم .

٢. إذا كان $P\cong Z_p$ فإن الحقل F ذا مميز P (P عدد أولي).

٦ – ٢٠ حلقـــة الكســـور :

تعريف : لتكن R حلقة تبديلية . نقول عن المجموعة الجزئية $S\subseteq R$ إنهـــا ضربيّة في R إذا تحقق الشرطان التاليان :

1. $1_R\in S$
2. $\forall x,y\in S \quad : \quad x\cdot y\in S$

بناء حلقـــة الكسور : لتكن R حلقة تبديلية ولتكن S مجموعة ضربية في R . لنعرف في المجموعة $R\times S$ العلاقة الثنائية $\sim$ كما يلي :

$$\forall(a,b),(a',b')\in R\times S \quad :$$

$$(a,b)\sim(a',b') \quad \Leftrightarrow \quad \exists\alpha\in S \quad : \quad \alpha(b'a-ba')=0_R$$

فنجـــد أن $\sim$ علاقة تكافـــؤ في $R\times S$. نرمز لصف تكافؤ العنصر (a,b) بالرمز $\frac{a}{b}$ وندعوه كسراً وندعو a بسطه و b مقامه . ونرمـــز لمجموعـــة الكسور بالرمز $S^{-1}R$ أي أن :

$$S^{-1}R=\left\{\frac{a}{b} \quad ; \quad a\in R \quad \wedge b\in S\right\}$$

$$\forall a \in R \quad , \quad b,b' \in S \quad : \quad \frac{a}{b} = \frac{b'a}{b'b}$$

لنعرف على المجموعة غير الخالية $S^{-1}R$ قانوني تشكيل داخليين

الجمع $(+)$: $\frac{a}{b} + \frac{a'}{b'} = \frac{b'a + ab'}{bb'}$

الضرب $(\cdot)$: $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'}$

حيث :

$$\frac{a}{b} \quad , \quad \frac{a'}{b'} \in S^{-1}R$$

فنجد أن $(S^{-1}R,+,\cdot)$ حلقة الكسور الموافقة للمجموعة S .

ملاحظة (١) : إذا أخذنا العلاقة :

$$\varphi_s : R \to S^{-1}R$$

المعرفة كما يلي :

$$\varphi(a) = \frac{a}{1_R} \quad \forall a \in R$$

فنجد أن φ_s تشاكلاً حلقياً . (تأكد من ذلك) . وأن كل عنصر من $\varphi_s(s)$ قلوب في $S^{-1}R$ ، فإذا كان $\frac{x}{y} \in \varphi_s(s)$ فإن : $\left(\frac{x}{y}\right)^{-1} = \frac{y}{x}$

ملاحظة (٢) :

إن التشاكل φ_s يكون متبايناً عندما تكون R منطقة تكاملية و $0_R \notin S$.

في الحقيقة :

$$\forall a \in \ker \varphi_s \quad \Rightarrow \quad \varphi_s(a) = \frac{0_R}{1_R}$$

$$\Rightarrow \quad \frac{a}{1_R} = \frac{0_R}{1_R}$$

وبالتالي يوجـــد $b \in S$ بحيث يكون $ba = 0_R$ وبالتالي :

$$(b = 0_R) \quad \vee \quad (a = 0_R)$$

إن $b = 0_R$ مرفوض لأن $0_R \notin S$ وبالتالي $a = 0_R$ ومنه $\ker \varphi_s = \{0_R\}$

أي أن φ_s متباين .

تعريف : نعرف حقـــل الكسور لحلقـــة تبديلية R بأنه حقـــل F بحيث يتحقق الشرطان التاليان :

١. يوجد في F حلقة جزئية R' بحيث $R \cong R'$.

٢. كل عنصر من F يكتب بالشكل $\frac{a}{b}$ حيث $a,b \in R'$ و $b \neq 0_{R'}$

مبرهنة :

إذا كانت R منطقـــة تكاملية فإنـــه يوجـــد لـــ R حقـــل كســـور.

الإثبات :

بما أن R منطقة تكاملية فإن المجموعة $S = R - \{0_R\}$ تكون ضربية في R وبالتالي توجـــد حلقـــة الكسور $S^{-1}R$ وعندئذٍ يكون التطبيق :

$$\varphi_s : R \to S^{-1}R$$

المعرف كما يلي :

$$\varphi_s(a) = \frac{a}{1_R} \quad \forall a \in R$$

تشـــاكلاً حلقياً متبايـــناً وحســـب مـــبرهنة التشاكلات الحلقيـــة يكون :

$$R \cong R' = \varphi_s(R) \subseteq S^{-1}R$$

كمـــا أن إذا كان

$$\frac{a}{b} \neq \frac{0_R}{1_R} \quad ; \quad a \in R \quad ,b \in S$$

فإن $a \in S$ وبالتالي يوجـــد في $S^{-1}R$ العنصر $\frac{b}{a}$ بحيث يكون

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

كما وأن كل عنصر من $S^{-1}R$ يكتب بالشكل :

$$\frac{a}{b} \quad ; \quad a,b \in R' \quad , \quad b \neq 0_{R'}$$

ويكون :

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

إذن $S^{-1}R$ حقـــل كسور لـــ R .

أمثلة :

١. إذا كان F حقلاً فإن المجموعـــة $S = F - \{0_F\}$ تكون ضربية في F وعندئـــذٍ يكون $F \cong S^{-1}F$.

٢. إذا أخذنا الحلقة Z فنجد أن المجموعة $S = Z - \{0\}$ مجموعة ضربية في Z وتكون حلقة الكسور $S^{-1}Z$ حقلاً هو حقل الأعـــداد العادية Q.

٦ – ٢١ الجـــداء المباشر للحلقـــات :

لتكن $\{R_i\}_{i=1,2,\dots,n}$ أسرة منتهية من الحلقـــات ولنأخذ الجداء الديكارتي

$$R = \prod_{i=1}^{n} R_i = R_1 \times R_2 \times \dots \times R_n$$
$$= \{(a_1, a_2, \dots, a_n) \quad ; \quad a_i \in R_i \quad i = 1,2,\dots,n\}$$

واضـــح أن $\phi \neq \prod_{i=1}^{n} R_i$.

ولنعرف على الجـــداء الديكارتي $\prod_{i=1}^{n} R_i$ قانوني تشكيل داخليين :

$$+ : (a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

$$\cdot : (a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n)$$

حيث :

$$(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in R$$

فنجـــد – بسهولة – أن البنية $(R, +, \cdot)$ حلقـــة ويكون :

$$0_R = (0_{R_1}, 0_{R_2}, \ldots, 0_{R_n}) \quad , \quad 1_R = (1_{R_1}, 1_{R_2}, \ldots, 1_{R_n})$$

ندعـــو هـــذه الحلقـــة بالجـــداء المباشر للحلقـــات R_i $(i = 1, 2, \ldots, n)$

ونلاحظ أن الحلقـــة R تكون تبديلية عندما R_i $(i = 1, 2, \ldots, n)$ تبديلية.

تمرينات محلولـــــة

التمرين الأول :

لتكن $(R,+,\cdot)$ حلقـــة تبديلية وليكن $a \in R$. والمطلوب :

١. أثبت أن المجموعة : $I = \{xa \quad ; \quad x \in R\}$

مثالـــي في الحلقـــة R .

٢. إذا كان M مثالياً في R بحيث $a \in M$ فأثبت أن $I \subseteq M$.

الحـــل :

١. إن $0_R = 0_R \cdot a \in I$

كما أن $I \subseteq R$ (من تعريف المجموعة I).

أي أن : $\phi \neq I \subseteq R$.

من جهة ثانية : أياً كان $xa, ya \in I$ فإن :

$$xa - ya = (x - y) \cdot a \in I$$

أي أن $(I,+)$ زمـــرة جزئيـــة من الزمـــرة $(R,+)$.

كما أنه أياً كان $xa \in I$ وأياً كان $y \in R$ فإن :

$$y \cdot (xa) = (y \cdot x) \cdot a \in I$$

مما سبق نجـــد أن I مثالي يساري في الحلقـــة R وبما أن الحلقـــة R تبديلية فإن I مثالي في R .

٢. ليكن M مثالياً في R بحيث $a \in M$ فإن $xa \in M$ (حسب تعريف المثالي في الحلقـــة) ومن تعريف المجموعة I نجـــد أن $I \subseteq M$.

التمرين الثاني :

لتكن : $R = \{a + \sqrt{5}bi \quad ; \quad a,b \in Z \quad ; \quad i^2 = -1\}$

منطقة تكاملية (تأكد من ذلك) .

نعرف نظيم العنصر $x = a + \sqrt{5}bi \in R$ بأنه العدد الصحيح غير السالب

$$N(x) = a^2 + 5b^2$$

المطلوب :

١. أثبت أن : $\forall x, y \in R \quad : \quad N(x \cdot y) = N(x) \cdot N(y)$

٢. عيّن المجموعة $U(R)$ (مجموعة العناصر القلوبة في R) .

٣. أثبت أن كل عنصر من المجموعة :

$$A = \{2 \ , \ 3 \ , \ 1 + \sqrt{5}i \ , \ 1 - \sqrt{5}i\}$$

بسيط في R .

٤. هل العنصر 2 أولي في R ولماذا ؟

الحـــل :

١. أياً كان $x, y \in R$ فإن :

$$x = a_1 + \sqrt{5}\, b_1 i \quad ; \quad a_1, b_1 \in Z$$

$$y = a_2 + \sqrt{5}\, b_2 i \quad ; \quad a_2, b_2 \in Z$$

وبالتالي :

$$\begin{aligned} N(x \cdot y) &= N\left((a_1 \cdot a_2 - 5b_1 \cdot b_2) + \sqrt{5}(a_1 \cdot b_2 + b_1 \cdot a_2)i\right) \\ &= (a_1 \cdot a_2 - 5b_1 \cdot b_2)^2 + 5(a_1 \cdot b_2 + b_1 \cdot a_2)^2 \\ &= (a_1^2 + 5b_1^2) \cdot (a_2^2 + 5b_2^2) \\ &= N(x) \cdot N(y) \end{aligned}$$

٢. ليكن $u \in R$ عنصراً قلوباً عندئذٍ يوجد $v \in R$ بحيث يكون $u \cdot v = 1$

ومنـــه :

$$N(u \cdot v) = N(u) \cdot N(v) = N(1) = 1$$

وبما أن $N(u), N(v)$ عددان صحيحان غير سالبين وبالتالي :

$$N(u) = N(v) = 1$$

ومن جهة ثانية : إذا كان $N(x) = 1$ فإن $a^2 + 5b^2 = 1$

وبالتالـــي $a = \mu 1 \quad \wedge \quad b = 0$ ومنـــه $x = \mu 1$

ومنـــه :

$$u \in \{-1,1\}$$

إذاً : $U(R) = \{-1,1\}$

٣. $\forall z \in \{2 \ , \ 3 \ , \ 1+\sqrt{5}i \ , \ 1+\sqrt{5}i\}$

فـــإن :

$$(z \neq 0) \ \wedge \ N(z) \neq 1$$

إذا فرضنا x قاسم لـــ z فيوجـــد في R عنصر مثل y بحيث يكون $z = x \cdot y$ وبالتالي يكون :

$$N(z) = N(x) \cdot N(y)$$

لكـــن :

$$(N(x) > 0) \wedge (N(y) > 0) \wedge (N(x), N(y) \in Z) \wedge N(z) = \{4,9,6\}$$

وبالتالـــي :

إمـــا $N(z) = N(y) \wedge N(x) = 1$ وبالتالي x قلوب في R

أي $x \in U(R)$

أو $N(x) = N(z) \wedge N(y) = 1$ وبالتالي y قلوب في R

أي أن y متشارك مع x في R .

مما سبق نجـــد أن كل عنصر $z \in A$ عنصر بسيط في R .

٤. وجدنا أن العنصر 2 بسيط في R وأن

$$2/(1+\sqrt{5}i)(1-\sqrt{5}i)$$

وأن 2 ليس قاسماً لأي من العنصرين $(1+\sqrt{5}i),(1-\sqrt{5}i)$ وبالتالي العنصر 2 ليس أولياً في R.

التمرين الثالث :

ليكن $I = m \cdot Z$ مثالياً في الحلقـــة Z بحيث $m \geq 2$. نعـــلم أن العـــدد m يكتب بالشكل :

$$m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \;\; ; \;\; r \geq 1$$

حيث :

$$k_1, k_2, \ldots, k_r \in N - \{0\} \quad ;$$

$p_1, p_2, \ldots, p_r$ أعداد أولية مختلفة

(راجع الأعداد الأولية في بحث الأعداد الطبيعية)

والمطلوب :

أثبت أن : $\sqrt{I} = p_1 \cdot p_2 \cdot \ldots \cdot p_r Z = \bigcap_{i=1}^{r} p_i Z$

الحـــل :

$$\forall x \in \sqrt{I} \;\; \Rightarrow \;\; \exists n \in N - \{0\} \;\; : \;\; x^n \in I$$

ومنـــه يوجـــد $z \in Z$ بحيث يكون $x^n = m \cdot z$

أي أن : $x^n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \cdot z$

وبما أن $p_i \ (i=1,2,\dots,r)$ أعداد أولية فإن

$$x = p_1 \cdot p_2 \cdot \dots \cdot p_r z' \ ; \ z' \in Z$$

وبالتالي :

$$\sqrt{I} \subseteq p_1 \cdot p_2 \cdot \dots \cdot p_r Z \qquad (1)$$

ومن جهة أخرى

$$\forall y \in p_1 \cdot p_2 \cdot \dots \cdot p_r Z \ \Rightarrow \ \exists z_1 \in Z : y = p_1 \cdot p_2 \cdot \dots \cdot p_r z_1$$

ومنه :

$$y \in p_i Z \quad \forall i = 1,2,\dots,r$$

وبالتالي :

$$y \in \mathop{\mathrm{I}}_{i=1}^{r} p_i Z$$

أي أن :

$$p_1 \cdot p_2 \cdot \dots \cdot p_r \cdot Z \subseteq \mathop{\mathrm{I}}_{i=1}^{r} p_i Z \qquad (2)$$

ومن جهة ثالثة :

$$\forall u \in \mathop{\mathrm{I}}_{i=1}^{r} p_i Z \Rightarrow \ u \in p_i Z \quad \forall i = 1,2,\dots,r$$

وبالتالي :

$$\forall i = 1,2,\dots,r \ : \ \exists z_i \in Z \ : \ u = p_i z_i$$

وبالتالي :

$$u^r = \prod_{i=1}^{r} p_i \cdot \prod_{i=1}^{r} z_i$$

ومنه : $u^{rk} = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r} \cdot z'' \ ; \ k = \sum_{i=1}^{r} k_i \ ; \ z'' \in Z$

وهـــذا يبين أن

$$u^{rk} \in I$$

ومنـــه :

$$u \in \sqrt{I}$$

أي أن :

$$\bigcap_{i=1}^{r} p_i Z \subseteq \sqrt{I} \qquad (3)$$

من (1)و (2)و (3) نجـــد المطلوب .

التمرين الرابع :

لتكـــن R, R' حلقتين تبديليتين ، وليكـــن $f : R \to R'$ تشاكلاً حلقياً والمطلوب :

١. إذا كان I' مثالياً أوليـــاً في R' فأثبت أن $\overleftarrow{f}(I')$ مثالياً أوليـــاً في R .

٢. إذا كان M' مثالياً أعظمياً في R' فأثبت أن $\overleftarrow{f}(M')$ مثالياً أولياً في R .

٣. أعط مثالاً يكون فيه M' مثالياً أعظمياً في R' لكن المتالي $\overleftarrow{f}(M')$ ليس أعظمياً .

الحـــل :

١. إذا كان I' مثالياً أوليـــاً في R' فـــإن $\overleftarrow{f}(I')$ مثالي في R . وبمـــا أن $f(1_R) = 1_{R'} \notin I'$ ومنـــه $1_R \notin \overleftarrow{f}(I')$ وبالتالـــي $\overleftarrow{f}(I') \neq R$.

من جهـــة أخرى :

$$\forall a, b \in R \quad : \quad a \cdot b \in \overleftarrow{f}(I') \quad \wedge \quad a \notin \overleftarrow{f}(I')$$

فـــإن :

$$f(a) \cdot f(b) = f(a \cdot b) \in I' \quad \wedge \quad f(a) \notin I'$$

ومنـــه : $f(b) \in I'$ وبالتالـــي $b \in \overline{f}(I')$.

٢. بما أن كل مثالـــي أعظمي هو مثالي أولي وبالتالي حسب الطلب السابق يكـــون (٢)محقـــق .

٣. لنأخـــذ التشاكل الحلقي :

$$f : Z \to Q$$

المعرف كمـــا يلي :

$$f(z) = \frac{z}{1} \quad ; \quad \forall z \in Z$$

ولنأخـــذ $M' = \{0\}$ فنجـــد أن M' مثالي أعظمي في Q بينمـــا المثالي $\overline{f}(M') = \{0\}$ ليس أعظمياً في Z .

ملاحظة : إذا كان $f : R \to R'$ تشاكلاً غامـــراً وكان M' مثالياً أعظمياً في R' فإن المثالي $\overline{f}(M')$ أعظمياً في R .

التمرين الخامس :

لتكـــن R منطقـــة تكامليـــة ذات مثاليـــات رئيســـة وليكـــن $a,b \in R - \{0\}$; $I =< a,b >$ مثالياً في R مـــولداً بالعنصرين a,b .

أثبت أنـــه إذا كان المثالي I رئيساً مـــولداً بـــ $d \in R$ (أي $I = dR$) فـــإن d قاسم مشترك أكـــبر لـــ a,b .

الحـــل :

بمـــا أن $I =< a,b >= dR$

فـــإن :

$$a \in I \quad \Rightarrow \quad \exists \quad x \in R \quad : \quad a = dx$$

أي أن : $d|a$

كمـــا أن :

$$b \in I \quad \Rightarrow \quad \exists \quad y \in R \quad : \quad b = dy$$

أي أن : $d|b$

لنفرض أن $d' \in R$ بحيث يكون :

$$(d'|a) \quad \wedge \quad (d'|b)$$

عندئـــذٍ يوجـــد $t,z \in R$ بحيث يكون :

$$(a = d'z) \quad \wedge \quad (b = d't)$$

وبمـــا أن $d \in < a,b >$ فإنـــه يوجـــد $\alpha,\beta \in R$ بحيث يكون :

$$d = \alpha \cdot a + \beta \cdot b$$

ومنـــه :

$$d = \alpha(d' \cdot z) + \beta(d' \cdot t) = d'(\alpha \cdot z + \beta \cdot t) \quad ; \quad \alpha \cdot z + \beta \cdot t \in R$$

وهـــذا يعـــني أن $d|d'$.

إذن d قاسم مشترك أكـــبر لـــ a,b .

تمرينات (٦)

التمرين الأول :

لتكن A مجموعة غير خالية . نعرف على مجموعة أجزائها $P(A)$ القانونيين Δ , I والمطلوب :

١. أثبت أن البنية $(P(A),\Delta,\mathrm{I})$ حلقة تبديلية .

٢. بفرض S مجموعة جزئية غير خالية من المجموعة A ولنأخذ التطبيق :

$$f : P(A) \to P(A)$$

المعرف كما يلي :

$$f(X) = X \,\mathrm{I}\, S \qquad \forall X \in P(A)$$

برهن أن f تشاكل حلقي ، عيّن $\ker f$.

التمرين الثاني :

لتكن $(R,+,\circ)$ حلقة ، ولتكن $a \in U(R)$ ولنأخذ التطبيق :

$$f_a : R \to R$$

المعرف كما يلي :

$$f_a(x) = a \cdot x \cdot a^{-1} \qquad \forall x \in R$$

برهن أن f تماثل حلقي .

التمرين الثالث :

لتكن R حلقة الأعداد الحقيقية ، $M_2(R)$ حلقة المصفوفات الحقيقية المربعة من المرتبة 2 .

ولنأخـــذ العلاقـــة : $f : R \to M_2(R)$

المعرفـــة كمـــا يلـــي :

$$f(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \quad ; \quad \forall x \in R$$

برهـــن أن f تشاكل حلقـــي متباين .

التمرين الرابع :

برهـــن أن في المنطقـــة التكاملية Z/pZ التي مميـــزها العـــدد الأولي p يكون :

$$x^p - x \pmod p$$

لأجل كل عـــدد صحيح x .

التمرين الخامس :

لتكن R حلقـــة تبديلية . أثبت أن القضيتين التاليتين متكافئتان :

I. R منطقـــة تكاملية.

II. المثالي $\{0\}$ بسيطة في R .

التمرين السادس :

ليكن $I = nZ$; $(n > 1)$ مثالياً في حلقـــة المثاليات الرئيسة Z .المطلوب:

١. أثبت صحـــة التكافـــؤ :

العـــدد $p = n$ أولـــي $\Leftrightarrow$ المثالي pZ بسيطة في Z .

٢. أثبت أن المثالـــي pZ (p أولـــي) أعظمـــي .

التمرين السابع :

لتكن R حلقـــة تبديلية ، R حلقـــة المثاليات الرئيسة ولتكن S مجموعـــة

جزئيـــة ضربية في R . أثبت أن الحلقة $S^{-1}R$ هي حلقة مثاليات رئيسة .

التمرين الثامن :

ليكن F حقـــلاً ذا مـــيز غـــير معـــدوم p (p أولـــي) ولتكن :

$$F^p = \{a^p \quad ; \quad a \in F\}$$

المطلوب :

١. أثبت أن F^p حقل جزئـــي من F .

٢. لنأخـــذ العلاقـــة :

$$f : F \to F^p$$

المعرفـــة كمـــا يلـــي :

$$f(x) = x^p \qquad \forall x \in F$$

أثبت أن f تماثـــلاً حقليـــاً .

الفصل السابع

حقـــل الأعـــداد العقديـــة

٧ – ١ بناء حقـــل الأعـــداد العقديـــة :

لتكن R مجموعـــة الأعـــداد الحقيقية . لنعرف على الجـــداء الديكارتـــي $R \times R = R^2$ قانوني تشكيل داخلين $(+)$ ، $(\cdot)$ كمـــا يلـــي :

أيـــاً كان $(a,b),(c,d) \in R^2$:

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

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

فنجـــد أن البنيـــة $(R^2,+,\cdot)$ حقـــل – تأكد من ذلك – . المحايـــد فيـــه بالنسبة لـــ $(+)$ هـــو العنصر $(0,0)$ ، والمحايـــد فيـــه بالنسبة لـــ $(\cdot)$ هو العنصر $(1,0)$ ، ونظير أي عنصر $(x,y) \in R^2$ بالنسبة لـــ $(+)$ هو العنصر $-(x,y)=(-x,-y)$ ، أمـــا مقلوب أي عنصر $(0,0) \neq (x,y) \in R^2$ فهـــو العنصر

$$(x,y)^{-1}=\left(\frac{x}{x^2+y^2} \ , \ \frac{-y}{x^2+y^2}\right)$$

ندعـــو هـــذا الحقـــل بحقـــل الأعـــداد العقديـــة ونرمـــز لـــه بـــ C .

ويصطلح على ترمـــيز العنصر $(0,1) \in C$ بالرمـــز i وعندئـــذ يكون

$$i^2=i\cdot i=(0,1)\cdot(0,1)=(-1,0)$$

٧ – ٢ الشكل المألوف للأعـــداد العقديـــة :

ليكن R حقل الأعداد الحقيقية ، C حقل الأعداد العقدية . لنأخذ العلاقـــة:

$$f : R \to C$$

المعرفـــة كمـــا يلـــي :

$$f(x) = (x,0) \quad ; \quad \forall x \in R$$

فنجـــد أن العلاقـــة f تطبيق متباين لأن :

$$\forall x_1, x_2 \in R \quad : \quad x_1 = x_2 \quad \Leftrightarrow \quad (x_1,0) = (x_2,0)$$
$$\Leftrightarrow \quad f(x_1) = f(x_2)$$

كمـــا أن التطبيق f يحافظ على العمليات (تشاكل حقلي) لأنـــه أيـــاً كان $a,b \in R$ فـــإن :

$$\begin{aligned} f(a+b) &= (a+b,0) \\ &= (a,0)+(b,0) \\ &= f(a)+f(b) \end{aligned}$$

$$\begin{aligned} f(a\cdot b) &= (a\cdot b,0) \\ &= (a,0)\cdot(b,0) \\ &= f(a)\cdot f(b) \end{aligned}$$

كمـــا أن :

$$f(1) = (1,0) \quad , \quad f(0) = (0,0)$$

ولوجـــود هـــذا التشاكل الحقـــلي المتباين يمكننا أن نطابق بين المنطلق R والمستقر الفعلي $\operatorname{Im} f$ بـــأن نطابـــق كل عنصر $(x,0) \in \operatorname{Im} f$ بالعنصر $x \in R$ أي $(x,0) = x$ وبالتالـــي يكون :

$$(1,0) = 1 \quad , \quad (0,0) = 0$$

$$i^2 = (0,1)\cdot(0,1) = (-1,0) = -1$$

وبالتالـــي أياً كان العـــدد العقـــدي $z = (a,b)$ فإن :

$$z=(a,b)=(a,0)+(0,b)$$
$$=a(1,0)+b(0,1)$$
$$=a+ib$$

وندعو الشكل السابق بالشكل الديكارتي للعدد العقدي z وندعو a القسم الحقيقي للعدد العقدي z ونرمز له بـ $\mathrm{Re}(z)$ وندعو b القسم التخيلي للعدد العقدي z ونرمز له بـ $\mathrm{Im}(z)$.

