م بداوي

نظرية الحلقات وامتداد الحقول

تأليف
يوسف عبدالله الخميس

فهرسة مكتبة الملك فهد الوطنية
٥١٢,٤ الخميس، يوسف عبدالله.
٦١٧خ نظرية الحلقات وامتداد الحقول / تأليف يوسف عبدالله الخميس. -
ط ١. - الرياض: النشر العلمي والمطابع، جامعة الملك سعود،
١٤١٩ هـ / ١٩٩٨م.
١٦٦ ص؛ ١٧×٢٤ سم.
ردمك ٩ - ٠٥٩ - ٠٥ - ٩٩٦٠ (جلد)
٠ - ٠٥٨ - ٩٩٦٠ (غلاف)
١ - الجبر. ٢ - الرياضيات. أ - العنوان.

رقم الإيداع: ١٤/١٤١٩

تم تحكيم الكتاب بواسطة لجنة متخصصة شكلها المجلس العلمي بالجامعة، وقد وافق المجلس على نشره في اجتماعه السابع للعام الدراسي ١٤١٢ / ١٤١٣ هـ المعقود بتاريخ ٢٥ / ٦ / ١٤١٢ هـ الموافق ٣١ / ١٢ / ١٩٩١ م.

مطابع جامعة الملك سعود ١٤١٩ هـ

تقديم

لقد جاءت فكرة هذا الكتاب من خلال تدريس مقرر الحلقات والحقول للمستوى الرابع في جامعة الملك سعود ومن خلال هذه التجربة فقد روعي فيه الأخذ بالمواءمة بين قضيّتين مهمتين:

الأولى وهي التعمق بعض الشيء بإطلاع القارىء على البنى الرياضية التي يتميز بها الجبر، مدعّمة بحوالي مائة وعشرين تمرينًا تستحث مَلَكَةَ البرهان لديه وتوسّع أساسه الجبري، **والأخرى** وهي محاولة تجنب الخطر الذي تتعرّض له الأفكار المجردة في المعالجة المباشرة والمفاجئة، وذلك عن طريق توسيع قاعدة الأمثلة المعطاة والتي ربا عددها عن ثمانين مثالاً، كما روعي عند معالجة كل موضوع توضيح أهميته في مقدمة كل فصل مع إعطاء مبرّرات تربط محتواه بأمثلة ملموسة أو بحيثيّات تاريخيّة أو رياضيّة.

لقد شمل الكتاب على أربعة فصول تغطّي مادة المقرر ٣٤٤ ريض (الحلقات والحقول) وقد عرضت مادة هذا الكتاب بطريقة تبرز الترابط بين كل فصل والفصول التي تليه. سيلاحظ القارىء في الفصل الأول أن كثيرا من المفاهيم الواردة عن الحلقات هي تعميم للمفاهيم نفسها في الزمر فالمثاليّات في الحلقات تقوم بالدور نفسه الذي تقوم به الزمر الجزئية الناظمية في الزمر كما تؤدي المثاليات إلى بناء حلقة القسمة التي هي تعميم لفكرة زمرة القسمة. سيعمم الهوموومورفزم الذي سبق أن عرض له القارىء في الزمر إلى الحلقات كما أن نظريات التشاكل في الحلقات هي تعميم لمثيلاتها في الزمر. يغطّي الفصل الثاني حقل القواسم لحلقة تامة ومميّز الحلقة والمجموع المباشر للحلقات

والحلقيّات، أمـا الفصـل الثالث فيغطي الحلقات الإقليدية وحلقة كثيرات الحدو
والفصل الأخير يتعرض لامتداد الحقول وحقول الانشطار والحقول المنتهية.

لقـد اعتمد الكتاب في مصطلحاته على ما اتّفق عليه مكتب تنسيق التعري
بالرباط التابع للمنظمة العربية للثقافة والتربية والعلوم، إضافةً إلى قاموس الرياضيا
الذي أصدرته مشكورة مؤسسة الكويت للتقدم العلمي.

استكمالاً للجهد العلمي فقد ذُيِّل الكتاب بدليل لمصطلحاته العلمية ورمو
وقـائمـة بالمـراجـع المستخـدمة أو المراجع التي قد يحتاجها القارىء الذي يرغب
الاستزادة، ونستميح القارىء عذرًا إذا صادف بعض الهنّات والأخطاء المطبعية.

هذا ولا يفوتني أن أوجه الشكر إلى جامعة الملك سعود على تشجيعها نشر الكت
العلمية. وختـامًـا نرجو من الله العلي القدير أن ينفع القارىء بهذا المطبوع ويح
القصد والعاقبة وآخر دعوانا أن الحمد لله رب العالمين.

المـؤلـ

المحتويـات

صفحة

صفحة

الفصل الثاني: بناء حلقات جديدة وحلقيّات

الفصل الثالث: الحلقات الإقليديّة وحلقة كثيرات الحدود

الفصل الرابع: امتداد الحقول

صفحة

الرمـوز
المستخدمة في الكتاب

$F(a)$	أصغر حقل يحوي الحقل الجزئي F والعنصر a
$R[a]$	أصغر حلقة تحوي الحلقة الجزئية R والعنصر a
id_R	تشاكل ذاتي محايد للحلقة R
$\cong_R$	تشاكل على الحلقة R
$\mathbb{C}$	حقل الأعداد المركبة
$\mathbb{R}$	حقل الأعداد الحقيقية
$\mathbb{Q}$	حقل الأعداد النسبية
$End_R M$ أو $Hom_R(M,M)$	حلقة الاندومورفزمات للحلقيّة M على الحلقة R
$End\, M$	حلقة الاندومورفزمات للزمرة الإبدالية M
$\mathbb{Z}$	حلقة الأعداد الصحيحة
$\mathbb{Z}_n$	حلقة الأعداد الصحيحة قياس n
R/I	حلقة القسمة للحلقة R بالمثالي I
$R[x]$	حلقة كثيرات الحدود على الحلقة R
M/N	حلقية القسمة للحلقية M على N
$\deg f$	درجة كثيرة الحدود f
$Aut\, R$	زمرة التشاكلات الذاتية للحلقة R
$Inn\, R$	زمرة التشاكلات الذاتية الداخلية للحلقة R
R^+	الزمرة الجمعية للحلقة R

$GL_n(F)$ أو $GL_F(V)$	الزمرة الخطية العامة من الدرجة n على الحقل F
$\langle a \rangle$	الزمرة الدائرية المولدة من قبل العنصر a
G_R	زمرة الوحدات للحلقة R
(a)	مثالي مولد من قبل العنصر a
$\Sigma^{\oplus}_{Ex}$	مجموع مباشر خارجي
$\Sigma^{\oplus}$	مجموع مباشر داخلي
$R^{\star}$	مجموعة العناصر غير الصفرية في R
$\operatorname{char} R$	مميّز الحلقة

الفصل الأول

الحلقـــات

مقدمـــة

سنبحث في هذا الفصل في نظم جبرية لها عمليتان ثنائيّتان، تسمى الحلقات وهي من الأفكـار الأسـاسية في موضـوع الجبر. من الأمثلة الواضحة على الحلقات الأعداد الصحيحة التي عرفت على أساسها أو صنعت على منوالها الحلقة وستظهر بصفة دائمة كمصدر للأمثلة والإلهام في دراسة الحلقات.

سيلاحظ القارىء أن كثيرًا من المفاهيم الواردة في هذا الفصل عن الحلقات هي تعميم للمفـاهيم نفسهـا التي في الـزمر فالمثاليّات ما هي إلا حلقات جزئية تقوم في الحلقات بالدور نفسه الذي تقوم به الزمر الجزئية الناظمية في الزمر كما تؤدي المثاليات إلى بناء حلقة القسمة التي هي تعميم لفكرة زمرة القسمة. والهوموم ورفزم (homomorphism) الـذي سبق أن استخدم في الزمر سيعمم إلى الحلقات وهو أداة يستخـدمهـا الرياضيون في دراسة بنية جبرية عن طريق بنية جبرية أخرى قد تكون معـروفة لديهم أو أسهل في دراستها من الأولى، وذلك باستحداث هوموم ورفزم من إحدى البنيتين إلى الأخرى. كما أن نظريات التشاكل في الحلقات هي تعميم لمثيلاتها في الزمر.

وأخـيرا سندرس في هذا الفصل صفات جبرية أخرى مهمة للحلقات تنطبق بصفة خاصة على حلقة الأعداد الصحيحة.

٢

الحلقة وزمرة وحداتها: تعاريف وأمثلة

تعريف (١ - ١)

الحلقة (ring) هي الثلاثي المرتب $(R,+,.)$ المتكوِّن من مجموعة غير خالية R (non-empty set) وعمليّتين ثنائيّتين (two binary operations) (+)، (.) معرّفتين على R بحيث إن:

١) $(R,+)$ زمرة إبدالية (abelian group).

٢) العملية (.) تجميعية (associative) على R.

٣) العملية (.) توزيعية (distributive) من اليسار واليمين على العملية (+).

يلاحظ القارىء أننا استخدمنا (+)، (.) لتعريف العمليّتين الثنائيّتين على الحلقة لكونهما مصطلحان قديمان كما يساعدان على تأكيد التناظر بين النتائج المستخلصة للحلقات وتلك التي للنظم العدديّة المألوفة.

وسنسمي العملية (+) عملية الجمع (addition) والعملية (.) عملية الضرب (multiplication) ويجب التأكيد على أن (+)، (.) تمثّلان عمليّتين ثنائيّتين مجرّدتين وليس عمليتي الجمع والضرب العاديّتين.

تعريف (١ - ٢)

* العنصر المحايد الجمعي للحلقة يسمى صفر الحلقة (zero of the ring) ويرمز له بالرمز 0. كما سيرمز للمعكوس الجمعي للعنصر a في الحلقة بالرمز $-a$.

* نقول عن الحلقة R إنّها حلقة بمحايد (ring with identity) إذا وجد عنصر e في R بحيث يتحقق لكل r في R: $re=er=r$. إذا كان مثل هذا العنصر موجودًا في R فإنه يسمّى العنصر المحايد للحلقة ويرمز له بالرمز 1.

في الحلقة بمحايد نقول عن العنصر a في R إنّه عنصر وحدة (unit) أو نقول إنه عنصر له معكوس (invertible) في R إذا وجد له معكوس ضربي. أي إذا وجد $b \in R$ بحيث إن:

$$ab = ba = 1$$

سيرمز للمعكوس الضربي للعنصر a في R بالرمز a^{-1} ويسمّى معكوس a.

* إذا كانت عملية الضرب عملية إبدالية على الحلقة R فإننا نقول عن R إنها حلقة إبدالية (commutative ring).

مبرهنـــة (١ - ١)

إذا كانت R حلقة بمحايد فإن :

(١) العنصر المحايد (identity element) للحلقة وحيد .

(٢) لكل عنصر وحدة في R يوجد معكوس وحيد .

البرهـــان

(١) إذا كان $1', 1$ عنصرين محايدين للحلقة R فإن :

$$1 = 1.1' = 1'$$

(٢) إذا كان a_1, a_2 معكوسين للعنصر a في الحلقة R فإن :

$$a_2 = a_2.1 = a_2(aa_1) = (a_2a)a_1 = 1.a_1 = a_1$$

مبرهنـــة (١ - ٢)

إذا كانت R حلقة فإن :

$$0.a = a.0 = 0 \qquad \forall\, a \in R$$

البرهـــان

بتطبيق قانون التوزيع من اليسار نحصل على المساواة :

$$a.0 + a.0 = a.(0+0) = a.0 = a.0 + 0$$

باستخدام قانون الاختصار (cancellation law)، لكون $(R,+)$ زمرة، نستنتج أن $a.0=0$.

وبالطريقة نفسها يمكن أن نثبت أن $0.a=0$.

تسمى الحلقة التي تحوي الصفر فقط بالحلقة الصفريّة (zero ring).

مبرهنـــة (١ - ٣)

إذا كانت a,b,c عناصر اختيارية من الحلقة R ولنعرِّف الطرح (substraction) في R كما يلي:

$$a - b = a + (-b)$$ فإن :

$$a(-b) = -(a\,b) \quad (١)$$

$$(-a)\,b = -(a\,b) \quad (٢)$$

$$(-a)(-b) = a\,b \quad (٣)$$

$$a(b-c) = a\,b - a\,c \quad (٤)$$

$$(a-b)\,c = a\,c - b\,c \quad (٥)$$

البرهـــان

سنكتفي ببرهنة (١)، (٤) ويمكن برهنة الباقي بالطريقة نفسها. لنبرهن الفقرة (١).

من تعريف المعكوس الجمعي نعلم أن:

$$b + (-b) = 0$$

وباستخدام خاصية التوزيع نستنتج أن:

$$a.b + a(-b) = a(b + (-b))$$

$$= a.0$$

$$= 0$$

ولكون عملية الجمع عملية إبداليّة على R فإن:

$$a(-b) + a\,b = a\,b + a(-b) = 0$$

وهذا يعني أن $a(-b)$ هو المعكوس الجمعي للعنصر $a\,b$ وبالتالي فإن:

$$a(-b) = -(a\,b)$$

لنبرهن الآن الفقرة (٤):

بما أن الضرب عملية توزيعية على الجمع من اليسار، فإن:

$$a(b-c) = a(b+(-c)) = ab + a(-c)$$
$$= ab + (-(ac))$$
$$= ab - ac$$

أي أن الضرب عملية توزيعية على الطرح من اليسار.

مبرهنـة (١ - ٤)

إذا كانت R حلقـة بمحـايد وإذا كانت G_R مجموعة عناصر الوحدة في R فإن G_R تشكّل زمرة بالنسبة لعملية الضرب.

البرهـان

المجموعة G_R مجموعة غير خالية لأنها تحوي على الأقل العنصر المحايد للحلقة الذي هو العنصر المحايد نفسه للمجموعة G_R. إذا كان $a,b \in G_R$ ، فإنه يوجد عنصران $a^{-1}, b^{-1} \in R$ بحيث إن :

$$a.a^{-1} = a^{-1}.a = 1 \text{ و } b.b^{-1} = b^{-1}.b = 1$$

وبالتالي :

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

وهذا يثبت أن $a.b \in G_R$ ، ولما كانت خاصية التجميع صحيحة بالوراثة على G_R (أي أنها صحيحة على G_R لكونها صحيحة على عناصر R ولأن G_R مجموعة جزئية من R) لذلـك فإن G_R تشكّـل زمـرة بالنسبـة لعملية الضرب. تسمّى G_R زمـرة الـوحدات (group of units) للحلقة R.

مثـال (١ - ١)

يلاحظ أن $(\mathbb{Z},+,.)$ ، $(\mathbb{Q},+,.)$ ، $(\mathbb{R},+,.)$ و $(\mathbb{C},+,.)$ تشكّل حلقات إبداليّة بمحـايد حيث إن $\mathbb{Z}$ هي حلقة الأعداد الصحيحة (integers) ، $\mathbb{Q}$ حلقة الأعداد النسبيّة (rational numbers) ، $\mathbb{R}$ حلقة الأعداد الحقيقية (real numbers) ، $\mathbb{C}$ حلقة

الأعداد المركّبة أو التخيّلية (complex numbers) ، والعمليتان (+)، (.) تمثلان عمليتي الجمع والضرب العاديتين، والعنصر المحايد لهذه الحلقات هو 1 كذلك فإن المجموعة $S=\{a+b\sqrt{3}:a,b\in\mathbb{Z}\}$ مع عمليتي الضرب والجمع العاديتين تشكّل حلقة إبداليّة بمحايد هو 1.

مثال (١ - ٢)

زمرة الوحدات للحلقة $\mathbb{Z}$ هي $\{-1,1\}$، بينما زمرة الوحدات للحلقات $\mathbb{Q}$ ، $\mathbb{R}$ ، $\mathbb{C}$ هي $\mathbb{Q}^*$ ، $\mathbb{R}^*$ ، $\mathbb{C}^*$ على الترتيب حيث $\mathbb{Q}^*=\mathbb{Q}\setminus\{0\}$ وهكذا بالنسبة لـ $\mathbb{R}^*$ ، $\mathbb{C}^*$.

تعريف (١ - ٣)

ليكن n عددًا صحيحًا موجبًا. يقال إن العددين الصحيحين a ، b متطابقان قياس n(congruent modulo n) ويكتب

$$a \equiv b \bmod n$$

إذا وإذا (if and only if) كان a - b يقبل القسمة على n . أي أن a ، b متطابقان قياس n إذا وإذا فقط كان a-b= kn ، حيث k عدد صحيح .

وكمثال على ذلك إذا كان n = 17 فإن :

$$5 \equiv 73 \bmod 17$$

$$-7 \equiv -24 \bmod 17$$

من السهولة بمكان إثبات أن العلاقة (relation) المعرّفة آنفًا (علاقة التطابق قياس n هي علاقة تكافؤ (equivalence relation) على مجموعة الأعداد الصحيحة وأن فصول التكافؤ (equivalence classes) لهذه العلاقة هي :

$$[0] , [1] , [2] , \dots , [n-1]$$

حيث $[a] = \{a + tn : t \in \mathbb{Z}\}$. لتكن $\mathbb{Z}_n$ مجمـوعـة فصول التطابق قياس n. تسمّى $\mathbb{Z}_n$ مجموعة الأعداد الصحيحة قياس n(set of integers modulo n).

مثـال (١ ـ ٣)

لنُعرّف العمليتين $\oplus$ ، $\otimes$ على $\mathbb{Z}_n$ بالقاعدتين :

$$[a] \oplus [b] = [a + b]$$

$$[a] \otimes [b] = [a\,b]$$

لكل $[a], [b] \in \mathbb{Z}_n$.

سنثبت أنّه لكل عدد صحيح موجب n فإن $(\mathbb{Z}_n, \oplus, \otimes)$ تشكّل حلقة إبداليّة بمحايد، تسمّى حلقة الأعداد الصحيحة قياس n (ring of integers modulo n).