ونقول عن العدد العقدي z أنه حقيقي عندما وفقط عندما $I_m(z)=0$. ونقول عن العدد العقدي z أنه تخيلي بحيث عندما وفقط عندما $(\mathrm{Re}(z)=0) \wedge (\mathrm{Im}(z)\neq 0)$.

ونقول عن العددين $z_1=a_1+ib_1$, $z_2=a_2+ib_2$

إنهما متساويان ونكتب $z_1=z_2$ عندما وفقط عندما $(a_1=a_2)\wedge(b_1=b_2)$

٧ – ٣ مرافق عدد عقدي :

تعريف : ليكن $z=a+ib$ عدداً عقدياً . نعرف مرافق العدد العقدي z بأنه العدد العقدي $a-ib$ ونرمز له بـ $\bar{z}$ أي $\bar{z}=a-ib$.

نتائج وملاحظات :

ليكن $z_1,z_2\in C$, z فإن القضايا التالية تكون صحيحة .

1. $\bar{\bar{z}}=\overline{(\bar{z})}=z$.
2. $z+\bar{z}=2\mathrm{Re}(z)$.
3. $z-\bar{z}=2\mathrm{Im}(z)$.
4. $\overline{z_1\cdot z_2}=\bar{z}_1\cdot\bar{z}_2$.
5. $\overline{(z^{-1})}=(\bar{z})^{-1}$
6. $\overline{z_1\pm z_2}=\bar{z}_1\pm\bar{z}_2$.

٧ ـ ٤ طويلة عـــدد عقـــدي :

تعريف : نعرف طويلة عـــدد عقـــدي $z = a + ib$ ونرمـــز لهـــا بـــ $|z|$ بأنهـــا العـــدد الحقيقي غـــير السالب $\sqrt{z \cdot \bar{z}}$.

أي :

$$|z| = \sqrt{z \cdot \bar{z}} = \sqrt{a^2 + b^2}$$

بملاحظة أن تابع الطويلة في C هـــو ممـــدود تابع القيمـــة المطلقـــة في R يمكننا بسهولة التحقق من الخواص التاليـــة :

1. $\forall z \in C \quad : \quad |z| = 0 \quad \Leftrightarrow \quad z = 0$
2. $\forall z_1, z_2 \in C \quad : \quad |z_1 \cdot z_2| = |z_1| \cdot |z_2|$
3. $\forall z_1, z_2 \subset C \quad : \quad |z_1 + z_2| \leq |z_1| + |z_2|$

٧ ـ ٥ المعنى الهندسي لعـــدد عقدي ـ الشكل المثلثي لعدد عقدي :

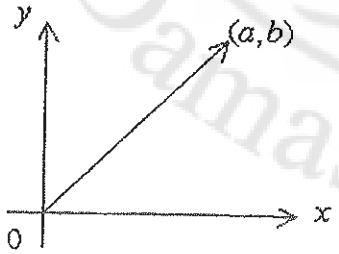
إذا أخـــذنا العلاقـــة :

$$f : C \to R^2$$

المعرفـــة كمـــا يلـــي :

$$f(z = a + ib) = (a,b) \qquad \forall z \in C \quad ; \quad a,b \in R$$

فنجـــد أن f تقابل وبالتالي كل عـــدد عقـــدي يقابله نقطة وحيدة (a,b) في المستوي المنسوب المحـــور الحقيقي والمحـــور التخيلي الذي يدعى بمستوي غاوص . وبالعكس كل نقطـــة (a,b) من مستوي غاوص يقابلها عـــدد عقـــدي $z = a + ib$.



وهـــذا يمكن تمثيل أي عـــدد عقـــدي غـــير صفري $z = a + ib$ بشـــعاع

مبـــدؤه نقطـــة الأصل ، ونـــهايته النقطـــة (a,b) .

وبالتالي يتعين العـــدد العقـــدي z بتعـــين طويلته $r=|z|$ وبتعين الزاوية θ المعرفـــة بالعـــلاقتين :

$$\cos\theta=\frac{a}{r} \quad \wedge \quad \sin\theta=\frac{b}{r} \qquad (*)$$

نرمـــز لمجموعـــة قيم $\theta\in R$ التي تحقق العلاقتين السابقتين بالرمز $\arg(z)$.

ونرمز للعنصر الوحيد $\arg(z)\,\mathrm{I}\,]-\pi,\pi]$ بالرمـــز $Arg(z)$.

وهـــذا إذا كان $z=a+ib$ عـــدداً عقـــدياً غـــير صفري فإن :

$$r^2=a^2+b^2 \quad \wedge \quad a=r\cos\theta \quad \wedge \quad b=r\sin\theta$$

وبالتالي يمكن أن نكتب العـــدد z بالشكل :

$$z=r(\cos\theta+i\sin\theta)$$

الذي يدعـــى الشكل المثلثي للعـــدد العقـــدي z والذي يكتب بالشكل المختزل $z=[r,\theta]$.

نتائـــج وملاحظـــات :

أياً كان $z_1=[r_1,\theta_1]$, $z_2=[r_2,\theta_2]$ فإن :

1. $z_1=z_2 \quad \Leftrightarrow \quad (r_1=r_2)\wedge(\theta_1=\theta_2(\mathrm{mod}\,2\pi))$
2. $z_1\cdot z_2=[r_1\cdot r_2\ ,\ \theta_1+\theta_2]$
3. $\dfrac{z_1}{z_2}=z_1\cdot z_2^{-1}=[\dfrac{r_1}{r_2},\theta_1-\theta_2] \quad ; \quad z_2\neq 0$
4. $z_1^{-1}=[\dfrac{1}{r_1},\theta_1] \quad ; \quad z_1\neq 0$

ويمكن تعميم الخاصة (2) إلى جداء عـــدد منته من الأعـــداد العقـــدية .

فإذا كان $z_i=[r_i,\theta_i] \quad i=1,2,\ldots,n$ فإن :

$$\prod_{i=1}^{n} z_i = z_1 \cdot z_2 \cdot \ldots \cdot z_n = \left[\prod_{i=1}^{n} r_i \quad , \quad \sum_{i=1}^{n} \theta_i\right]$$

٧ – ٦ الشكل الأسي للعـــدد العقـــدي :

لنأخـــذ التابع :

$$f(\theta) = \cos\theta + i\sin\theta \qquad \forall \theta \in R$$

فنجـــد أنـــه أياً كان $\theta, \varphi \in R$ فإن :

$$\begin{aligned} f(\theta+\varphi) &= \cos(\theta+\varphi) + i\sin(\theta+\varphi) \\ &= (\cos\theta \cdot \cos\varphi - \sin\theta \cdot \sin\varphi) + i(\cos\theta \cdot \sin\varphi + \sin\theta \cdot \cos\varphi) \\ &= (\cos\theta + i\sin\theta) \cdot (\cos\varphi + i\sin\varphi) \\ &= f(\theta) \cdot f(\varphi) \end{aligned}$$

$$\begin{aligned} f'(\theta) &= -\sin\theta + i\cos\theta = i(\cos\theta + i\sin\theta) \\ &= if(\theta) \end{aligned}$$

وهـــذا يبرر لنا ترمـــيز $f(\theta)$ بالرمـــز $e^{i\theta}$ ، وبالتالي أي عـــدد عقدي غـــير صفري $z = [r, \theta]$ يمكن كتابته بالشكل : $z = r \cdot e^{i\theta}$ الذي يدعى الشكل الأسي للعـــدد العقـــدي .

ملاحظة:

بمقارنة الشكلين المثلثي والأسي للعـــدد العقـــدي نجـــد أن :

$$z = r \cdot (\cos\theta + i\sin\theta) = r \cdot e^{i\theta}$$

وبالتالي :

$$e^{i\theta} = \cos\theta + i\sin\theta$$

كمـــا أن :

$$e^{-i\theta} = \cos(-\theta) + i\sin(-\theta) = \cos\theta - i\sin\theta$$

وعندئذ نجـــد أن :

$$\cos\theta = \frac{e^{i\theta}+e^{-i\theta}}{2} \quad ; \quad \sin\theta = \frac{e^{i\theta}-e^{-i\theta}}{2}$$

إن الشكل الأســـي للعـــدد العقـــدي يسمح لنا بسهولة التعبير عن عمليتي الضرب والقسمة (القوى ، الجذر) في C .

فإذا كان $z = r \cdot e^{i\theta}$ عـــدداً عقـــدياً غـــير صفري فـــإن :

$$z^{-1} = \frac{1}{z} = \frac{1}{r} \cdot e^{-i\theta}$$

وإذا كان $z_1 = r_1 \cdot e^{i\theta_1}$, $z_2 = r_2 \cdot e^{i\theta_2}$ فإن :

$$z_1 \cdot z_2 = r_1 \cdot e^{i\theta_1} \cdot r_2 \cdot e^{i\theta_2} \qquad (1)$$

$$= r_1 \cdot r_2 \cdot e^{i(\theta_1+\theta_2)}$$

$$\frac{z_1}{z_2} = z_1 \cdot z_2^{-1} = \frac{r_1}{r_2} \cdot e^{i(\theta_1-\theta_2)} \qquad (2)$$

يمكن تعميم الخاصة (١) من أجل عـــدد منته من الأعـــداد العقـــدية . فإذا كانت $k = 1,2,\ldots,n$ $z_k = r_k \cdot e^{i\theta_k}$ أعـــداداً عقـــدية غـــير معدومة فإن :

$$\prod_{k=1}^{n} z_k = \prod_{k=1}^{n} r_k \cdot e^{i\sum_{k=1}^{n}\theta_k}$$

وبحـــالة خاصة عندما $r_k = 1$ $(\forall k = 1,2,\ldots,n)$ فإن :

$$(e^{i\theta})^n = e^{in\theta} \qquad \forall n \in N \quad , \quad \theta \in R$$

تدعى العلاقـــة الأخـــيرة علاقـــة موافر De Moivre . والتي يعبر عنها بالشكل المثلثي :

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta \qquad \forall n \in N, \theta \in R$$

وتجـــدر الإشارة أن لعلاقـــة موافـــر دور هـــام في المثلثات ، فبالاستفادة منهـــا يمكن الحصول على كثير من المتطابقات المثلثية الهـــامة .

استناداً إلى دستور الكرخي – نيوتن نجـــد أن :

$$\cos n\theta + i\sin n\theta = (\cos\theta + i\sin\theta)^n$$
$$= \cos^n\theta + C_n^1 i\cos^{n-1}\theta\cdot\sin\theta - C_n^2\cos^{n-2}\theta\cdot\sin^2\theta + \ldots$$

بمطابقة القسمين الحقيقيين في الطرفين وبمطابقة القسمين التخيليين في الطرفين نحصل على أن :

$$\cos n\theta = \cos^n\theta - C_n^2\cos^{n-2}\theta\cdot\sin^2\theta + C_n^4\cos^{n-4}\theta\cdot\sin^4\theta + \ldots$$
$$\sin n\theta = C_n^1\cos^{n-1}\theta\cdot\sin\theta - C_n^3\cos^{n-3}\theta\cdot\sin^3\theta$$
$$+ C_n^5\cos^{n-5}\theta\cdot\sin^5\theta + \ldots..$$

حيث :

$$C_n^k = \frac{n!}{k!(n-k)!} \quad ; \quad n \le k$$

فمن أجل $n = 3$ نجـــد أن :

$$\cos 3\theta = \cos^3\theta - 3\cos\theta\cdot\sin^2\theta$$
$$\sin 3\theta = 3\cos^2\theta\cdot\sin\theta - \sin^3\theta$$

وأخـــيراً . إذا كان $z = r\cdot e^{i\theta}$ عـــدداً عقـــدياً غـــير صفري فإن جذور العـــدد z والتي عـــددها n هـــي الأعـــداد :

$$z_k = \sqrt[n]{r}\cdot e^{i\frac{\theta+2\pi k}{n}} \quad ; \quad k = 0,1,\ldots,n-1$$

ويبرهن على أن مجموعة الجـــذور من المرتبـــة n للواحـــد زمـــرة جزئيـــة من الزمـــرة $(C^*,\bullet)$.

أن جميع النقاط الممثلة للجذور المختلفة والتي عددها n هي رؤوس مضلع منتظم مرسوم داخل دائرة نصف قطرها $\sqrt[n]{r}$ ومركزها مبدأ الإحداثيات (نقطة الأصل) .

٧ – ٧ بعض المعادلات الشهيرة في C :

١. إن المعادلة $|z| = r$ تمثل محيط الدائرة التي مركزها مبدأ الإحداثيات ونصف قطرها r .

٢. إن المعادلة $|z - z_0| = r$ تمثل محيط الدائرة التي مركزها $z_0(x_0, y_0)$ ونصف قطرها r .

٣. إن المتراجحة $|z - z_0| \le r$ تمثل مجموعة نقاط المستوي الواقعة داخل وعلى محيط الدائرة التي مركزها $z_0(x_0, y_0)$ ونصف قطرها r

٤. إن المتراجحة $|z - z_0| < r$ تمثل مجموعة نقاط المستوي الواقعة داخل الدائرة التي مركزها $z_0(x_0, y_0)$ ونصف قطرها r .

٥. إن المتراجحة $|z - z_0| \ge r$ تمثل مجموعة نقاط المستوي الواقعة خارج وعلى محيط الدائرة التي مركزها $z_0(x_0, y_0)$ ونصف قطرها r

٦. إن المتراجحة $\mathrm{Re}(z) \ge x_0$ تمثل مجموعة نقاط نصف المستوي الأيمن المحدد بالمستقيم $x = x_0$ بما في ذلك نقاط هذا المستقيم .

٧. إن المتراجحة $\mathrm{Im}(z) \ge y_0$ تمثل مجموعة نقاط نصف المستوي العلوي المحدد بالمستقيم $y = y_0$ بما في ذلك نقاط المستقيم .

٨. إن المتراجحة $\mathrm{Re}(z) < x_0$ تمثل مجموعة نقاط المستوي الأيسر المحدد بالمستقيم $x = x_0$ ما عدا نقاط هذا المستقيم .

٩. إن المتراجحة $\mathrm{Im}(z) < y_0$ تمثل مجموعة نقاط المستوي السفلي المحدد

بالمستقيم $y = y_0$ ما عـــدا نقاط المستقيم .

تمرينات محلولـــــة

التمرين الأول :

أوجـــد الجـــذور التكعيبية للعـــدد العقـــدي $z = 8i$ ثم برهـــن أن النقاط الممثلـــة لهـــذه الجـــذور هـــي رؤوس لمثلث متساوي الأضلاع مرسوم في دائـــرة عين مركزهـــا ونصف قطرهـــا .

الحـــل : إن :

$$z = 8i = [8, \frac{\pi}{2}] = 8e^{i\pi/2}$$

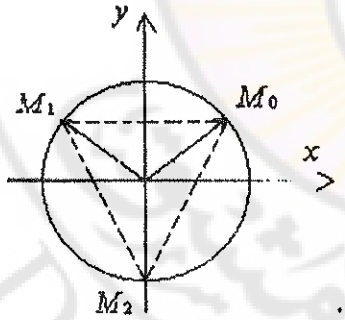
فالجـــذور التكعيبية الثلاثـــة لـــ z هـــي :

$$z_k = \sqrt[3]{8} \cdot e^{i\frac{\frac{\pi}{2}+2\pi k}{3}} \qquad ; \qquad k = 0,1,2$$

وبالتالـــي :

$$z_0 = [2, \frac{\pi}{6}] \quad , \quad z_1 = [2, \frac{5\pi}{6}] \quad , \quad z_2 = [2, \frac{3\pi}{2}]$$

إذا كانت M_0, M_1, M_2 النقـــاط الممثلة للجـــذور z_0, z_1, z_2 على الترتيب فنجـــد بحساب بسيط أن المثلث $M_0M_1M_2$ متساوي الأضلاع وهـــو مرسوم في دائـــرة مركزها مبـــدأ الإحداثيـــات و نصف قطرهـــا 2 .



التمرين الثاني :

انطلاقـــاً من منشور كل من $\cos\theta$, $\sin\theta$, e^{θ} استنتج الشكل الأسي للعـــدد العقـــدي .

الحـــل : إن :

$$\cos\theta = 1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \frac{\theta^6}{6!} + \dots$$

$$\sin\theta = \frac{\theta}{1!} - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} + \dots$$

$$e^{\theta} = 1 + \frac{\theta}{1!} + \frac{\theta^2}{2!} + \frac{\theta^3}{3!} + \dots$$

وباستبدال $i\theta$ بـــ θ في المنشور الأخـــير نجـــد أن :

$$e^{i\theta} = 1 + \frac{i\theta}{1!} + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \dots$$

$$= 1 + i\frac{\theta}{1!} - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \dots$$

كمـــا أن :

$$\cos\theta + i\sin\theta = 1 + i\frac{\theta}{1!} - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + \dots$$

بمقارنة المنشور الأخـــير مع منشور $e^{i\theta}$ نجـــد أن :

$$\cos\theta + i\sin\theta = e^{i\theta}$$

ومنـــه :

$$r\cdot(\cos\theta + i\sin\theta) = r\cdot e^{i\theta}$$

أي أن :

$$z = r\cdot e^{i\theta}$$

تمرينات (٧)

التمرين الأول :

ليكن z عـــدداً عقـــدياً بحيث $|z|=1$. برهـــن صحـــة القضيتين الآتيتين

1. $z^{-1}=\bar{z}$
2. $\forall z_0 \in C \quad : \quad |z-z_0|=|z_0\bar{z}-1|$

التمرين الثاني :

احسب كلاً من :

$$\cos 4\theta \quad , \quad \sin 4\theta \quad , \quad \cos 5\theta \quad , \quad \sin 5\theta$$

بدلالـــة قوى $\sin\theta$, $\cos\theta$.

التمرين الثالث :

أوجـــد مجموعـــة الأعـــداد العقـــدية z في كل من الحالات :

1. $\bar{z}=z^2$
2. $|z|=|z^{-1}|=|1-z|$
3. $z^6+z^3+1=0$
4. $R_e(z-1)=|z|$

التمرين الرابع :

ليكن $z_1, z_2 \in C$ بحيث $|z_1|=|z_2|=1$, $z_1 \neq z_2$. برهـــن أنـــه أياً كان العـــدد العقـــدي z فإن :

$$\frac{z+z_1\cdot z_2\cdot\bar{z}-(z_1+z_2)}{z_1-z_2}\in iR$$

التمرين الخامس :

ليكن $z_1, z_2 \in C$ بحيث $z_2 \neq 0$. برهـــن صحـــة التكافـــؤ :

$$|z_1 + z_2| = |z_1 - z_2| \quad \Leftrightarrow \quad (\exists \lambda \in R \quad : \quad z_2 = i\lambda z_1)$$

الفصل الثامن

حلقـــة الحـــدوديات

(كثيرات الحـــدود)

٨ – ١ بناء حلقـــة الحـــدوديات :

لتكن R حلقـــة تبديلية واحـــدية ولتكن S مجموعـــة كل المتتاليات التي حـــدودها من R والتي جميـــع حـــدودها معـــدومة (تساوي 0_R) ما عـــدا عـــدد منته منهـــا ، ولنعرف على المجموعـــة غـــير الخاليـــة S قانوني تشكيل داخليين $(+)$, $(\cdot)$ كمـــا يلـــي :

$$\forall a=(a_0,a_1,\dots,a_n,\dots) \quad , \quad b=(b_0,b_1,\dots,b_n,\dots)\in S$$

$$a+b=(a_0,a_1,\dots,a_n,\dots)+(b_0,b_1,\dots,b_n,\dots)$$

$$=(a_0+b_0,a_1+b_1,\dots,a_n+b_n,\dots)$$

$$a\cdot b=(a_0,a_1,\dots,a_n,\dots)\cdot(b_0,b_1,\dots,b_n,\dots)$$

$$=(t_0,t_1,\dots,t_n,\dots)$$

حيث : $t_i=\sum_{j+k=i} a_j\cdot b_k \qquad \forall i=0,1,\dots$

فنجـــد أن $(S,+,\cdot)$ حلقـــة تبديلية واحـــدية

- صفرهـــا هـــو المتتالية $0_S=(0_R,0_R,\dots,0_R,\dots)$
- واحدهـــا هـــو المتتالية $1_S=(1_R,0_R,\dots,0_R,\dots)$ وأن $1_S\neq 0_S$
- ونظير العنصر $a=(a_0,a_1,\dots,a_n,\dots)$ بالنسبة لـــ $(+)$ هو المتتالية

$$\cdots a = -(a_0, a_1, \ldots, a_n, \ldots) = (-a_0, -a_1, \ldots, -a_n, \ldots) \in S$$

تدعى الحلقة $(S,+,\cdot)$ حلقة الحدوديات على الحلقة R .

لنعرف على S القانون التشكيل الخارجي الذي مجموعة مؤثراته R :

$$\forall \alpha \in R \quad , \quad \forall a = (a_0, a_1, \ldots, a_n, \ldots) \in S \quad :$$

$$\alpha \cdot a = \alpha \cdot (a_0, a_1, \ldots, a_n, \ldots) = (\alpha \cdot a_0, \alpha \cdot a_1, \ldots, \alpha \cdot a_n, \ldots)$$

فنجد أنه أياً كان $\alpha, \beta \in R$ وأياً كان $a, b \in S$ فإن :

1. $1_R \cdot a = a$
2. $(\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a$
3. $\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b$
4. $(\alpha \cdot \beta) \cdot a = \alpha \cdot (\beta \cdot a)$

٨ ـ ٢ الشكل المألوف للحدودية :

لتكن R حلقة تبديلية واحدية ولتكن S حلقة الحدوديات على R

ولنأخذ العلاقة :

$$f : R \to S$$

المعرفة كما يلي :

$$f(a) = (a, 0_R, \ldots) \qquad \forall a \in R$$

فنجد أن العلاقة f تطبيق متباين لأن :

$$\forall a_1, a_2 \in R \quad : \quad a_1 = a_2 \quad \Leftrightarrow \quad (a_1, 0_R, \ldots) = (a_2, 0_R, \ldots)$$

$$\Leftrightarrow \quad f(a_1) = f(a_2)$$

كما أن التطبيق f تشاكل حلقي (يحافظ على العمليات) لأن :

$$\forall a_1, a_2 \in R \quad : \quad f(a_1 + a_2) = (a_1 + a_2, 0_R, \ldots)$$

$$= (a_1, 0_R, \ldots) + (a_2, 0_R, \ldots)$$

$$= f(a_1) + f(a_2)$$

$$\begin{aligned} f(a_1 \cdot a_2) &= (a_1 \cdot a_2, 0_R, \ldots) \\ &= (a_1 \cdot 0_R, \ldots) \cdot (a_2, 0_R, \ldots) \\ &= f(a_1) \cdot f(a_2) \end{aligned}$$

كما أن :

$$f(1_R) = (1_R, 0_R, \ldots)$$

ولوجود هذا التطبيق المتباين المتشاكل يمكن أن نطابق بين عناصر الحلقة R وبين المستقر الفعلي $\operatorname{Im} f$ بأن نطابق أي عنصر $a \in R$ بصورته وفق f أي نطابق العنصر $a \in R$ بالعنصر $(a, 0_R, \ldots) \in S$.

لنرمّز العنصر $(0_R, 0_R, \ldots, 1_R, 0_R, \ldots)$ من الحلقة S بالرمز δ_k أي أن δ_k هي متتالية من S التي جميع حدودها أصفار ما عدا الحد الذي دليله k فهو 1_R .

ولنرمّز العنصر $\delta_1 = (0_R, 1_R, 0_R, \ldots)$ بالرمز x فيكون :

$$\delta_0 = (1_R, 0_R, \ldots) = 1_S$$

$$\delta_1 = (0_R, 1_R, 0_R, \ldots) = x$$

$$\delta_2 = (0_R, 0_R, 1_R, 0_R, \ldots) = \delta_1 \cdot \delta_2 = x^2$$

$$\ldots \quad \ldots\ldots \quad \ldots\ldots \quad \ldots\ldots \quad \ldots\ldots \quad \ldots\ldots \quad \ldots\ldots \quad \ldots\ldots$$

$$\delta_n = (0_R, 0_R, \ldots, 0_R, 1_R, 0_R, \ldots) = x^n$$

وبالتالي أياً كان العنصر $(a_0, a_1, \ldots, a_n, 0_R, \ldots)$ من حلقة الحدوديات S فإن :

$$\begin{aligned} (a_0, a_1, \ldots, c_n, 0_R, \ldots) &= a_0(1_R, 0_R, \ldots) + a_1(0_R, 1_R, 0_R, \ldots) + \ldots \\ &\quad + \ldots + a_n \cdot (0_R, 0_R, \ldots, 1_R, 0_R, \ldots) + \ldots \end{aligned}$$

$$= a_0 \cdot 1 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_n \cdot x^n + \ldots$$
$$= \sum_{i \geq 0} a_i \cdot x^i$$

وهو الشكل النموذجي المألوف للحدودية (لكثير الحدود) . تدعى العناصر $a_0, a_1, \ldots, a_n, \ldots$ بمعاملات الحدودية وندعو x متحولاً . مما سبق يمكننا أن نرمّز حلقة الحدوديات على حلقة واحدية تبديلية R بالرمز $R[x]$.

نتائج وملاحظات :

١. إن $R \subseteq R[x]$ وبالتالي كل عنصر من الحلقة R هو حدودية ندعوها الحدودية الثابتة وبحالة خاصة ندعو 0_R الحدودية الصفرية .

٢. إذا كانت R منطقة تكاملية فإن $R[x]$ تكون منطقة تكاملية .

٣. إذا كانت R حقلاً فإن $R[x]$ منطقة تكاملية وليست حقلاً .

٨ – ٣ درجة الحدوديّة :

تعريف (١) : لتكن $P = \sum_{k \geq 0} a_k \cdot x^k$ حدودية من $R[x]$. نسمي أكبر عدد صحيح n من أجله $a_n \neq 0_R$ بدرجة الحدودية P ونكتب $\deg P = n$. ونصطلح على أن $\deg 0_R = -\infty$.

تعريف (٢) : لتكن $P = \sum_{k \geq 0} a_k \cdot x^k$ حدودية غير صفرية من $R[x]$ ولتكن $\deg P = n$. نسمي الحد $a_n \cdot x^n$ الحد الأعلى في P وإذا كان $a_n = 1$ فنقول عن P إنها حدودية واحدية .

مبرهنة :

إذا كانت $P,Q \in R[x]$ فإن :

١. $\deg(P+Q) \le \max(\deg P, \deg Q)$.

٢. $\deg(P \cdot Q) \le \deg P + \deg Q$.

٣. إذا كانت R منطقة تكاملية فإن :

$$\deg(P \cdot Q) = \deg P + \deg Q$$

الإثبات :

إذا كان $(Q = 0_R) \vee (P = 0_R)$ فمن الواضح أن المبرهنة صحيحة .

لنفرض إذن أن : $(\deg Q = m) \wedge (\deg P = n)$ $n,m \ge 0$ وليكن :

$$P = \sum_{k=0}^{n} a_k \cdot x^k \quad ; \quad a_n \ne 0_R$$

$$Q = \sum_{k=0}^{m} b_k \cdot x^k \quad ; \quad b_m \ne 0_R$$

١. وليكن $r = \max(n,m)$ عندئذٍ يكون :

$$P + Q = \sum_{k=0}^{r} (a_k + b_k) \cdot x^k$$

وبالتالي :

$$\deg(P+Q) \le r$$

أي أن :

$$\deg(P+Q) \le \max(\deg P, \deg Q)$$

٢. حسب تعريف الضرب في $R[x]$ يكون :

$$P \cdot Q = \sum_{k \ge 0} c_k \cdot x^k \quad ; \quad c_p = \sum_{t+s=p} a_t \cdot b_s$$

وبالتالي : $\deg(P \cdot Q) \le \deg P + \deg Q$

٣. إذا كانت R منطقـــة تكاملية فإنه من أجل $(b_m \neq 0_R) \wedge (a_n \neq 0_R)$

فإن $a_n \cdot b_m \neq 0_R$ وبالتالي :

$$\deg(P \cdot Q) = \deg P + \deg Q$$

ملاحظة هامة : إن الدور الأكـــبر للحـــدوديات هـــي الحـــدوديات على حقـــل F ولذلك في الفقرات التاليـــة في هـــذا الفصل سنتعامل مع حلقة F ونرمـــز لهـــا بـــ $F[x]$ مع الانتباه أن $F[x]$ منطقـــة تكامليـــة .

٨ – ٤ قابليـــة القسمة في $F[x]$:

تعريف : لتكن A,B حـــدوديتين من الحلقـــة $F[x]$ ، $B \neq 0_R$. نقول إن B قاسم لـــ A ونكتب $B|A$ إذا وفقـــط إذا وجـــدت $Q \in F[x]$ بحيث $A = Q \cdot B$.

مبرهنة :

إذا كانت A,B حـــدوديتين غـــير صفريتين من $F[x]$ وكان $(B|A) \wedge (A|B)$ فإنـــه يوجـــد $\lambda \in F - \{0\}$ بحيث $A = \lambda \cdot B$.

الإثبات :

$$A|B \quad \Leftrightarrow \quad \exists Q_1 \in F[x] \quad : \quad B = Q_1 \cdot A$$

$$B|A \quad \Leftrightarrow \quad \exists Q_2 \in F[x] \quad : \quad A = Q_2 \cdot B$$

وبالتالي :

$$A = Q_2 \cdot Q_1$$

ومنـــه :

$$Q_2 \cdot Q_1 = 1_F$$

وبالتالي : $\deg(Q_2 \cdot Q_1) = 0$

وبالتالـــي :

$$\deg Q_2 + \deg Q_1 = 0$$

وبالتالـــي :

$$\exists \lambda, \lambda' \in F - \{0_F\} \quad : \quad Q_2 = \lambda \quad \wedge \quad Q_1 = \lambda'$$

أي أن :

$$\exists \lambda \in F - \{0_F\} \quad : \quad A = \lambda \cdot B$$

تعريف : لتكن $A, B \in F[x]$ و $A \neq 0_F$, $B \neq 0_F$. نقول عن A و B إنهمـــا شريكان إذا وفقـــط إذا وجـــد $\lambda \in F - \{0_F\}$ بحيث $A = \lambda \cdot B$.

نتيجة : إذا كان $A, B \in F[x]$ فإن :

$$A, B \text{ شريكان في } F[x] \quad \Leftrightarrow \quad (A|B) \quad \wedge \quad (B|A)$$

مبرهنة: (خوارزميـــة القسمة في $F[x]$).

إذا كانت $A, B \in F[x]$ وكان $B \neq 0_F$ فإنـــه توجـــد حـــدوديتين واحـــدتين $Q, R \in F[x]$ بحيث يكون :

$$A - Q \cdot B + R \qquad \wedge \qquad \deg R < \deg B \qquad (*)$$

الإثبات : لنبرهـــن أولاً الوجـــود .

إذا كان $\deg A = -\infty$ فإن $A = 0_F$ وبالتالي يوجـــد في $F[x]$ الحدوديتان $Q = R = 0_F$ اللتان تحققان (*) .

إذا كان $\deg A = 0$ فإن $A = \alpha \in F - \{0\}$ وبالتالي نكون أمام الحالات التاليـــة :

I. إذا كان $\deg B = 0$ فإن $B = \beta \in F - \{0\}$ وبالتالي يوجد في

$F[x]$ الحـــدوديتان $Q=\alpha\cdot b^{-1}$, $R=0_F$ اللتان تحققان (*)

II. إذا كان $\deg B=m>0$ فإنـــه يوجـــد في $F[x]$ الحـــدوديتان $Q=0_F$ ، $R=A$ اللتان تحققان (*) .

لنفرض الآن أن من أجـــل كل حـــدودية C من $F[x]$ درجتهـــا أقل من n يوجـــد في $F[x]$ الحـــدوديتان Q_1,R_1 اللتان تحققان (*) أي :

$$C=Q_1\cdot B+R_1 \quad ; \quad \deg R_1<\deg B$$

ليكن $\deg A=n$ فإنـــه إذا كان $\deg A<\deg B$ فإنـــه يوجـــد في $F[x]$ الحـــدوديتان $Q=0_F$, $R=A$ اللتـــان تحققـــان (*)

أمـــا إذا كان $\deg A\geq\deg B$ فلنفترض أن :

$$A=\sum_{k=0}^{n}a_k\cdot x^k \quad ; \quad a_n\neq 0_F$$

$$B=\sum_{k=0}^{m}b_k\cdot x^k \quad ; \quad b_m\neq 0_F$$

حيث $n\geq m$

وعندئذٍ تكون :

$$\deg(A-a_n\cdot b_m^{-1}\cdot x^{n-m}\cdot B)<n$$

فحسب الفرض الاستقرائي يوجـــد في $F[x]$ حـــدوديتان Q_1,R_1 بحيث يكون :

$$C=(A-a_n\cdot b_m^{-1}\cdot x^{n-m}\cdot B)=Q_1\cdot B+R_1 \quad ; \quad \deg R_1<\deg B$$

ومنـــه :

$$A=(a_n\cdot b_m^{-1}\cdot x^{n-m}+Q_1)\cdot B+R_1 \quad ; \quad \deg R_1<\deg B$$

أي أن الحـــدوديتان : $R_1=R$, $Q=a_n\cdot b_m^{-1}\cdot x^{n-m}+Q$

تحققـــان (*) .

وأخـــيراً لنبرهـــن الوحـــدانية .

لنفرض أنـــه يوجـــد في $F[x]$ الحـــدوديات Q,Q',R,R' بحيث يكون

$$A = Q\cdot B + R = Q'\cdot B + R' \quad ;$$

$$(\deg R < \deg B) \quad \wedge \quad (\deg R' < \deg B)$$

عندئذٍ يكون :

$$(Q-Q')\cdot B = R' - R \qquad (1)$$

وبالتالـــي :

$$\deg(R'-R) < \max(\deg r', \deg r) < \deg B$$

$$\deg((Q-Q')\cdot B) = \deg(Q-Q') + \deg B$$

ومنـــه :

$$\deg(Q-Q') + \deg B < \deg B$$

وهـــذه المتراجحـــة تتحقق فقط عندما يكون :

$$\deg(Q-Q') = -\infty$$

أي : $Q-Q' = 0_F$ وحسب العلاقـــة (١) سيكون $R'-R = 0_F$

إذن :

$$Q = Q' \quad \wedge \quad R = R'$$

تعريف : نقول عن العنصر $\alpha \in F$ إنـــه صفر (جـــذر) للحدودية $P(x) \in F[x]$ عندما وفقط عندما يكون $P(\alpha) = 0_F$.

مبرهنة : (مبرهنـــة الباقي) .

إذا كانت $A,B \in F[x]$ بحيث $\alpha \in F$; $B = x - \alpha$ فـــإن باقـــي قسمة A على B هـــو $R = A(\alpha)$.

الإثبات : حسب خوارزمية القسمة في $F[x]$ يوجد $Q,R \in F[x]$ بحيث يكون :

$$A = Q\cdot(x-\alpha)+R \quad ; \quad \deg R < \deg(x-\alpha) = 1$$

وهذا يعني أن $R \in F$ (حدودية ثابتة) وبالتالي من أجل $x=\alpha$ نجد

$$A(\alpha) = Q\cdot 0_F + R$$

ومنه $$R = A(\alpha)$$

مبرهنة:

إذا كانت $A \in F[x]$ وكان $\alpha \in F$ فإن

$$[\ F[x] \text{ في } A \text{ تقسم } (x-\alpha)\ ] \Leftrightarrow A(\alpha) = 0_F$$

الإثبات : ليكن $A(\alpha) = 0_F$.

حسب مبرهنة خوارزمية القسمة في $F[x]$ وحسب مبرهنة الباقي نجد

$$A = Q\cdot(x-\alpha) + A(\alpha)$$

وبما أن $A(\alpha) = 0_F$ فإن :

$$A = Q\cdot(x-\alpha)$$

وهذا ما يبرهن على أن $(x-\alpha)$ تقسم A في $F[x]$.

لنفرض الآن $(x-\alpha)$ تقسم A في $F[x]$ وبالتالي يوجد في $F[x]$ حدودية Q بحيث يكون $A = Q\cdot(x-\alpha)$. بوضع $x=\alpha$ نحصل على أن : $$A(\alpha) = Q(\alpha)\cdot 0_F = 0_F$$

وهذا يثبت أن α جذر للحدودية A .

مبرهنة:

إن حلقة الحدوديات $F[x]$ حلقة رئيسة .

الإثبات : ليكن I مثالياً غير صفرياً في الحلقة $F[x]$ ولنبرهن على أن I مثالي رئيس في $F[x]$.

ليكن $P_0 \in I - \{0\}$ بحيث :

$$\deg P_0 = \min\{\deg P \quad ; \quad P \in I - \{0\}\}$$

عندئذٍ بملاحظة أن :

$$P_0 \cdot F[x] = \{P_0 \cdot Q \quad ; \quad Q \in F[x]\}$$

نجد أن :

$$P_0 \cdot F[x] \subseteq I \qquad (1)$$

من جهة أخرى . أياً كان $P \in I$ فإنه توجد $Q, R \in F[x]$ بحيث

$$P = Q \cdot P_0 + R \qquad , \qquad \deg R < \deg P_0$$

إن $R = 0$ لأنه إذا كان $R \neq 0$ يكون :

$$R = P - Q P_0 \quad \in I \quad \wedge \quad \deg R < \deg P_0$$

وهذا يناقض تعريف P_0 . إذاً $R = 0$ وبالتالي :

$$P = Q \cdot P_0 \qquad ; \quad Q \in F[x]$$

أي أن :

$$P \in P_0 F[x]$$

ومنه :

$$I \subseteq P_0 F[x] \qquad (2)$$

من (١) و (٢) نجد أن :

$$I = P_0 \cdot F[x]$$

أي أن المثالي I رئيس .

تعريف : لتكن $A_1, A_2, \ldots, A_n$ حدوديات غير صفرية من $F[x]$.

نعرف القاسم المشترك الأكبر للحدوديات $(i=1,2,\dots,n)$ A_i بأنها الحدودية الواحدية $D \in F[x]$ التي تحقق الشرطين التاليين :

١. $D \setminus A_i \quad \forall i=1,2,\dots,n$

٢. إذا كان $D' \in F[x]$ بحيث $D' \setminus A_i \ (i=1,2,\dots,n)$ فإن $D' \setminus D$ ونكتب $d(A_1, A_2, \dots, A_n) = D$.

نتيجة: من المبرهنة السابقة والتعريف السابق نستنتج أن القاسم المشترك الأكبر D يتحقق :

$$D \cdot F[x] = A_1 \cdot F[x] + A_2 \cdot F[x] + \dots + A_n \cdot F[x]$$

وبالتالي يوجد $\alpha_i \in F[x] \quad i=1,2,\dots,n$ بحيث :

$$D = \alpha_1 \cdot A_1 + \alpha_2 \cdot A_2 + \dots + \alpha_n \cdot A_n$$

تعريف : لتكن $A_1, A_2, \dots, A_n$ حدوديات غير صفرية من $F[x]$. نقول إن الحدوديات $(i=1,2,\dots,n)$ A_i أنها أولية فيما بينها إذا وفقط إذا كان $d(A_1, A_2, \dots, A_n) = 1$.

نتيجة :

$$[\text{أولية فيما بينها } A_i; i=1,2,\dots,n] \Leftrightarrow d(A_1, A_2, \dots, A_n) = 1$$

$$\Leftrightarrow F[x] = A_1 F[x] + A_2 F[x] + \dots + A_n F[x]$$

$$\Leftrightarrow \exists \alpha_i \in F[x] \quad : \quad \sum_{i=1}^{n} \alpha_i \cdot A_i = 1$$

ملاحظة: يمكن استخدام خوارزمية إقليدس المعممة المدرجة في الفصل الرابع لإيجاد القاسم المشترك الأكبر للحدوديتين A, B ولتعيين $\alpha, \beta \in F[x]$ بحيث :

$$D = \alpha \cdot A + \beta \cdot B$$

مثال : لتكن لدينا الحـــدوديتين :

$$A = x^5 + x^4 + 2\ x^3 + 2\ x^2 - x - 1$$

$$B = x^4 + x^3 + 2\ x^2 + x - 1$$

أوجـــد D القاســـم المشـــترك الأكـــبر للحـــدوديتين A, B ثـــم عيّن $\alpha, \beta \in F[x]$ بحيث يكون : $D = \alpha \cdot A + \beta \cdot B$

الحـــل:

k	R_k	Q_k	α_k	P_k
0	$x^5+x^4+2x^3+2x^2-x-1$	–	1	0
1	$x^4+x^3+2x^2+x-1$	x	0	1
2	x^2-1	x^2+x+3	1	$-x$
3	$2x+2$	$\frac{1}{2}x-\frac{1}{2}$	$-x^2-x-3$	x^3+x^2+3x+1
4	0			

إن : $D = \frac{1}{2}(2x+2) = x+1$

كمـــا أن :

$$2x + 2 = (-x^2 - x - 3) \cdot A + (x^3 + x^2 + 3x + 1) \cdot B$$

ومنـــه :

$$x + 1 = \frac{1}{2}(-x^2 - x - 3) \cdot A + \frac{1}{2}(-x^3 - x^2 - 3x + 1) \cdot B$$

تعريف : لتكن $A_1, A_2, \ldots, A_n$ حـــدوديات غـــير صفريـــة من الحلقـــة $F[x]$.

نعرف المضاعف المشترك الأصغر للحدوديات $A_1, A_2, \ldots, A_n$ بأنه الحدودية $C \in F[x]$ التي تحقق الشرطان :

١. $A_i | C \quad \forall i = 1,2,\ldots,n$

٢. إذا كانت $C' \in F[x]$ بحيث $A_i | C' \quad \forall i = 1,2,\ldots,n$ فإن $C | C'$

تعريف : نقول عن الحدودية $P \in F[x]$ إنها غير قابلة للتحليل في $F[x]$ إذا وفقط إذا تحقق الشرطان :

1. $\deg P > 0$
2. $\forall Q \in F[x] : Q | P \Rightarrow (\deg Q = \deg P) \vee (\deg Q = 0)$

نتائج وملاحظات :

١. إذا كانت $P \in F[x]$ وكانت $\deg P = 1$ فإن P غير قابلة للتحليل في $F[x]$.

٢. إذا كانت $P \in F[x]$ حدودية غير قابلة للتحليل في $F[x]$ وكانت $A \in F[x]$ فإن :

A, P أوليتان فيما بينهما $\Leftrightarrow$ P لا تقسم A .

(لاحظ أن $d(A,P)$ تقسم P) .

٣. إذا كانت $P \in F[x]$ حدودية غير قابلة للتحليل في $F[x]$ وكانت $A_i \in F[x] \quad ; \quad i = 1,2,\ldots,n$ فإن :

P تقسم الجداء $A_1 \cdot A_2 \cdot \ldots \cdot A_n \Leftrightarrow P$ تقسم إحدى الحدوديات A_i

مبرهنة:

إذا كانت $P \in F[x]$ حدودية وكانت $1 < \deg P \leq 3$ فإن الحدودية P قابلة للتحليل في $F[x]$ عندما وفقط عندما يوجد لـ P جذر في F

الإثبات :

لنفرض أن $P(x)$ قابلة للتحليل في $F[x]$ عندئذٍ يوجد $Q(x) \in F[x]$ بحيث يكون :

$$P(x) = (x-\alpha)\cdot Q(x) \quad ; \quad 0 < \deg Q < \deg P \quad ; \quad \alpha \in F$$

ومنه $P(\alpha) = 0_F$ وهذا يعني أن α جذر لـ $P(x)$ في F .

وبالعكس ، إذا كان $\alpha \in F$ جذر لـ $P(x)$ فإن الحدودية تقبل القسمة على $(x-\alpha)$ وبالتالي توجد $Q(x)$ من $F[x]$ بحيث يكون :

$$P(x) = (x-\alpha)\cdot Q(x) \quad ; \quad 0 < \deg Q < \deg P$$

وهذا يعني أن P قابلة للتحليل في $F[x]$.

تعريف:

لتكن $P(x)$ حدودية من الحلقة $F[x]$ ، $\alpha \in F$. نقول عن α أنه جذر مضاعف من المرتبة k عندما وفقط عندما $(x-\alpha)^k$ تقسم P و $(x-\alpha)^{k+1}$ لا تقسم P . ونقول عن α أنه جذر بسيط لـ P إذا كان α جذراً من المرتبة ١ للحدودية P .

مبرهنة:

إذا كانت P حدودية من $F[x]$ وكان $\alpha \in F$ فإن القضيتين التاليتين متكافئتان :

١. يوجد $Q \in F[x]$ و $Q(\alpha) \neq 0$ بحيث $P = (x-\alpha)^k \cdot Q$

٢. α جذر مضاعف من المرتبة k للحدودية P .

الإثبات:

$(1 \Rightarrow 2)$: حسب الفرض $(x-\alpha)^k$ تقسم P ولنفرض جدلاً أن $(x-\alpha)^{k+1}$

تقسم P عندئـــذٍ $(x-\alpha)^{k+1}$ تقسم $Q(\alpha)(x-\alpha)^k$ وبملاحظة أن :

$$Q=(x-\alpha)\cdot Q_1+Q(\alpha)$$

نجـــد أن $Q(\alpha)=0$ وهـــذا يناقض الفرض .

إذاً α جـــذر مضاعف من المرتبـــة k للحـــدودية P .

٨ – ٥ مشتق الحـــدودية :

تعريف :

لتكن $P(x)=\sum_{k\geq 0} a_k\cdot x^k$ حـــدودية من الحلقـــة $F[x]$. نعرف مشتق $P(x)$ ونرمـــز له بـــ $P'(x)$ بأنـــه الحـــدودية :

$$P'(x)=\sum_{k\geq 0}(k+1)\cdot a_{k+1}\cdot x^k$$

نتائـــج وملاحظات :

١. إذا كان مـــيز الحقـــل F معدومـــاً فإن :

$$\deg P'=\deg P-1 \qquad \forall \deg P\geq 1$$

$$P'=0 \qquad ; \qquad \deg P=0$$

٢. أياً كان $P,Q\in F[x]$ فإن :

$$(P+Q)'=P'+Q'$$

$$(\lambda\cdot P)'=\lambda\cdot P' \qquad \forall\lambda\in F$$

$$(P\cdot Q)'=P'\cdot Q+P\cdot Q'$$

مبرهنة:

إذا كانت P حـــدودية من $F[x]$ وكان $\alpha\in F$ جـــذراً مضاعفاً من المرتبة k للحـــدودية P فإن :

١. إذا كان $k=1$ فإن α ليس جـــذراً للمشتق P' .

٢. إذا كان $k>1$ وكان مميز الحقـــل F معـــدوماً فإن α يكون جـــذراً مضاعفاً من المرتبـــة $(k-1)$ للمشتق P' .

الإثبات :

١. بما أن $\alpha \in F$ جـــذر من المرتبة ١ للحـــدودية P فإنه توجد $Q \in F[x]$ لا تقبل القسمة على $(x-\alpha)$ بحيث :

$$P(x)=(x-\alpha)\cdot Q(x)$$

باشتقاق الطرفين نحصل على :

$$P'(x)=Q(x)+(x-\alpha)\cdot Q'(x)$$

وبالتالي :

$$P'(\alpha)=Q(\alpha)\neq 0_F$$

أي أن α ليس جـــذراً للمشتق $P'(x)$.