البرهـان

سنثبت أولاً أن العمليّتين $\oplus$ ، $\otimes$ لا تعتمدان على الممثّلين المختارين لفصلي التكافؤ. ليكن $[a]=[a']$ ، $[b]=[b']$ وبالتالي فإن : $a \equiv a' \bmod n$ ، $b \equiv b' \bmod n$. أي أن $n \mid (a'-a)$ ، $n \mid (b'-b)$ ، لذلك فـإن $n \mid [(a'+b')-(a+b)]$ وبالتـالي فـإن $(a'+b') \equiv (a+b) \bmod n$ وهذا يؤدي إلى أن : $[a+b]=[a'+b']$. أي أن عـمليـة الجمع $\oplus$ حسنة التعريف(well defined) . كذلك فإن : $[a]=[a']$ ، $[b]=[b']$ يؤدي إلى أن : $a'-a=k_1 n$ ، $b'-b=k_2 n$ ، حيث k_1 ، k_2 عددان صحيحان . إذن :

$$a'b' = (a+k_1 n)(b+k_2 n) = ab + ak_2 n + bk_1 n + k_1 k_2 n^2$$

ومنه نستنتج أن $a'b' \equiv ab \bmod n$ وبالتالي فإن : $[a'b']=[ab]$ ، وهكذا فإن العمليتين $\oplus$ ، $\otimes$ حسنتا التعريف بغض النظر عن اختيار ممثلي فصول التكافؤ.

لنـبرهن أولا أنَّ $(\mathbb{Z}_n, \oplus)$ تُشَكِّل زمرة إبداليّة . لنفرض أنَّ $[a],[b],[c] \in \mathbb{Z}_n$. لما كانت عملية الجمع العادي عملية تجميعيّة وإبداليّة على $\mathbb{Z}$ فإنّ :

$$([a] \oplus [b]) \oplus [c] = [a+b] \oplus [c]$$

$$= [(a+b)+c]$$

$$= [a+(b+c)]$$

$$= [a] \oplus [b+c]$$
$$= [a] \oplus ([b] \oplus [c])$$

وبالمثل فإن :

$$[a] \oplus [b] = [a+b] = [b+a] = [b] \oplus [a]$$

من تعريف عملية الجمع $\oplus$ ، يتضح أن [0] هو العنصر المحايد الجمعي . وكذلك [n–a] هو المعكوس الجمعي للعنصر [a] وبالتالي فإن $(\mathbb{Z}_n, \oplus)$ تشكّل زمرة إبدالية.

ولكون عملية الضرب العادي عملية تجميعية وتوزيعية على الجمع على $\mathbb{Z}$ فإنّ :

$$([a] \otimes [b]) \otimes [c] = [a\,b] \otimes [c]$$
$$= [(a\,b)c]$$
$$= [a(b\,c)]$$
$$= [a] \otimes [b\,c]$$
$$= [a] \otimes ([b] \otimes [c])$$

أي أن عملية الضرب $\otimes$ عملية تجميعية على $\mathbb{Z}_n$ كذلك فإن :

$$[a] \otimes ([b] \oplus [c]) = [a] \otimes [b+c]$$
$$= [a(b+c)]$$
$$= [ab+ac]$$
$$= [ab] \oplus [ac]$$
$$= ([a] \otimes [b]) \oplus ([a] \otimes [c])$$

أي أن عملية الضرب $\otimes$ توزيعية من اليسار على عملية الجمع $\oplus$. وبالطريقة نفسها نثبت أن عملية الضرب $\otimes$ توزيعية من اليمين على عملية الجمع $\oplus$. لذلك فإن $(\mathbb{Z}_n, \oplus, \otimes)$ تُشَكِّل حلقة بمحايد هو [1]. وحيث إن عملية الضرب العادي على **Z** عملية إبدالية فإن :

$$[a] \otimes [b] = [a\,b] = [b\,a] = [b] \otimes [a]$$

وبالتالي فإن $(\mathbb{Z}_n, \oplus, \otimes)$ حلقة إبدالية بمحايد .

للتبسيط سنعبّر عن حلقة الأعداد الصحيحة قياس n كما يلي :

$$Z_n = \{0,1,2,\ldots,n-1\}$$

وسنعبّر عن الجمع في Z_n بالرمز (+) والضرب في Z_n بالرمز (.).

وكمثال على ذلك فإن جدول جمع وضرب العناصر في Z_4 هو كما يلي:

(+)	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(.)	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

ومنه نستنتج أن عناصر الوحدة في Z_4 هي 3,1 فقط ويلاحظ أن $2.2=0$ في Z_4 بينما $2\neq 0$ في Z_4.

مثـال (١ ـ ٤)

لتكن E مجموعة الأعداد الزوجية الصحيحة. نلاحظ ببساطة أن $(E,+,.)$ تشكل حلقة إبدالية مع عمليتي الجمع والضرب العاديتين ولكن لا يوجد في هذه الحلقة محايد.

مثـال (١ ـ ٥)

يستطيع القارىء أن يتأكد بنفسه أن مجموعة المصفوفات (matrices) المربّعة على حلقة الأعداد الحقيقية $M_2(\mathbb{R})$ مع عمليتي جمع وضرب المصفوفات تشكل حلقة بمحايد وغير إبدالية.

تعريـف (١ ـ ٤)

نقول عن عنصر غير صفري a في حلقة R إنّه قاسم للصفر (zero divisor) في الحلقة R إذا وجد عنصر غير صفري b في R بحيث إما $a\,b=0$ أو $b\,a=0$.

مثـال (١ - ٦)

نلاحظ أن العنصر 2 قاسم للصفـر في الحلقـة $\mathbb{Z}_4$ وكذلك العنصرين 2,3 في $\mathbb{Z}_6$. كما نلاحظ في الحلقة $M_2(\mathbb{R})$ أنّه إذا كان:

$$a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad , \quad b = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

فإنّ $a \neq 0$ ، $b \neq 0$ ، لكن $a\,b = 0$ ، بالتـالي فإنّ العنصرين a,b هما قاسمين للصفر في الحلقة $M_2(\mathbb{R})$.

تعريـف (١ - ٥)

الحلقة التامّة (integral domain) هي حلقة إبدالية بمحايد ولا يوجد بها قواسم للصفر.

مثـال (١ - ٧)

يلاحظ أن حلقة الأعداد الصحيحة هي حلقة تامّة لأنها إبدالية بمحايد وإذا كان $a,b \in \mathbb{Z}$ بحيث إنّ $a\,b = 0$ ، فإنه إما $a = 0$ أو $b = 0$.

الحقـول

تعريـف (١ - ٦)

الحقل (field) هو حلقة إبدالية بمحايد وكل عنصر غير صفري فيهـا هـو عنصر وحـدة .

ملاحظـة (١ - ١)

* لتكن R حلقـة بمحـايد وليكن a عنصر وحـدة في R ولنفـرض أنـه يوجد عنصر b في R بحيث إن $a\,b = 0$. لما كان a عنصر وحـدة في R فإنـه يوجـد له معكوس a^{-1} في R وبـالـتـالي فإن $a^{-1}(a\,b) = 0$ وهـذا يؤدي إلى أن $b = 0$. أي أنّ كل عنصر وحدة في R لا يمكن أن يكون قاسما للصفر فيها.

* لما كان كل عنصر غير صفري في الحقل هو عنصر وحدة فإن هذا يؤدي إلى أن F لا يحوي قواسم للصفر وبالتالي فإن كل حقل هو حلقة تامة. لاحظ أن العكس غير صحيح لأن $\mathbb{Z}$ حلقة تامة ولكنها ليست حقلا.

* من تعريف الحقل نستنتج أن F^* هي زمرة الوحدات للحقل F وهي زمرة إبدالية.

مثـال (١ ـ ٨)

من الواضح أن الحلقات الإبدالية بمحايد $\mathbb{C},\mathbb{R},\mathbb{Q}$ تشكّل حقولاً تسمّى على التوالي حقل الأعداد النسبية، حقل الأعداد الحقيقية، حقل الأعداد المركّبة أو التخيّلية.

مثـال (١ ـ ٩)

لتكن $F=\{a+b\sqrt{3}:a,b\in\mathbb{Q}\}$ ، يمكن التأكد بسهولة أن $(F,+,.)$ تشكّل حلقة إبدالية بمحايد، وصفر الحلقة هو 0 ، حيث (+)، (.) هما عمليتا الجمع والضرب العاديتين.

لإثبات أن F حقل يجب أن نتأكد أن كل عنصر غير صفري هو عنصر وحدة. لذلك نفترض أن $a+b\sqrt{3}$ عنصر غير صفري في F وهذا يعني أنّه إما a أو b لا يساوي الصفر.

من الواضح أن:

$$(a+b\sqrt{3})^{-1}=\frac{1}{(a+b\sqrt{3})}=\frac{1}{a+b\sqrt{3}}\frac{a-b\sqrt{3}}{a-b\sqrt{3}}$$

$$=\frac{a}{a^2-3b^2}-\frac{b\sqrt{3}}{a^2-3b^2}$$

يلاحظ أن $a^2-3b^2\neq 0$ وإلا كان $\sqrt{3}$ عددًا نسبيًّا وبالتالي فإن $a/(a^2-3b^2)$ ، $-b/(a^2-3b^2)$ عددان نسبيان،وهذا يؤدي إلى أن المعكوس عنصر في F.

مبرهنـة (١-٥)

حلقـة الأعـداد الـصـحيحـة قياس n تكـوّن حقـلاً إذا وإذا فقط كان n عددًا أوليًا (prime integer).

البرهـان

نثبت أولا أنه إذا كان n عددًا غير أولي فإن $\mathbb{Z}_n$ ليست حقلاً. لذلك نفرض أن $n = ab$ حيث $0<a,b<$ ، لذلك فإن:

$$[a] \otimes [b] = [a\,b] = [n] = [0]$$

ولكن [a] ، [b] عنصرين غير صفريين في $\mathbb{Z}_n$. إذن [a] ، [b] قاسمين للصفر في $\mathbb{Z}_n$ وهذا يعني أن $\mathbb{Z}_n$ ليست حلقة تامة وبالتالي ليست حقلا.

نفرض الآن أن n عدد أولي ونودّ أن نبرهن على أن $\mathbb{Z}_n$ حقل. لذلك نفرض أن [a] عنصر غير صفري في $\mathbb{Z}_n$ ، أي أن $a \in \mathbb{Z}$ بحيث إن $0<a<n$. لمّا كان القاسم المشترك الأعظم للعددين a,n يساوي الواحد فإنّه يوجد عددان صحيحان q,s بحيث إن $1 = a\,q + s\,n$.

الآن نلاحظ أن:

$$\begin{aligned}[a] \otimes [q] &= [a\,q] \oplus [0] \\ &= [a\,q] \oplus [n\,s] \\ &= [a\,q + n\,s] \\ &= [1]\end{aligned}$$

وهذا يعني أن [q] هو معكوس [a] وعليه فإنّ $\mathbb{Z}_n$ حقل.

مبرهنـة (١ - ٦)

كل حلقة تامّة منتهية (finite) هي حقل.

البرهـان

لتكن $r_1,\ldots,r_n$ عناصر الحلقة R وليكن r عنصرًا غير صفري في R. نلاحظ أنّه إذا كان $rr_i = rr_j$ فإنّ $r(r_i - r_j) = 0$ ولكون R حلقة تامة فإنّ هذا يؤدي إلى أن $r_i = r_j$. لذلك فإنّ

$rr_1, rr_2, \ldots, rr_n$ هي جميع عناصر الحلقة R. أي أننا نستطيع أن نعبّر عن كل عنصر في R بالصيغة rr_i حيث $1 \leqslant i \leqslant n$. ولكن $1 \in R$ ، لذلك فإن $1 = rr_i$ وحيث إن R حلقة إبدالية فإنّ $1 = r_i r = rr_i$ وهذا يعني أن معكوس r هو العنصر r_i. وهذا يثبت أن كل عنصر غير صفري في R له معكوس. لذلك فإن R حقل.

تعريـف (١ - ٧)

لتكـن $(R,+,.)$ حلقـة، S مجمـوعـة جزئية غير خالية من R. إذا كانت $(S,+,.)$ حلقة فإنّ S تسمّى حلقة جزئية (subring) من الحلقة R وتسمى حلقة جزئية فعلية من R إذا كانت $S \neq R$.

مثـال (١ - ١٠)

لكل حلقة R حلقتان جزئيتان تافهتان هما الحلقة الصفرية، والحلقة R نفسها.

مثـال (١ - ١١)

من الواضح أن $\mathbb{Z}$ حلقة جزئية من $\mathbb{Q}$ ، $\mathbb{Q}$ حلقة جزئية من $\mathbb{R}$ ، $\mathbb{R}$ حلقة جزئية من $\mathbb{C}$.

مثـال (١ - ١٢)

يلاحظ أنّ حلقة الأعداد الزوجية الصحيحة E تشكّل حلقة جزئية من حلقة الأعـداد الصحيحـة $\mathbb{Z}$ كما يلاحظ أن $\mathbb{Z}$ حلقـة بمحـايد بينـما لا يوجـد في الحلقة الجزئية E محايد.

مثـال (١ - ١٣)

اعتبر حلقة الأعداد الصحيحة قياس 6. من السهولة التأكد من أن $\{0,2,4\}$ ، $\{0,3\}$ يشكّـلان حلقتـين جزئيّتـين من $\mathbb{Z}_6$ والعنصر المحايد لهما على التوالي 3,4 وهما يختلفان عن العنصر المحايد للحلقة $\mathbb{Z}_6$.

ملاحظـة (١ - ٢)

لقد سبق أن تعرض القارىء في موضوع الزمر إلى الشرط اللازم والكافي لتكوّن مجمـوعـة جزئـية غير خالـية H زمـرة جزئـية (subgroup) من زمـرة G وهـو أن يكون $a\,b^{-1}\in H$ لكل $a,b\in H$. سنستخدم ذلك في تعميم هذه الفكرة على الحلقات في المبرهنة التالية.

مبرهنـة (١ - ٧)

إذا كانت R حلقـة، S مجمـوعـة جزئية غير خالية من R، فإن S حلقـة جزئية من R إذا وإذا فقط كان $a\,b\in S$ ، $a-b\in S$ لكل $a,b\in S$.

البرهـان

لتكن S حلقة جزئية من R وبالتالي فإن S زمرة جزئية من R بالنسبة لعملية الجمع. مـن المـلاحـظة السـابقـة نستنتج أن $a-b\in S$ لكـل $a,b\in S$ ، ولكون S حلقة جزئية من R فإن $a\,b\in S$ لكل $a,b\in S$.

نفرض العكس، أي أنّ $a-b\in S$ ، $a\,b\in S$ لكـل $a,b\in S$. باستخدام الملاحظة السابقة نستنتج أن S زمرة جزئية جمعية من R ولكون خاصية الإبدال صحيحة بالنسبة للجمع على R فهي صحيحة على S ، وبالتالي فإن S زمرة جزئية إبدالية. كما أن خاصتي الدمج والتوزيع على الجمع بالنسبة لعملية الضرب خاصتان صحيحتان على R وبالتالي تتحققان على S ، ولكون S مجموعة جزئية من R لذلك فهي حلقة جزئية من R .

مثـال (١ - ١٤)

لتكن $S=\{a+b\sqrt{3}: a,b\in\mathbb{Z}\}$. إذا كانت $a,b,c,d\in\mathbb{Z}$ فإنّ :

$$(a+b\sqrt{3})-(c+d\sqrt{3})=(a-c)+(b-d)\sqrt{3}\in S$$

$$(a+b\sqrt{3})(c+d\sqrt{3})=(ac+3bd)+(bc+ad)\sqrt{3}\in S$$

وهذا يثبت أنّ S حلقة جزئية من حقل الأعداد الحقيقية $\mathbb{R}$.

تعريـف (١ ـ ٨)

ليكن K حقلاً وليكن F مجموعة جزئية غير خالية من K ، نقول عن F إنّه حقل جزئي (subfield) من K إذا كان يشكّل حقلا بالنسبة للعمليات المعرَّفة على K. لكل حقل يوجد حقل جزئي تافه هو الحقل نفسه.

مثـال (١ ـ ١٥)

من الواضح أن $\mathbb{Q}$ حقل جزئي من $\mathbb{R}$ ، $\mathbb{R}$ حقل جزئي من $\mathbb{C}$.

تعريـف (١ ـ ٩)

الحقل الذي لا يملك حقولاً جزئيّة فعليّة يدعى حقلاً أوليًّا (prime field).

مثـال (١ ـ ١٦)

نفرض أنّ F حقل جزئي من حقل الأعداد النسبية $\mathbb{Q}$. إذن F يحوي 1 وبالتالي فإنّه يحوي حلقة الأعداد الصحيحة $\mathbb{Z}$ لأن $\mathbb{Z}$ مولدة من قبل 1 كزمرة جمعيّة. ليكن n/m عنصرًا في $\mathbb{Q}$ ، إذن n,m عنصران من $\mathbb{Z}$ ، $m\neq 0$ ، وبالتالي فإنّ 1/m عنصر من F. لذلك فإنّ $n/m = n(1/m)$ عنصر من F، وهذا يؤدي إلى أنّ $F\supset\mathbb{Q}$ ، وبالتالي فإن $F=\mathbb{Q}$ وهذا يثبت أن $\mathbb{Q}$ حقل أولي.

مثـال (١ ـ ١٧)

لأي عدد أولي p نلاحظ أنّ $\mathbb{Z}_p$ كزمرة جمعيّة هي زمرة بسيطة أي لا توجد بها زمرة جزئيّة غير تافهة، وهذا يؤدي إلى أن $\mathbb{Z}_p$ حقل أولي.

تعريـف (١ ـ ١٠)

لتكن R' حلقة ولتكن R حلقة جزئيّة من R' ، $a\in R'$. يرمز لأصغر حلقة جزئيّة من R' تحوي R وتحوي العنصر a بالرمز R[a] ، مثل هذه الحلقة الجزئيّة موجودة لأنها تقـاطع (intersection) كل الحلقات الجزئية من R' التي تحوي R وتحوي العنصر a.

كذلك إذا كان K حقلا، F حقل جزئي من K ، $a \in K$ ، يرمز لأصغر حقل جزئي من K يحوي الحقل الجزئي F ويحوي العنصر a بالرمز F(a) .

تمـاريـــن (١ - ١)

١) أثبت أنه توجد على الأقل حلقة واحدة رتبتها n لكل $n \in \mathbb{N}$.

٢) لتكن R حلقة تتمتع بالخاصة التالية :

لكل $a \in R$ فإن $a^2 = a$

أثبت أن R حلقة إبداليّة .

٣) إذا كان a,b عنصرين من حلقة إبدالية R ، وكان n عددًا صحيحًا موجبًا فأثبت أن

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

حيث $\binom{n}{k} = n! / (n-k)!\, k!$.