٢. بما أن $\alpha \in F$ جذر من المرتبة $k>1$ للحدودية P فإنه توجد $Q \in F[x]$ لا يقبل القسمة على $(x-\alpha)$ بحيث :

$$P(x)=(x-\alpha)^k\cdot Q(x)$$

باشتقاق الطرفين نحصل على :

$$\begin{aligned}P(x)&=k\cdot(x-\alpha)^{k-1}\cdot Q(x)+(x-\alpha)^k\cdot Q'(x)\\&=(x-\alpha)^{k-1}\cdot[mQ(x)+(x-\alpha)\cdot Q'(x)]\\&=(x-\alpha)^{k-1}\cdot A(x)\quad;\quad A(x)=m\cdot Q(x)+(x-\alpha)\cdot Q'(x)\end{aligned}$$

إن الحـــدودية A لا تقبل القسمة على $(x-\alpha)$ لأنه إذا كانت A تقبل القسمة على $(x-\alpha)$ فإنه توجـــد $B(x)$ من $F[x]$ بحيث يكون

$$m \cdot Q(x) = (x-\alpha) \cdot B(x)$$

وبالتالي يكون

$$m \cdot Q(\alpha) = 0_F$$

لكن $0_F \neq Q(\alpha) \in F$ وبالتالي أصبح لدينا

$$m \cdot Q(\alpha) = 0_F \quad \wedge \quad (0_F \neq Q(\alpha) \in F)$$

وهـذا يناقض كون أن الحقـل F ذا مميـز معـدوم . إذن الحـدودية A لا تقبل القسمة على $(x-\alpha)$ ومنـه α جـذراً مضاعفاً من المرتبة $(k-1)$ للمشتق P' .

مبرهنة :

إذا كانت A, B_1, B_2 ثلاث حـدوديات من $F[x]$ فإن

١. إذا كان $A|B_1 \cdot B_2$ وكان $d(A, B_2) = 1$ فإن $A|B_1$

٢. إذا كان $d(A, B_i) = 1 \quad (\forall i = 1,2)$ فإن $d(A, B_1 \cdot B_2) = 1$

٣. إذا كان : $d(B_1, B_2) = 1 \quad \wedge \quad B_i|A \quad : \quad \forall i = 1,2$

فإن : $B_1 \cdot B_2|A$

الإثبات:

١. إذا كانت $d(A, B_2) = 1$ فإنه يوجـد $\alpha_1, \alpha_2 \in F[x]$ بحيث

$$\alpha_1 \cdot A + \alpha_2 \cdot B_2 = 1$$

ومنـه :

$$\alpha_1 \cdot B_1 \cdot A + \alpha_2 \cdot B_1 \cdot B_2 = B_1$$

وبمـا أن $A|B_1 \cdot B_2$ فإنـه من العلاقـة الأخـيرة سنجد أن $A|B_1$

.٢

$$d(A,B_1)=1 \Rightarrow \exists \alpha_1,\beta_1 \in F[x] \quad : \quad \alpha_1 \cdot A+\beta_1 \cdot B_1=1$$

$$d(A,B_2)=1 \Rightarrow \exists \alpha_2,\beta_2 \in F[x] \quad : \quad \alpha_2 \cdot A+\beta_2 \cdot B_2=1$$

بضرب العلاقتين طرفاً بطرف نجـــد :

$$(\alpha_1 \cdot B_2 \cdot \beta_2+\alpha_2 \cdot B_1 \cdot \beta_1+\alpha_1 \cdot \alpha_2 \cdot A) \cdot A+(\beta_1 \cdot \beta_2) \cdot (B_1 \cdot B_2)=1$$

أي أن

$$\alpha \cdot A+\beta \cdot (B_1 \cdot B_2)=1 \quad ; \quad \alpha,\beta \in F[x]$$

وهـــذا ما يثبت أن $d(A,B_1 \cdot B_2)=1$

٣. إذا كان $B_1|A$ فإنه يوجـــد $P_1 \in F[x]$ بحيث $A=P_1 \cdot B_1$

وحسب القضية (١) يكون :

$$B_2|P_1 \cdot B_1 \quad \wedge \quad d(B_1,B_2)=1$$

وبالتالي $B_2|P_1$ وعندئذٍ توجـــد $P_2 \in F[x]$ بحيث $P_1=p_2 \cdot B_2$

وبالتالي يكون :

$$A=P_2 \cdot (B_1 \cdot B_2)$$

أي أن : $(B_1 \cdot B_2)|A$

ملاحظة : يمكن تعميم القضيتين (٢) ، (٣) من المبرهنة السابقة على عـــدد منته من الحـــدوديات فتصبحان على الشكل التالي :

٢. إذا كانت $A,B_1,B_2,\dots,B_n$ حـــدوديات من $F[x]$ وكان

$$d(A,B_i)=1 \qquad \forall i=1,2,\dots,n$$

فإن :

$$d(A,\prod_{i=1}^{n} B_i)=1$$

٣.إذا كانت $A, B_1, B_2, \ldots, B_n$ حـــدوديات من $F[x]$ وكان

$$(\forall i = 1,2,\ldots,n) \quad \wedge \quad d(B_i, B_j) = 1 \quad \forall i \neq j$$

فإن :

$$(B_1 \cdot B_2 \cdot \ldots \cdot B_n) | A$$

نتيجة (١):

ليكن $a, b \in F$ بحيث $a \neq b$ وليكن

$$P_1 = (x-a)^n \in F[x] \quad ; \quad n \in N^*$$

$$P_2 = (x-b)^m \in F[x] \quad ; \quad m \in N^*$$

فإن :

$$d(P_1, P_2) = 1$$

البرهان: بملاحظـــة أن :

$$\frac{1}{b-a}(x-a) - \frac{1}{b-a}(x-b) = 1$$

نجـــد أن :

$$d(x-a \quad , \quad x-b) = 1$$

وإذا أخـــذنا

$$A = x-a \quad , \quad B_i = x-b \quad \forall i = 1,2,\ldots,m$$

فإنـــه حسب (٢) من المبرهنـــة المعممـــة السابقـــة نجـــد أن

$$d(A, P_2) = 1$$

وإذا أخـــذنا

$$A = (x-b)^m \quad \wedge \quad B_i = (x-a) \quad ; \quad i = 1,2,\ldots,n$$

فنجـــد حسب (٢) من المبرهنـــة المعممـــة السابقـــة أن

$$d((x-a)^n,(x-b)^m)=1$$

أي أن :

$$d(A,B)=1$$

نتيجة (٢) :

لتكن $P\in F[x]$ ولتكن $a_1,a_2,\dots,a_n\in F$ ومختلفـــة مثنى مثنى وليكن a_i جـــذراً من المرتبـــة k_i للحـــدودية P $(\forall i=1,2,\dots,n)$ عندئذ :

$$\prod_{i=1}^{n}(x-a_i)^{k_i}\Big|\ P$$

البرهان :

بمـــا أن a_i جـــذر من المرتبـــة k_i للحـــدودية P $(\forall i=1,2,\dots,n)$ فـــإن :

$$(x-a_i)^{k_i}\Big|\ P \qquad \forall i=1,2,\dots,n$$

وبمـــا أن الحـــدوديات :

$$(x-a_i)^{k_i} \qquad i=1,2,\dots,n$$

أوليـــة فيما بينهـــا (حسب النتيجـــة (١)) فـــإن :

$$\prod_{i=1}^{n}(x-a_i)^{k_i}\Big|\ P$$

مبرهنة :

إذا كانت $P\in F[x]$ وكان $\deg P=n\geq 1$ فإنـــه يوجـــد على الأكـــثر n جـــذراً مختلفاً للحـــدودية P .

الإثبات : لنأخـــذ المجموعـــة :

$$X = \{\alpha \in F \quad : \quad P(\alpha) = 0_F\}$$

ولنفرض أن $cardX = m$. عندئذ الحـــدودية $Q = \prod_{\alpha \in X}(x - \alpha)$ التي

درجتهـــا تساوي m تقسم الحـــدودية P وبالتالي يكون

$$m = \deg Q \leq \deg \mathrm{P} = n$$

أي أن : $cardX \leq n$

تمرينات محلولـــــة

التمرين الأول :

ليكن F حقـــلاً ما ولتكن A,B حـــدوديتين غـــير صفريتين من الحلقـــة $F[x]$ ولتكن $D \in F[x]$ حـــدودية واحـــدية ولنأخـــذ المثالي الرئيسي $D \cdot F[x]$ والذي يساوي $A \cdot F[x] + B \cdot F[x]$.

برهـــن أن الحـــدودية D القاسم المشترك الأكـــبر للحـــدوديتين A,B

الحـــل : بمـــا أن :

$$D \cdot F[x] = A \cdot F[x] + B \cdot F[x]$$

فإن : $A \in D \cdot F[x]$

وبالتالـــي توجـــد $Q \in F[x]$ بحيث يكون $A = D \cdot Q$ ومنـــه $D|A$.

ومن جهـــة أخـــرى: $B \in D \cdot F[x]$

وبالتالـــي توجـــد $P \in F[x]$ بحيث يكون $B = D \cdot P$ ومنـــه $D|B$.

كمـــا أنـــه إذا كانت $C \in F[x]$ وكانت $(C|A) \wedge (C|B)$

فإنـــه توجـــد حـــدوديتان $P_1, P_2 \in F[x]$ بحيث :

$$A = P_1 \cdot C \quad \wedge \quad B = P_2 \cdot C$$

بمـــا أن :

$$D \cdot F[x] = A \cdot F[x] + B \cdot F[x]$$

فإنـــه توجـــد $\alpha, \beta \in F[x]$

بحيث $D = \alpha \cdot A + \beta \cdot B$

وبالتالـــي :

$$D=(\alpha\cdot P_1+\beta\cdot P_2)\cdot c \qquad \alpha\cdot P_1+\beta\cdot p_2\in F[x]$$

وهـــذا يبين أن $C|D$ إذاً D قاسم مشترك أكـــبر للحـــدوديتين A,B

التمرين الثاني :

ليكن F حقـــلاً ما ولتكن A,B حـــدوديتين غـــير صفريتين من الحلقـــة $F[x]$ ولتكن $D\in F[x]$ القاسم المشترك الأكبر للحـــدوديتين A,B . برهـــن أن :

$$D\cdot F[x]=A\cdot F[x]+B\cdot F[x]$$

الحـــل :

إن مجمـــوع المثاليين الرئيسين $B\cdot F[x]$, $A\cdot F[x]$ هـــو مثالي رئيس مولـــد بحـــدودية مثل $P\in F[x]$ أي أن :

$$P\cdot F[x]=A\cdot F[x]+B\cdot F[x]$$

وحسب التمرين الأول يكون P القاسم المشترك الأكبر للحدوديتين A,B وبمـــا أن القاسم المشترك الأكـــبر للحـــدوديتين A,B وحيد فإن $P=D$ وبالتالي :

$$D\cdot F[x]=A\cdot F[x]+B\cdot F[x]$$

التمرين الثالث :

ليكن F حقـــلاً ما ولتكن A,B حـــدوديتين غـــير صفريّين من الحلقـــة $F[x]$ ولتكن $C\in F[x]$ حـــدودية واحـــدية . ولنأخـــذ المثالي الرئيس $C\cdot F[x]$ الذي يساوي $A\cdot F[x]\,\mathrm{I}\,B\cdot F[x]$.

برهـــن أن الحـــدودية C المضاعف المشترك الأصغر للحدوديتين A,B .

الحـــل : بمـــا أن :

$$C \cdot F[x] = A \cdot F[x] \cap B \cdot F[x]$$

فإن $C \in A \cdot F[x]$ وبالتالي توجـــد حـــدودية $Q \in F[x]$ بحيث يكون

$C = A \cdot Q$ ومنه $B|C$

كمـــا أنـــه إذا كانت $C_1 \in F[x]$ بحيث $(B|C_1) \quad \wedge \quad (A|C_1)$

فإنه توجـــد حـــدوديتان $P_1, P_2 \in F[x]$ بحيث :

$$C_1 = A \cdot P_1 \in A \cdot F[x] \quad \wedge \quad C_1 = B \cdot P_2 \in B \cdot F[x]$$

وبالتالي :

$$C_1 \in A \cdot F[x] \cap B \cdot F[x]$$

أي أن :

$$C_1 \in C \cdot F[x]$$

وبالتالي توجـــد حـــدودية $\alpha \in F[x]$ بحيث يكون $C_1 = C \cdot \alpha$

أي أن : $C|C_1$

إذاً . C المضاعف المشترك الأصغر للحدوديتين A, B .

التمرين الرابع :

ليكن F حقـــلاً ما ولتكن A, B حـــدوديتين غـــير صفريتين من الحلقـــة $F[x]$ ولتكن الحـــدودية C المضاعف المشترك الأصغر للحدوديتين A, B . برهـــن أن :

$$C \cdot F[x] = A \cdot F[x] \cap B \cdot F[x]$$

الحـــل : إن تقاطع المثاليين الرئيسيان $A \cdot F[x]$, $B \cdot F[x]$ هـــو مثالي رئيس

غـــير صفري مولـــد بحـــدودية مثل $P \in F[x]$ أي أن :

$$P \cdot F[x] = A \cdot F[x] \mathrm{I}\ B \cdot F[x]$$

وحسب التمرين السابق تكون الحـــدودية P المضاعف المشـــترك الأصغر للحـــدوديتين A,B . وبمـــا أن المضاعف المشـــترك الأصغر للحـــدوديتين A,B وحيد فإن $P = C$ وبالتالي :

$$C \cdot F[x] = A \cdot F[x] \mathrm{I}\ B \cdot F[x]$$

التمرين الخامس :

أثبت أن الحـــدوديات الثلاث الآتية والتي هـــي من الحلقـــة $R[x]$

$$A = x^3 - x^2 + x - 1$$
$$B = x^2 + x - 2$$
$$C = x^2 + 1$$

أوليـــة فيمـــا بينهـــا .

الحـــل : نوجـــد $d(A,B)$ فنجـــد أن

$$d(A,b) = D = x - 1$$

نوجـــد $d(D,C)$ فنجـــد أن .

$$d(D,C) = 1$$

وبالتالـــي :

$$d(A,B,C) = 1$$

إذن الحـــدوديات A,B,C أوليـــة فيمـــا بينهمـــا .

التمرين السادس :

أثبت أن الحـــدودية $P = x^2 - 2$ غـــير قابلة للتحليل في $Q[x]$ لكنها قابلـــة للتحليل في $R[x]$.

(حيث Q حقل الأعـــداد العادية ، R حقل الأعـــداد الحقيقية).

الحـــل : لنوجـــد جـــذور الحـــدودية P .

$$x^2 - 2 = 0 \quad \Rightarrow \quad x = \mu\sqrt{2}$$

فنجـــد أنـــه لا توجـــد جـــذور لـــ P في الحقل Q وبالتالي P غـــير قابلة للتحليل في الحلقـــة $Q[x]$ لكن $\mu\sqrt{2} \in R$ أي توجـــد للحـــدودية P جـــذور في الحقل R وبالتالي فإن الحدودية P قابلة للتحليل في $R[x]$ ويكون :

$$P(x) = (x - \sqrt{2}) \cdot (x + \sqrt{2})$$

تمرينات (٨)

التمرين الأول :

أوجد القاسم المشترك الأكبر D للحدوديتين A,B ثم أوجد الحدوديتين $\alpha(x),\beta(x)\in R[x]$ بحيث يكون :

$$D=\alpha\cdot A+\beta\cdot B$$

في كل من الحالتين الآتيتين :

1. $\begin{cases} A=x^4+3x^3-x^2-4x-3 \\ B=3x^3+10x^2+2x-3 \end{cases}$

2. $\begin{cases} A=x^6+2x^4-4x^3-3x^2+8x-5 \\ B=x^5+x^2-x+1 \end{cases}$

التمرين الثاني :

أثبت أن الحدودية

$$A=x^3+3x+2 \quad \in Z/5Z[x]$$

غير قابلة للتحليل في الحلقة $Z/5Z[x]$.

التمرين الثالث :

أثبت أن الحدودية

$$A=x^3+3x-1$$

غير قابلة للتحليل في الحلقة $Q[x]$. (Q حقل الأعداد العادية) .

التمرين الرابع :

أثبت أن الحدودية $A = x^5 + x - 1$ قابلة للتحليل في الحلقة $Q[x]$.

ثم أوجد $P,Q \in Q[x]$ بحيث $A = P \cdot Q$.

التمرين الخامس :

ليكن $A,B \in C[x]$ وليكن :

$$A(\alpha) = 0 \quad \Leftrightarrow \quad B(\alpha) = 0 \qquad ; \quad \alpha \in C$$

$$(A-1)(\beta) = 0 \quad \Leftrightarrow \quad (B-1)(\beta) = 0 \quad ; \quad \beta \in C$$

أثبت أن $A = B$.

التمرين السادس :

ليكن $n,m \in N^*$ وليكن d القاسم المشترك الأكبر للعددين n,m

وليكن t المضاعف المشترك الأصغر للعددين n,m وليكن $a \in R$

والمطلوب :

١. أثبت أن $d(x^n - a^n, x^m - a^m) = x^d - a^d$

٢. $(x^n - a^n)(x^m - a^m) \mid (x^d - a^d)(x^t - a^t)$

التمرين السابع :

لتكن $A \in R[x]$ (حيث R حقل الأعداد الحقيقية) .

وليكن $\deg A = 2n+1$ (حيث $n \in N$) . أثبت أن الحدودية قابلة للتحليل في الحلقة $R[x]$.

(إرشاد : برهن على وجود جذر حقيقي واحد على الأقل لـ A في R) .

الفصل التاسع

الفضاءات الشعاعية على حلقة تبديلية واحدية

المودولات (المقاسات)

٩ – ١ المقاس :

تعريف : لتكن R حلقة تبديلية واحدية ولتكن $M \neq \phi$ مجموعة غير خالية ولنعرف على M قانون تشكيل الأول داخلي $(+)$ وندعوه الجمع . والثاني خارجي $(\cdot)$ مجموعة مؤثراته الحلقة R .

فنقول عن البنية $(M,+,\cdot)$ مقاس على الحلقة R إذا تحققت الشروط التالية:

I. البنية $(M;+)$ زمرة تبديلية .

II. أياً كان $\alpha,\beta \in R$ وأياً كان $x,y \in M$ فإن :

1. $1_R \cdot x = x$
2. $(\alpha+\beta)\cdot x = \alpha\cdot x + \beta\cdot x$
3. $\alpha\cdot(x+y) = \alpha\cdot x + \alpha\cdot y$
4. $\alpha\cdot(\beta\cdot x) = (\alpha\cdot\beta)\cdot x$

نرمز لمحايد الزمرة $(M,+)$ بالرمز 0 وندعوه صفر المقاس M .

وسنرمز بـ $M(R)$ للتعبير عن المقاس M على الحلقة التبديلية الواحدية R .

أمثلة:

١. لتكن R حلقة تبديلية واحدية وليكن n عدداً صحيحاً موجباً ولنعرف على المجموعة :

$$R^n = \{(a_1, a_2, \dots, a_n) \quad ; \quad a_i \in R \quad i = 1,2,\dots,n\}$$

قانوني التشكيل :

$(+) : (a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$ داخلي

$(\bullet) : \lambda \cdot (a_1, a_2, \dots, a_n) = (\lambda \cdot a_1, \lambda \cdot a_2, \dots, \lambda a_n)$ خارجي مؤثراته R

وذلك أياً كان

$$(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in R^n \quad , \quad \lambda \in R$$

فنجد أن $(R^n, +, \bullet)$ مقاس على الحلقة R .

في حالة خاصة عندما $n = 1$ نجد أن $(R, +, \bullet)$ مقاس على R .

أي أن كل حلقة تبديلية واحدية مقاس على نفسها .

٢. لتكن R حلقة تبديلية واحدية ولنعرف على المجموعة $R[x]$ (حلقة الحدوديات) ذات المتحول x على الحلقة R قانوني التشكيل :

$(+) : \forall P = \sum_{k \geq 0} a_k \cdot x^k \ , \ Q = \sum_{k > 0} b_k \cdot x^k \in R[x]$: داخلي

$$P + Q = \sum_{k \geq 0} (a_k + b_k) \cdot x^k$$

$(\bullet) : \forall \lambda \in R \ , \ \forall P = \sum_{k \geq 0} a_k \cdot x^k$: خارجي مؤثراته R

$$\lambda \cdot P = \sum_{k \geq 0} (\lambda \cdot a_k) \cdot x^k$$

فنجد $(R[x], +, \bullet)$ مقاس على الحلقة R .

٣. لتكن R حلقة تبديلية واحدية ولنعرف على المجموعة $M_{m \times n}(R)$ (مجموعة المصفوفات من المرتبة $m \times n$ والتي عناصرها من الحلقة R).

قانوني التشكيل :

داخلي $(+)$: $\forall A=(a_{ij})\ ,\ B=(b_{ij})\in M_{m\times n}(R)$:

$$A+B=(a_{ij}+b_{ij})\ ;\ i=1,2,\dots,n\ ,\ j=1,2,\dots,m$$

خارجي مؤثراته R $(\bullet)$: $\forall\lambda\in R\ ,\ \forall A=(a_{ij})\in M_{m\times n}(F)$:

$$\lambda\cdot A=(\lambda\cdot a_{ij})$$

فنجـــد أن $(M_{m\times n}(R),+,\bullet)$ مقاس على الحلقـــة R .

٤. لتكن R حلقـــة تبديلية واحـــدية ولتكن $\phi\neq K\subseteq R$ و لتكن M مجموعـــة التطبيقات $f:K\to R$ ولنعرف على M قانوني التشكيل :

الداخلي $(+):\forall f,g\in M:(f+g)(x)=f(x)+g(x)\quad\forall x\in K$

خارجي مؤثراته R $(\bullet):\lambda\in R\ ,\ \forall f\in M:(\lambda\cdot f)(x)=\lambda\cdot f(x)$

فنجـــد أن $(M,+,\bullet)$ مقاس على R .

٥. كل زمـــرة تبديلية هـــي مقاس على الحلقـــة Z .

مبرهنة:

إذا كان $M(R)$ مقاس على الحلقـــة R فإنه أياً كان $x\in M\ ,\ \alpha\in R$

1. $0_R\cdot x=0_M$
2. $\alpha\cdot 0_M=0_M$
3. $(-\alpha)\cdot x=\alpha\cdot(-x)=-(\alpha\cdot x)$

الإثبات: يُترك للقارئ لسهولته .

٩ – ٢ المقاسات الجزئيـــة :

تعريف : ليكن $M(R)$ مقاساً وليكن $\phi\neq N\subseteq M$. نقول عن N إنـــه مقاساً جزئيـــاً من المقاس M عنـــدما وفقط عنـــدما يتحقق :

1. $\forall x,y \in N : x-y \in N$ ($(N,+)$ زمرة جزئية من الزمرة $(M,+)$)

2. $\forall \alpha \in R \ , \ x \in N : \alpha \cdot x \in N$

ويبرهن على أن الشرطين السابقين يكافئان الشرط التالـــي :

$$\forall \alpha,\beta \in R \ , \ \forall x,y \in N \ : \ \alpha \cdot x + \beta \cdot y \in N$$

أمثلة :

١. إذا كان $M(R)$ مقاساً فإن $\{0_M\}$ مقاس جزئي من المقاس M . ندعوه المقاس الصفري .

٢. كل زمرة جزئية من زمرة تبديلية هي مقاس جزئي من تلك الزمرة (على Z)

٣. كل مثالي من حلقـــة تبديلية واحدية (التي هي مقاس على نفسها) هـــو مقاس جزئي من تلك الحلقـــة .

مبرهنة:

إذا كانت $\{N_i \ ; \ i=1,2,\dots,n\}$ أسرة منتهية من المقاسات الجزئيـــة من مقاس $M(R)$ فإن $\bigcap_{i=1}^{n} N_i$ مقاس جزئي من المقاس M .

الإثبات:

إن :

$$0 \in N_i \subseteq M \qquad \forall i=1,2,\dots,n$$

وبالتالـــي : $0 \in \bigcap_{i=1}^{n} N_i \subseteq M$

أي أن : $\phi \neq \bigcap_{i=1}^{n} N_i \subseteq M$

من جهة ثانية : أياً كان $\alpha,\beta \in R$ وأياً كان $x,y \in \bigcap_{i=1}^{n} N_i$ فإن :

$$x, y \in N_i \qquad \forall i = 1,2,\dots,n$$

وبالتالـــي :

$$\alpha \cdot x + \beta \cdot y \in N_i \qquad \forall i = 1,2,\dots,n$$

وبالتالـــي : $\alpha \cdot x + \beta \cdot y \in \mathop{\mathrm{I}}_{i=1}^{n} N_i$

إذن : $\mathop{\mathrm{I}}_{i=1}^{n} N_i$ مقاس جزئي من المقاس M .

تعريف: لتكن $\{N_i \;\; ; \;\; i = 1,2,\dots,n\}$ أسرة مقاسات جزئيـــة من مقاس $M(R)$

نعرف مجموع أسرة المقاسات الجزئيـــة ونرمز لها بـــ $\sum_{i=1}^{n} N_i$ بأنه المجموعة

$$\sum_{i=1}^{n} N_i = \{x \in M \;\; \Big| \;\; x = \sum_{i=1}^{n} x_i \;\; ; \;\; x_i \in N_i \;\; ; \;\; i = 1,2,\dots,n\}$$

مبرهنة:

إذا كانت $\{N_i \;\; ; \;\; i = 1,2,\dots,n\}$ أسرة مقاسات جزئيـــة من مقاس $M(R)$ فإن $\sum_{i=1}^{n} N_i$ مقاس جزئي من المقاس $M(R)$.

الإثبات: من الواضـــح أن $\sum_{i=1}^{n} N_i \subseteq M$.

كمـــا أن :

$$0_M = 0_M + 0_M + \dots + 0_M \in \sum_{i=1}^{n} N_i$$

أي أن :

$$\phi \neq \sum_{i=1}^{n} N_i \subseteq M$$

من جهة ثانية :

أياً كان $\alpha, \beta \in R$ وأياً كان $x, y \in \sum_{i=1}^{n} N_i$ فإن :

$$x=\sum_{i=1}^{n} x_i \quad ; \quad x_i \in N_i \quad i=1,2,\dots,n$$

$$y=\sum_{i=1}^{n} y_i \quad ; \quad y_i \in N_i \quad i=1,2,\dots,n$$

وبالتالي يكون :

$$\alpha \cdot x+\beta \cdot y=\alpha \cdot \sum_{i=1}^{n} x_i+\beta \cdot \sum_{i=1}^{n} y_i$$

$$=\sum_{i=1}^{n}(\alpha \cdot x_i+\beta \cdot y_i) \quad ; \quad \alpha \cdot x_i+\beta \cdot y_i \in N_i \quad i=1,2,\dots,n$$

أي أن :

$$\alpha \cdot x+\beta \cdot y \in \sum_{i=1}^{n} N_i$$

إذاً $\sum_{i=1}^{n} N_i$ مقاس جزئي من المقاس $M(R)$.

تعريف: لتكن X مجموعة جزئية من مقاسٍ $M(R)$. إن تقاطع جميع المقاسات الجزئية من M والتي تحوي X هو مقاس جزئي من M ويحوي X ندعوه المقاس الجزئي المولّد بالمجموعة X ونرمز له بـ $<X>$ ، وندعو X المجموعة المولّدة للمقاس $<X>$.

<u>بعبارة أخرى :</u>

$<X>$ = أصغر مقاس جزئي من المقاس M يحوي X

و إذا كانت X مجموعة منتهية فنقول عن المقاس $<X>$ مودولاً منتهي التوليد.

وفي حالة خاصة إذا كانت $X=\{a\}$ فنقول عن المقاس $<X>$ أنه دوار.

تعريف: لتكن $X=\{x_1,x_2,\dots,x_n\}$ مجموعة جزئية من مقاسٍ $M(R)$.

نعرف مجموعة كل التراتيب الخطية للمجموعة X و نرمز لها بـ $Lc(X)$ بأنها المجموعة :

$$Lc(X)=\{x\in M : x=\sum_{i=1}^{n}\alpha_i\cdot x_i \quad ; \quad \alpha_i\in R \quad i=1,2,\dots,n\}$$

ملاحظة(١) : إذا كانت X مجموعة ما من مقاس $M(R)$ فإن

$$<X>=\begin{cases}\{0\} & ; \quad X=\phi\\ Lc(X) & ; \quad X\neq\phi\end{cases}$$

ملاحظة(٢) : إذا كانت $X=\{x_1,x_2,\dots,x_n\}$ مجموعة منتهية غير خالية من مقاس $M(R)$ فإن :

$$<X>=\sum_{i=1}^{n}\alpha_i\cdot x_i \quad ; \quad \alpha_i\in R$$

٩ – ٣ مقاس خارج القسمة :

ليكن N مقاساً جزئياً من مقاسٍ $M(R)$ ولنأخذ المجموعة :

$$M/N=\{x+N \quad ; \quad x\in M\}$$

واضح أن :

$$N=0+N\in M/N$$

أي أن $\phi\neq M/N$

لنعرف على المجموعة M/N قانوني التشكيل :

$(+)$: داخلي $\quad \forall(x+N),(y+N)\in M/N:$

$$(x+N)+(y+N)=(x+y)+N$$

$(\cdot)$: خارجي مؤثراته R $\quad \forall\alpha\in R \quad , \quad \forall(x+N)\subset M/N:$

$$\alpha\cdot(x+N)=\alpha\cdot x+N$$

فنجد أن $(M/N,+,\cdot)$ مقاس على الحلقة R ، ندعوه مقاس خارج قسمة المقاس M على المقاس الجزئي منه N .

(لاحـــظ أن صفر المقاس M/N هـــو $0+N=N$) .

٩ ـ ٤ التشاكلات المقاسيّة :

تعريف (١): لتكن M,M' مقاســين على حلقــة تبديلية واحــدية .

نعرف التشاكل المقاسي بأنــه كل تطبيق :

$$f:M\to M'$$

الذي يحقق الشرطان التاليان :

1. $\forall x,y\in M \quad : \quad f(x+y)=f(x)+f(y)$
2. $\forall \alpha\in R \quad , \quad \forall x\in M \quad : f(\alpha\cdot x)=\alpha\cdot f(x)$

ويبرهـــن على أن الشرطين يكافئان الشرط التالي :

$$\forall \alpha,\beta\in R,\forall x,y\in M : f(\alpha\cdot x+\beta\cdot y)=\alpha\cdot f(x)+\beta\cdot f(y)$$

تعريف (٢): نقول عن التشاكل المقاسي $f:M\to M'$ إنــه تماثل إذا كان f غامراً ومتبايناً ، ونقول عندئذ إن M',M متماثلان ونكتب $M\cong M'$

تعريف (٣): ليكن $f:M\to M'$ تشاكلاً مقاسياً . نعرف نــواة f ونرمز لهــا بـــ $\ker f$ بأنها المجموعــة :

$$\ker f=\{x\in M \quad : \quad f(x)=0_{M'}\}=\overleftarrow{f}\{0_{M'}\}$$

مبرهنة:

إذا كان $f:M\to N$ تشاكلاً مقاسياً فإن :

١. $f(0_M)=0_N$

٢. أياً كان $x\in M$ فإن $f(-x)=-f(x)$

٣. إذا كان N_1 مقاساً جزئيــاً من المقاس N فإن $\overleftarrow{f}(N_1)$

٤. $\ker f$ مقاس جزئــي من M .

الإثبات: سهل يترك للقارئ كتمرين .

مبرهنة:

إذا كانت M,N,L ثلاثة مقاسات على حلقة R . وإذا كان $f:M\to N$ ، $g:M\to L$ تشاكلين مقاسيين بحيث f غامر ، فإن القضيتين التاليتين متكافئتان :

(I). يوجد تشاكل مقاسي وحيد $h:N\to L$ بحيث $h\circ f=g$

(II). $\ker f\subseteq \ker g$

وأكثر من ذلك: h متباين $\Leftrightarrow$ $\ker f=\ker g$

الإثبات:

(I) $\Leftarrow$ (II): أياً كان $x\in\ker f$ فإن :

$$g(x)=(h\circ f)(x)=h(f(x))=h(0_N)=0_L\Rightarrow x\in\ker g$$

ومنه :

$$\ker f\subseteq\ker g$$

(II) $\Leftarrow$ (I):

$$\begin{aligned}\forall x,y\in M: f(x)=f(y)&\Rightarrow f(x)-f(y)=0_N\\&\Rightarrow f(x-y)=0_N\\&\Rightarrow x-y\in\ker f\end{aligned}$$

وبما أن :

$$\ker f\subseteq\ker g$$

فإنه يكون :

$$x-y\in\ker g$$

ومنـــه

$$g(x-y)=0_L$$

ومنـــه

$$g(x)=g(y)$$

وحسب المبرهنـــة من الفقرة (٩ - ٢) فإنـــه يوجـــد تطبيق $h:N\to L$ بحيث $h\circ f=g$

وبمـــا أن f غامر فإنـــه منتظم يميني وهـــذا يعني أن h وحيـــد .

ولنثبت الآن أن h تشاكل مقاسي :

أياً كان $y_1,y_2\in N$ فإنـــه يوجـــد $x_1,x_2\in M$ بحيث:

$$y_1=f(x_1)\quad\wedge\quad y_2=f(x_2)$$

(لاحـــظ أن f غامـــر).

وعندئذٍ يكون :

$$\begin{aligned}\forall\alpha,\beta\in R: h(\alpha\cdot y_1+\beta\cdot y_2)&=h\big(\alpha\cdot f(x_1)+\beta\cdot f(x_2)\big)\\&=h\big(f(\alpha\cdot x_1+\beta\cdot x_2)\big)\\&=h\circ f(\alpha\cdot x_1+\beta\cdot x_2)\\&=g(\alpha\cdot x_1+\beta\cdot x_2)\\&=\alpha\cdot g(x_1)+\beta\cdot g(x_2)\\&=\alpha\cdot h\big(f(x_1)\big)+\beta\cdot h\big(f(x_2)\big)\\&=\alpha\cdot h(y_1)+\beta\cdot h(y_2)\end{aligned}$$

لنفرض الآن أن h متباين ولنبرهـــن على أن $\ker f=\ker g$

لدينا حسب الفرض أن :

$$\ker f\subseteq\ker g\qquad(1)$$

من جهة ثانية :

$$\begin{aligned}
\forall x \in \ker g \quad &\Rightarrow \quad g(x) = 0_N \\
&\Rightarrow \quad (h \circ f)(x) = 0_N \\
&\Rightarrow \quad h(f(x)) = h(0_M) \\
&\Rightarrow \quad f(x) = 0_M \qquad \text{(لأن } h \text{ متباين)} \\
&\Rightarrow \quad x \in \ker f
\end{aligned}$$

أي أن :

$$\ker g \subseteq \ker f \qquad (2)$$

من (١) و (٢) نجـــد أن : $\ker f = \ker g$.

لنفرض أن $\ker f = \ker g$ ولنبرهـــن على أن h متباين .

بمـــا أن f غامـــر فإنـــه :

$$\forall y \in N \quad : \quad \exists x \in M \quad : \quad y = f(x)$$

عندئذٍ :

$$\begin{aligned}
\forall y \in \ker h \quad &\Rightarrow \quad h(y) = 0_L \\
&\Rightarrow \quad h(f(x)) = 0_L \\
&\Rightarrow \quad g(x) = 0_L \\
&\Rightarrow \quad x \in \ker g = \ker f \\
&\Rightarrow \quad x \in \ker f \\
&\Rightarrow \quad f(x) = 0_N \\
&\Rightarrow \quad y = 0_N
\end{aligned}$$

أي أن : $\ker h = \{0_N\}$

وهـــذا يثبت أن h متباين .

ملاحظـــة: يمكن تمثيل المبرهنـــة السابقة بالمخطط التالي :

$$\begin{tikzcd} M \arrow[r, "g"] \arrow[d, "f"'] & L \\ N \arrow[ur, dashed, "h"'] & \end{tikzcd} \quad ; \quad h \circ f = g$$

غامر

مبرهنة:

إذا كانت M, N, L ثلاثـــة مقاسات على حلقـــة R . وإذا كان :

$f : N \to M$ ، $g : L \to M$ تشاكلين مقاسيين بحيث f متباين

فإن القضيتين التاليتين متكافئتان :

(I′) . يوجـــد تشاكل مقاسي وحيـــد $h : L \to N$ بحيث $f \circ h = g$

(II′) . $I_m g \subseteq I_m f$

وأكـــثر من ذلك h غامـــر $\Leftrightarrow$ $I_m g = I_m f$

الإثبات:

(II′) $\Leftarrow$ (I′) :

$$\forall x \in L \quad : \quad g(x) = (f \circ h)(x)$$

$$= f(h(x)) \in I_m f$$

ومنـــه :

$$I_m g \subseteq I_m f$$

(I′) $\Leftarrow$ (II′) : حسب المبرهنـــة الثانية من الفقرة (٢ - ٢) يوجد تطبيق

$h : L \to N$ بحيث $f \circ h = g$.

وبما أن f متباين فإنه منتظم يساري وهذا يعني أن h وحيد .

ولنثبت الآن أن h تشاكل مقاسي :

أياً كان $\alpha, \beta \in R$ وأياً كان $x, y \in L$ فإن :

$$\begin{aligned} f\big(h(\alpha \cdot x + \beta \cdot y)\big) &= g(\alpha \cdot x + \beta \cdot y) \\ &= \alpha \cdot g(x) + \beta \cdot g(y) \\ &= \alpha \cdot f\big(h(x)\big) + \beta \cdot f\big(h(y)\big) \\ &= f\big(\alpha \cdot h(x) + \beta \cdot h(y)\big) \end{aligned}$$

وبما أن f متباين فإن

$$h(\alpha \cdot x + \beta \cdot y) = \alpha \cdot h(x) + \beta \cdot h(y)$$

لنفرض الآن أن h غامر ولنبرهن على أن $I_m g = I_m f$.

لدينا حسب الفرض أن :

$$I_m g \subseteq I_m f \qquad (1)$$

من جهة ثانية :

$$\forall f(y) \in I_m f \quad ; \quad y \in N \quad \Rightarrow \quad \exists x \in L \quad : \quad y = h(x)$$

(لأن h غامر)

وبالتالي يكون :

$$f(y) = f\big(h(x)\big) = g(x) \in I_m g$$

أي أن :

$$I_m f \subseteq I_m g \qquad (2)$$

من (١) و (٢) نجد أن :

$$I_m f = I_m g$$

لنفرض أن $I_m g = I_m f$ ولنبرهن على أن h غامر .

بمـــا أن $I_m f = I_m g$ فإن :

$$\forall y \in N \quad : \quad \exists x \in L \quad : \quad f(y) = g(x)$$

$$= f\big(h(x)\big)$$

$$= y = h(x) \qquad (\text{لأن } f \text{ متباين})$$

وهـــذا ما يثبت أن h غامـــر .

ملاحظـــة: يمكن تمثيل المبرهنـــة السابقة بالمخطط التالي :

$$\begin{tikzcd} & L \arrow[dl, dashed, "h"'] \arrow[d, "g"] \\ N \arrow[r, "f \text{ متباين}"'] & M \end{tikzcd} \qquad ; \qquad f \circ h = g$$

تمرينات محلولـــــة

التمرين الأول:

لتكن N_1, N_2, N_3 ثلاثة مقاسات جزئيـــة من مقاسٍ $M(R)$ بحيث $N_3 \subseteq N_1$. برهـــن أن :

$$N_1 \mathrm{I}\ (N_2 + N_3) = (N_1 \mathrm{I}\ N_2) + N_3$$

الحـــل:

$$\forall x \in N_1 \mathrm{I}\ (N_2 + N_3) \Rightarrow x \in N_1 \quad \wedge \quad x \in N_2 + N_3$$

$$\Rightarrow x \in N_1 \wedge x = x_2 + x_3 \quad ; \quad x_2 \in N_2, x_3 \in N_3$$

$$(\text{لأن } N_3 \subseteq N_1) \Rightarrow x \in N_1 \wedge x = x_2 + x_3 \quad ; \quad x_2 \in N_2, x_3 \in N_1$$

$$\Rightarrow x \in N_1 \wedge x_2 - x - x_3 \in N_1$$

أصبح لدينا :

$$x_2 \in N_2 \quad \wedge \quad x_2 \in N_1$$

وبالتالي :

$$x_2 \in N_1 \mathrm{I}\ N_2$$

إذاً :

$$x = x_2 + x_3 \quad ; \quad x_2 \in N_1 \mathrm{I}\ N_2 \quad \wedge \quad x_3 \in N_3$$

أي أن :

$$x \in (N_1 \mathrm{I}\ N_2) + N_3$$

ومنـــه :

$$N_1 \mathrm{I}\ (N_2 + N_3) \subseteq (N_1 \mathrm{I}\ N_2) + N_3 \qquad (1)$$

من جهة ثانية : بما أن $N_3 \subseteq N_1$ فإن $N_1 + N_3 = N_1$

و بالتالي يكون :

$$(N_1 \mathrm{I}\ N_2) + N_3 \subseteq N_1 + N_3 \wedge (N_1 \mathrm{I}\ N_2) + N_3 \subseteq N_2 + N_3$$

ومنـــه :

$$(N_1 \mathrm{I}\ N_2) + N_3 \subseteq (N_1 + N_3) \mathrm{I}\ (N_2 + N_3)$$

وبالتالي :

$$(N_1 \mathrm{I}\ N_2) + N_3 \subseteq N_1 \mathrm{I}\ (N_2 + N_3) \qquad (2)$$

من (١) و (٢) يكون :

$$N_1 \mathrm{I}\ (N_2 + N_3) = (N_1 \mathrm{I}\ N_2) + N_3$$

التمرين الثاني :

ليكن $f : M \to N$ تشاكلاً مقاسياً وليكن M_1 مقاساً جزئياً من M وليكن N_1 مقاساً جزئياً من N . برهـــن أن :

$$\overleftarrow{f}\left(\overrightarrow{f}(M_1)\right) = M_1 + \ker f$$

الحـــل: من جهـــة أولى :

$$\begin{aligned}
\forall x \in \overleftarrow{f}\left(\overrightarrow{f}(M_1)\right) &\Rightarrow f(x) \in \overrightarrow{f}(M_1) \\
&\Rightarrow \exists a \in M_1 \quad : \quad f(x) = f(a) \\
&\Rightarrow f(x) - f(a) = 0_N \\
&\Rightarrow f(x - a) = 0_N \\
&\Rightarrow x - a \in \ker f \\
&\Rightarrow \exists b \in \ker f \quad : \quad x - a = b \\
&\Rightarrow x = a + b \quad ; \quad a \in M_1 \wedge b \in \ker f
\end{aligned}$$

أي أن : $\overleftarrow{f}\left(\overrightarrow{f}(M_1)\right) \subseteq M_1 + \ker f \qquad (1)$

من جهـــة ثانية :

$$\forall x \in M_1 + \ker f \Rightarrow x = x_1 + x_2 \quad ; \quad x_1 \in M_1 \wedge x_2 \in \ker f$$

$$\Rightarrow f(x) = f(x_1 + x_2)$$

$$\Rightarrow f(x) = f(x_1) + f(x_2)$$

$$\Rightarrow f(x) = f(x_1) + 0_N \qquad (\text{لأن } x_2 \in \ker f)$$

$$\Rightarrow f(x) = f(x_1) \quad ; \quad x_1 \in M_1$$

$$\Rightarrow x \in \overleftarrow{f}\left(\overrightarrow{f}(M_1)\right)$$

أي أن :

$$M_1 + \ker f \subseteq \overleftarrow{f}\left(\overrightarrow{f}(M_1)\right) \qquad (2)$$

من (١) و (٢) نجـــد أن :

$$M_1 + \ker f = \overleftarrow{f}\left(\overrightarrow{f}(M_1)\right)$$

التمرين الثالث :

ليكن $f : M \to N$ تشاكلاً مقاسياً وليكن M_1 مقاساً جزئياً وليكن N_1 مقاساً جزئياً من N . برهـــن أن :

$$\overleftarrow{f}\left(\overrightarrow{f}(N_1)\right) = N_1 1 \ \operatorname{Im} f$$

الحـــل: من جهـــة أولى :

$$\forall y \in \overleftarrow{f}\left(\overrightarrow{f}(N_1)\right) \Rightarrow \exists x \in \overleftarrow{f}(N_1) \quad : \quad y = f(x)$$

وبالتالي يكون :

$$f(x) \in N_1$$

لكن :

$$f(x) \in \operatorname{Im} f$$

وبالتالي :

$$f(x) = y \in N_1 \quad \wedge \quad y \in \operatorname{Im} f$$

ومنـــه :

$$\overrightarrow{f}\left(\overleftarrow{f}(N_1)\right) \subseteq N_1 \cap \operatorname{Im} f \qquad (1)$$

من جهـــة ثانيـــة :

$$\begin{aligned}
\forall y \in N_1 \cap \operatorname{Im} f &\Rightarrow y \in N_1 \quad \wedge \quad y \in I_m f \\
&\Rightarrow y \in N_1 \quad \wedge \quad \exists x \in M : f(x) = y \\
&\Rightarrow f(x) \in N_1 \\
&\Rightarrow x \in \overleftarrow{f}(N_1) \\
&\Rightarrow f(x) = y \in \overrightarrow{f}\left(\overleftarrow{f}(N_1)\right)
\end{aligned}$$

أي أن :

$$N_1 \cap \operatorname{Im} f \subseteq \overrightarrow{f}\left(\overleftarrow{f}(N_1)\right) \qquad (2)$$

من (١) و (٢) نجـــد أن :

$$\overrightarrow{f}\left(\overleftarrow{f}(N_1)\right) = N_1 \cap \operatorname{Im} f$$

تمرينات (٩)

التمرين الأول :

ليكن N_1, N_2, N_3 ثلاثة مقاسات جزئية من مقاسٍ $M(R)$ بحيث

$$N_1 \subseteq N_2 \quad \wedge \quad N_1 + N_3 = N_2 + N_3 \quad \wedge \quad N_1 \cap N_3 = N_2 \cap N_3$$

أثبت أن $N_1 = N_2$.

التمرين الثاني :

ليكن $f : M \to N$ تشاكلاً مقاسياً وليكن M_1 مقاساً جزئياً من M .
وليكن N_1 مقاساً جزئياً من N . أثبت أن :

$$\bar{f}\left(M_1 \cap \bar{f}(N_1)\right) = \bar{f}(M_1) \cap N_1$$

التمرين الثالث :

ليكن لدينا التشاكلات المقاسية :

$$f : X \to Y \quad ; \quad g : Y \to Z \quad ; \quad \varphi : Y \to A$$

حيث g غامر و أن $\ker g = \operatorname{Im} f$ و أن $\varphi \circ f = 0$.

(لاحظ المخطط)

$$\begin{tikzcd}
X \arrow[r, "f"] & Y \arrow[r, "g"] \arrow[d, "\varphi"'] & Z \arrow[r] \arrow[dl, dashed, "h"] & 0 \\
& A & &
\end{tikzcd}$$

أثبت أنه يوجد تشاكل مقاسي وحيد $h : Z \to A$ من أجله يكون

$$h \circ g = \varphi$$

التمرين الرابع :

ليكن $f : M \to N$ تشـــاكلاً مقاسياً وليكن $g : \ker f \to M$ التباين القانوني (تشاكل مقاسي) . المطلوب :

١. أثبت أن $f \circ g = 0$.

٢. إذا كان P مقاساً وكان $\varphi : P \to M$ تشاكلاً مقاسياً بحيث $f \circ h = 0$ فأثبت أنـــه يوجـــد تشاكل مقاسي وحيـــد $h : P \to \ker f$ من أجلـــه يكون $g \circ h = \varphi$.

(لاحـــظ المخطط)

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "h"'] \arrow[d, "\varphi"] & \\
\ker f \arrow[r, "g"'] & M \arrow[r] & N
\end{tikzcd}$$

التمرين الخامس :

ليكن لدينـــا التشاكلات المقاسية :

$$f : X \to Y \quad ; \quad g : Y \to Z \quad ; \quad \varphi : A \to Y$$

حيث f متباين و أن $\ker f = \operatorname{Im} g$ و أن $g \circ \varphi = 0$.

أثبت أنـــه يوجـــد تشاكل مقاسي وحيـــد $h : A \to X$ من أجلـــه يكون $f \circ h = \varphi$.