٤) لتكن M زمـرة إبدالية ولتكن End M مجموعة كل الهوموم‌ورفزمات من M إلى M ولتكن $\phi, \varphi \in \text{End } M$. عُرِّف الجمع والضرب على End M كما يلي :

$$(\varphi + \phi)(a) = \varphi(a) + \phi(a)$$

$$(\varphi\, \phi)(a) = \varphi(\phi(a))$$

لكل $a \in M$. لاحظ أن عملية الضرب هي تركيب الهوموم‌ورفزمات (composition) أثبت أن End M تُشكّـل حلقة غير إبدالية بمحايد. تسمّى هذه الحلقة بحلقة الأندوم‌ورفزمات للزمرة M (the ring endomorphisms of M) ويرمز لها بالرمز End M.

٥) أوجد زمرة الوحدات للحلقات $\mathbb{Z}_{12}, \mathbb{Z}_{16}, \mathbb{Z}_{27}$.

٦) أثبت أن زمرة الوحدات للحلقة $\mathbb{Z}_n$ هي المجموعة : $\{x \in \mathbb{Z}_n : (x,n)=1\}$.

٧) أثبت أن قواسم الصفر للحلقة $\mathbb{Z}_n$ هي عناصر $\mathbb{Z}_n$ التي ليست أولية نسبةً إلى n (not relatively prime to n).

٨) أثبت أنّ $2+\sqrt{3}$ يمثّل عنصر وحدة في الحلقة $\mathbb{Z}[\sqrt{3}]$ ثم أوجد عنصر وحدة آخر في الحلقة $\mathbb{Z}[\sqrt{3}]$.

٩) أوجـد زمـرة الوحدات لحلقة المصفوفات المربّعة $M_2(\mathbb{Z}_3)$. تسمّى هذه الزمرة بالزمرة **الخطيّة العامّة من الدرجة الثانية على الحقل $\mathbb{Z}_3$ (general linear group of degree 2 over $\mathbb{Z}_3$)** **ويرمز لها بالرمز $GL_2(\mathbb{Z}_3)$** .

١٠) أثبت أنّ كل عنصر في حلقة منتهية بمحايد إما أن يكون عنصر وحدة أو أن يكون قاسما للصفر.

١١) أثبت أنّ الحلقة تكون بدون قواسم للصفر إذا وإذا فقط كانت تحقق قانون الاختصار لعملية الضرب.

١٢) لنفرض أن S حلقة جزئيّة غير صفريّة من حلقة R ، ولكل من S ، R **عنصران محايدان** مختلفان. أثبت أن المحايد للحلقة الجزئية S يجب أن يكون قاسما للصفر في الحلقة الأصلية R.

١٣) هل الحلقة الجزئية من حقل تُشَكِّل حقلاً جزئيًّا؟

١٤) أثبت أنّ تقاطع حلقتين جزئيتين من حلقة يشكِّل حلقة جزئيّة، هل اتحاد حلقتين جزئيتين من حلقة يشكِّل حلقة جزئيّة؟

١٥) ناقش أيا من المجموعات التالية تُشكِّل حلقة جزئيّة من حلقة المصفوفات المربعة الأعداد الحقيقية $M_2(\mathbb{R})$:

(أ) $H = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{R}\right\}$

(ب) $J = \left\{\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a,b \in \mathbb{R}\right\}$

(جـ) $I = \left\{\begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{R}\right\}$

(د) $K = \left\{\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}\right\}$

(هـ) $L = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a,b \in \mathbb{R}\right\}$

١٦) أعطِ مثالاً لحلقة جزئيّة إبدالية من حلقة غير إبدالية .

١٧) ليكن:

$$F = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a,b,c \in \mathbb{Q}\}$$

$$K = \{a + b\sqrt{2} : a,b \in \mathbb{Z}\}$$

أثبت أن $F = \mathbb{Q}(\sqrt[3]{2})$ ، $K = \mathbb{Z}[\sqrt{2}]$ ، هل يُشكِّل K حقلاً؟

المثاليّات وحلقة القسمة

أولا : المثاليــات

تعريــف (١ - ١١)

الحلقة الجزئيّة I من حلقة R تسمّى مثاليًّا من اليسار left ideal (مثاليًّا من اليمين right ideal) إذا كان (ar)ra عنصرًا من I لكل r∈R ولكل a∈I ويسمّى I مثاليًّا (ideal) إذا كان مثاليًّا من اليسار ومثاليًّا من اليمين.

ويعرف المثالي في بعض الكتب بالصيغة المكافئة التالية :

تعريــف (١ - ١٢)

إذا كانت I مجموعة جزئيّة غير خالية من R ، فإن I مثالي من اليسار (مثالي من اليمين) إذا وإذا فقط

(١) $a - b \in I$ لكل $a,b \in I$.

(٢) $ra \in I$ $(ar \in I)$ ، لكل $r \in R$ ولكل $a \in I$.

ومن المناسب الإشارة إلى أنّه في حالة الحلقة الإبدالية فإن المثالي من اليسار هو مثالي من اليمين والعكس صحيح .

مثــال (١ - ١٨)

في أي حلقة R ، الحلقتان الجزئيّتان التافهتان R ، {0} ، هما حلقتان مثاليّتان للحلقة R .

ملاحظــة (١ - ٣)

يلاحظ أن صفـر الحلقـة R ينتمي لأي مثالي I للحلقة R فلو فرضنا أنّ x∈I فحسب تعريف المثالي فإن 0=0.x ينتمي إلى I.

مثــال (١ - ١٩)

من الواضح أن $I_1 = \{0,2,4\}$ ، $I_2 = \{0,3\}$ يشكّلان مثاليين للحلقة $\mathbf{Z}_6$.

مثـــال (١ - ٢٠)

يمكن التأكد بسهولة أن $I_1 = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a,b \in \mathbb{Z}\right\}$ يشكّل مثاليًّا من اليسار لحلقة المصفوفات المربعة على حلقة الأعداد الصحيحة $M_2(\mathbb{Z})$ ، بينما $I_2 = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{Z}\right\}$ يشكّل مثاليًّا من اليمين للحلقة نفسها.

مثـــال (١ - ٢١)

ليكن n عددًا صحيحًا ولتكن A مجموعة كل مضاعفات العدد n في حلقة الأعداد الصحية $\mathbb{Z}$ ، أي أنّ :

$$A = \{n\,r : r \in \mathbb{Z}\}$$

نلاحظ أنّ $na - nb = n(a - b)$ وكذلك $b(n\,a) = n(b\,a)$ حيث $a,b \in \mathbb{Z}$ لذلك فإن $A = n\mathbb{Z}$ يشكّل مثاليًّا للحلقة $\mathbb{Z}$.

تعريـــف (١ - ١٣)

يقال لأي مثالي يختلف عن الحلقة R بأنّه مثالي فعلي (proper ideal) ويقال عن الحلقة التي لا تحوي مثاليًّا فعليًّا غير المثالي الصفري بأنها حلقة بسيطة (simple ring).

ملاحظـــة (١ - ٤)

إذا كان I مثاليًّا لحلقة بمحايد وكان $1 \in I$ فإنّ $I = R$ لأن $r = r.1 \in I$ لكل $r \in R$. وأيضًا إذا كان I يحوي عنصر وحدة a من R فإنّ $I = R$ لأن $a\,a^{-1} = 1 \in I$.

مثـــال (١ - ٢٢)

إذا كان F حقلاً فإنّ F حلقة بسيطة لأن المثالي الفعلي الوحيد له هو {0}؛ حيث إن كل مثالي غير صفري يحوي عنصرًا غير صفري وبالتالي فإنّه يحوي عنصر وحدة، لذلك فإنّه يساوي F حسب الملاحظة السابقة.

ثانيا : حلقة القسمة

لتكن R حلقة وليكن I مثاليًّا للحلقة R. لمّا كان I يُشكِّل زمرة جزئية من زمرة إبدالية R بالنسبة لعملية الجمع، فإنّ R/I هي زمرة قسمة (quotient group) للزمرة R بالزمرة الجزئية الناظميّة I، ولذلك فإنّ جمع عناصر R/I (التي هي المجموعات المشاركة (cosets) لـ I في R) معرف بالقاعدة التالية :

$$(a + I) + (b + I) = (a + b) + I$$

حيث $a,b \in R$. ولما كانت R إبدالية بالنسبة لعملية الجمع فإن R/I إبداليّة كذلك . تُعرّف عملية الضرب في R/I بالقاعدة التالية :

$$(a + I)(b + I) = a\,b + I$$

نودّ أن نتأكد أولا أن ضرب المجموعات المشاركة لا يعتمد على الممثلين للمجموعات المشاركة المستعملة، لذلك نفرض أن :

$$a + I = a' + I \quad , \quad b + I = b' + I$$

لذلك فإن $a - a' = a_1$ ، $b - b' = b_1$ حيث a_1, b_1 عنصران من I.

إذن :

$$\begin{aligned} a\,b + I &= (a' + a_1)(b' + b_1) + I \\ &= a'\,b' + a'\,b_1 + a_1\,b' + a_1\,b_1 + I \\ &= a'\,b' + I \end{aligned}$$

حيث إن $a'\,b_1,\ a_1\,b',\ a_1 b_1 \in I$ ، وهكذا فإنّ ضرب المجموعات المشاركة عملية حسنة التعريف .

مبرهنـة (١ ـ ٨)

إذا كان I مثاليا للحلقة R ، فإن R/I تُشكِّل حلقة تعرف بحلقة القسمة لـ R بـ I (quotient ring of R by I).

سنحـذف تفاصيل البرهان ونشير إلى أنّ $0+I=I$ هو صفر حلقة القسمة R/I والعنصر $-a+I$ هو المعكوس الجمعي للعنصر $a+I$.

مثـال (١ - ٢٣)

لنعتبر حلقة القسمة لـ $\mathbf{Z}$ بـ $n\mathbf{Z}$. نلاحظ أنّ عناصر $\mathbf{Z}/n\mathbf{Z}$ هي :

$$n\mathbf{Z}\,,\ 1+n\mathbf{Z}\,,\ 2+n\mathbf{Z}\,,\ \ldots\,,\ (n-1)+n\mathbf{Z}$$

ليكن $I=n\mathbf{Z}$ ، لقد سبق أن أوضحنا أنّ I مثالي للحلقة $\mathbf{Z}$ ،

الهوموموررفزم في الحلقات

تعريـف (١ - ١٤)

لتكن R ، S حلقتين وليكن ϕ تطبيقًا (mapping) من R إلى S. يقال إنّ ϕ هوموموررفزم من R إلى S إذا حقق الشرطين التاليين :

(١) لكلّ $a,b\in R$ يكون $\phi(a+b)=\phi(a)+\phi(b)$ ، أي يحافظ على الجمع.

(٢) لكلّ $a,b\in R$ يكون $\phi(a\,b)=\phi(a)\,\phi(b)$ ، أي يحافظ على الضرب.

مثـال (١ - ٢٤)

لتكن R ، S حلقتين اختياريتين وليكن ϕ هو التطبيق الذي يرسل كل عنصر من R إلى صفر الحلقة S الذي نرمز له بالرمز $0'$. نلاحظ أنّه لكل $a, b\in R$ فإن :

$$\phi(a+b)=0'=0'+0'=\phi(a)+\phi(b)$$

$$\phi(a\,b)=0'=0'\,.\,0'=\phi(a)\,.\,\phi(b)$$

لذلك فإن ϕ هوموموررفزم ويسمى بالهوموموررفزم التافه (trivial homomorphism).

مثـال (١ - ٢٥)

التطبيق $\phi(a)=2a$ من حلقة الأعداد الصحيحة $\mathbf{Z}$ إلى حلقة الأعداد الزوجيّة الصحيحة E ليس هوموموررفزما لأنه لا يحافظ على الضرب حيث :

$$\phi(a\,.\,b)=2ab\neq(2a)\,(2b)=\phi(a)\,\phi(b)$$

مثـال (١ - ٢٦)

لتكن R حلقة بمحايد وليكن x عنصر وحدة في R. نعرّف التطبيق ψ_x بالقاعدة $\psi_x(r)=x\,r\,x^{-1}$ لكل $r\in R$. نلاحظ أن :

$$\psi_x (r_1 + r_2) = x(r_1 + r_2) x^{-1}$$
$$= x r_1 x^{-1} + x r_2 x^{-1}$$
$$= \psi_x (r_1) + \psi_x (r_2)$$

وكذلك :

$$\psi_x (r_1 r_2) = x r_1 r_2 x^{-1} = x r_1 (x^{-1}x) r_2 x^{-1}$$
$$= (x r_1 x^{-1}) (x r_2 x^{-1})$$
$$= \psi_x (r_1) \psi_x (r_2)$$

لكل $r_1, r_2 \in R$ ، إذن ψ_x هوموم ورفزمًا من الحلقة R إلى نفسها .

من مبرهنة مماثلة في الزمر نحصل على المبرهنة التالية :

مبرهنـــة (١ ـ ٩)

إذا كان ϕ هوموم ورفزمًا من الحلقة R إلى الحلقة S وإذا رمزنا لصفر الحلقة R بالرمز 0 وصفر الحلقة S بالرمز $0'$ فإن :

(١) $\phi (0) = 0'$

(٢) $\phi (-r) = -\phi (r)$

تعريـــف (١ ـ ١٥)

إذا كان ϕ هوموم ورفزما من الحلقة R إلى الحلقة S وإذا كان $0'$ هو صفر الحلقة S فإن نواة (kernel) ϕ هي المجموعة :

$$\text{Ker}\, \phi = \{r \in R : \phi (r) = 0'\}$$

وصورة (image) ϕ هي المجموعة :

$$\text{Im}\, \phi = \{\phi (r) : r \in R\} = \phi (R)$$

وكما في موضوع الزمر نقول عن ϕ إنّه أُحادي (one - one) إذا كانت $\text{Ker}\, \phi = \{0\}$ ، ونقول عنه إنّه غامر (on to) إذا كانت $\text{Im}\, \phi = S$.

مبرهنـــة (١ - ١٠)

إذا كانت R ، S حلقتين وإذا كان ϕ هومومورفزمًا من R إلى S فإنّ :

(١) $\text{Ker}\,\phi$ مثالي للحلقة R.

(٢) $\text{Im}\,\phi$ حلقة جزئية من S.

البرهـــان

(١) لنـرمـز لصفر الحلقة R بالرمز 0 ولصفر الحلقة S بالرمز $0'$ ، من المبرهنة (١ - ٩) نستنتج أنّ صفر الحلقة R هو عنصر من عناصر $\text{Ker}\,\phi$، لذلك فإنّ $\text{Ker}\,\phi$ مجموعة غير خالية. افرض أنّ $a, b \in \text{Ker}\,\phi$ ، وبالتالي فإن $\phi(a)=\phi(b)=0'$. باستخدام $\phi(-b)=-\phi(b)$ نحصل على :

$$\begin{aligned}\phi(a-b) &= \phi(a + (-b)) \\ &= \phi(a) + \phi(-b) \\ &= \phi(a) - \phi(b) \\ &= 0' - 0' = 0'\end{aligned}$$

أي أنّ $a-b \in \text{Ker}\,\phi$. إذا كان r عنصرًا اختياريًّا من R فإنّ

$$\phi(r\,a) = \phi(r)\,\phi(a) = \phi(r)\,.\,0' = 0'$$

أي أنّ $ra \in \text{Ker}\,\phi$. وبطريقة مماثلة نثبت أن $a\,r \in \text{Ker}\,\phi$. لذلك فإن $\text{Ker}\,\phi$ مثالي للحلقة R.

(٢) ليكـن $a, b \in \text{Im}\,\phi$. إذن يوجـد عنصران x, y في الحلقـة R بحيث إن $a=\phi(x)$ ، $b=\phi(y)$ إذن :

$$\begin{aligned}a - b &= \phi(x) - \phi(y) = \phi(x) + \phi(-y) \\ &= \phi(x - y)\end{aligned}$$

إذن $a - b \in \text{Im}\,\phi$. كذلك :

$$a\,b = \phi(x)\,\phi(y) = \phi(xy)$$

أي أنّ $a\,b \in \text{Im}\,\phi$ ، وبالتالي فإن $\text{Im}\,\phi$ تشكّل حلقة جزئية من S .

ملاحظـة (١ ـ ٥)

لاحـظنـا من برهـان المـبرهنة السابقة أن الهوموم‍ورفزم يحافظ (preserve) على الطرح. أي أنّ:

$$\phi(a-b) = \phi(a) - \phi(b)$$

لكل $a, b \in R$.

تعريـف (١ ـ ١٦)

ليكن ϕ هوموم‍ورفزما من الحلقة R إلى الحلقة S . نقول إن ϕ تشاكل (isomorphism) من الحلقة R إلى الحلقة S إذا كان ϕ أحاديًّا وغامراً ونقول في هذه الحالة إن الحلقتين R ، S متشاكلتان (isomorphic) ونعبّر عن هذا بالرمز: $R \cong S$.

مثـال (١ ـ ٢٧)

لتكن R هي حلقة المجموعات المشاركة لـ $n\mathbf{Z}$ في $\mathbf{Z}$ أي أنّ $R = \mathbf{Z}/n\mathbf{Z}$ ولتكن $S = \mathbf{Z}_n$ هي حلقة الأعداد الصحيحة قياس n. لنعرف ϕ من R إلى S كما يلي:

$$\phi(a + n\mathbf{Z}) = [a]$$

نلاحظ أن:

$$\phi((a+n\mathbf{Z}) + (b+n\mathbf{Z})) = \phi(a+b+n\mathbf{Z}) = [a+b]$$
$$= [a]+[b] = \phi(a+n\mathbf{Z}) + \phi(b+n\mathbf{Z})$$

أي أنّ ϕ تحافظ على عملية الجمع. كذلك:

$$\phi((a+n\mathbf{Z})(b+n\mathbf{Z}) = \phi(ab+n\mathbf{Z})$$
$$= [ab] = [a][b]$$
$$= \phi(a+n\mathbf{Z})\,\phi(b+n\mathbf{Z})$$

أي أن ϕ تحافظ على عملية الضرب، لذلك فإن ϕ هوموم‍ورفزم. ليكن $\phi(a+n\mathbf{Z}) = [0]$ ولكن $\phi(a+n\mathbf{Z}) = [a]$ ، إذن $[a] = [0]$ وهذا يعني أن $a \in [0]$. أي أن $a+n\mathbf{Z} = n\mathbf{Z}$ ، ولكن $n\mathbf{Z}$ هو صفـر الحلقة $\mathbf{Z}/n\mathbf{Z}$ ، إذن ϕ أحادي. إذا كان $[a]$ عنصرًا اختياريًّا من $\mathbf{Z}_n$ فإنّ $\phi(a+n\mathbf{Z}) = [a]$ ، لذلك فإن ϕ غامر. وهكذا فإنّ ϕ تشاكل من الحلقة $\mathbf{Z}/n\mathbf{Z}$ إلى الحلقة $\mathbf{Z}_n$ وبالتالي فإن الحلقتين $\mathbf{Z}/n\mathbf{Z}$ ، $\mathbf{Z}_n$ متشاكلتان.