(لاحـــظ المخطط) .

$$\begin{tikzcd}
 & A \arrow[dl, dashed, "h"'] \arrow[d, "\varphi"] & \\
0 \arrow[r] & X \arrow[r, "f"'] & Y \arrow[r, "g"'] & Z
\end{tikzcd}$$

الفصل العاشر

تمديد الحقــول ـ الحقــول المنتهية

١٠ – ١ مقدمـــة:

سندرس في هذا الفصل تمـديد الحقول وكثيرات الحـدود (الحـدوديات) على حقـول منتهيـة لمـا لهـذين الموضوعين من أهمية كبيرة في دراسـة وفهـم كثير من موضوعات نظـرية المعلومـات .

١٠ – ٢ تمـديد الحقـل :

تعريف: نقول عن الحقـل K إنـه ممـدد للحقـل F إذا وجـد في K حقـلاً يماثل الحقـل F .

أمثـلة :

١. الحقـل R ممـدد للحقـل Q .

٢. الحقـل C ممـدد للحقـل R .

مبرهـنة:

إذا كان K حقـلاً ما . فـإن :

١. إذا كان مميز الحـقل K معـدوماً فإن K ممدد للحقل Q .

٢. إذا كان مميز الحقل K عـدداً أولياً P فإن K ممـدد للحقل Z / pZ

الإثبات :

١. إذا كان مميز الحقـل K معدوماً ، نأخـذ العلاقـة :

$$f : Z \to K$$

المعرفـــة كمـــا يلي :

$$f(z) = z \cdot z \cdot 1_k \qquad \forall z \in Z$$

فنجـــد بسهولة أن f تشاكل حلقـــي متباين (تأكد من ذلك) وبالتالي :

$\operatorname{Im} f \cong Z$ ومنـــه حقـــل الكسور لـــ $\operatorname{Im} f$ يماثل Q .

إذاً الحقل K ممـــدد للحقـــل Q .

٢. إذا كان مميـــز الحـــقل K عـــدداً أولياً P نأخـــذ العلاقـــة :

$$f : Z \to K$$

المعـــرفة كمـــا يلي :

$$f(z) = z \cdot 1_K$$

فنجـــد أن العلاقـــة f تشاكل حلقـــي نواتـــه $\ker f = pZ$ وعندئذٍ

التطبيق :

$$\varphi : Z / pZ \to K$$

المعرف كمـــا يلي :

$$\varphi[x] = x \cdot 1_K \qquad \forall [x] \in Z / pZ$$

تشاكل حلقـــي متباين وبالتالي الحقـــل الجزئـــي $\operatorname{Im}\varphi$ يماثل Z / pZ

إذاً K ممـــدد للحقـــل Z / pZ .

ترميز :

ليكن $F[x]$ حلقـــة الحـــدوديات على حقـــل F وليكن $P \in F[x]$

حـــدودية نرمّز المثالي الرئيس المـــولد بـــ P بالرمز $< P >$ أي :

$$< P > = P \cdot F[x]$$

مبرهنة:

إذا كانت $P \in F[x]$ حدودية غير قابلة للتحليل على F فإن $F[x]/<P>$ هو ممدد للحقل F وللحدودية P صفر في الحقل $F[x]/<P>$

الإثبات:

بما أن المثالي الرئيس $<P>$ أعظمي في $F[x]$ وبالتالي $F[x]/<P>$ حقل كما أن المجموعة :

$$K = \{a+<P> \quad ; \quad a \in F\}$$

حقل جزئي من الحقل $F[x]/<P>$ وأن K يماثل F وهذا ما يثبت أن $F[x]/<P>$ ممدد للحقل F .

نفرض أن :

$$P = \sum_{i=0}^{n} a_i \cdot x^i$$

وبالتالي أياً كانت $x+<P> \in F[x]/<P>$ فإن :

$$\begin{aligned} P(x+<P>) &= a_0 + a_1(x+<P>) + \ldots + a_n(x+<P>)^n \\ &= <P> + \sum_{i=0}^{n} a_i \cdot x^i \\ &= <P> + P(x) \\ &= <P> \end{aligned}$$

لكن صفر الحقل $F[x]/<P>$ هو $<P>$ وبالتالي $x+<P>$ صفر للحدودية $P(x)$ في $F[x]/<P>$.

مبرهنة:

إذا كانت $F[x]$ حلقة الحدوديات على الحقل F وكانت $P \in F[x]$ بحيث $\deg P > 0$ فإن للحدودية P صفراً في أحد الحقول الممددة للحقل F

الإثبات:

إذا كانت P حدودية غير قابلة للتحليل على الحقل F فإن للحدودية P صفراً في الحقل $F[x]/<P>$ الذي هو ممدد للحقل F .

أما إذا كانت الحدودية P قابلة للتحليل على الحقل F فإنه توجد حدودية غير قابلة للتحليل $q(x) \in F[x]$ بحيث :

$$P(x) = q(x) \cdot f(x) \quad ; \quad f(x) \in F[x]$$

وبالتالي للحدودية $q(x)$ صفر في ممدد الحقل F وبملاحظة أن صفر الحدودية q هو صفر للحدودية P يكون قد تم المطلوب .

ملاحظة: إن أهمية المبرهنة السابقة تكمن في أنها توضح كيفية بناء حقل يمتلك صفراً للحدودية P انطلاقاً من حقل F .

مثال (١):

أوجد ممدداً للحقل $Z/2Z$ بمساعدة الحدودية $P(x) = x^2 + x + 1$

الحل:

بداية لنرمِّز الحقل Z/pZ بالرمز F_p .

إن :

$$\forall x \in F_2 \quad : \quad x^2 + x + 1 = 0$$

أي أن الحدودية $P(x) = x^2 + x + 1$ غير قابلة للتحليل في $F_2[x]$

وبالتالي المثالي $<P> = P \cdot F[x]$ أعظمي في $F_2[x]$.

وبالتالي يكون $K = F_2[x]/<P>$ حقلاً ممدداً للحقل F_2 ويمتلك صفراً للحدودية P .

مثال (٢):

أوجـــد ممـــدداً للحقـــل Q يحـــوي صفراً للحـــدودية $P(x)=x^2-2$

الحـــل:

إن الحـــدودية $P(x)=x^2-2$ غـــير قابلة للتحليل في Q وبالتالي :

$Q[x]/<P>$ ممـــدد الحقـــل Q . إن

$$Q(x)/<P>=\{(a+bx)+P \quad ; \quad a,b\in Q\}$$

لنأخـــذ العلاقـــة :

$$\varphi : Q[x]/<P> \quad \rightarrow \quad Q(\sqrt{2})$$

المعرفة كما يلي :

$$\varphi((a+bx)+P)=a+b\sqrt{2}$$

حيث :

$$Q(\sqrt{2})=\{a+b\sqrt{2} \quad ; \quad a,b\in Q\}$$

حقـــلاً (تأكد من ذلك).

فنجـــد بسهولة أن φ تماثل وبالتالي :

$$Q[x]/<P>=Q(\sqrt{2})$$

أي أن ممـــدد الحقـــل Q الذي يمتلك صفر للحـــدودية $P(x)=x^2-2$

هـــو الحقـــل :

$$Q(\sqrt{2})=\{a+b\sqrt{2} \quad ; \quad a,b\in Q\}$$

١٠ – ٣ العناصر الجـــبرية والعناصر المتسامية :

تعريف : ليكن K ممـــدداً للحقـــل F وليكن $\alpha\in K$. نقول عن α إنه جـــبري على F إذا وجـــدت حـــدودية $0\neq P(x)\in F[x]$

بحيث $P(\alpha)=0$. وإن لم يكن α جبرياً على F فإن α يدعى متسامياً على F .

أمثلة:

١.العدد $\sqrt{2}$ جبري على Q لأن R ممدد الحقل Q وأن $\sqrt{2}\in R$ وتوجد حدودية $P(x)=x^2-2$ في حلقة الحدوديات $R[x]$ بحيث $P(\sqrt{2})=0$.

٢.العدد i جبري على Q لأن C ممدد للحقل Q وأن $i\in C$ وتوجد حدودية $P(x)=x^2+1\in C[x]$ بحيث $P(i)=0$.

٣.إن العدد π متسامٍ على Q أثبت ذلك النمساوي Ferdinand Lindemann عام ١٨٨٢ ولا مجال لذكره الآن .

كما أن العدد e متسامٍ على Q أثبت ذلك العالم الفرنسي Charles Hermite عام ١٨٧٣ .

تبقى مبرهنة أولر التي وضعها عام ١٩٠٠ من أهم المبرهنات المتعلقة بالأعداد المتسامية على الحقل Q التي تنص :

" إذا كان $1\neq x\neq 0$ جبرياً على Q وكان $\alpha\neq 0$ جبرياً على Q فإن العدد x^{α} متسامٍ على Q ".

وحسب أولر يكون :

العدد $2^{\sqrt{3}}$ متسامياً على Q .

العدد $5^{2\sqrt{5}}$ متسامياً على Q .

بينما العدد $\sqrt{1+\sqrt{3}}$ جبريٌ على Q .

تعريف: ليكن الحقـــل K ممـــدداً للحقـــل F وليكن $\alpha \in F$.عندئذٍ التطبيق :

$$\varphi_\alpha : F[x] \to K$$

المعرف كما يلي :

$$\varphi_\alpha(P(x)) = P(\alpha) \qquad \forall P(x) \in F[x]$$

تشاكل ندعوه التشاكل الأساسي الموافق لـــ α .

مبرهنة:

إذا كان الحقـــل K ممـــدداً للحقـــل F وكان $\alpha \in F$ فإن :

(α متسامٍ على F) $\Leftrightarrow$ (التشاكل الأساسي φ_α متباين)

الإثبات: إن :

$$\varphi_\alpha : F[x] \to K$$
$$\varphi_\alpha(P(x)) = P(\alpha) \qquad \forall P(x) \in F[x]$$

($\Leftarrow$): لنفرض أن α متسامٍ على F عندئذٍ :

$$\forall 0 \neq P(x) \in F[x] \quad : \quad P(\alpha) \neq 0$$

وبالتالي :

$$\forall \quad f(x) \in \ker \varphi_\alpha \quad \Rightarrow \quad \varphi_\alpha(f(x)) = 0$$
$$\Rightarrow \quad f(\alpha) = 0$$

وبما أن α متسامٍ فإن $f(x) = 0$ وبالتالي : $\ker \varphi_\alpha = \{0\}$

أي أن التشاكل الأساسي φ_α متباين .

($\Rightarrow$): لنفرض أن التشاكل الأساسي φ_α متباين ولنفرض جدلاً أن α جبري على F عندئذٍ توجـــد حـــدودية $0 \neq P(x) \in F[x]$ بحيث $P(\alpha) = 0$

وبالتالي يكون :

$$P(x) \in \ker \varphi_\alpha \quad \wedge \quad P(x) \neq 0$$

وهـــذا يناقض كون φ_α متباين .

إذاً α ليس جـــبرياً على F فهو متسامٍ على F .

مبرهنة:

إذا كان الحقـــل K ممـــدداً للحقـــل F وكان $0 \neq \alpha \in K$ جـــبرياً على F فإنـــه توجـــد حـــدودية غـــير قابلة للتحليل $P(x) \in F[x]$ بحيث $\deg P > 1$. وإذا كانت $f(x) \in F[x]$ بحيث $f(\alpha) = 0$ فإن $P(x) | f(x)$.

الإثبات: لنأخـــذ التشاكل الأساسي :

$$\varphi_\alpha : F[x] \to K$$

$$\varphi_\alpha(P(x)) = P(\alpha) \qquad \forall P(x) \in F[x]$$

حسب المـــبرهنة الســـابقة ولكون α جـــبرياً فـــإن $\ker \varphi_\alpha \neq \{0\}$ وبمـــا أن $\ker \varphi_\alpha$ مثـــالي رئيس في الحلقـــة $F[x]$ وبالتالـــي يوجـــد $0 \neq P(x) \in F[x]$ بحيث $\deg P > 1$ من أجلها :

$$\ker \varphi_\alpha = < P(x) >$$

كمـــا أن الحـــدودية $P(x)$ غـــير قابلة للتحليل على F لأنـــه إذا فرضنا جـــدلاً أن الحـــدودية $P(x)$ قابلة للتحليل على F عندئذٍ توجد حدوديتين غـــير ثابتتين $q(x), r(x) \in F[x]$ بحيث :

$$P(x) = q(x) \cdot r(x) \quad ; \quad \deg q, \deg r < \deg P$$

وبمـــا أن $P(\alpha) = 0$ فإن :

$$q(\alpha) = 0 \quad \vee \quad r(\alpha) = 0$$

وهـــذا يناقض اختيار الحـــدودية $P(x)$.

إذاً الحـــدودية $P(x)$ غـــير قابلة للتحليل على F .

وأخـــيراً إذا كانت $0 \neq f(x) \in F[x]$ وكان $f(\alpha) = 0$ فـــإن :

$f(x) \in \ker \varphi_\alpha$ أي $f(x) \in < P(x) >$ وبالتالي $P(x) | f(x)$.

ملاحـــظة:

إذا وجـــدت حـــدودية أخرى $P_1(x)$ تحقق المـــبرهنة السابقة فإن :

$$P_1(x) = a \cdot P(x) \quad ; \quad 0 \neq a \in F$$

وبذلك الحـــدودية $P(x)$ المعرفـــة في المـــبرهنة السابقة وحيدة بغض النظر عن الثابت a .

تعريف:

ليكن الحقـــل K ممـــدداً للحقـــل F وليكن $\alpha \in K$ جـــبرياً على F ندعو الحـــدودية (الوحيدة) ذات الدرجـــة الأصغر التي تقبل α صفراً لها بالحـــدودية غـــير القابلة للتحلل لـــ α على F ونرمز لها بـــ $irr(\alpha, F)$ وندعـــو درجـــة الحـــدودية $irr(\alpha, F)$ بدرجـــة α على F ونرمز لهـــا بـــ $\deg(\alpha, F)$

مثال: إن العـــدد $\sqrt{2} \in R$ جـــبري على Q وهـــو جـــذر للحـــدودية $P(x) = x^2 - 2 \in Q[x]$ غـــير القابلة للتحليل على Q وهـــي الحـــدودية ذات الدرجـــة الأصغر في $Q[x]$ التي تقبل $\sqrt{2}$ صفراً لهـــا وبالتالي :

$$irr(\sqrt{2}, Q) = x^2 - 2$$

وأن :

$$\deg(\sqrt{2}, Q) = \deg(x^2 - 2) = 2$$

١٠ – ٤ التمـــديد البسيط :

إن دراســة التمــديد المنتهي للحقــول يعتمــد على مفهــوم قاعــدة الفضاء الشعاعي المنتهي البعــد على الحقــل F ولذلك سنذكر بتعــريف الفضاء الشعاعي V على الحقــل F وبمفهوم قاعدة وبعد الفضاء V .

تذكــرة: ليكن F حقــلاً ولتكن $V \neq \phi$ مزودة بقانــوني تشكيل الأول داخلي $(+)$ والآخــر خارجي (يساري) بمجموعــة مؤثراته F .

عندئــذٍ نقول عن البنية $(V,+,\circ)$ إنهــا فضاء شعاعي على F إذا تحققت الشروط :

I. البنية $(F,+)$ زمــرة تبديلية .

II. أياً كان $u,v \in V$ وأياً كان $\alpha,\beta \in F$ فإن :

1. $1 \cdot v = v$
2. $(\alpha+\beta)\cdot v = \alpha \cdot v + \beta \cdot v$
3. $\alpha \cdot (u+v) = \alpha \cdot u + \alpha \cdot v$
4. $\alpha \cdot (\beta \cdot v) = (\alpha \cdot \beta) \cdot v$

وتكون المجموعــة المنتهية $B = \{v_1, v_2, \ldots, v_n\}$ قاعدة للفضاء الشعاعي V عندما وفقط عندما كل عنصر $v \in V$ يكتب بوصفه تركيباً خطياً وبشكل وحيد لعناصر B أي أن :

$$\forall v \in V : \quad v \equiv \sum_{i=1}^{n} \alpha_i \cdot v_i \quad ; \quad \alpha_i \in F$$

وفي هــذه الحالــة يكون الفضاء V منتهي البعد نرّمز بعده بالرمز $\dim V$ وهــو يساوي قــدرة المجموعــة B أي أن :

$$\dim V = card B$$

وهنا نشير إلى أنه إذا كان V فضاءً شعاعياً بعـــده n $(n \neq 0)$ على حقل F فإن V يماثل F^n (الذي هو فضاء شعاعي على F) ، وأن كل حقل F هو فضاء شعاعي على نفسه بعده يساوي الواحد أي أن $(\dim F = 1)$

تعريف:

ليكن الحقـــل K ممـــدداً للحقـــل F . إذا كان K فضاءً شعاعياً منتهي البعـــد وكان $\dim K = n$ على F فإننا نقول إن K ممـــدد بسيط من الدرجـــة n للحقـــل F ونكتب $(K:F) = n$.

مثال:

إن C ممـــدد بسيط من الدرجـــة ٢ للحقـــل R أي $(C:R) = 2$.لأن C هـــو فضاء شعاعي على R ويقبل المجموعـــة $\{1,i\}$ قاعـــدة لـــه .

مبرهنة:

إذا كان E ممـــدداً بسيطاً من الدرجـــة n للحقـــل F وكان K ممـــدداً بسيطاً من الدرجة m للحقـــل E فإن K ممـــدد بسيط من الدرجة $n \cdot m$ للحقـــل F .

الإثبات: (واضح أن K ممـــدد للحقـــل F) نفرض أن $B = \{v_1, v_2, \ldots, v_n\}$ قاعـــدة للفضاء الشعاعي E على F ولنفرض أن $S = \{u_1, u_2, \ldots, u_n\}$ قاعـــدة للفضاء الشعاعي K على E عندئذ :

$$\forall x \in K \quad : \quad x \equiv \sum_{j=1}^{m} \alpha_j \cdot u_j \quad ; \quad \alpha_j \in E \quad j = 1,2,\ldots,m$$

وبما أن $\alpha_j \in E$ $(j = 1,2,\ldots,m)$ وبما أن B قاعـــدة لـــ E على F فإن :

$$\forall j=1,2,\dots,m \quad ; \quad \alpha_j \equiv \sum_{i=1}^{n} a_{ij}\cdot v_i \quad , \quad a_{ij}\in F \quad ; \quad i=1,2,\dots,n$$

وبالتالـــي :

$$\forall \quad x\in K \quad : \quad x \equiv \sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{ij}\cdot v_i\right)\cdot u_j$$

$$\equiv \sum_{i,j} a_{ij}\cdot(v_i\cdot u_j)$$

وهـــذا يعني أن المجمـــوعة :

$$B\cdot S=\{v_i\cdot u_j \quad ; \quad i=1,2,\dots,n \quad ; \quad j=1,2,\dots,m\}$$

قاعدة في الفضاء الشعاعي K على F وبملاحظة أن $card(B\cdot S)=n\cdot m$

أي أن :

$$(K:F)=(K:E)\cdot(E:F)$$

نتيجة: إذا كان F_i ممـــدداً بسيطاً للحقـــل F_{i-1} $(i=1,2,\dots,n)$ فإن F_n ممـــدد بسيط للحقـــل F_1 وأن :

$$(F_n:F_1)=(F_n:F_{n-1})\cdot(F_{n-1}:F_{n-2})\cdot\dots\cdot(F_2:F_1)$$

ملاحظة: إذا كان الحقـــل K ممـــدداً للحقـــل F وإذا كان $\alpha_1,\alpha_2\in K$ فـــإن $F(\alpha_1)$ هـــو أصغر حقـــل ممـــدد للحقل F ويحقق :

$$\alpha_1\in F(\alpha_1) \qquad \wedge \qquad F(\alpha_1)\subseteq K$$

وكذلك $(F(\alpha_1))\cdot(\alpha_2)$ هـــو أصغر حقـــل ممـــدد للحقل $F(\alpha_1)$ ويحقق :

$$\alpha_1,\alpha_2\in(F(\alpha_1))(\alpha_2) \quad \wedge \quad (F(\alpha_1))(\alpha_2)\subseteq K$$

وأن :

$$(F(\alpha_1))(\alpha_2)=(F(\alpha_2))(\alpha_1)$$

ولذلك نرمز لهذين الحقلين بالرمز $F(\alpha_1,\alpha_2)$.

وبشكل عام إذا كانت $\alpha_1,\alpha_2,\ldots,\alpha_n \in K$ فإن $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ هو أصغر حقل ممدد للحقل F بحيث :

$$\alpha_i \in F(\alpha_1,\alpha_2,\ldots,\alpha_n) \quad i=1,2,\ldots,n$$

حيث :

$$F(\alpha)=\{a+b\sqrt{\alpha} \quad ; \quad a,b\in F\}$$

مثال: نعلم أن :

$$Q(\sqrt{2})=\{a+b\sqrt{2} \quad ; \quad a,b\in Q\}$$

ممدد للحقل Q وأن المجموعة $B_1=\{1,\sqrt{2}\}$ قاعدة للفضاء $Q(\sqrt{2})$ على Q. كما أن $(Q(\sqrt{2}))(\sqrt{3})$ ممدد للحقل $Q(\sqrt{2})$ على $Q(\sqrt{2})$ وأن المجموعة $B_2=\{1,\sqrt{3}\}$ قاعدة للفضاء $(Q(\sqrt{2}))(\sqrt{3})$ على $Q(\sqrt{2})$ وبالتالي المجموعة :

$$B_1\cdot B_2=\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$$

قاعدة للحقل $Q(\sqrt{2},\sqrt{3})$ على Q .

مبرهنة:

إذا كان K حقلاً منتهياً فإن مميز K عدد أولي P ويوجد $n\in N-\{0\}$ بحيث $cardK=P^n$.

الإثبات:

بما أن K حقل فإن مميزه معدوماً أو عدد أولي P . فإذا كان مميز الحقل K معدوماً فإن K ممدد للحقل Q وهذا يناقض كون K حقلاً منتهياً . إذاً مميز الحقل K عدد أولي P وبالتالي K ممدد للحقل $Z/PZ=F_P$. وبما أن الحقل K منته فإن K ممدد بسيط

للحقـــل F_P وليكن درجـــة هـــذا الممـــدد :

$$(K : F_p) = \dim K = n$$

عندئذٍ الفضاء الشعاعي K يماثل الفضاء F_P^n على F_P أي أن :

$$cardK = \dim K = \dim F_P^n = P^n$$

مبرهنة:

إذا كانت $P(x) \in F_P[x]$ حـــدودية غـــير قابلة للتحليل على F_P وإذا كان $\deg P = n > 0$ فإن الحقـــل $K = F_P[x]/< P >$ منتهٍ وأن :

$$cardK = P^n$$

الإثبات: لنأخـــذ العلاقـــة :

$$\varphi : F_P^n \to K$$

المعرفـــة كمـــا يلي :

$$\varphi(a_0, a_1, \ldots, a_{n-1}) = \sum_{i=0}^{n-1} a_i \cdot x^i \qquad \forall a_i \in F_P \quad ; \quad i = 0, \ldots, n-1$$

إن العلاقـــة φ تطبيق متباين لأن :

$$\forall (a_0, a_1, \ldots, a_{n-1}), (b_0, b_1, \ldots, b_{n-1}) \in F_P^n :$$

$$\varphi(a_0, a_1, \ldots, a_{n-1}) = \varphi(b_0, b_1, \ldots, b_{n-1}) \Leftrightarrow$$

$$\Leftrightarrow \sum_{i=0}^{n-1} a_i \cdot x^i = \sum_{i=0}^{n-1} b_i \cdot x^i$$

$$\Leftrightarrow (\sum_{i=0}^{n-1} (a_i - b_i) \cdot x^i \in < P(x) >) \quad \vee \quad P(x) \Big| \sum_{i=0}^{n-1} (a_i - b_i) \cdot x^i$$

وبما أن :

$$\deg(\sum_{i=0}^{n-1} (a_i - b_i) \cdot x^i) < \deg P$$

فإن :

$$\varphi(a_0,a_1,\dots,a_{n-1})=\varphi(b_0,b_1,\dots,b_{n-1}) \Leftrightarrow$$
$$\Leftrightarrow \sum_{i=0}^{n-1}(a_i-b_i)\cdot x^i=0$$
$$\Leftrightarrow a_i=b_i \quad ; \quad i=0,1,\dots,n-1$$
$$\Leftrightarrow (a_0,a_1,\dots,a_{n-1})=(b_0,b_1,\dots,b_{n-1})$$

كمـــا أن التطبيق φ غامر لأن :

أيـــاً كان $[f]\in K$ فإن $f\in F_P[x]$ وبالتالي حســـب خوارزمية القسمة يوجـــد $q,r\in F_P[x]$ بحيث :

$$f=p\cdot q+r \quad ; \quad \deg r<\deg p$$

أي أن :

$$[f]=r\in \operatorname{Im}\varphi$$

إذن φ تطبيق متباين وغامر فهـــو تقابل ومنـــه :

$$cardK=card(F_p^n)=P^n$$

١٠ – ٥ تطبيقات تمـــديد الحقول في الإنشاءات الهندسية :

إن الإنشاء الهنـــدسي يعتمـــد فقط على الفرجـــار والمسطرة ، فباستخدام الفرجار والمسطرة يمكن إنشاء بعض الإنشاءات الهندسية مثل :

- منصف قطاع زاوي .
- مستقيم D يمر من نقطة معلومة M_0 ويوازي مستقيماً آخراً D' .
- إنشاء قطاع زاوي قياسه يساوي مجموع قياسي قطاعين زاويين معلومين.
- إنشاء مماس لدائـــرة مرسوم من نقطة تقع خارج الدائـــرة .