تعريـف (١ ـ ١٧)

لتكن R حلقة، نقول عن التشاكل من الحلقة R إلى نفسها بأنه تشاكل ذاتي (automorphism) للحلقة R.

مثـال (١ ـ ٢٨)

يمكن التأكد بسهولة أن التطبيق من حلقة ما إلى نفسها، ولتكن R ، والذي يثبّت كل عنصر من عناصر الحلقة (يرسل كل عنصر إلى نفسه)، هو تشاكل ذاتي للحلقة، ويسمى التشاكل الذاتي المحايد (identity automorphism) ويرمز له بالرمز id_R.

مثـال (١ ـ ٢٩)

لتكن R حلقة بمحايد ولنعرّف التطبيق ψ_x من R إلى نفسها بالقاعدة التالية: $\psi_x(r)=xrx^{-1}$ لكل $r\in R$. لقد سبق أن برهنّا في مثال (١ ـ ٢٦) أن ψ_x هوموم‌ورفزم من الحلقة R إلى نفسها. لنفرض أن $\psi_x(r)=0$ حيث $r\in R$ ، إذن $xrx^{-1}=0$ بالضرب من اليمين بـ x وباليسار بـ x^{-1} نحصل على $r=0$. لذلك فإن ψ_x أحادي. إذا كان $r\in R$ ، فإن:

$$\psi_x(x^{-1}rx) = x(x^{-1}rx)x^{-1} = (xx^{-1})r(xx^{-1}) = r$$

أي أن ψ_x غامر وبالتالي فإن ψ_x تشاكل ذاتي للحلقة R. يسمى مثل هذا التشاكل بالتشاكل الذاتي الداخلي (inner automorphism).

سنقدم فيما يلي النظرية الأولى للتشاكل في الحلقات

(first isomorphism theorem)

نظريـة (١ ـ ١١)

إذا كان ϕ هوموم‌ورفزما من الحلقة R إلى الحلقة S فإنّ:

$$R/\mathrm{Ker}\,\phi \equiv \mathrm{Im}\,\phi$$

البرهـان

لنعرف التطبيق $\psi: R/\text{Ker}\,\phi \to \text{Im}\,\phi$ بالقاعدة التالية :

$$\psi\,(r + \text{Ker}\,\phi) = \phi\,(r)$$

لكل $r+\text{Ker}\,\phi \in R/\text{Ker}\,\phi$. نلاحظ أن ψ حسنة التعريف، لأنه إذا كانت :

$$r + \text{Ker}\,\phi = s + \text{Ker}\,\phi$$

فإن $r=s+x$ حيث $x \in \text{Ker}\,\phi$ وبالتالي فإن :

$$\begin{aligned}\psi\,(r+\text{Ker}\,\phi) = \phi\,(r) = \phi\,(s+x) = \phi\,(s) + \phi\,(x) &= \phi(s) + 0' \\ &= \phi\,(s) \\ &= \psi\,(s + \text{Ker}\,\phi)\end{aligned}$$

حيث $0'$ هو صفر الحلقة S. أيضا ψ تحافظ على عملية الجمع في $R/\text{Ker}\,\phi$ لأنّ :

$$\begin{aligned}\psi\,((r+\text{Ker}\,\phi) + (s+\text{Ker}\,\phi)) &= \psi\,(r+s+\text{Ker}\,\phi) \\ &= \phi\,(r+s) \\ &= \phi\,(r) + \phi\,(s) \\ &= \psi\,(r+\text{Ker}\,\phi) + \psi\,(s+\text{Ker}\,\phi)\end{aligned}$$

كذلك فإن ψ تحافظ على عملية الضرب في $R/\text{Ker}\,\phi$ لأن :

$$\begin{aligned}\psi\,((r+\text{Ker}\,\phi)\,(s+\text{Ker}\,\phi)) &= \psi\,(rs+\text{Ker}\,\phi) = \phi\,(rs) \\ &= \phi\,(r)\,\phi\,(s) \\ &= \psi\,(r+\text{Ker}\,\phi)\,\psi\,(s+\text{Ker}\,\phi)\end{aligned}$$

لتكن $\psi(r+\text{Ker}\,\phi)=0'$ ، لكن $\psi(r+\text{Ker}\,\phi)=\phi(r)$ ،

إذن $\phi(r)=0'$ وهذا يعني أن $r \in \text{Ker}\,\phi$ ولذلك فإن $r+\text{Ker}\,\phi=\text{Ker}\,\phi$ ، لكن $\text{Ker}\,\phi$ هو صفر الحلقة $R/\text{Ker}\,\phi$ ، إذن ψ أحادي . ليكن $s \in \text{Im}\,\phi$ ، يوجد $r \in R$ بحيث إن $\phi(r)=s$ ولكن $\psi(r+\text{Ker}\,\phi) = \phi(r) = s$ ، إذن ψ غامر. وهكذا فإن ψ تشاكل من $R/\text{Ker}\,\phi$ إلى $\text{Im}\,\phi$.

ملاحظـة (١ ـ ٦)

نستطيع أن نثبت بصفة عامة كما في النظرية السابقة أنه يوجد هوموم ورفزم غامر

من الحلقة R إلى الحلقة R/I ، حيث I مثالي للحلقة R ، ونواته هو المثالي I. يسمّى هذا الهوموومورفزم بالهوموومورفزم الطبيعي (natural homomorphism).

مبرهنة (١ - ١٢)

إذا كان ϕ هوموومورفزما من الحلقة R إلى الحلقة R' فإنّه :

(١) إذا كانت S حلقة جزئية من R فإن $\phi(S)$ حلقة جزئية من R'.

(٢) إذا كانت S' حلقة جزئية من R' فإن $\phi^{-1}(S)$ حلقة جزئية من R.

(٣) إذا كان I' مثاليا للحلقة R' فإن الحلقة الجزئية $\phi^{-1}(I')$ تشكل مثاليا للحلقة R.

(٤) إذا كان ϕ غامـرا وكان I مثاليا للحلقة R فإن الحلقة الجزئية $\phi(I)$ تشكل مثاليا للحلقة R'.

البرهـــان

سنكتفي بإثبات (١)، (٣) ويمكن إثبات الباقي بالطريقة نفسها :

(١) لما كان $\phi(0)=0'$ حيث إن $0'$ هو صفـر الحلقـة R' ، فإن $\phi(S)$ مجموعة ليست خالية . ليكن $x,y\in\phi(S)$ ، لذلك فإنه يوجد $a,b\in S$ بحيث إن $x=\phi(a)\,,\,y=\phi(b)$:

$$x - y = \phi(a) - \phi(b) = \phi(a - b)$$

لذلك فإن $x - y \in \phi(S)$. كذلك :

$$xy = \phi(a)\,\phi(b) = \phi(ab)$$

لذلك فإن $xy \in \phi(S)$. وهكذا فإن $\phi(S)$ حلقة جزئية من R'.

(٣) حيث إن $\phi(0)=0'$ فإن $0\in\phi^{-1}(I')$ وبـالتالي فإن $\phi^{-1}(I')$ ليست مجموعة خالية. نفرض أن $a,b\in\phi^{-1}(I')$ ، أي أنه يوجد $x,y\in I'$ بحيث إن $x=\phi(a)\,,\,y=\phi(b)$:

$$\phi(a - b) = \phi(a) - \phi(b) = x - y$$

لذلك فإن $a - b \in \phi^{-1}(I')$. كذلك لكل $r \in R$:

$$\phi(ra) = \phi(r)\,\phi(a) = \phi(r)\,x = I'$$

لذلك $ra \in \phi^{-1}(I')$. وبالطريقة نفسها نثبت أن $ar\in\phi^{-1}(I')$ ، وهكذا فإن $\phi^{-1}(I')$ تشكل مثاليًا للحلقة R.

ملاحظة (١ ـ ٧)

إذا كان ϕ هومومورفزما من الحلقة R إلى الحلقة R' وإذا كان I مثاليًا للحلقة R فليس من الضروري أن يكون $\phi(I)$ مثاليًا للحلقة R' ، وكمثال على ذلك اعتبر $R=\mathbb{Z}$ ، $R'=\mathbb{Q}$ ، ϕ هوموموروفزم الاحتواء (inclusion homomorphism) من $\mathbb{Z}$ إلى $\mathbb{Q}$ (يرسل كل عنصر إلى نفسه من $\mathbb{Z}$ إلى $\mathbb{Q}$) ، $I=n\mathbb{Z}$. لقد سبق أن أثبتنا أن I مثالي للحلقة $\mathbb{Z}$. من الواضح أن $\phi(n\mathbb{Z})=n\mathbb{Z}$ وبالتالي فإن $\phi(I)=I$، ولكن I لا يُشكّل مثاليًا للحلقة $\mathbb{Q}$ لأنه مثلا $1=(1/n)n\notin I$. لذلك إذا لم يكن ϕ غامرا فإنه ليس من الضروري أن يكون $\phi(I)$ مثاليا للحلقة R'.

مبرهنة (١ ـ ١٣)

إذا كان I مثاليًا للحلقة R فإنه يوجد تناظر أحادي بين مثاليّات الحلقة R التي تحوي I ومثاليّات الحلقة R/I.

البرهان

ليكن $\phi:R\to R/I$ الهومومورفزم الطبيعي وليكن J مثاليًا للحلقة R يحوي I. نلاحظ أن $\phi(J)=\{x+I:x\in J\}=J/I$ يشكل مثاليا للحلقة R/I حسب (٤) من المبرهنة السابقة لأن ϕ غامر. نفرض أن J' مثالي للحلقة R/I، لذلك فإن $I\in J'$ لأن I هو صفر الحلقة R/I. ليكن $J=\phi^{-1}(J')$ ، نلاحظ أن J مثالي للحلقة R حسب (٣) من المبرهنة السابقة. أيضا لكون :

$$\phi(I)=\{r+1:r\in I\}=I\in J'$$

فإن $I\subset\phi^{-1}(J')$، أي أن $I\subset J$. وهكذا أثبتنا على وجود مثالي J للحلقة R يحوي المثالي I ويناظر المثالي J' للحلقة R/I.

ملاحظة (١ ـ ٨)

لو تأملنا في المبرهنة السابقة لتأكد لدينا أن مثاليات الحلقة R/I هي من النوع $J/I=\{x+I:x\in J\}$ حيث إن J هو مثالي للحلقة R يحوي المثالي I ، والتناظر الذي تشير إليه

المبرهنة السابقة هو بين مثالي اختياري J للحلقة R يحوي I والمثالي المناظر له J/I للحلقة R/I.

مبرهنـــة (١ - ١٤)

إذا كان ϕ هومومورفزما غامرًا من الحلقة R إلى الحلقة R' وإذا كان I مثاليًّا للحلقة R يحوي $\text{Ker}\phi$ ، فإن :

$$R/I \cong R'/\phi(I)$$

البرهـــان

لنعرّف التطبيق : $\psi: R/I \to R'/\phi(I)$ بالقاعدة التالية :

$$\psi(r + I) = \phi(r) + \phi(I)$$

لكل $r \in R$ ، نلاحظ أنّ :

$$\begin{aligned}\psi(r_1 + r_2 + I) &= \phi(r_1 + r_2) + \phi(I)\\ &= \phi(r_1) + \phi(r_2) + \phi(I)\\ &= (\phi(r_1) + \phi(I)) + (\phi(r_2) + \phi(I))\\ &= \psi(r_1 + I) + \psi(r_2 + I)\end{aligned}$$

كذلك :

$$\begin{aligned}\psi(r_1 r_2 + I) &= \phi(r_1 r_2) + \phi(I)\\ &= \phi(r_1)\,\phi(r_2) + \phi(I)\\ &= (\phi(r_1) + \phi(I))\,(\phi(r_2) + \phi(I))\\ &= \psi(r_1 + I)\,\psi(r_2 + I)\end{aligned}$$

لكل $r_1, r_2 \in R$. لذلك فإن ψ هومومورفزم .

نفـــرض أن $r' + \phi(I) \in R'/\phi(I)$ حيث $r' \in R'$ ، لما كان ϕ غامـــرًا فإنـه يوجد $r \in R$ بحيث إن $\phi(r) = r'$. إذن :

$$\psi(r + I) = \phi(r) + \phi(I) = r' + \phi(I)$$

أي أن ψ غامر.

أيضا نفرض أن :

$$\psi(r + I) = \phi(I)$$

وهذا يعني أن :

$$\phi(r) + \phi(I) = \phi(I)$$

لذلك $\phi(r) \in \phi(I)$. ليكن $\phi(r)=\phi(a)$ حيث $a \in I$. نلاحظ أن $\phi(r - a)=0$ ، وبالتالي $r - a \in \text{Ker}\ \phi$ ، ولكن $I \supset \text{Ker}\ \phi$ ، لذلك $r \in I$. وهكذا فإن $r+I=I$ ، أي أن $r+I$ هو صفر الحلقة R/I وبالتالي فإن ψ أحادي .

مبرهنـة (١ ـ ١٥)

ليكن ψ هوموم‌ورفزما غامرا من الحلقة R إلى الحلقة R' وليكن I' مثاليًّا للحلقة R' ، عندئذ فإن :

$$R/\phi^{-1}(I') \cong R'/I'$$

البرهـان

حسب المبرهنة (١ ـ ١٢) (٣) فإن $\phi^{-1}(I')$ يشكل مثاليًّا للحلقة R. لما كان $\phi^{-1}(I') \supset \text{Ker}\ \phi=\phi^{-1}(0')$ لأن $0' \in I'$ ، حيث $0'$ هو صفر الحلقة R'. باستخدام المبرهنة السابقة نحصل على :

$$R/\phi^{-1}(I') \cong R'/\phi\phi^{-1}(I')=R'/I'$$

تمـارين (١ ـ ٢)

١) أثبت أنّ تقاطع مثاليّين لحلقة هو مثالي .

٢) أوجد تقاطع المثاليّين $m\mathbb{Z}=\{mr:r \in \mathbb{Z}\}$ ، $n\mathbb{Z}=\{nr:r \in \mathbb{Z}\}$ ، للحلقة $\mathbb{Z}$.

٣) أثبت أنّ اتّحاد (union) مثاليّين لحلقة ليس من الضروري أن يكون مثاليًّا .

٤) لتكن R حلقة إبدالية . نقول عن العنصر x في R إنّه عنصر متلاشٍ (nilpotent) إذا وجد عدد صحيح موجب n بحيث إن $x^n=0$. برهن أنّ مجموعة العناصر المتلاشية في R تشكل مثاليا . يسمى هذا المثالي بجذر الحلقة (radical of the ring)

٥) (ا) أوجد العدد الصحيح الموجب m بحيث إنّ $\mathbb{Z}_m$ ليس بها عناصر متلاشية غير صفرية.

(ب) أثبت أنّه إذا كان a عنصرًا متلاشيًا في حلقة إبدالية بمحايد فإنّ 1 - a عنصر وحدة في هذه الحلقة.

٦) أوجد جذور الحلقات:

$$\mathbb{Z}_{49}, \mathbb{Z}_{27}, \mathbb{Z}_{16}, \mathbb{Z}_9, \mathbb{Z}_6$$

٧) لتكن R حلقة، $x \in R$. أثبت أن المجموعة $\text{Ann } x = \{r \in R : rx = 0\}$ تُشكِّل مثاليا من اليسار للحلقة R. يسمى هذا المثالي مُفْنِ (annhilator) x.

٨) تعرف الحلقة القاسمية (division ring) أو الحقل المتخالف (skew field) بأنّها حقل غير إبدالي. أثبت أنّ كل حلقة غير إبدالية بمحايد لا يوجد فيها مثالي غير تافه من اليسار (من اليمين) هي حلقة قاسميّة.

٩) لتكن R', R حلقتين بمحايدين $1', 1$ على الترتيب، وليكن ϕ هومومورفزما غامرا من R إلى R'. أثبت أنّ:

(ا) $$\phi(1) = 1'$$

(ب) $$\phi(a^{-1}) = (\phi(a))^{-1}$$

لكل عنصر وحدة a في R.

١٠) لتكن $A = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$. أثبت أن A حلقة جزئية من $M_2(\mathbb{R})$ وأنّ $\phi: \mathbb{C} \to A$ المعرّف بالقاعدة $\phi(a+ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ يمثل تشاكلاً.

١١) لتكن R حلقة، I مثاليا للحلقة R. ناقش هل من الممكن أن يكون في R/I قواسم للصفر بينما لا توجد قواسم للصفر في R.

١٢) أثبت أنّـه يوجد هوموم‌ورفزم أحادي من الحلقة بمحايد R إلى End R^+ حيث R^+ هي الزمرة الجمعيّة للحلقة R.

١٣) لتكن R حلقة، وليكن I ، J مثاليّين للحلقة بحيث إن $J \supset I$. أثبت أن :

$$(R/I)/(J/I) \cong R/J$$

١٤) أثبت أنّ كل هوموم‌ورفزم غير تافه من حقل إلى حلقة يجب أن يكون أحاديًّا .

١٥) لتكن G زمـرة رتبتها أربعة وغير دائرية . أوجد End G واكتب جداول الجمع والضرب لها .

١٦) لتكن Aut R مجموعة التشاكلات الذاتيّة للحلقة R. أثبت أنّ Aut R تشكّل زمرة مع عملية تركيب التطبيقات ، وأثبت أنّ مجموعة التشاكلات الذاتية الداخلية للحلقة R تشكل زمرة ناظمية جزئية من Aut R .

(يرمز لزمرة التشاكلات الذاتية بالرمز Aut R بينما يرمز لزمرة التشاكلات الذاتية الداخلية بالرمز Inn R).

١٧) أثبت أنّ أي هوموم‌ورفزم من الحلقة Z إلى نفسها إما أن يكون التافه أو المحايد id_Z ثم أثبت أنّ $\text{Aut } \mathbf{Z} = \{id_{\mathbf{Z}}\}$.

١٨) أثبت أنّ $\text{End } \mathbf{Z}^+ \cong \mathbf{Z}$

١٩) أثبت أنّ $\text{End } \mathbf{Z}_n^+ \cong \mathbf{Z}_n$

الحلقـــة الرئيســـة

ملاحظـــة (١ ـ ٩)

لتكن R حلقـــة، $a\in R$ ، ولتكن Ra مجمـــوعـة كل حواصـل الضرب ra في الحلقة R ، حيث $r\in R$ ، أي أنّ $Ra=\{ra:r\in R\}$. من الملاحظ أن Ra تشكّل مثاليًا من اليسار وكذلك aR تشكل مثاليا من اليمين. إذا لم تكن الحلقة R بمحايد فإنّه قد لا تكون المثاليّات المذكورة آنفا تحوي a ، وفي حالة كون الحلقة إبدالية فمن الواضح أن:

$$aR = Ra$$

تعريـــف (١ ـ ١٨)

لتكن R حلقة، نقول عن مثالي من اليسار (مثالي من اليمين) إنه مثالي رئيس من اليسار left principal ideal (مثالي رئيس من اليمين right principal ideal) إذا وجد عنصر $a\in I$ بحيث إن $I=Ra(I=aR)$ ، ونقـــول عن المثـــالي I إنـــه مثـــالي رئيس (principal ideal) إذا وجد عنصر $a\in I$ بحيث إن $I=aR=Ra$ وفي هذه الحالة نقول I مولّد من قبل a ونرمز له بالرمز $I=(a)$.

مثـــال (١ ـ ٣٠)

المثاليّان التافهان في أية حلقة بمحايد R هما مثاليّان رئيسان حيث إنّ $R=(1)$ والمثالي الصفري $(0)=\{0\}$.

مثـــال (١ ـ ٣١)

ليكن n عددًا صحيحًـا ولتكن A مجمـوعـة مضـاعفـات n في حلقـة الأعداد الصحيحة Z . لقد لاحظنا في مثال (١ ـ ٢١) أنّ A مثالي للحلقة Z وأنّ $A=\{nr:r\in Z\}$ وبالتالي فإنّ: $A=n\,Z$. أي أن A مثالي رئيس.

تعريـــف (١ ـ ١٩)

نقول عن الحلقة الإبدالية بمحايد إنها حلقة رئيسة (principal ring) إذا كان كل مثالي فيها هو مثالي رئيس.

مثـــال (١ ـ ٣٢)

الحقل هو خلقة رئيسة لأن المثاليّين الوحيدين للحقل هما المثاليّان التافهان وهما مثاليّان رئيسان.

مثـــال (١ ـ ٣٣)

حلقة الأعداد الصحيحة قياس 6 هي حلقة رئيسة لأنّ المثاليّات للحلقة $\mathbb{Z}_6$ هي المثاليّات $\{0\}$ ، $I_1=\{0,3\}$ ، $I_2=\{0,2,4\}$ ، $\mathbb{Z}_6$ حيث إنّ $I_1=3\mathbb{Z}_6$ ، $I_2=2\mathbb{Z}_6$.

نظريـــة (١ ـ ١٦)

حلقة الأعداد الصحيحة هي حلقة رئيسة.

البرهـــان

ليكن I مثاليا للحلقة $\mathbb{Z}$. إذا كان I هو المثالي الصفري فهومثالي رئيس ، لذلك نفرض أنّ I مثالي غير صفري. ليكن n أقل عدد صحيح موجب في I. من الواصح أنّ $n\mathbb{Z}$ محتواة في I ، نَوَد البرهنة على أنّ I محتواة في $n\mathbb{Z}$. نفرض أنّ $x\in I$ ، يمكن كتابة x كما يلي:

$$x = qn + r \text{ حيث } r,q \in \mathbb{Z} \text{ و } 0 \leqslant r < n$$

ينتج عن ذلك أن $r=x-qn$ عنصر من I ، ولكن ذلك يؤدي إلى أن $r=0$ لأننا اخترنا n كأصغر عدد صحيح موجب. لذلك فإن $x\in n\mathbb{Z}$ وبالتالي $I=n\mathbb{Z}$.

بعض العمليات على المثاليـــات

تعريـــف (١ ـ ٢٠)

لتكـن R حلقـة، وليكـن I_1 ، I_2 مثـاليّين للحلقـة R. يعـرف مجمـوع (sum) المثاليّـين I_1 ، I_2 بأنّه المجموعة التي تحوي العناصر $a+b$ حيث a عنصر من I_1 ، b عنصر I_2 ويرمز لمجموع المثاليّين I_1 ، I_2 بالرمز I_1+I_2.

نفرض أنّ $a_1+b_1 \in I_1+I_2$ و a_2+b_2 و $r \in R$.

نلاحظ أنّ:

$$(a_1+b_1)-(a_2+b_2)=(a_1-a_2)+(b_1-b_2) \in I_1+I_2$$

$$r(a_1+b_1)=r\,a_1+r\,b_1 \in I_1+I_2$$

لذلك فإن I_1+I_2 يشكل مثاليًا للحلقة R ، بل هو أصغر مثالي للحلقة R يحوي المثاليّين I_1 ، I_2. لإثبات ذلك نفرض أنّ I مثالي للحلقة يحوي المثاليّين I_1 ، I_2 وليكن $a+b \in I_1+I_2$ حيث $a \in I_1$ ، $b \in I_2$ ، لما كان $a,b \in I$ فإنّ $a+b \in I$ وبالتالي فإن $I_1+I_2 \subset I$. وكما عرّفنا مجموع مثاليّين نُعرّف بالطريقة نفسها مجموع المثاليّات $I_1+I_2+\ldots+I_n$ حيث $I_1,I_2,\ldots,I_n$ مثاليات للحلقة R.

تعريف (١ - ٢١)

يعرّف حاصل ضرب (product) المثاليّين I_1 ، I_2 بأنه المثالي المولّد من قبل العناصر ab حيث $a \in I_1$ ، $b \in I_2$ (أصغر مثالي يحوي العناصر ab حيث $a \in I_1$ ، $b \in I_2$) ويرمز له بالرمز I_1I_2. كما يمكن تعريف $I_1I_2=\left\{\sum_{i=1}^{n} a_ib_i : a_i \in I_1, b_i \in I_2, n \in \mathbb{N} \cup \{o\}\right\}$ وبالطريقة نفسها نعرّف حاصل ضرب المثاليّات $I_1I_2\ldots I_n$ حيث $I_1,I_2,\ldots,I_n$ مثاليات للحلقة R.

مثال (١ - ٣٤)

ليكن $I_1=n\,Z$ ، $I_2=m\,Z$ مثاليّين لحلقة الأعداد الصحيحة Z. نودّ أن نجد المثالي I_1+I_2 للحلقة Z ، وأن نبرهن على أنّ $I_1+I_2=d\,Z$ حيث d هي القاسم المشترك الأعظم للعددين m,n. لما كانت d قاسما مشتركاً أعظماً للعددين m,n فهذا يعني أنّ $d|m,n$ وبالتالي فإن $n,m \in d\,Z$. لذلك فإن $n\,Z + m\,Z \subset d\,Z$. ومن ناحية أخرى فإن d قاسم مشترك أعظم للعددين m,n. وحسب إحدى النظريات في الأعداد فإنه يوجد عددان $a,b \in Z$ بحيث إنّ $d=na+mb$. ولكن هذا يعني أنّ $d \in n\,Z + m\,Z$ وبالتالي $d\,Z \subset n\,Z + m\,Z$ لذلك فإن، $I_1+I_2=n\,Z + m\,Z = d\,Z$.

كما يلاحظ أن $nmb=(n1)(mb)$ ، حيث $b \in Z$ ، لذلك فإنّ:

$$n\,Z\,m\,Z \subset nm\,Z$$

ومن ناحية أخرى إذا كانت $a,b\in \mathbf{Z}$ فإنّ :

$$(na)(mb) = n(am)b = n(ma)b = (nm)(ab)$$

وبالتالي فإن $n\mathbf{Z}\, m\mathbf{Z} \supset nm\mathbf{Z}$ لذلك فإنّ :

$$I_1 I_2 = n\mathbf{Z}\, m\mathbf{Z} = nm\mathbf{Z}$$

المثاليّات الأوليّة والأعظميّة

تعريـف (١ ـ ٢٢)

لتكن R حلقة، وليكن I مثاليًّا فعليًّا للحلقة R . نقول إنّ I مثالي أولي (prime ideal) إذا كان $a,b\in R$ بحيث إن : $ab\in I$ يؤدي إلى أنه إما $a\in I$ أو $b\in I$.

مثـال (١ ـ ٣٥)

المثالي الصفري لحلقة تامّة هو مثالي أولي لأنّه إذا كان $a,b\in R$ بحيث إن $ab=0$ فإنـه إمـا $a=0$ أو $b=0$. لذلك فإن المثالي الصفري للحلقة $\mathbf{Z}$ هو مثالي أولي وكذلك فإن المثالي الصفري لأي حقل هو مثالي أولي.

مثـال (١ ـ ٣٦)

ليكن $I=(p)$ حيث p عدد صحيح أولي وليكن $a,b\in \mathbf{Z}$ بحيث إنّ $ab=px$ حيث $x\in \mathbf{Z}$. إذن $p|ab$ ولكن p عدد أولي لذلك فإنّه إما $p|a$ أو $p|b$ ، أي أنّه إما $a=py$ أو $b=pz$ حيث $y,z\in \mathbf{Z}$. لذلك إما $a\in I$ أو $b\in I$ وهكذا فإن I مثالي أولي.

تعريـف (١ ـ ٢٣)

المثـالي من اليسـار I (من اليمـين) للحلقـة R هو مثـالي أعـظمي من اليسار maximal left ideal (مثالي أعظمي من اليمين maximal right ideal) بشرط أن $I\neq R$ وكلما كان J مثاليا من اليسار (مثاليا من اليمين) للحلقة R يحوي فعليًّا I فإن $J=R$. يقال عن المثالي I للحلقة R إنه مثالي أعظمي (maximal ideal) إذا كان $I\neq R$ وكلما وجد مثالي

آخر J للحلقة R يحوي فعليًا I فإن J=R. أي أن المثالي I يكون أعظميًا إذا لم يحوه أيُّ مثالي آخر سوى الحلقة نفسها.

مثـــال (١ - ٣٧)

المثالي الصفري لأي حقل هو مثالي أعظمي، لأنّه لا يوجد مثالي آخر في الحقل يحوي المثالي الصفري سوى الحقل نفسه.

لاحظ أن المثالي الصفري للحلقة Z مثالي غير أعظمي لأنّه محتوىً في أي مثالي آخر غير صفري.

مبرهنـــة (١ - ١٧)

المثالي (n) للحلقة Z مثالي أعظمي إذا وإذا فقط كان n عددًا أوليًا.

البرهـــان

ليكن (n) مثاليا أعظميًا للحلقة $\mathbb{Z}$. إذا كان العدد n غير أولي، فإنّ $n=n_1n_2$ حيث $1<n_1, n_2<n$، وهذا يعني أن:

$$\mathbb{Z} \supsetneq (n_1) \supsetneq (n) , \mathbb{Z} \supsetneq (n_2) \supsetneq (n)$$

مما يناقض كون (n) مثاليا أعظميًا للحلقة $\mathbb{Z}$.

نفرض أنّ n عدد أولي. لكي نبرهن أن (n) مثالي أعظمي نفرض أنه يوجد مثالي J للحلقة Z بحيث إنّ $\mathbb{Z} \supset J \supset (n)$. وبما أن Z حلقة رئيسة فإنه يوجد عدد صحيح m بحيث إن: J=(m). لما كان $(m) \supset (n)$ فإنـه يوجد عدد صحيح k بحيث إن n=mk. ولكن n عدد أولي وبالتالي فهو غير قابل للتحليل، إذن إما $k=\pm 1$ أو $m=\pm 1$. إذا كان $k=\pm 1$ فإن $n=\pm m$ وبالتالي (m)=(n) وإذا كان $m=\pm 1$ فإن $(m)=\mathbb{Z}$، لذلك فإنّ (n) مثالي أعظمي للحلقة Z.

مبرهنـــة (١ - ١٨)

إذا كان ϕ هومومورفزما من الحلقة R إلى الحلقة R′ وإذا كان q مثاليا أوليًا للحلقة R′، عندئذ فإن $\phi^{-1}(q)$ مثالي أولي للحلقة R.

البرهان

ليكن $a,b\in R$ بحيث إن $ab\in\phi^{-1}(q)$ ، هذا يعني أن $\phi(ab)\in q$ ، ولكن ϕ هوموم‌ورفزم ، إذن $\phi(ab)=\phi(a)\ \phi(b)$ وبالتالي فإن : $\phi(a)\ \phi(b)\in q$ ، وحيث إنّ q مثالي أولي للحلقة R' فإنه إما $\phi(a)=q$ أو $\phi(b)\in q$ وهذا يعني أنّه إمّا $a\in\phi^{-1}(q)$ أو $b\in\phi^{-1}(q)$.

ملاحظة (١ ـ ١٠)

إذا كان ϕ هوموم‌ورفزما من الحلقة R إلى الحلقة R' وإذا كان M مثاليا أعظميًّا للحلقة R' ، فليس من الضروري أن يكون $\phi^{-1}(M)$ مثاليا أعظميا للحلقة R ، وكمثال على ذلك اعتبر $R=\mathbb{Z}$ ، $R'=\mathbb{Q}$ ، $M=\{0\}$ ، ϕ هوموم‌ورفزم الاحتواء (يرسل كل عنصر في $\mathbb{Z}$ إلى نفسه في $\mathbb{Q}$) فإن $\phi^{-1}(\{0\})=\{0\}$ ليس مثاليا أعظميا للحلقة $\mathbb{Z}$. عندما يكون ϕ غامرًا فإن $\phi^{-1}(M)$ يكون مثاليا أعظميا للحلقة R حسب ما توضحه المبرهنة التالية .

مبرهنة (١ ـ ١٩)

ليكن ϕ هوموم‌ورفزما غامرًا من الحلقة R إلى الحلقة R' وليكن M مثاليا أعظميا للحلقة R' عندئذ فإن $\phi^{-1}(M)$ مثالي أعظمي للحلقة R.

البرهان

ليكن $I=\phi^{-1}(M)$. بما أن ϕ غامر. فإنه حسب المبرهنة (١ ـ ١٥) :

$$R/I\cong R'/M$$

ولكن M مثالي أعظمي في R' ، لذلك فإن $I=\phi^{-1}(M)$ مثالي أعظمي في R.

والآن سنستخدم حلقات القسمة لمعرفة متى يكون المثالي لحلقة إبدالية بمحايد أوليًّا أو أعظميًّا .

نظرية (١ ـ ٢٠)

لتكن R حلقة إبدالية بمحايد وليكن I مثاليا للحلقة R فإن

١) الحلقة R/I حلقة تامة إذا وإذا فقط كان I مثاليا أوليا .

(٢) الحلقة R/I حقل إذا وإذا فقط كان I مثاليا أعظميا.

البرهـــان

(١) لتكن R/I حلقة تامّة ولنفرض أن $a,b\in R$ بحيث إنّ $ab\in I$ ولكن :

$$(a + I)(b + I) = ab + I = I$$

ولما كانت R/I حلقة تامّة، إذن إما $a+I=I$ أو $b+I=I$ وهذا يعني $a\in I$ أو $b\in I$ ، لذلك فإن I مثالي أولي.

نفرض أنّ I مثالي أولي للحلقة R. حيث إنّ R حلقة إبدالية بمحايد فإن R/I حلقة إبدالية بمحايد. لذلك لكي نبرهن أن R/I حلقة تامة يكفي أن نبرهن أنه لا يوجد فيها قواسم للصفر. نفرض أن $a+I, b+I\in R/I$ بحيث إن $(a+I)(b+I)=I$. من ذلك نستنتج أن $ab+I=I$ وبالتالي $ab\in I$. ولكن I مثالي أولي، إذن إمّا $a\in I$ أو $b\in I$ وبالتالي إمّا $a+I=I$ أو $b+I=I$ ، لذلك فإن R/I حلقة تامّة.

(٢). ليكن R/I حقلاً وليكن J مثاليا للحلقة R بحيث $R\supset J\supset I$. نفرض أن I مجموعة جزئية فعليّة من J ، لذلك فإنه يوجد عنصر $a\in J$ بحيث إن $a\notin I$ ، أي أنّ $a+I\neq I$ وبالتالي فإن $a+I$ عنصر غير صفري في الحقل R/I ، لذلك يوجد له معكوس في R/I وليكن $b+I$ ، أي أن :

$$(a + I)(b + I) = 1 + I$$

وهذا يعني أن :

$$ab + I = 1 + I$$

لذلك فإنه يوجد عنصر $x\in I$ بحيث إن $ab+x=1$ ولكن ذلك يعني أن $1\in J$ وبالتالي $J=R$. إذن I مثالي أعظمي للحلقة R.

نفرض أنّ I مثالي أعظمي للحلقة R. حيث إن R حلقة إبدالية بمحايد فإن R/I حلقة إبدالية بمحايد، فلكي نثبت أنّ R/I حقل يكفي أن نثبت أن كل عنصر غير صفري في R/I هو عنصر وحدة. ليكن $a+I\neq I$ حيث $a\in R$ ولنعتبر المثالي $Ra+I$. من الواضح أن المثالي $Ra+I$ يحوي I كمجموعة جزئية فعليّة لأن $a\notin I$ ، وحيث إن I مثالي أعظمي، إذن $Ra+I=R$. لذلك فإنه يوجد : $x\in I, b\in R$ بحيث إن $ba+x=1$ وبالتالي فإن : $ba+x+I=1+I$ ، أي أن $ba+I=1+I$ وهذا يؤدي إلى أن $(b+I)(a+I)=1+I$.

وحيث إن R/I إبدالية فإن b+I هو معكوس a+I ، وبالتالي فإن a+I عنصر وحدة في R/I. وحيث إن a+I عنصر اختياري من R/I لذلك فإن R/I حقل.

نتيجـة

إذا كانت R حلقة إبدالية بمحايد وإذا كان I مثاليا أعظميا، عندئذ فإن I مثالي أولي.

البرهـان

باستخـدام (٢) من النظرية السابقة نستنتج أن R/I حقل وبالتالي حلقة تامة لذلك فإن I مثالي أولي باستخدام (١) من النظرية السابقة.

ملاحظـة (١ ـ ١١)

عكس النتيجة السابقة ليس صحيحًا لأن المثالي الصفري في الحلقة $\bar{Z}$ يشكِّل مثاليا أوليًّا وليس أعظميا.

تعريـف (١ ـ ٢٤)

الحلقة التامة الرئيسة (principal ideal domain) هي حلقة تامة وكذلك رئيسة.

مثـال (١ ـ ٣٨)

حلقة الأعداد الصحيحة هي حلقة تامة رئيسة.

مبرهنـة (١ ـ ٢١)

إذا كانت R حلقة تامة رئيسة فإن كل مثالي غير تافه للحلقة R هو مثالي أولي إذا وإذا فقط كان مثاليا أعظميا.