لكن هناك بعض الرسوم الهندسية التي لا يمكن إنشاؤها بالفرجار والمسطرة

مثل : ١- إنشاء مربع مساحته تساوي مساحة دائرة معلومة .

٢- إنشاء مستقيمين يثلثان قطاع زاوي قياسه 60° .

وهنا يُطرح التساؤل التالي : أي من الإنشاءات الهندسية يمكن إنشاؤها بالفرجار والمسطرة وأيها غير ممكن . إن الإجابة على هذا التساؤل يكمن في المبرهنة التالية التي نعرضها دون برهان (لأن الإثبات خارج نطاق الكتاب).

مبرهنة:

إذا كان $\alpha \in R$ قابلاً للإنشاء الهندسي فإنه يوجد $k \in N$ بحيث

$$\deg(\alpha, Q) = 2^k$$

مثال (١): ليكن لدينا مكعباً حجمه $V = 1$. أثبت أنه لا يمكن إنشاء طول ضلع مكعب آخر بحيث يكون حجمه $V' = 2V$.

الحل: بما أن حجم المكعب الأصلي $V = 1$ فإن طول ضلعه $\lambda = 1$ وبما أن حجم المكعب المراد إنشاء ضلعه هو $V' = 2V = 2$ فإن طول ضلعه $\lambda' = \sqrt[3]{2}$ وبملاحظة أن العدد $\alpha = \sqrt[3]{2}$ جبري على Q حيث أنه صفر للحدودية $P(x) = x^3 - 2 \in Q[x]$ وأن $P(x)$ غير قابلة للتحليل في Q فإن :

$$irr(\sqrt[3]{2}, Q) = x^3 - 2$$

وبالتالي :

$$\deg(\sqrt[3]{2}, Q) = 3$$

لكن لا يوجد $k \in N$ بحيث $2^k = 3$ وبالتالي $\lambda' = \sqrt[3]{2}$ غير قابل للإنشاء الهندسي .

مثال (٢): أثبت أنه لا يمكن تثليث قطاع زاوي قياسه 60° .

الحـــل: إن :

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

وبالتالي إمكانية تثليث القطاع 3θ يكافئ إنشاء الطول $|\cos\theta|$.

إن $3\theta = 60$ وبالتالي $\cos 3\theta = \frac{1}{2}$ ولنفرض أن $\cos 20 = \cos\theta = \alpha$

فنجـــد أن :

$$\frac{1}{2} = 4\alpha^3 - 3\alpha$$

ومنـــه :

$$\alpha^3 - \frac{3}{4}\alpha - \frac{1}{8} = 0$$

أي أن α صفر للحـــدودية $P(x) = x^3 - \frac{3}{4}x - \frac{1}{8} \in Q[x]$ وأن $P(x)$

غـــير قابلة للتحليل في Q .(تأكد من ذلك) وبالتالي :

$$irr(\alpha, Q) = x^3 - \frac{3}{4}x - \frac{1}{8}$$

وبالتالي :

$$\deg(\alpha, Q) = 3$$

وبما أنه لا يوجـــد $k \in N$ من أجله $2^k = 3$ فإن إنشاء $|\cos\theta|$ غير ممكن.

مثال (٣): أثبت أنه لا يمكن إنشاء مربع يكافئ بالمساحة دائـــرة نصف قطرها ١ .

الحـــل: إن مساحة الدائـــرة $S = \pi$ وبالتالي يكون طول ضلع المربع $\lambda = \sqrt{\pi}$

وبما أن π عـــدد متسامٍ على Q فإن $\sqrt{\pi}$ متسامٍ على Q وبالتالي لا يمكن إنشاء $\lambda = \sqrt{\pi}$. أي لا يمكن إنشاء المربع .

سنعرض الآن مبرهنة تبين الشروط الواجب توافرهـــا لإنشاء ضلع منتظم .

مبرهنة:

إذا كان λ مضلعاً عـــدد أضلاعه n فإن λ قابلاً للإنشاء إذا وفقط إذا كان

$$n = 2^k \quad \vee \quad n = 2^k \cdot p_1 \cdot \ldots \cdot p_m$$

حيث :

$$k \in N \quad ; \quad p_j = 2^{(2^{\lambda})} + 1 \quad ; \quad \lambda \in N \quad j = 1,2,\ldots,m$$

مثال (١): إن المضلع المنتظم الذي عـــدد أضلاعه $n = 60$ قابل للإنشاء الهندسي لأن :

$$n = 4 \cdot 3 \cdot 5 = 2^2 \cdot (2^1 + 1) \cdot (2^2 + 1)$$

تمرينات محلولـــة

التمرين الأول:

أوجـــد ممـــدداً للحقـــل Q بمساعدة الحـــدودية :

$$P(x) = x^4 - 5x^2 + 6$$

وهل هـــذا الممـــدد وحيد أم لا مع التعليل .

الحـــل: إن الحـــدودية $P(x)$ قابلة للتحليل على Q لأن :

$$P(x) = (x^2 - 2)\cdot(x^2 - 3)$$

إن كلاً من الحـــدوديتين :

$$P_1(x) = x^2 - 2 \quad , \quad P_2(x) = x^2 - 3$$

غير قابلة للتحليل في Q . وبالتالي يمكن إيجاد ممـــدد للحقل Q بطريقتين .

الطريقة الأولى : إذا أخـــذنا الـــحدودية $P_1(x) = x^2 - 2$ حصلنا على الممـــدد $Q[x]/< P_1 >$ لـــ Q حيث :

$$Q[x]/< P_1 > \cong Q(\sqrt{2}) = \{a + b\sqrt{2} \quad ; \quad a,b \in Q\}$$

الطريقة الثانية : إذا أخـــذنا الـــحدودية $P_2(x) = x^2 - 3$ حصلنا على الممـــدد $Q[x]/< P_2 >$ لـــ Q حيث :

$$Q[x]/< P_2 > \cong Q(\sqrt{3}) = \{a + b\sqrt{3} \quad ; \quad a,b \in Q\}$$

لاحظ أن كلاً من $Q(\sqrt{2})$, $Q(\sqrt{3})$ يحوي صفراً للحدودية $P(x)$.

التمرين الثاني :

أثبت أن العـــدد الحقيقي $\alpha = \sqrt{1+\sqrt{3}}$ جـــبري على Q ثـــم عيّن

$$\deg(\alpha, Q) \quad , \quad irr(\alpha, Q)$$

الحـــل: إن : $\alpha = \sqrt{1+\sqrt{3}}$

وبالتالي :

$$\alpha^2 = 1+\sqrt{3} \quad , \quad \alpha^4 = 1+2\sqrt{3}+3$$

وبالتالي يكون :

$$\alpha^4 - 2\alpha^2 - 2 = 0$$

أي أن α هـو صفر للحـدودية :

$$P(x) = x^4 - 2x^2 - 2 \in Q[x]$$

وهـذا يثبت أن العـدد $\sqrt{1+\sqrt{3}}$ جـبري على Q .

لنوجـد الآن $irr(\alpha,Q)$:

إن الحـدودية $P(x) = x^4 - 2x^2 - 2$ غـير قـابلة للتحـليل على Q .

(تأكد من ذلك) وتقبل العـدد $\alpha = \sqrt{1+\sqrt{3}}$ صفراً لهـا وبالتالي :

$$irr(\alpha,Q) = x^4 - 2x^2 - 2$$

وبالتالي :

$$\deg(\alpha,Q) = 4$$

التمرين الثالث :

أوجـد $(Q(\sqrt{2},\sqrt{3}):Q)$ ثـم أوجـد

$\left(Q(\sqrt{2},\sqrt[3]{2}):Q(\sqrt[6]{2})\right)$ واستنتج أن $Q(\sqrt{2},\sqrt[3]{2}) = Q(\sqrt[6]{2})$

وأن : $\left(Q(\sqrt{2},\sqrt[3]{2}):Q\right) = 6$

الحـل: إن الحقـل $Q(\sqrt{2})$ ممـدد للحقـل Q وأن المجموعـة $B_1 = \{1,\sqrt{2}\}$

قاعـدة للحقـل $Q(\sqrt{2})$ على الحقـل Q .

كما أن صفر الحـدودية $P(x) = x^3 - 2 \in Q[x]$ لا ينتمي إلى $Q(\sqrt{2})$

أي أن $\sqrt[3]{2} \notin Q(\sqrt{2})$ وبالتالي المجمـــوعة :

$$B_2 = \{1, \sqrt[3]{2}, \sqrt[3]{2^2}\}$$

قاعـــدة للحقـــل $Q(\sqrt{2}, \sqrt[3]{2})$ على الحقـــل $Q(\sqrt{2})$ وبالتالي المجموعة:

$$B_1 \cdot B_2 = \{1, \ \sqrt{2} \ , \ \sqrt[3]{2} \ , \ \sqrt[6]{2^5} \ , \ \sqrt[3]{2^2} \ , \ \sqrt[6]{2^7}\}$$

قاعـــدة للحقـــل $Q(\sqrt{2}, \sqrt[3]{2})$ على Q . وبملاحظة أن :

$$\sqrt[6]{2} \in Q(\sqrt{2}, \sqrt[3]{2}) \quad ; \quad \sqrt[6]{2^7} = 2\sqrt[6]{2}$$

وأن $\sqrt[6]{2}$ صفر للحـــدودية $x^6 - 2 \in Q[x]$ غـــير القابلة للتحليل على Q فإن $Q(\sqrt[6]{2})$ ممـــدد للحقـــل Q . كما أن الحقـــل $Q(\sqrt{2}, \sqrt[3]{2})$ ممدد للحقـــل $Q(\sqrt[6]{2})$.إذاً المجموعـــة :

$$S = \{1, \ \sqrt{2} \ , \ \sqrt[3]{2} \ , \ \sqrt[6]{2^5} \ , \ \sqrt[3]{2^2} \ , \ 2\sqrt[6]{2}\}$$

قاعـــدة للحقـــل $Q(\sqrt{2}, \sqrt[3]{2})$ على Q وبالتالي :

$$\left(Q(\sqrt{2}, \sqrt[3]{2}) : Q\right) = cardS = 6$$

ويكون :

$$\begin{aligned}\left(Q(\sqrt{2}, \sqrt[3]{2}) : Q\right) &= \left(Q(\sqrt{2}, \sqrt[3]{2}) : Q(\sqrt[6]{2})\right) \cdot \left(Q(\sqrt[6]{2}) : Q\right) \\ &= \left(Q(\sqrt{2}, \sqrt[3]{2}) : Q(\sqrt{2})\right) \cdot 6\end{aligned}$$

ومنـــه :

$$\left(Q(\sqrt{2}, \sqrt[3]{2}) : Q(\sqrt[6]{2})\right) = 1$$

وأن :

$$Q(\sqrt{2}, \sqrt[3]{2}) = Q(\sqrt[6]{2})$$

تمرينات (١٠)

التمرين الأول :

بيّن أيّاً من الأعـــداد التاليـــة جـــبري على Q وأيهـــا متسامٍ :

$$1+\sqrt{2} \quad , \quad \sqrt{\pi} \quad , \quad \pi^2 \quad , \quad \sqrt{1+\sqrt[3]{2}} \quad , \quad 1+i \quad , \quad \sqrt{2}+i$$

وفي الحالـــة التي يكون فيهـــا العـــدد α جـــبرياً عيّن $irr(\alpha,Q)$ ، $\deg(\alpha,Q)$

التمرين الثاني :

لنفرض أن $Z/pZ = F_p$ ولنأخـــذ الحـــدودية :

$$P(x) = x^3 + x^2 + 1 \in F_2[x]$$

والمطلوب :

١. أثبت أن الحـــدودية $P(x)$ غير قابلة للتحليل على F_2 .

٢. بفرض α صفر للحـــدودية $P(x)$ في ممـــددٍ للحقل F_2 أوجـــد $F_2(\alpha)$.

التمرين الثالث :

ليكن الحقـــل K ممـــدداً للحقـــل F ولنأخـــذ المجموعـــة :

$$A = \{\alpha \in K \quad ; \quad \alpha \text{ جـــبري على } F\}$$

برهـــن أن A حقـــل جزئـــي من الحقـــل K يحـــوي F .

التمرين الرابع :

احسب المقاديـــر :

1. $\left(Q(\sqrt{2},\sqrt{3}):Q\right)$
2. $\left(Q(\sqrt[3]{2},\sqrt{3}):Q\right)$
3. $\left(Q(\sqrt{3},\sqrt[3]{5}):Q\right)$
4. $\left(Q(\sqrt{2},\sqrt{6}):Q(\sqrt{3})\right)$

التمرين الخامس :

برهـــن أن الحـــدودية :

$$P(x)=x^2-3\in Q[x]$$

غـــير قابلـــة للتحليل على $Q(\sqrt[3]{2})$.

التمرين السادس :

اثبت أنـــه يمـــكن إنشـــاء مضلع منتظم عـــدد أضلاعـــه n في كل من الحالات الآتيـــة :

1). $n=5$
2). $n=10$
3). $n=120$

التمرين السابع :

اثبت أنـــه يمكن تثليث قطاع زاوي قياسه 45° .

الفصل الحادي عشر

مبادئ نظريـــة الجبـــور

١١ – ١ تعاريف :

١. لتكن R حلقـــة تبديلية واحـــدها 1_R ولتكن A مجموعـــة غير خالية مزودة بثلاثة قوانين تشكيل :

الأول : داخلي $(+)$ وندعوه الجمـــع في A .

الثاني : خارجي (يساري) $(\cdot)$ مجموعـــة مؤثراته الحلقة R وندعـــوه الضرب بعنصر من R .

الثالث : داخلي $(\cdot)$ وندعوه الضرب في A .

نقول عن البنية $(A,+;\cdot,\cdot)$ إنهـــا جبر على R إذا تحققت الشروط التالية:

١. البنية $(A,+,\cdot)$ مقاس على R .

٢. الضرب في A توزيعي على الجمـــع في A .

٣. أياً كان $a,b \in A$ وأياً كان $\alpha \in R$ فإن :

$$\alpha \cdot (a \cdot b) = (\alpha \cdot a) \cdot b = a \cdot (\alpha \cdot b)$$

ونقول عن الجـــبر A إنـــه جـــبر تجميعي إذا كان الضرب في A تجميعياً .

ونقول عن الجـــبر A إنـــه جـــبر تبديلي إذا كان الضرب في A تبديلياً .

ونقول عن الجـــبر A إنه جبر واحدي إذا وجد في A عنصراً محايداً بالنسبة لقانون الضرب في A .

أمثلة: ١. إن مجموعة الأعداد العقدية C جبر تجميعي تبديلي واحدي على R .

٢. إن كل حلقـــة هـــي جـــبر على Z .

ملاحظة هامة :

فيما يلي دوماً نعدّ الحلقة R هي حلقة تبديلية واحدية .

١١ – ٢ الجبر الجزئي :

تعريف (١) : ليكن A جبراً على الحلقة R ولتكن $\phi \neq B \subseteq A$.

نقول عن B إنه جبر جزئي من الجبر A عندما وفقط عندما يتحقق الشرطان التاليان :

1. $\forall \alpha, \beta \in R \quad , \quad \forall a, b \in B \quad : \quad \alpha \cdot a + \beta \cdot b \in B$
2. $\forall a, b \in B \quad : \quad a \cdot b \in B$

بعبارة مكافئة :

نقول عن المجموعة $\phi \neq B \subseteq A$ إنها جبر جزئي من الجبر A إذا تحقق الشرطان التاليان :

١. B مقاس جزئي من المقاس A .

٢. B مغلقة بالنسبة للضرب في A .

مثال: إذا كان A جبراً على حلقة R ولنأخذ المجموعة :

$$B = \{x \cdot y \quad ; \quad x, y \in A\}$$

فنجد بسهولة أن B جبر جزئي من الجبر A . (تأكد من ذلك)

١١ – ٣ المثاليات في الجبر :

تعريف : ليكن A جبراً على حلقة R وليكن $\phi \neq I \subseteq A$.

- نقول عن I إنه مثالي يساري في الجبر A إذا تحقق الشرطان التاليان:

أ- I مثالي جزئي من المقاس A .

ب- أياً كان $a \in A$ ، وأياً كان $x \in I$ فإن $a \cdot x \in I$

• نقول عن I إنــه مثالي يميني في الجــبر A إذا تحقق الشرطان التاليان:

أ- I مقاس جزئــي من المقاس A .

ب- أياً كان $a \in A$ ، وأيــاً كان $x \in I$ فإن $x \cdot a \in I$.

• نقول عن I إنــه مثالي في الجــبر A إذا كان I مثالياً يسارياً ويمينياً في A في آن واحــد .

ملاحظة (١): كل مثالي I في الجــبر A هــو جــبر جزئــي من A .

ملاحظة (٢): كل عنصر $\phi \neq a \in A$ يولد مثالياً $I = < a >$ يدعى المثالي الرئيس المولد بـــ a .

١١ – ٤ جــبر القسمة :

بناء جــبر القسمة : ليكن A جــبراً على حلقــة R وليكن I مثالياً في A ولنأخــذ المجموعــة :

$$A/I = \{a + I \quad ; \quad a \in A\}$$

لاحــظ أن البنية $(I,+)$ زمــرة تبديلية وبالتالــي يمكن أن نأخــذ كل المرافقات A/I . كما أن $A/I \neq \phi$ لأن $I = 0_A + I \in A/I$.

ولنعرف في A/I قوانين التشكيل الآتيــة :

$+ : (x+I)+(y+I) = (x+y)+I$ داخلي (الجمــع)

$\bullet : \alpha \cdot (x+I) = (\alpha \cdot x)+I$ خارجي بمجموعة مؤثراته R

$\bullet : (x+I)\cdot(y+I) = (x \cdot y)+I$ داخلي (الضرب)

حيث :

$$(x+I),(y+I) \in A/I \quad , \quad \alpha \in R$$

عندئذ نجـــد أن :

١. A/I مقاس على R (مقاس القسمة للمقاس A على I) .

٢. أياً كان $(x+I),(y+I),(z+I) \in A/I$ فيكون :

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

وبطريقة مشابهة نجـــد أن :

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

٣. أياً كان $(x+I),(y+I) \in A/I$ وأياً كان $\alpha \in R$ فإن :

$$\begin{aligned}\alpha\cdot[(x+I)\cdot(y+I)] &= \alpha\cdot(x\cdot y+I) \\ &= \alpha\cdot(x\cdot y)+I \\ &= (\alpha\cdot x)\cdot y+I \\ &= x\cdot(\alpha\cdot y)+I \\ &= (\alpha\cdot x+I)\cdot(y+I) \\ &= (x+I)\cdot(\alpha\cdot y+I)\end{aligned}$$

مما سبق نجـــد أن A/I جـــبر على A ندعوه جـــبر قسمة الجـــبر A على المثالي I .

ملاحظة: إن صفر الجـــبر A/I هو المثالـــي I . وإذا كان الجـــبر A واحـــدياً واحده 1_A فإن الجـــبر A/I واحـــدي أيضاً وعنصره المحايد هـــو 1_A+I ويبرهن على أنـــه إذا كان A جـــبراً على حلقـــة R وكان I مثالياً في الجـــبر A فإنـــه يوجـــد تقابل يحافظ على الاحتواء بين مجموعـــة الجبور

الجزئيـــة من جـــبر القسمة A/I وبين مجموعـــة المثاليات N في A بحيث يكون $I \subseteq N \subseteq A$. وبذلك يكون كل جـــبر جزئـــي من الجبر A/I من الشكل N/I بحيث $I \subseteq N \subseteq A$.

١١ ـ ٥ التشاكلات الجـــبرية :

تعاريف: ليكن A_1, A_2 جـــبران على الحلقـــة R . نقول عن التطبيق : $f : A_1 \to A_2$ إنـــه تشاكل جـــبري إذا تحققت الشروط :

1. $f(a+b) = f(a) + f(b)$
2. $f(a \cdot b) = f(a) \cdot f(b)$
3. $f(\lambda \cdot a) = \lambda \cdot f(a)$

وذلك أيـــاً كان $a,b \in A_1$ ، وأيـــاً كان $\lambda \in R$.

وإذا كان التشاكل الجـــبري غامراً ومتبايناً فيدعى عندئذٍ تماثلاً ونقول عندئذٍ إن الجـــبران A_1, A_2 متماثلان ونكتب $A_1 \cong A_2$.

ملاحظة: يمكن دمج الشرطين (١) و (٢) بشرط مكافئ والذي هـــو :

$$\forall \alpha, \beta \in R, \forall a,b \in A_1 : f(\alpha \cdot a + \beta \cdot b) = \alpha \cdot f(a) + \beta \cdot f(b)$$

مبرهنة:

إذا كان $f : A_1 \to A_2$ تشاكلاً جـــبرياً فإن :

(١). $\ker f$ مثالي في A_1 .

(٢). $\operatorname{Im} f$ جـــبر جزئـــي من A_2 .

الإثبات: (١) : إن $\ker f$ مقاس جزئـــي من المقاس A_1 (انظر الفصل الثامن) ، كما أنـــه :

$$\forall a \in A_1, \forall b \in \ker f : f(a \cdot b) = f(a) \cdot f(b) = f(a) \cdot 0 = 0$$

$$f(b \cdot a) = f(b) \cdot f(a) = 0 \cdot f(a) = 0$$

أي أن :

$$a \cdot b \in \ker f \quad \wedge \quad b \cdot a \in \ker f$$

إذاً $\ker f$ مثالي في الجسر A_1 .

(٢) : إن $\operatorname{Im} f$ مقاس جزئي من المقاس A_2 كما أنه :

$$\forall y_1, y_2 \in \operatorname{Im} f \ : \ \exists x_1, x_2 \in A_1 \ : \ y_1 = f(x_1) \wedge y_2 = f(x_2)$$

وبالتالي يكون :

$$y_1 \cdot y_2 = f(x_1) \cdot f(x_2) = f(x_1 \cdot x_2) \in \operatorname{Im} f$$

إذاً : $\operatorname{Im} f$ جبر جزئي من A_2 .

تمرين: ليكن A جبراً على حلقة R وليكن I مثالياً في A ولنأخذ التطبيق :

$$\pi : A \to A/I$$

المعرف كما يلي :

$$\pi(a) = a + I \qquad \forall a \in A$$

أثبت أن π تشاكل جبري غامر نواته I .

الحل: أياً كان $a, b \in A$ وأياً كان $\lambda \in R$ فإن :

1. $$\begin{aligned} \pi(a+b) &= (a+b) + I \\ &= (a+I) + (b+I) \\ &= \pi(a) + \pi(b) \end{aligned}$$

2. $$\begin{aligned} \pi(a \cdot b) &= (a \cdot b) + I \\ &= (a+I) \cdot (b+I) \\ &= \pi(a) \cdot \pi(b) \end{aligned}$$

3. $$\begin{aligned} \pi(\lambda \cdot a) &= \lambda \cdot a + I \\ &= \lambda(a+I) \\ &= \lambda \pi(a) \end{aligned}$$

أي أن π تشاكل جبري . كما أن التطبيق π غامر لأنه

$$\forall (a+I) \in A/I \quad : \quad \exists a \in A \quad : \quad \pi(a) = a+I$$

وأخيراً :

$$\begin{aligned} \forall x \in \ker \pi \quad &\Leftrightarrow \quad \pi(x) = I \\ &\Leftrightarrow \quad x + I = I \\ &\Leftrightarrow \quad x \in I \end{aligned}$$

أي أن : $\ker \pi = I$.