البرهـان

على ضوء نتيجة النظرية السابقة يكفي أن نثبت أنه إذاكان I=(a) مثاليا أوليًا غير تافه للحلقة R فإنه أيضا مثالي أعظمي. ليكن J أي مثالي للحلقة R بحيث إن $R \supset J \supset I$.

حيث إن R حلقة رئيسة فإنه يوجد $b\in J$ بحيث إن $J=(b)$ وبالتالي فإن $a\in(b)$ أي أن $a=br$ حيث $r\in R$. ولكن I مثاليا أوليا، إذن إما $b\in I$ أو $r\in I$. إذا كان b عنصرًا من I فإن $I=J$. نفرض أن $r\in I$ وبالتالي فإن $r=sa$ حيث $s\in R$ ، وهكذا فإن $a=bsa$. ولكون قانون الاختصار بالنسبة للضرب يمكن تطبيقه في الحلقة التامّة (انظر تمرين ١ - ١ - ١١)، إذن $1=bs$. وهذا يعني أن b عنصر وحده في R ، ولكن $b\in J$ ، إذن $J=R$. لذلك برهنا أنه لا يوجد مثالي بين I والحلقة R. إذن I مثالي أعظمي للحلقة R.

نتيجـــة

أي مثالي غير تافه في حلقة الأعداد الصحيحة يكون أوليًّا إذا وإذا فقط كان أعظميا.

الآن نودُّ الحصول على نتيجة عامة تؤكد على وجود مثالي أعظمي واحد على الأقل للحلقـة الإبدالية بمحايد، وللبرهنة على وجود مثل هذا المثالي الأعظمي نحتاج إلى بديهية في نظريات المجموعات تسمى مأخوذة زورن (Zorn's lemma) ولكونها خارجة عن نطاق الكتاب فسنكتفي بذكر منطوقها والقارىء الذي يرغب في تتبع الموضوع عليه أن يرجع إلى [٣].

قبل أن نذكر مأخوذة زورن نَوَدُّ أن نشير إلى تعريف السلسلة (chain): لتكن $\leqslant$ علاقة ترتيب جزئي على مجموعة S ولتكن $S\supset C$. تسمى C سلسلة في S إذا كان لكل a,b تنتمي لـ C فإن $a\leqslant b$ أو $b\leqslant a$. كما يقال إن $u\in C$ حد أعلى للسلسلة C إذا كان $a\leqslant u$ لكل $a\in C$.

مأخوذة زورن Zorn's lemma

لتكن T مجمـوعة، ولتكن S عائلة من المجموعات الجزئية من T والمرتّبة جزئيًّا (partially ordered) بالنسبة لعلاقة الاحتواء في S وبحيث إن أي سلسلة C في S لها حد أعلى في S ، عندئذ يوجد عنصر أعظم M في S غير محتوٍ فعليًّا في أي عنصر آخر من S.

نظرية (١ - ٢٢)

كل حلقة إبدالية بمحايد R لها على الأقل مثالي أعظمي واحد.

البرهـان

لتكن S مجموعة كل المثاليات الفعليّة للحلقة R. نلاحظ أن S مجموعة غير خالية لأن المثالي الصفري أحد عناصرها. لنرتب S بواسطة علاقة الاحتواء. من السهولة التـأكـد أن $(S,\subset)$ مجمـوعـة مرتّبـة جزئيًا. لتكن C سلسلة في S وليكن A اتّحاد المثاليات A_α المـوجـودة في السلسلة C. نودُّ أن نثبت أن A مثـالي فعـلي للحلقة R. ليكن $a,b\in A$ ، عند ذلك يوجد مثاليّان A_α,A_β في السلسلة C بحيث إن $a\in A_\alpha, b\in A_\beta$ ، لكن C سلسلة في S ، لذلك إمّا $A_\beta\supset A_\alpha$ أو $A_\alpha\supset A_\beta$. لنفرض أن $A_\beta\supset A_\alpha$ لذلك فإن $a-b\in A_\beta$ وبالتالي $a-b\in A$. إذا كان $r\in R, a\in A$ فإنه يوجد مثالي A_α للحلقة R في C بحيث إن $a\in A_\alpha$ وهكذا فإن $ra,ar\in A_\alpha$ وبالتالي $ra,ar\in A$. إذن A مثالي. نفرض أن $1\in A$ ، لذلك فإنه يوجد مثالي A_α في C بحيث إن $1\in A_\alpha$ وهذا يناقض كون عناصر S مثاليات فعليّة.

من الـواضـح أن A يشكّـل حدًّا أعـلى لعنـاصر C وهو عنصر في S ، لذلك تحققت شروط مأخـوذة زورن وبـالتـالي فإنه توجد مجموعة عظمى M في العائلة S. ولكن عناصر S مثاليات فعليّة للحلقة R لذلك فإن M مثالي أعظمي للحلقة R.

نتيجـة (١)

إذا كانت R حلقة إبدالية بمحايد وإذا كان I مثاليا فعليًّا للحلقة R فإنه يوجد مثالي أعظمي للحلقة R يحوي I.

البرهـان

نطبق النظرية السابقة على الحلقة R/I ونستنتج أنه يوجد مثالي أعظمي J/I للحلقة R/I ، حيث J مثالي للحلقة R (انظر ملاحظة (١ - ٨)). حيث إن الهومومورفزم Φ الطبيعي من الحلقة R إلى الحلقة R/I غامر ولما كان $J=\Phi^{-1}(J/I)$ فإن J مثالي أعظمي

للحلقة R حسب المبرهنة (١ - ١٩). والمثالي J يحوي المثالي I حسب الملاحظة (١ - ٨).

نتيجـــة (٢)

إذا كانت R حلقة إبدالية بمحايد والعنصر a ليس بعنصر وحدة من عناصر R فإنه يوجد مثالي أعظمي للحلقة R يحوي a.

البرهـــان

نعتبر المثالي I=(a) ، حسب النتيجة السابقة فإنه يوجد مثالي أعظمي للحلقة R يحوي I وبالتالي يحوي العنصر a.

ملاحظـــة (١ - ١٢)

من المناسب الإشارة إلى أنّه يوجد في كثير من الحلقات أكثر من مثالي أعظمي واحد، فقد سبق أن أوضحنا أنه إذا كان p عددًا أوليًّا فإن (p) مثالي أعظمي للحلقة $\underline{Z}$ وبـالتـالي فإنه يوجد عدد لانهائي من المثاليات الأعظمية للحلقة $\underline{Z}$ ، كما أن لحلقة الأعداد الصحيحة قياس 6 مثاليّين أعظميّين هما (2) و (3) ، والمبرهنة السابقة توضح أنه يوجد على الأقل مثالي أعظمي واحد للحلقة. والحلقات التي لها مثالي أعظمي وحيد هي حلقات خاصة نُعَرِّفُها فيما يلي:

تعريـــف (١ - ٢٥)

نقول عن الحلقة R إنها حلقة محليّة (local ring) إذا كان يوجد للحلقة R مثالي أعظمي وحيد.

مثـــال (١ - ٣٩)

من السهولة التأكد أن الحلقات:

$$\mathbf{Z}_{27}, \mathbf{Z}_{25}, \mathbf{Z}_{9}, \mathbf{Z}_{8}, \mathbf{Z}_{4}$$

حلقات محليّة ومثاليّاتها الأعظمية هي على التوالي :

$$(3), (5) , (3) , (2) , (2)$$

بينما نلاحظ أن الحلقة $\mathbf{Z}_6$ والحلقة $\mathbf{Z}$ حلقات ليست محليّة لاحتوائها على أكثر من مثالي أعظمي واحد .

تمارين (١ - ٣)

١) لتكن R حلقة وليكن I_1, I_2 مثاليّين للحلقة R. يسمى I_1+I_2 المجموع المباشر (direct sum) للمثاليّين I_1,I_2 إذا كان $I_1\cap I_2=\{0\}$ ويرمز له بالرمز $I_1\oplus I_2$. أثبت أنّ كل عنصر في $I_1\oplus I_2$ يعبّر عنه بطريقة وحيدة كحاصل جمع عنصرين أحدهما من I_1 والآخر من I_2.

٢) إذا كان I_1,I_2 مثاليّين أوليّين للحلقة R. فأثبت أنّ المثالي $I_1\cap I_2$ ليس من الضروري أن يكون مثاليًّا أوليًّا .

٣) لتكن R حلقة غير صفرية ، I مثالي للحلقة R. أثبت أنّ الحلقة R/I تخلو من قواسم الصفر إذا وإذا فقط كان I مثاليًّا أوليًّا ، ثم استنتج أنه إذا كانت R إبدالية منتهية ولها محايد فإن كل مثالي أولي في R هو مثالي أعظمي .

٤) ليكن ϕ هومومورفزما غامرًا من الحلقة R إلى الحلقة R'. أثبت أنّه :

(ا) إذا كان I مثاليًّا أعظميًّا للحلقة R فإن $\phi(I)$ مثالي أعظمي للحلقة R'.

(ب) إذا كان I مثاليا أوليًّا للحلقة R مع كون $I\supset \text{Ker}\ \phi$ فإن $\phi(I)$ مثالي أولي للحلقة R'.

٥) أثبت أنّ أية حلقة غير صفرية R تخلو من قواسم الصفر إذا وإذا فقط كان الصفر مثاليا أوليًّا .

٦) برهن أن الحلقة الإبدالية بمحايد تُشكِّل حقلا إذا وإذا فقط كان المثاليان الوحيدان هما المثاليان التافهان.

٧) استخدم النظرية (١ - ٢٠)(٢) في إيجاد المثاليات الأعظمية للحلقات التالية:

$$\mathbf{Z}+\mathbf{Z}\,,\mathbf{Z}_{30}\,,\mathbf{Z}_{27}\,,\mathbf{Z}_{15}\,,\mathbf{Z}_{12}$$

٨) برهن أنّ كل حلقة غير إبدالية بمحايد، لها مثالي أعظمي من اليسار.

٩) أثبت أنّ كل عنصر ليس له معكوس في حلقة غير إبدالية بمحايد محتوى في مثالي أعظمي من اليسار.

١٠) أثبت أنّ الحلقة $\mathbf{Z}_{p^n}$، حيث p عدد أولي، n عدد صحيح موجب، حلقة محليّة مثاليّها الأعظمي هو (p).

١١) إذا كانت R حلقة، وإذا كان I و J مثاليّين للحلقة R ، فأثبت أن:

$$J/I \cap J \cong I + J/I$$

بناء حلقات جديدة و حلقيات

مقدمـــة

لقد لاحظنا في الفصل السابق كيفية تكوين حلقات جديدة من حلقات معطاة وذلك بتكوين الحلقات الجزئية وحلقات القسمة. في هذا الفصل سنناقش بناء حلقتين مهمتين وهما حقل القواسم لحلقة تامة والمجموع المباشر للحلقات. لقد تمّ بناء حقل القواسم لحلقة تامة على منوال بناء حقل الأعداد النسبية على حلقة الأعداد الصحيحة والذي يشكّل حقل القواسم لها. وسيدرس المجموع المباشر للحلقات والذي أهميته ناتجة عن أنّه بالإضافة إلى كونه مصدرًا جديدًا لأمثلة ملموسة عن الحلقات فإنه يمكن بواسطته معرفة التركيب الجبري لحلقة اعتمادًا على مركّباتها إذا كانت مجموعًا مباشرًا لحلقات أخرى. كما سندرس في هذا الفصل صفة مميزة للحلقة تسمى مميّز الحلقة.

وأخيرا سندرس في هذا الفصل بنية جبريّة أخرى تسمى الحلقيّة، حيث أول ما ظهرت هذه البنية كانت لتوسعة الجبر الخطّي باستخدام حلقة بدلا من حقل ولكن تبيّن بعد ذلك أنه تركيب جبري أو بنية جبريّة (structure) لها استخدامات متعددة الجوانب كما أنها تعتبر أداة لا يمكن الاستغناء عنها في بعض التخصصات الرياضيّة مثل التبولوجي. سنُعرِّف الحلقيّة بالشروط نفسها التي سبق أن تعرَّف عليها القارىء في تعريف الفضاء المتّجه والاختلاف الوحيد هو أن العوامل (scalars) مأخوذة من حلقة بدلا من أن تكون مأخوذة من حقل.

حقـــل القواســـم

بنـاء حقل القواسم لحلقة تامّة

لتكن D حلقـة تامـة، D^* مجمـوعـة العناصر غير الصفرية في D. نُعرِّف على المجموعة $K=D\times D^*$ العلاقة التالية:

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc$$

لكلِّ $(a,b), (c,d) \in K$. نلاحظ ما يلي:

(ا) إذا كان $(a,b)\in K$ فإن $ab=ba$ وبالتالي $(a,b)\sim(a,b)$. أي أن العلاقة $\sim$ انعكاسية (reflexive).

(ب) إذا كان $(a,b),(c,d)\in K$ بحيث إنّ $(a,b)\sim(c,d)$ ، فإن $ad=bc$ وبالتالي $cb=da$ ولذلك $(c,d)\sim(a,b)$ ، أي أن العلاقة تناظرية (symmetric).

(ج) إذا كان $(a,b),(c,d),(e,f)\in K$ بحيث $(a,b)\sim(c,d)$ ، $(c,d)\sim(e,f)$ فإن $cf=de, ad=bc$. من $cf=de$ نحصل على $bcf=bde$ ، ولكن $bc=ad$ لذلك فإن $adf=bde$ وبالتالي $afd=bed$ لأن D حلقة إبدالية. ولكون $d\neq 0$ و D حلقة تامة فإن $af=be$ ، أي أن $(a,b)\sim(e,f)$ ، لذلك فإن العلاقة $\sim$ متعديّة (transitive). وهكذا فإن $\sim$ علاقة تكافؤ على المجموعة K.

لنـرمـز لفصـل التكـافؤ للعـلاقـة $\sim$ بالرمز $[a,b]$ وليكن F مجموعة فصول التكافؤ $[a,b]$ حيث $(a,b)\in K$. نعرف عمليتي الجمع والضرب على F كما يلي:

$$[a,b] + [c,d] = [ad + bc,bd]$$

$$[a,b]\,[c,d] = [ac,bd]$$

لما كانت D حلقة تامة، $b\neq 0$ ، $d\neq 0$ فإن $bd\neq 0$ ، وهكذا فإن $[ad+bd,bd]\in F$ وكذلك $[ac,bd]\in F$. نودّ أن نبرهن أن الجمع والضرب عمليتـان حسنتـا التعـريف، أي لا تعتمدان على اختيار ممثلي فصول التكافؤ. نفرض أنّ $[a,b]=[a',b']$ ، $[c,d]=[c',d']$. لذلك فإن $ab'=ba'$ وكذلك $cd'=dc'$.

الآن

$$(ad+cb)b'd' - (a'd'+b'c')db = (ab'-ba')dd' + (cd'-dc')bb'$$
$$= 0(dd') + 0(bb')$$
$$= 0$$

وهذا يعني أن :

$$[ad + cd,bd] = [a'd' +c'b',b'd']$$

أي أن :

$$[a,b] + [c,d] = [a',b'] + [c',d']$$

وبالتالي فإن عملية الجمع حسنة التعريف. نستطيع أن نثبت بالطريقة نفسها أن عملية الضرب حسنة التعريف، أي أن :

$$[a,b]\,[c,d] = [a',b']\,[c',d']$$

نظرية (٢ - ١)

المجموعة F مع عمليتي الضرب والجمع المعرَّفة عليها تُشكِّل حقلاً يسمى حقل قواسم الحلقة التامة D .

البرهـــان

يمكن التأكد بسهولة من أنّ عمليتي الجمع والضرب على F هما عمليتان تجميعيتان وإبداليتان. نلاحظ أنّ [0,b] هو العنصر المحـايد الجمعي وأن [-a,b] هو المعكـوس الجمعي للعنصر [a,b] ، لذلك فإن (F,+) تشكِّل زمرة إبدالية. علما أنه لكل $a\in D^*$ ولكل $[c,d]\in F$ فإن :

$$[a,a]\,[c,d] = [ac,ad] = [c,d]$$

وبـالتـالي فإن [a,a] يُشكِّـل المحـايد الضربي. كما يمكن بسهولة ملاحظة أنّ عملية الضرب تتوزع على عملية الجمع وبالتالي فإن F حلقة إبدالية بمحايد.

ليكن [a,b] عنصرًا غير صفـري في F ، فيكـون $a\neq 0$ ولـذلك فإن : $[b,a]\in F$

وبالتالي فإن :

$$[a,b]\,[b,a] = [ab,ba] = [ab,ab]$$

بما أن $ab\neq 0$ فإن [ab,ab] هو العنصر المحايد. لذلك فإن $[a,b]^{-1}=[b,a]$ وهكذا فإن F حقل.

تعريـف (٢ - ١)

لتكن S,R حلقتين. نقول إن الحلقة S مغمورة (imbedded) في الحلقة R إذا وجدت حلقة جزئية من R تشاكل S.

مبرهنـة (٢ - ٢)

كل حلقة تامة ممكن أن تغمر في حقل قواسمها.

البرهـان

لتكن D حلقة تامة وليكن F حقل قواسمها ولنعرف التطبيق $\phi:D\to F$ المعرّف بالقاعدة $\phi(a)=[a,1]$ لكل $a\in D$ نلاحظ أن:

$$\phi(a+b)=[a+b,1]=[a,1]+[b,1]$$
$$=\phi(a)+\phi(b)$$
$$\phi(ab)=[ab,1]=[a,1]\,[b,1]$$
$$=\phi(a)\,\phi(b)$$

لذلك فإن ϕ هوموورفزم من D إلى F. لنفرض أن $\phi(a)=[0,b]$ ، أي أن $[a,1]=[0,b]$ وهذا يعني أن $ab=0$ ولكن $b\neq 0$ إذن $a=0$ أي أن ϕ أحادي. بتطبيق النظرية الأساسية في التشاكل نستنتج أن $D\cong\phi(D)$ ، وبالتالي فإن D مغمورة في الحقل F.

ملاحظـة (٢ - ١)

حيث كل حلقة تامة D ممكن أن تغمر في حقل قواسمها F فإنه يمكن مطابقة كل عنصر $a\in D$ مع صورته $[a,1]$ في F ولذلك نستطيع أن نعتبر أن D حلقة جزئية من حقل قواسمها F ، وحيث إن كل عنصر $[a,b]$ في F يمكن كتابته بالصيغة التالية:

$$[a,b]=[a,1]\,[1,b]=[a,1]\,[b,1]^{-1}=ab^{-1}$$

لذلك يمكن أن نعتبر عناصر F هي ab^{-1} حيث $a\in D$ ، $b\in D^*$.

مثـال (٢ - ١)

حقل الأعداد النسبية $\mathbb{Q}$ هو حقل القواسم لحلقة الأعداد الصحيحة.

مبرهنـــة (٢ - ٣)

إذا كانت D حلقة تامة، فإن أي حقل K يحوي D يحوي حقـــل قواسمها.

البرهـــان

إذا كان $ab^{-1}\in F$ فإن $a,b\in D$, $b\neq 0$ لذلـــك فإن $a,b\in K$ ، لكن b عنصر غير صفري، إذن $b^{-1}\in K$ وهكذا فإن $a\,b^{-1}\in K$ بالتالي فإن $K\supset F$.

نظرية (٢- ٤)

إذا كان D ، D' حلقتين تامتين و F ، F' حقلي قواسمهما على الترتيب. إذا كان ϕ تشـــاكـــلا من D إلى D' فإنـه يوجـد تشـاكـل φ من F إلى F' بحيث إن قيد φ(restriction) على D يساوي ϕ.

البرهـــان

لنعرف $\varphi:F\to F'$ بالقاعدة:

$$\varphi(ab^{-1}) = \phi(a)\,(\phi(b))^{-1}$$

لكـل $ab^{-1}\in F$. لما كان $b\neq 0$ و ϕ تشـــاكـــل فإن $\phi(b)\neq 0$. لكي نبرهن أنّ φ حسنـــة التعـريف نفـرض أن $ab^{-1}=cd^{-1}$ وبـالتـالي فإن $ad=cb$. كذلـك فإن $\phi(ad)=\phi(cb)$ وهـذا يـؤدي إلى أن $\phi(a)\phi(d)=\phi(c)\phi(b)$ وبالتـالي فإن $\phi(a)(\phi(b))^{-1}=\phi(c)(\phi(d))^{-1}$. أي أنّ $\varphi(ab^{-1})=\varphi(cd^{-1})$ ، لذلك فإن φ حسنة التعريف.

ليكن $ab^{-1}, cd^{-1}\in F$ عندئذ فإن:

$$\varphi(ab^{-1}+cd^{-1})=\varphi((ad+cb)(b^{-1}d^{-1}))=\varphi((ad+bc)(db)^{-1})$$
$$=\phi(ad+bc)(\phi(db))^{-1}$$
$$=(\phi(a)\phi(d)+\phi(b)\phi(c))(\phi(d)\phi(b))^{-1}$$
$$=\phi(a)(\phi(b))^{-1}+\phi(c)(\phi(d))^{-1}$$
$$=\varphi(ab^{-1})+\varphi(cd^{-1})$$

أي أنّ φ تحافظ على عملية الجمع. كذلك فإنّ:

$$\varphi((ab^{-1})(cd^{-1}))=\varphi(ac(bd)^{-1})$$
$$=\phi(ac)(\phi(bd))^{-1}=$$

$$=\phi(a)\phi(c)(\phi(b)\phi(d))^{-1}$$
$$=\phi(a)\phi(c)(\phi(d))^{-1}(\phi(b))^{-1}$$
$$=\phi(a)(\phi(b))^{-1}\phi(c)(\phi(d))^{-1}$$
$$=\varphi(ab^{-1})\varphi(cd^{-1})$$

لذلك فإن φ هومومورفزم. ليكن $\varphi(ab^{-1})=0$ وبالتالي فإنَّ: $\phi(a)(\phi(b))^{-1}=0$. وهذا يعني أنّ $\phi(a)=0$ لأن $b\neq 0$ ، ولكن ϕ أحادي إذن $a=0$ وبالتالي فإن $ab^{-1}=0$ ، لذلك فإن φ أحادي. ليكن $cd^{-1}\in F'$ حيث $c,d\in D'$ ، $d\neq 0$ ، بالتالي يوجد $a\in D$ ، $b\in D^*$ بحيث إنَّ $\phi(a)=c$ ، $\phi(b)=d$ وبالتالي فإن $\varphi(ab^{-1})=cd^{-1}$. أي أن φ غامر. وهكذا فإنَّ F يشاكل F'.

مـمـيّز الحلقـة

تعريـف (٢ - ٢)

لتكن R حلقة فإنّ مميّز (characteristic) الحلقة R هو أصغر عدد صحيح موجب a بحيث إن $ar=0$ لكل $r\in R$. إذا لم يوجد مثل هذا العدد الصحيح الموجب فنقول إن مميّز الحلقة R هو الصفر.

مثـال (٢ - ٢)

الحلقـات $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ حلقات مميّزاتها تساوي صفرًا بينما الحلقات $\mathbb{Z}_2$، $\mathbb{Z}_4$، $\mathbb{Z}_{15}$، $\mathbb{Z}_n$ حلقات مميزاتها على الترتيب 2 ، 4 ، 15 ، n.

مبرهنـة (٢ - ٥)

لتكن R حلقة بمحايد، عندئذ فإن R لها مميّز a إذا وإذا فقط كان a أصغر عدد صحيح موجب بحيث إنّ $a\,1=0$.

البرهـان

نفرض أن a مميّز الحلقة وأنّ $n1=0$ حيث $0<n<a$ ، لذلك فإنه لكل $r\in R$ يكون:

$$nr=n(1r)=(n1)r=0r=0$$

ومن تعريف مميّز الحلقة نستنتج أن a أصغر من أو يساوي n ولكن ذلك يناقض اختيار $n<a$. لذلك فإن a أصغر عدد صحيح موجب بحيث إنّ $a\,1=0$. نفرض الآن أنّ a أصغر عدد صحيح موجب بحيث إنّ $a\,1=0$. لذلك فإنه لكل $r\in R$ يكون:

$$ar = a(1r) = (a1)r =0r = 0$$

ومن التعريف (٢ ـ ٢) نستنتج أن a هو مميز الحلقة.

نظريـة (٢ ـ ٦)

لتكن R حلقة بمحايد e ، عندئذ فإن التطبيق $\phi(n)=ne$ يعرف هومومورفزما من حلقة الأعداد الصحيحة $\mathbb{Z}$ إلى الحلقة R.

البرهـــان

ليكن 0' صفر الحلقة R. نلاحظ أنّه لكل $m,n\in Z$ فإنّ ϕ تحافظ على عملية الجمع :

$$\phi(m+n)=(m+n)e=me+ne=\phi(m)+\phi(n)$$

كما نلاحظ أنّ :

$$\phi(m)\,\phi(n)=m\,e\,n\,e$$

$$=(e+\ldots+e)n\,e$$

m– مرة

$$=e\,n\,e+\ldots+e\,n\,e$$

لأن قانوني التوزيع ساريا المفعول في R.

$$=n\,e^2+\ldots+n\,e^2$$

$$=n\,e+\ldots+n\,e$$

$$=m\,n\,e$$

$$=\phi(m\,n)$$

ملاحظـــة (٢ ـ ٢)

حيث **Z** حلقة رئيسة وحيث إن Ker ϕ مثالي للحلقة **Z** ، فإنّه يوجد $a\in Ker\ \phi$ بحيث إن Ker $\phi=(a)$ ، ومن برهان النظرية (١ ـ ١٦) نستنتج أنّ a هو أصغر عدد صحيح موجب في Ker ϕ ويولدها. لكن Ker $\phi=\{r\in Z:re=0\}$ ، إذن a هو مميّز الحلقة حسب المبرهنة (٢ ـ ٥). أي أن التعريف الجبري لمميّز الحلقة R بمحايد e هو أصغر عدد صحيح موجب يولد نواة الهومومورفزم من Z إلى R المعرّف بالقاعدة $\phi(n)=n\,e$.

نتيجـــة (١)

إذا كانت R حلقة بمحايد e ، فإنّ $ne=0$ إذا وإذا فقط كان مميّز الحلقة a يقسم n.

البرهـــان

إذا كان ϕ الهوموموفزم المعرّف في المبرهنة السابقة فإن :

$$\phi(n)=ne=0\Leftrightarrow n\in Ker\,\phi=a\,Z\Leftrightarrow a\ \ n$$

نتيجـة (٢)

إذا كانت R حلقة بمحايد وليس بها قواسم للصفر، فإنَّ مميّزها صفر أو عدد أولي.

البرهـان

ليكن ϕ الهوموم‌ورفزم المعرّف في النظرية السابقة ولتكن $\mathbb{Z}\ a = \text{Ker}\ \phi$ ، حيث a هو مميّز الحلقة. حسب النظرية الأساسية في التشاكل للحلقات فإن :

$$\mathbb{Z} / a\,\mathbb{Z} \cong \text{Im}\ \phi$$

ولما كانت $\text{Im}\ \phi$ حلقة جزئية من R ، فإن $\text{Im}\ \phi$ ليس بها قواسم للصفر أصلا. وحيث إن $\mathbb{Z}$ إبدالية بمحايد فإن $\mathbb{Z}/a\ \mathbb{Z}$ إبدالية بمحايد وبالتالي فإن $\text{Im}\ \phi$ إبدالية بمحايد ولا يوجد بها قواسم للصفر. أي أن $\text{Im}\ \phi$ حلقة تامة وهذا يؤدي إلى أن $a\ \mathbb{Z}$ مثالي أولي وبالتالي فإنَّه إما $a=0$ أو a عدد أولي.

نتيجـة (٣)

لتكن R حلقة بمحايد ومميّزها صفرا فإن R حلقة غير منتهية (infinite).

البرهـان

ليكن ϕ الهوموم‌ورفزم المعرّف في النظرية (٢ ـ ٦)، فإنَّه حسب النظرية الأساسية في التشاكل للحلقات يكون :

$$\mathbb{Z} / \{0\} \cong \text{Im}\ \phi$$

ولكن

$$\mathbb{Z} / \{0\} \cong \mathbb{Z}$$

لذلك $\text{Im}\ \phi \cong \mathbb{Z}$ وهذا يعني أنَّ $\text{Im}\ \phi$ حلقة غير منتهية، ولكن $\text{Im}\ \phi$ حلقة جزئية من R ، إذن R حلقة غير منتهية.

مبرهنـة (٢ ـ ٧)

إذا كان F حقلا فإن F يحوي حقلاً جزئيًّا يشاكل $\mathbb{Q}$ أو يشاكل $\mathbb{Z}_p$ حيث p عدد أولي.

البرهـــان

حسب النتيجة (٢) النظرية السابقة فإن مميّز الحقل F إما أن يساوي صفرا أو يساوي عددًا أوليًّا. إذا كان مميّز الحقل يساوي صفرا، فإن F يحوي $\mathrm{Im}\,\phi$ كحلقة جزئية تشاكل Z وبالتالي فإن F يحوي حقل قواسم $\mathrm{Im}\,\phi$ الذي يشاكل حقل قواسم Z وهو Q (انظر المبرهنة (٢ - ٤)). إذا كان مميّز الحقل عددا أوليا وليكن p فإن $\mathrm{Ker}\,\phi=(p)$ حيث ϕ هو الهومومورفزم المعرّف في النظرية (٢ - ٦) وبالتالي فإن:

$$\mathbf{Z}_p \cong \mathbf{Z}/(p) \cong \mathrm{Im}\,\phi$$

لذلك فإن $\mathrm{Im}\,\phi$ حقل جزئي من F يشاكل $\mathbf{Z}_p$.

المجمـوع المباشـر للحلقـــات

بناء حلقة المجموع المباشر الخارجي لمجموعة منتهية من الحلقات

لتكن $R_1,R_2,\ldots,R_n$ مجمـوعـة منتهية من الحلقـات وليكن R حاصل الضرب الـديكـارتي (cartesian Product) للحلقـات $R_1,R_2,\ldots,R_n$. لنعـرِّف عمليتي الجمع والضرب على R كما يلي:

$$(r_1,\ldots,r_n)+(s_1,\ldots,s_n)=(r_1+s_1,r_2+s_2,\ldots,r_n+s_n)$$

$$(r_1,\ldots,r_n)(s_1,\ldots,s_n)=(r_1s_1,r_2s_2,\ldots,r_ns_n)$$

يمكن بسهولة التأكد من أن العمليتين المعرّفتين آنفا تحوّل R إلى حلقة، وصفر هذه الحلقة هو $(0,\ldots,0)$ وعنصرها المحايد هو $(1,\ldots,1)$. كما نلاحظ أن الإسقاطات (projections) $\pi_i\,(r_1,\ldots,r_n)\to r_i$ تشكل هوموموروفزما غامرًا من R إلى R_i.

تعريـــف (٢ - ٣)

تسمى الحلقة R المعرّفة آنفا المجموع المباشر الخارجي (the external direct sum) للحلقات $R_1,\ldots,R_n$ ويرمز لها بالرمز $R=\sum_{i=1}^{n\oplus Ex} R_i$.

لتكن I_i هي مجمـوعة العناصر $(0,\ldots,r_i,0,\ldots,0)$ في R حيث r_i تقع في المركبة i وتنتمي إلى R_i. يمكن للقـارىء ملاحظة أنّ I_i مثالي للحلقة R وأن قيد الإسقاط π_i

على I_i ينتج عنه تشاكل بين I_i و R_i ، كما يلاحظ أن :

$$R = \sum_{i=1}^{n} I_i \, , \, I_i \cap \sum_{j \neq i} I_j = \{0\}$$

وهذه الحقائق تؤدي إلى التعريف التالي .

تعريـف (٢ - ٤)

لتكن R حلقة ولنفرض أن $I_1, I_2, \ldots, I_n$ مثاليّات للحلقة R بحيث إن :

$$\text{(i)} \quad R = \sum_{i=1}^{n} I_i \quad , \quad \text{(ii)} \quad I_i \cap \sum_{j \neq i} I_j = \{0\}$$

عند ذلك فإن R تسمى المجموع المباشر الداخلي (internal direct sum) للمثاليّات $I_1, I_2, \ldots I_n$ ويرمز لهذا المجموع بالرمز:

$$R = \sum_{i=1}^{n}{}^{\oplus} I_i$$

ملاحظـة (٢ - ٣)

يلاحظ أنَّ المجمـوع المبـاشر الخارجي هو بناء حلقة أكثر تعقيدا من حلقات معطاة، بينما المجموع المباشر الداخلي هو تهشيم الحلقة المعطاة إلى مركبّات أبسط .

ملاحظـة (٢ - ٤)

لقد سبق أن لاحظنا أنَّه إذا كانت R مجموعا مباشرا خارجيًّا للحلقات $R_1, \ldots, R_n$ فإنه يمكن أن تحوّل الحلقة R إلى مجموع مباشر داخلي للمثاليّات $I_1, \ldots, I_n$ للحلقة R حيث $I_1, \ldots, I_n$ حسبما وضّحناه آنفا . كما نلاحظ أنّ التطبيق :

$$(r_1, r_2, \ldots, r_n) \to r_1 + r_2 + \ldots + r_n$$

من R (مجموع مباشر خارجي) إلى R (مجموع مباشر داخلي) يمثل تشاكلا وهذا يعني أنَّه لا يوجد اختلاف من ناحية جبرية بين المجموع المباشر الخارجي والمجموع المباشر الداخلي وإنَّما الاختلاف واقع بينهما كمجموعات .

مبرهنـة (٢ - ٨)

لتكن R حلقة وليكن $I_1, \ldots, I_n$ مثاليات للحلقة R ، عندئذ فإنَّ R تكون المجموع

المباشر الداخلي للمثاليات $I_1,\ldots,I_n$ إذا وفقط إذا كان لكل عنصر r من R تمثيل وحيد على الصورة التالية :

$$r = r_1 + r_2 + \ldots + r_n$$

حيث $r_i \in I_i$.

البرهـــان

لنفرض أنّ الحلقة R هي المجموع المباشر الداخلي للمثاليات $I_1,\ldots,I_n$ عندئذ فإن :

$$R = \sum_{i=1}^{n} \oplus I_i$$

نفرض أنّه لكل r في R تمثيلان على الصورة التالية :

$$r = r_1 + r_2 + \ldots + r_n = r_1' + r_2' + \ldots + r_n'$$

حيث $r_i, r_i' \in I_i$ وبالتالي فإنّ :

$$r_i - r_i' = \sum_{j \neq i} (r_j' - r_j) \in I_i \cap \sum_{j \neq i} I_j$$

لذلك فإن $r_i = r_i'$ ، وبالتالي فإنّ التمثيل وحيد .

نفرض الآن أن لكل عنصر $r \in R$ تمثيلا وحيدا وبالتالي من الواضح أنّ

$$R = \sum_{i=1}^{n} I_i$$

لنفرض الآن :

$$x \in I_i \cap \sum_{j \neq i} I_j$$

وهذا يعني أنّ :

$$x = r_i = \sum_{\substack{j \neq i \\ j=1}}^{n} r_j$$

ولكن تمثيل العنصر r وحيد . لذلك فإنّ $r_i = 0$ وبالتالي فإن $x = 0$.

أي أنّ :

$$I_i \cap \sum_{j \neq i} I_j = \{0\}$$

لذلك فإنّ R تشكّل المجموع المباشر الداخلي للمثاليات $I_1,\ldots,I_n$.

مثـــال (٢ ـ ٣)

لتكن $R=\mathbb{Z}_2\oplus_{Ex}\mathbb{Z}_2$. نلاحظ أنَّ عناصر R هي : (0,0) ، (1,0) ، (0,1) ، (1,1). لنفرض أنَّ $I_1=\{(0,0),(1,0)\}$ ، $I_2=\{(0,0),(0,1)\}$. من الواضح أن I_1,I_2 مثاليّان للحلقة R وأن R هو المجموع المباشر الداخلي للمثاليّين I_1,I_2.

مثـــال (٢ ـ ٤)

لقد سبق أن أشرنا إلى أن $I_1=(2)$ ، $I_2=(3)$ يشكّلان مثاليّين للحلقة $\mathbb{Z}$. كما يلاحظ مباشرة أن $\mathbb{Z}_6=I_1+I_2$ وكذلك $I_1\cap I_2=\{0\}$ ، وبالتالي فإن $\mathbb{Z}_6$ هو المجموع المباشر الداخلي للمثاليّين I_1,I_2.

تمـــاريـــن (٢ ـ ١)

١) أثبت أنّ أي حقل يشاكل حقل قواسمه.

٢) ليكن F حقل قواسم للحلقة التامة D ، F' حقل يحوي D كحلقة جزئية ولا يوجد حقل جزئي فعلي من F' يحوي D. أثبت أنّ

$$F\cong F'$$

٣) أوجد حقل القواسم للحلقة التامة $\mathbb{Z}[\sqrt{2}]$.