يدعى هذا التشاكل الغامر بالغمر القانوني في الجبر A .

مبرهنة:

إذا كان $f : A \to B$ تشاكلاً جبرياً فإن :

$$A/\ker f \cong \operatorname{Im} f$$

الإثبات: لنأخذ التطبيق :

$$\varphi : A/\ker f \to \operatorname{Im} f$$

المعرف كما يلي :

$$\varphi(a + \ker f) = f(a)$$

فنجد أن φ تطبيق متباين لأن :

$$\forall (a+\ker f), (b+\ker f) \in A/\ker f :$$

$$\begin{aligned} \varphi(a+\ker f) = \varphi(b+\ker f) &\Leftrightarrow f(a) = f(b) \\ &\Leftrightarrow f(a-b) = 0 \\ &\Leftrightarrow a - b \in \ker f \\ &\Leftrightarrow a + \ker f = b + \ker f \end{aligned}$$

كما أن φ غامر لأن :

$$\forall y \in I_m f \quad : \quad \exists x \in A \quad : \quad y = f(x)$$

وبالتالي يوجـــد $x + \ker f \in A/\ker f$ بحيث يكون :

$$\varphi(x + \ker f) = f(x) = y$$

كما أن φ تشاكل جـــبري لأن :

$$\forall (a + \ker f), (b + \ker f) \in A/\ker f \quad ; \quad \alpha, \beta \in R :$$

1. $$\begin{aligned}\varphi(\alpha(a + \ker f) + \beta(b + \ker f)) &= \varphi((\alpha a + \ker f) + (\beta b + \ker f)) \\ &= \varphi(\alpha \cdot a + \beta \cdot b + \ker f) \\ &= f(\alpha \cdot a + \beta \cdot b) \\ &= \alpha \cdot f(a) + \beta \cdot f(b) \\ &= \alpha\varphi(a + \ker f) + \beta\varphi(b + \ker f)\end{aligned}$$

2. $$\begin{aligned}\varphi((a + \ker f) \cdot (b + \ker f)) &= \varphi(a \cdot b + \ker f) \\ &= f(a \cdot b) \\ &= f(a) \cdot f(b) \\ &= \varphi(a + \ker f) \cdot \varphi(b + \ker f)\end{aligned}$$

مما سبق نجـــد أن φ تماثل جـــبري وبالتالي :

$$A/\ker f \cong \operatorname{Im} f$$

نتيجة: إذا كان f غامراً فإن $\operatorname{Im} f = B$ وعندئذٍ يكون $A/\ker f \cong B$

١١ – ٦ تشاكل الاشتقاق :

تعريف: ليكن A جـــبراً على الحلقـــة R . نعرف التشاكل الاشتقاق على الجبر A بأنه تشاكل مقاسي : $d : A \to A$ الذي يحقق الشرط :

$$\forall x, y \in A \quad : \quad d(x \cdot y) = dx \cdot y + x \cdot dy$$

ونرمز لمجموعة كل التشاكلات الاشتقاق على الجبر A بالرمز $Der(A)$

إذا عرفنا في المجموعة $Der(A)$ قانون التشكيل :

داخلي $(+)$: $\forall d_1, d_2 \in Der(A), \forall x \in A:$

$$(d_1 + d_2)x = d_1 x + d_2 x$$

خارجي بمجموعة مؤثراته R $(\cdot)$: $\forall \lambda \in R \quad , \forall x \in A \quad ; \forall d \in Der(A)$

$$\lambda(dx) = (\lambda d)x$$

فنجد أن $Der(A)$ مقاس على الحلقة R - تأكد من ذلك -

١١ - ٧ جبر لي : Lie Algebra

تعريف: نعرف جبر لي بأنه جبر L على الحقل F و يحقق الضرب فيه الشرطين التاليين :

1). $x \cdot x = 0 \qquad \forall x \in L$

2). $x \cdot (y \cdot z) + y \cdot (z \cdot x) + z \cdot (x \cdot y) = 0 \qquad \forall x, y, z \in L$

وعادة يرمز للجداء $x \cdot y$ في جبر لي بالرمز $[x, y]$ وبذلك نكتب الشرطين السابقين بالشكل :

1). $[x, y] = 0 \qquad \forall x \in L$

2). $[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0 \qquad \forall x, y, z \in L$

وتعرف العلاقة (٢) بمتطابقة جاكوبي .

ملاحظة هامة: إذا كان $L \neq \{0\}$ فإن جبر لي L ليس واحدياً لأنه إذا كان واحدياً لكان : $[1_L, 1_L] = 0 \quad \Rightarrow \quad 1_L = 0$

وعندئذٍ يكون :

$$\forall x \in L \neq \{0\} \quad : \quad x = [x, 1_L] = [x, 0] = 0$$

وهـــذا تناقض . إذن كل جـــبر لي يحـــوي عنصراً محايـــداً يكون تافـــهاً .

نتيجـــة: في جـــبر لي L يكون :

$$\forall x,y \in L \quad : \quad [x,y] = -[y,x]$$

البرهـــان: إن

$$\forall x,y \in L \quad : \quad [(x+y),(x+y)] = 0$$

وبالتالي :

$$[x,x]+[x,y]+[y,x]+[y,y] = 0$$

وحسب الشرط (١) يكون :

$$[x,y]+[y,x] = 0$$

ومنـــه : $[x,y] = -[y,x]$

ويُبرهن على أنـــه إذا كان مميـــز الحقـــل F مختلفاً عن 2 فإن القضيتين التاليتين متكافئتان :

1. $\forall x \in L \quad : \quad [x,x] = 0$
2. $\forall x,y \in L \quad : \quad [x,y] = -[y,x]$

مثال: ليكن A جـــبراً تجميعياً على الحقـــل F ولنعرف في A عملية الضرب $[,]$ كما يلي :

$$\forall x,y \in A \quad : \quad [x,y] = x \cdot y \quad y \cdot x$$

حيث العملية . في الطرف الأيمن هي عملية الضرب في الجـــبر A .

عندئذٍ يكون A جـــبر لي لأن A جـــبراً على الحقـــل F (فرض) كما أن:

1. $\forall x \in A \quad : \quad [x,x] = x \cdot x - x \cdot x = 0$

$$\forall x,y,z \in A \quad : \quad [x,[y,z]] = [x, y \cdot z - z \cdot y]$$

$$= x\cdot(yz - zy) - (yz - zy)\cdot x$$
$$= xyz - xzy - yzx - zyx \quad \dots \quad (1)$$

$$[y,[z,x]] = [y, zx - xz]$$
$$= y\cdot(zx - xz) - (zx - xz)\cdot y$$
$$= yzx - yxz - zxy - xzy \quad \dots \quad (2)$$

$$[z,[x,y]] = [z, xy - yx]$$
$$= z\cdot(xy - yx) - (xy - yx)\cdot z$$
$$= zxy - zyx - xyz - yxz \quad \dots \quad (3)$$

بجمع (1) و (2) و (3) نجـد أن :

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$$

كما أن الضرب [,] توزيعي على الجمـع :

$$\forall x,y,z \in A \quad : \quad [x,(y+z)] = x\cdot(y+z) - (y+z)\cdot x$$
$$= xy + xz - yx - zx$$
$$= (xy - yx) + (xz - zx)$$
$$= [x,y] + [x,z]$$

وبطريقة مشابهة نبرهن أن : $[(y+z),x] = [y,x] + [z,x]$

١١ – ٨ جـبر لـي التبادلي :

تعريف (١): ليكن L جـبر لي وليكن $x,y \in L$. نقول عن x,y إنهما تبادليان في A إذا كان $[x,y] = 0$.

تعريف (٢): نقول عن الجـبر لي L إنـه تبادلي إذا كان

$$[x,y] = 0 \qquad \forall x,y \in A$$

مثال: جـبر لي A في المثال السابق يكون تبادلياً إذا كان

$$xy = yx \qquad \forall x,y \in A$$

تمرينات محلولـــــة

التمرين الأول :

ليكن A جـــبراً على الحلقـــة R ولتكن $Der(A)$ مجموعـــة تشاكلات الاشتقاق على A . وليكن $d \in Der(A)$. أثبت أنه من أجل أي عـــدد $n \in N - \{0\}$ يكون :

$$d^n(xy) = \sum_{r=0}^{n} \binom{n}{r} d^r \cdot x\, d^{n-r} \qquad \forall x, y \in A \qquad (*)$$

حيث :

$$\binom{n}{r} = C_n^r = \frac{n!}{P!(n-P)!}$$

الحـــل :

لنثبت صحـــة العلاقة (*) اعتماداً على طريقة الاستقراء الرياضي على n

من أجل $n = 1$ يكون :

$$d(x \cdot y) = dx \cdot y + x \cdot dy$$

وهو تعريف تشاكل الاشتقاق على A .

نفرض أن العلاقة (*) صحيحة من أجل $k = n$ أي أن

$$\forall x, y \in A \quad : \quad d^n(xy) = \sum_{r=0}^{n} \binom{n}{r} d^r x \cdot d^{n-r} y$$

ولنبرهن صحة العلاقة (*) من أجل $k = n+1$. إن :

$$\forall x, y \in A \quad : d^{n+1}(x \cdot y) = d\left(d^n(xy)\right)$$

$$= d\left(\sum_{r=0}^{n} \binom{n}{r} d^r x \cdot d^{n-r} y\right)$$

$$= \sum_{r=0}^{n}\binom{n}{r} d^{r+1}x \cdot d^{n-r}y + \sum_{r=0}^{n}\binom{n}{r} d^{r}x \cdot d^{n-r+1}y$$

$$= d^{n+1}(xy) + \sum_{r=0}^{n}\binom{n}{r} d^{r+1}x \cdot d^{n-r}y +$$

$$+ \sum_{r=1}^{n}\binom{n}{r} d^{r}x \cdot d^{n-r+1}y + x \cdot d^{n+1}y$$

$$= d^{n+1}xy + \sum_{r=1}^{n}\left[\binom{n}{r-1} + \binom{n}{r}\right] d^{r}x \cdot d^{n-r+1}y + x\,d^{n+1}y$$

$$= d^{n+1}xy + \sum_{r=1}^{n}\binom{n+1}{r} d^{r}x \cdot d^{n-r+1}y + x\,d^{n+1}y$$

$$= \sum_{r=0}^{n+1}\binom{n+1}{r} d^{r}x \cdot d^{(n+1)-r}y$$

أي أن العلاقة (*) صحيحة من أجل $k = n+1$ وبالتالي فهي صحيحة مهما تكن $n \in N - \{0\}$.

التمرين الثاني :

ليكن L جبر لي على الحقل F وليكن $Der(L)$ مجموعة تشاكلات الاشتقاق في L .

أثبت أن :

$$[Der(L), Der(L)] \subseteq Der(L)$$

الحل :

أياً كان $d \in Der(L)$ فإن d هو التشاكل $d : L \to L$ الذي يحقق :

$$d(x \cdot y) = dx \cdot y + x \cdot dy \qquad \forall x, y \in L$$

وبالتالي يكون :

$$\forall x, y \in L : [d_1, d_2](x \cdot y) = (d_1 d_2 - d_2 d_1)(x \cdot y)$$

$$
\begin{aligned}
&= d_1 d_2(x\cdot y) - d_2 d_1(x\cdot y)\\
&= d_1(d_2 x\cdot x\cdot dy) - d_2(d_1 x\cdot y + x\cdot dy)\\
&= d_1 d_2\cdot y + d_2 x\cdot d_1 y + d_1 x\cdot d_2 y +\\
&\quad + x\cdot d_1 d_2 y - d_2 d_1 x\cdot y - d_1 x\cdot d_2 y -\\
&\quad - d_2 x\cdot d_1 y - x\cdot d_2 d_1 y\\
&= d_1 d_2 x\cdot y - d_2 d_1 x\cdot y + x\cdot d_1 d_2 y - x\cdot d_2 d_1 y\\
&= (d_1 d_2 - d_2 d_1)x\cdot y + x\cdot(d_1 d_2 - d_2 d_1)y\\
&= ([d_1,d_2]x)\cdot y + x\cdot([d_1,d_2]y)
\end{aligned}
$$

وبالتالي : $[d_1,d_2]\in Der(L)$

التمرين الثالث :

ليكن L جبر لي على الحقل F وليكن $Der(L)$ مجموعة تشاكلات الاشتقاق في L. ولنعرف في $Der(L)$ عملية الضرب $[,]$ كما يلي

$$[d_1,d_2] = d_1 d_2 - d_2 d_1 \qquad \forall\, d_1,d_2\in Der(L)$$

الحل :

إن $Der(L)$ مقاس على R – تأكد من ذلك – كما أنه :

$$\forall\, d_1,d_2\in Der(L) \quad : \quad [d_1,d_2]\in Der(L)$$

وذلك حسب التمرين الأول ، ولنبرهن على بقية شروط الجبر لي أي يكفي أن نبرهن : $\forall d,d_1,d_2,d_3\in Der(L) \quad , \quad \forall\alpha\in R$

1. $[(d_1+d_2),d_3] = [d_1,d_2]+[d_2,d_3]$

   $[d_3,(d_1+d_2)] = [d_3,d_1]+[d_3,d_2]$
2. $\alpha[d_1,d_2] = [\alpha d_1,d_2] = [d_1,\alpha d_2]$
3. $[d,d] = 0$
4. $[d_1,[d_2,d_3]]+[d_2,[d_3,d_1]]+[d_3,[d_1,d_2]] = 0$

إن :

1. $$\begin{aligned}[(d_1+d_2),d_3] &= (d_1+d_2)\cdot d_3 - d_3(d_1+d_2)\\ &= d_1d_3+d_2d_3-d_3d_1-d_3d_2\\ &= (d_1d_3-d_3d_1)+(d_2d_3-d_3d_2)\\ &= [d_1,d_3]+[d_2,d_3]\end{aligned}$$

وبطريقة مماثلة نبرهن أن :

$$[d_3,(d_1+d_2)] = [d_3,d_1]+[d_3,d_2]$$

2. $$\begin{aligned}\alpha[d_1,d_2] &= \alpha(d_1d_2-d_2d_1)\\ &= \alpha d_1d_2-\alpha d_2d_1\\ &= (\alpha d_1)d_2-d_2(\alpha d_1)\\ &= [\alpha d_1,d_2]\end{aligned}$$

وبطريقة مماثلة نبرهن أن :

$$\alpha[d_1,d_2] = [d_1,\alpha d_2]$$

3. $$[d,d] = dd-dd = 0$$

4. $$\begin{aligned}[d_1,[d_2,d_3]] &= [d_1,d_2d_3-d_3d_2]\\ &= d_1(d_2d_3-d_3d_2)-(d_2d_3-d_3d_2)d_1\\ &= d_1d_2d_3-d_1d_3d_2-(d_2d_3d_1-d_3d_2d_1)\\ &= d_1d_2d_3-d_1d_3d_2-d_2d_3d_1+d_3d_2d_1 \quad \dots \quad (1)\end{aligned}$$

وبالمثل نجـــد أن :

$$[d_2,[d_3,d_1]] = d_2d_3d_1-d_2d_1d_3-d_3d_1d_2+d_1d_3d_2 \quad \dots \quad (2)$$

$$[d_3,[d_1,d_2]] = d_3d_1d_2-d_3d_2d_1-d_1d_2d_3+d_2d_1d_3 \quad \dots \quad (3)$$

بجمـــع (1)و (2)و (3) نجـــد أن :

$$[d_1,[d_2,d_3]]+[d_2,[d_3,d_1]]+[d_3,[d_1,d_2]] = 0$$

تمرينات (١١)

التمرين الأول :

ليكن A جبراً على حلقة R وليكن

$$C(A)=\{a\in A \quad : \quad a\cdot x=x\cdot a \quad ; \quad \forall x\in A\}$$

المطلوب :

١. برهن أن $C(A)$ قياس على الحلقة R .

٢. بفرض أن الجبر A تجميعي فأثبت أن $C(A)$ جبر جزئي من الجبر A .

التمرين الثاني :

ليكن A جبراً تجميعياً على حلقة R وليكن B جبراً جزئياً من الجبر A ولتكن X,Y مجموعتين جزئيتين من الجبر A ولنأخذ المجموعتين:

$$C_A(X)=\{a\in A \quad : \quad a\cdot x=x\cdot a \qquad \forall x\in X\}$$

$$C\ (A)=\{a\in A \quad : \quad a\cdot x=x\cdot a \qquad \forall a\in A\}$$

المطلوب :

١. أثبت أن $C_A(X)$ جبر جزئي من الجبر A وأن $C(A)\subseteq C_A(X)$

٢. إذا كان $X\subseteq Y$ فأثبت أن $C_A(Y)\subseteq C_A(X)$.

التمرين الثالث :

لنأخذ $L=R^3$ ولنعرف على L العمليات :

$+$: الجمع في L : $(x_1,x_2,x_3)+(y_1,y_2,y_3)=(x_1+y_1,x_2+y_2,x_3+y_3)$

$\bullet$: خارجي بمجموعة مؤثراته R : $\alpha(x_1,x_2,x_3)=(\alpha x_1,\alpha x_2,\alpha x_3)$

(الجداء الخارجي (الشعاعي) للشعاعين u,v) $[u,v]=u\times v$: الضرب في L

حيث :

$$\forall(x_1,x_2,x_3),(y_1,y_2,y_3)\in R^3 \quad , \quad \forall\alpha\in R$$

برهن أن R^3 جبر لي على R .

التمرين الرابع :

ليكن L جبر لي على الحقل F وليكن I مثالياً في L . برهن أن L/I جبر لي على F .

التمرين الخامس :

ليكن B جبراً جزئياً من جبر لي L على الحقل F . ولتكن Y مجموعة جزئية من L ولنأخذ المجموعات :

$$N_L(B)=\{x\in L \quad : \quad [x,b]\in B\}$$

$$C_L(Y)=\{x\in L \quad : \quad [x,y]=0\}$$

$$Z(L)=\{x\in L \quad : \quad [x,z]=0 \quad \forall z\in L\}$$

المطلوب :

١. برهن أن $N_L(B)$ جبر جزئي من L وهو أكبر جبر جزئي من L يحوي B .

٢. برهن أن $C_L(Y)$ جبر جزئي من L .

٣. برهن أن $Z(L)$ مثالي في L ويكون L تبادلياً عندما وفقط عندما $Z(L)=L$

المصطلحات العلمية

Minimum	أصغر عنصر
Maximum	أكبر عنصر
Mathematical Induction	استقراء رياضي
Implication	اقتضاء
Natural Numbers	الأعداد الطبيعية
Integers Numbers	الأعداد الصحيحة
Rational Numbers	الأعداد العادية
Real Numbers	الأعداد الحقيقية
Complex Numbers	الأعداد العقدية
Relatively Prime	أوليان فيما بينهما
Family	أسرة (مجموعات)
Algebraic Structure	بنية جبرية
Graphe	بيان علاقة
Mapping	تطبيق
Injective Mapping (One-One)	تطبيق متباين
Surjective Mapping (Onto)	تطبيق غامر
Bijection	تطبيق تقابل
Partition Of a set	تجزئة مجموعة
Permutation	تبديل
Canonical	قانوني

Permutation	تبديل
Canonical Injection	تباين قانوني
Commutative	تبديلي
Associative	تجميعي
Distributive	توزيعي
Composition Of Mappings	تركيب التطبيقات
Homomorphism	تشاكل
Isomorphism	تماثل (تشاكل تقابلي)
Linear Congruence	توافق خطي
Algebra Of sets	جبر المجموعات
Cartesian Product	جداء ديكارتي
Truth Table	جدول الحقيقة
Root	جذر
Multiple Root	جذر مضاعف
Imaginary Part	الجزء التخيلي
Real Part	الجزء الحقيقي
Additive	جمعي
Greatest Lower Bound	الحد الأدنى
Least Upper Bounds	الحد الأعلى
Field	حقل
Subfield	حقل جزئي
Finite Fild	حقل منته

Ring	حلقة
Boolean Ring	حلقة بوليا نية
Commutative Ring	حلقة تبديلية
Subring	حلقة جزئية
Entire Ring	حلقة تامة
Principal Ideal Ring	حلقة ذات المثاليات الرئيسة
Euclidean Ring	حلقة إقليدية
Ring With Identity	حلقة واحدية
Algorithm	خوارزمية
Properties	خواص
Degeree	درجة (حدودية)
Cardinality Of Aset	رئيس (قدرة) مجموعة
Order Of An Element	رتبة عنصر
Order Of A group	رتبة زمرة
Argument	زاوية (عدد عقدي)
Group	زمرة
Group Of Permutations	زمرة التبادل
Abelian Group	زمرة تبديلية
Sub Group	زمرة جزئية
Additive Group	زمرة جمعية
Quotient Group	زمرة القسمة
Multiplicative Group	زمرة ضربية

Cycpic Group	زمرة دوارة
Finite Group	زمرة منتهية
Lattice	شبكة
Complete Lattice	شبكة تامة
Polar Form	شكل قطبي
Equivalence Class	صف تكافؤ
Zero Of Polynomial	صفر الحدودية
Direct Image	الصورة المباشرة
Inverse Image	الصورة العكسية
Multiplication	الضرب
Combinatorics	طرائق العد
Modulus	طويلة (قياس)
Prime Number	عدد أولي
Integer	عدد صحيح
Relation	علاقة
Reflexive Relation	علاقة انعكاسية
Antisymmetric Relation	علاقة تخالفية
Symmetric Relation	علاقة تناظرية
Partial Order Relation	علاقة ترتيب جزئي
Total Order Relation	علاقة ترتيب كلي
Equivolence	علاقة تكافؤ
Element	عنصر

Two Coprime Element	عنصران أوليان فيما بينهما
Minimal Element	عنصر أصغري
Maximal Element	عنصر أعظمي
Identity Element	عنصر محايد
Irreducible Element	عنصر غير قابل للتحليل
Upper Bound	عنصر راجح
Lower Bound	عنصر قاصر
Difference	فرق (المجموعات)
Symmetric Difference	فرق تناظري
Vector Space	فضاء شعاعي
Subvector	فضاء شعاعي جزئي
Greatest Common Divisor	القاسم المشترك الأكبر
Law Of Composition	قانون تشكيل
Commutative Law	قانون تبديلي
Associative Law	قانون تجميعي
Distributive Law	قانون توزيعي
Polynomial	كثير حدود (حدودية)
Ideal	مثالي
Prime Ideal	مثالي أولي
Principal Ideal	مثالي رئيس
Set	مجموعة
Subset	مجموعة جزئية

Empty Set	مجموعة خالية
Orderd Set	مجموعة مرتبة
Totally Orderd Set	مجموعة مرتبة كلياً
Finite Set	مجموعة منتهية
Infinite Set	مجموعة غير منتهية
Conjugate Of Acompley Number	مرافق عدد عقدي
Matrix	مصفوفة
Least Commun Divisor	المضاعف المشترك الأصغر
Equation	معادلة
Restriction Of a mapping	مقصور تطبيق
Extension Of a mapping	ممدود تطبيق
Inverse	مقلوب
Integral Domain	منطقة تكاملية
Semi-group	نصف زمرة
Kernel	نـــواة
Symmetric Of an Element	نظير عنصر

المراجـــع العلميـــة

1. Atiyah . M.F , Macdonald I.G – Introduction To Commutative Algebra.
2. Blyth - Module Theory.
3. Cohn - Algebra I.
4. Hall M-The Theory Of Groups.
5. Hartley B., Hawbes T.O – Rings , Modules And Linear Algebra.
6. Kostikin - Introduction To Algebra.
7. Kurosh A.G – Group Theory.
8. Kurosh A.G – Lectures On General Algebra.
9. Kurosh A.G – Higher Algebra.
11. Lang – Algebra.
12 Lambek J – Lectures On Ringes And Modules.
13. Lipschuts – Set Theory And Ralated Topics.
14. Sah.c. – Abstract Algebra.
15. Scott W.R. – Group Theory.
16. Zariski U. , Samuel P. – Commutative Algebra.

اللجنة العلميـــــــة

الأستاذ الدكتور صفوان عويرة

الأستاذ المساعد إيلي قدسي

الأستاذ المساعد غسان نعمة

المدقق اللغوي

الدكتورة منى طعمة