٤) أوجد حقل القواسم للحلقة التامة $\mathbb{Z}[i]$ حيث $i=\sqrt{-1}$.

٥) ليكن p عددا أوليًّا ولتكن $\mathbb{Q}_p$ هي حلقة كل الأعداد النسبية a/b بحيث إنّ p لا يقسم b. أثبت أنّ $\mathbb{Q}_p$ حلقة رئيسة وأوجد مثاليّاتها وزمرة وحداتها.

٦) برهن أنَّه إذا كان F حقلا أوليًّا فإن $\mathrm{Aut}\,F=\{id_F\}$.

٧) أعط مثالا لحلقة إبدالية مميّزها n.

٨) ليكن F حقلا مميّزه عدد أولي p ولتكن $a,b\in F$. عرّف التطبيق ϕ من F إلى F بالقاعدة التالية : $\phi(x)=x^p$ لكل $x\in F$. أثبت أنّ :

(أ) $\phi(a+b)=a^p+b^p$.

(ب) ϕ هومومورفزم أحادي .

(جـ) إذا كان F منتهيا فأثبت أنّ ϕ تشاكل ذاتي للحقل F.

٩) لتكن R_1,R_2 حلقتين لكل منهما محايد، عُرِّف على حاصل الضرب الديكارتي للحلقتين $R_1\times R_2$ عمليتي الجمع والضرب كما يلي :

$$(r_1,r_2)+(s_1,s_2)=(r_1+s_1,r_2+s_2)$$

$$(r_1,r_2)(s_1,s_2)=(r_1s_1,r_2s_2)$$

لكل $(r_1,r_2),(s_1,s_2)\in R_1\times R_2$. أثبت أنّ $R_1\times R_2$ تشكّل حلقة، وأوجد مثاليّاتها، وأثبت أنّ $G_R=G_{R_1}\times G_{R_2}$ ، أي أثبت أنّ زمرة الوحدات للحلقة R تساوي حاصل الضرب المباشر (direct product) لزمرتي وحدات الحلقتين R_1,R_2.

١٠) عبِّر عن الحلقات التالية كمجموع مباشر داخلي لبعض مثاليّاتها $\mathbf{Z}_{105}$. $\mathbf{Z}_{77}$,$\mathbf{Z}_{35}$,$\mathbf{Z}_{21}$.

١١) أثبت أن الحلقتين $\mathbf{Z}\oplus_{Ex}\mathbf{Z}$,$\mathbf{Z}$ غير متشاكلتين .

١٢) لتكن R,S,T حلقات لكل منها محايد، أثبت أنّ

$$R\oplus(S\oplus T)\cong(R\oplus S)\oplus T$$

١٣) لتكن R المجموع المباشر الداخلي $R=I_1\oplus I_2$ حيث I_1,I_2 مثاليّان للحلقة R ولتكن S حلقة جزئية من R تحوي I_1. أثبت أن :

$$S=I_1\oplus(S\cap I_2)$$ وكذلك $R/I\cong I_2$

١٤) لتكن R أية حلقة، ولتكن $\bar{R}=R\oplus_{Ex}\mathbb{Z}$ المجموع المباشر الخارجي، عُـرِّف على $(\bar{R},+)$ عملية الضرب كما يلي:

$$(r,n)(r',n')=(rr'+nr'+n'r,nn')$$

أثبت أن ذلـك الضرب يجعـل $\bar{R}$ حلقـة بمحايد هو $(0,1)$ ، وأثبت أيضا أنّ المجموعة $\{(r,0):r\in R\}$ تشكّل حلقة جزئية من $\bar{R}$ تشاكل R ، وهذا يعني أن أية حلقة ممكن أن تغمر (imbedded) في حلقة بمحايد.

١٥) لتكن A مجموعة غير خالية ولنُعرِّف العملية Δ على مجموعة المجموعات الجزئية $P(A)$ للمجموعة A بالقاعدة التالية:

$$\forall B,C\in P(A)$$

$$B\,\Delta\,C=(B\setminus C)\cup(C\setminus B)$$

أثبت أنَّ النظام $(P(A),\Delta,\cap)$ حلقة إبدالية بمحايد تحوي قواسمًا للصفر ومميّزها 2. لاحظ أنه إذا كانت A مجموعة غير منتهية فإن $(P(A),\Delta,\cap)$ حلقة غير منتهية مميّزها عدد أولي.

الحلقيات والحلقيات الجزئيـــة

تعريـــف (٢ - ٥)

لتكن R حلقة بمحايد، نقول عن الزمرة الإبدالية M بأنها حلقيّة على الحلقة R (module over a ring R or R-module) ، إذا وجد تطبيق من $R\times M$ إلى M معرَّف بالقاعدة: $(r,m)\to rm$ يحقق الشروط التالية:

(i) $r(m_1+m_2)=rm_1+rm_2$

(ii) $(r_1+r_2)m=r_1m+r_2m$

(iii) $(r_1r_2)m=r_1(r_2m)$

(iv) $1.m=m$

لكلّ $r,r_1,r_2\in R$ ولكلّ $m,m_1,m_2\in M$.

ملاحظـة (٢ - ٥)

لكي نكون أكثر دقّة علينا أن نشير إلى أن ما تم تعريفه سابقا يمكن تسميته حلقيّة على الحلقة R من اليسار (left R-module) وبالطريقة نفسها تعرّف الحلقيّة على الحلقة R من اليمين (right R-module) حيث إنّ عناصر R تكتب من اليمين. وحيث إنّنا لن نحتاج إلى تعريف الحلقية من اليمين في هذا الكتاب لذلك سنسمي الحلقيّة من اليسار على الحلقة R بالحلقية على الحلقة R.

باستخدام طريقة برهان المبرهنة (١ - ٣) نستطيع أن نثبت النتائج التالية اعتمادا على تعريف الحلقيّة.

مبرهنـة (٢ - ٩)

إذا كانت R حلقة بمحايد وإذا كانت M حلقيّة على R فإنَّ :

(i) $0_R\, m = 0_M$

(ii) $r\, 0_M = 0_M$

(iii) $(-r)m = -(rm) = r(-m)$

مثـال (٢ - ٥)

يلاحـظ أن أي فضـاء متجـه (vector space) على حقـل K يعتـبر حلقيـة على الحقـل K.

مثـال (٢ - ٦)

لتكن A زمرة جمعية إبدالية، وليكن $a\in A, n\in \mathbb{Z}$. نلاحظ أنه إذا كانت $n>0$ فإنَّ :

$$na = a + a + \ldots + a$$

أي أننا جمعنا العنصر a عدد n مرة. إذا كانت $n<0$ فإن :

$$na = (-n)(-a) = -(a + a + \ldots + a)$$

أيضا $0a=0$. لذلك فإنه إذا كانت $a,b\in A\ ,\ n,m\in \mathbb{Z}$ فإن :

$$n(a + b) = na + nb$$

$$(n + m)a = na + ma$$

$$(nm)a = n(ma)$$

$$1.a = a$$

لذلك فإنَّ أية زمرة جمعية إبدالية هي حلقية على Z لأن التطبيق : $(n,a)\to na$ من $Z\times A$ إلى A يحقق شروط الحلقية .

مثـال (٢ - ٧)

أيةُ حلقـة بمحـايد يمكن اعتبارها حلقية على نفسها بطريقة طبيعية ، وذلك بتعريف التطبيق من $R\times R^{+}$ إلى R^{+} بالقاعدة $(r,s)\to rs$. نلاحظ أن الشرطين الأولين من شروط الحلقية تتحقق باستخدام خاصة التوزيع في R ، والشرط الثالث يتحقق من خاصة الدمج في R ، والشرط الرابع يتحقق من تعريف العنصر المحايد للحلقة R ، ويرمز للحلقة R إذا اعتبرت حلقية على نفسها بالرمز $_{R}R$.

تعريـف (٢ - ٦)

لتكن M حلقيّة على الحلقة بمحايد R. الحلقية الجزئية على R من M (R-submodul of M) هي مجموعة جزئية غير خالية N من M بحيث إنَّ :

(ا) N تشكل زمرة جزئية من M.

(ب) لكل $r\in R$ ، $n\in N$ فإنّ $rn\in N$.

لاحظ أنَّ N تشكّل حلقيّة على الحلقة المعطاة R.

باستخـدام المـبرهنة في نظرية الزمر، التي تنص على أنَّ المجموعة الجزئية غير الخـالية H من الـزمـرة G تكـوّن زمرة جزئية من G إذا وإذا فقط كان $ab^{-1}\in H$ لكلّ $a,b\in H$ ، فإنّنا نحصل على المبرهنة التالية .

مبرهنـة (٢ - ١٠)

إذا كانت M حلقيّة على الحلقة بمحايد R ، فإن المجموعة الجزئية غير الخالية N من M تكون حلقيّة جزئية على R من M إذا وإذا فقط كان $n_1-n_2\in N, rn\in N$ لكل $n,n_1,n_2\in N$ ، ولكل $r\in R$.

مثـال (٢ - ٨)

لكل حلقية M على حلقة بمحايد R ، لها حلقيّتان جزئيّتان $M,\{0\}$.

مثـــال (٢ - ٩)

يلاحظ أنّه إذا كانت B زمرة جزئية من زمرة إبدالية جمعيّة A وكان $b \in B$ فإنّ:

$$nb = \pm (b + \ldots + b)$$

ولذلك فإنّ $nb \in B$. وهكذا فإن الحلقيّات الجزئيّة على $\mathbb{Z}$ من A هي الزمر الجزئية من A.

مثـــال (٢ - ١٠)

نلاحظ أن الفضاءات الجزئية (vector subspaces) من فضاء متّجه على حقل هي حلقيّات جزئيّة منه إذا اعتبر حلقيّة على الحقل.

مثـــال (٢ - ١١)

إذا اعتبرت الحلقة بمحايد كحلقيّة على نفسها فإنّه من الواضح أنّ الحلقيّات الجزئيّة من $_RR$ هي المثاليات من اليسار للحلقة R.

تعريـــف (٢ - ٧)

نقول إنّ الحلقيّة M على الحلقة بمحايد R **مُوَلّدة نهائيا** (finitely generated) إذا كانت مولّدة على R من قبل مجموعة نهائية من عناصرها ونقول إنها **دائرية** (cyclic) إذا كانت مولّدة على R من أحد عناصرها.

مثـــال (٢ - ١٢)

الفضاء المتّجه على حقل يكون حلقيّة مولّدة نهائيًّا على حقل إذا وإذا فقط كان بعده (dimension) كفضاء متّجه على حقل بعدًا منتهيًا، ويكون دائريًّا إذا وإذا فقط كان بعده كفضاء متّجه على حقل يساوي صفرا أو يساوي الواحد.

مثـــال (٢ - ١٣)

لتكن A زمرة جمعيّة إبداليّة، فإنّ A حلقيّة مولّدة نهائيًّا على $\mathbb{Z}$ إذا وإذا فقط كانت زمرة مولّدة نهائيًّا وتكون حلقيّة دائريّة على $\mathbb{Z}$ إذا وإذا فقط كانت زمرة دائريّة.

مثـــال (٢ - ١٤)

لتكن R حلقة بمحايد وليكن M حلقية جزئية من $_RR$ وبالتالي مثالي من اليسار للحلقة R. نلاحظ أن M حلقية دائرية على R إذا وإذا فقط كانت M مثاليا رئيسا من اليسار وبصفة خاصة $_RR$ حلقية دائرية لأن : $R = R.1$.

حلقيّة القسمة وهوموومورفزم الحلقيّات

لتكن M حلقيّة على الحلقة بمحايد R ولتكن N حلقية جزئية على R من M. لقد سبق للقارىء أن تعرف على زمرة القسمة .

$$M/N = \{m + N : m \in M\}$$

وهي زمرة إبدالية لأن M إبدالية . لكي نحوّل هذه الزمرة الإبدالية إلى حلقية على R نحتاج إلى أن نعرف ضرب عناصر R بعناصر زمرة القسمة M/N وليكن ذلك كما يلي:

$$r(m + N) = r\,m + N$$

لكلّ $r \in R$ ولكل عنصر $m+N \in M/N$. نودُّ أن نثبت أنّها عملية حسنة التعريف، أي لا تعتمد على ممثلي المجموعة المشاركة لذلك نفرض أنّ : $m+N=m'+N$ ، وبالتالي فإنّ $m-m' \in N$ ولكون N حلقية جزئية من M فإن $r(m-m') \in N$. أي أنّ $rm - rm' \in N$ لذلك فإنّ $rm+N=rm'+N$ ، وبالتالي فإن ضرب عناصر الحلقة R بعناصر M/N عمليّة حسنة التعريف .

يستطيع القارىء بسهولة التأكد من أن M/N تُشكّل حلقيّة على الحلقة R ، لذلك سنذكر ذلك كمبرهنة دون الحاجة إلى إثباتها .

مبرهنـــة (٢ - ١١)

إذا كانت M حلقيّة على الحلقة بمحايد R وكانت N حلقية جزئية من M فإنّ M/N تشكّل حلقيّة على R تسمى بحلقية القسمة لـ M على N (quotient module of M by N).

تعريـــف (٢ - ٨)

ليكن M,N حلقيات على الحلقة بمحايد R ، نقول عن التطبيق ϕ من M إلى N

إذا كان : (R-homomorphism) R إنّه هوموم ورفزم على

(i) $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$

(ii) $\phi(r\,m) = r\,\phi(m)$

لكل $m, m_1, m_2 \in M$ ولكل $r \in R$.

لاحظ أنّ تعريف الهوموم ورفزم في الحلقيات يفترض أن تكون الحلقيات مأخوذة على حلقة واحدة.

تعريـف (٢ - ٩)

يعرف الهوموم ورفزم الأحادي على الحلقة R والهوموم ورفزم الغامر على الحلقة R والتشاكل (R-isomorphism) على الحلقة R والتشاكل الذاتي على الحلقة R بين الحلقيات بالطريقة نفسها التي يعرف بها في الزمر والحلقات ويرمز للتشاكل على الحلقة R بالرمز $\cong_R$.

مثـال (٢ - ١٥)

لتكن M,N حلقيّتين على الحلقة بمحايد R. نلاحظ أنَّ التطبيق التافه الذي يرسل كل عنصر من M إلى صفر الحلقيّة N يشكِّل هوموم ورفزما على R ، كذلك إنَّ التطبيق المحايد من M إلى M يشكِّل هوموم ورفزما.

مثـال (٢ - ١٦)

إذا كانت A,B زمرتين جمعيّتين إبداليّتين معتبرتين كحلقيّتين على Z. عندئذ الهوموم ورفزمات على Z من A إلى B هي الهوموم ورفزمات من A إلى B كزمر.

تعريـف (٢ - ١٠)

لتكن M,N حلقيّتين على الحلقة بمحايد R وليكن $\phi: M \to N$ هوموم ورفزما من M إلى N ، تسمى فيما يلي المجموعة :

$$\operatorname{Ker}\phi = \{m \in M : \phi(m) = 0\}$$

بنواة ϕ. كذلك تسمّى المجموعة :

$$\operatorname{Im}\phi = \{\phi(m) : m \in M\}$$

بصورة ϕ.

مبرهنـة (٢ - ١٢)

لتكن M,N حلقيّتين على الحلقة بمحايد R وليكن ϕ هوممورفزما على R من M إلى N ، عندئذ فإنَّ :

(ا) $\text{Ker}\,\phi$ حلقية جزئية من M.

(ب) $\text{Im}\,\phi$ حلقية جزئية من N.

البرهـان

(ا) ليكن $m,m_1,m_2 \in \text{Ker}\,\phi$ و $r \in R$ ، عندئذ فإنَّ :

$$\phi(m_1-m_2) = \phi(m_1+(-m_2)) = \phi(m_1) + \phi(-m_2)$$
$$= \phi(m_1) - \phi(m_2) = 0 - 0 = 0$$

لذلك فإنَّ $m_1 - m_2 \in \text{Ker}\,\phi$. كذلك :

$$\phi(r\,m) = r\phi(m) = r.0 = 0$$

لذلك فإنَّ $r\,m \in \text{Ker}\,\phi$ وبالتالي فإنّ $\text{Ker}\,\phi$ حلقية جزئية على R من M.

(ب) ليكن $n,n_1,n_2 \in \text{Im}\,\phi$ و $r \in R$ ، عندئذ يوجد $m,m_1,m_2 \in M$ بحيث إنّ $n=\phi(m), n_1=\phi(m_1), n_2=\phi(m_2)$ وبالتالي فإنَّ :

$$n_1 - n_2 = \phi(m_1) - \phi(m_2)$$
$$= \phi(m_1) + \phi(-m_2)$$
$$= \phi(m_1 + (-m_2))$$
$$= \phi(m_1 - m_2)$$

وكذلك :

$$r\,n = r\,\phi(m) = \phi(r\,m)$$

لذلك فإنَّ $rn,\ n_1-n_2 \in \text{Im}\,\phi$ وبالتالي فإنَّ $\text{Im}\,\phi$ حلقية جزئية من N.

لما كان إثبات النظرية الأساسية للتشاكل في الحلقيات هو في الأغلب نقل حرفي لإثبات النظرية الأساسية للتشاكل في الحلقات فإننا سنترك تفاصيل البرهان للقارىء ونكتفي بذكر نص النظرية .

نظرية (٢ - ١٣)

ليكن M,N حلقيّتين على الحلقة بمحايد R وليكن $\phi:M\to N$ هومومورفزما على الحلقة R من M إلى N ، عندئذ فإنَّ :

$$M/\text{Ker}\,\phi \cong_R \text{Im}\,\phi$$

تعريـف (٢ - ١١)

إذا كانت M حلقية على الحلقة R فإنَّ الإندومورفزمات للحلقية M على R هي الهوموموفزمات على R من M إلى M ، والتي سيرمز لها بالرمز $\text{Hom}_R(M,M)$ أو الرمز $\text{End}_R M$. إذا كانت R حلقة بمحايد فإن $\text{Hom}_R(M,M)$ حلقة بمحايد (انظر التمرين ٢ - ٢ - ٢).

ليكن V فضاء متّجهًا ذي بعد n على حقل F ، ولتكن $v_1,v_2,v_3,\ldots,v_n$ أساسًا (basis) لـ V على F. لقد سبق أن لاحظ القارىء في الجبر الخطي أن التطبيق φ المعرف بالقاعدة :

$$\varphi(\phi) = [a_{ji}]$$

يمثـل تشـاكلاً من $\text{Hom}_F(V,V)$ إلى $M_n(F)$ حيث $\varphi(v_i)=\sum_{j=1}^{n} a_{ij}v_j$ لكل $i=1,2,\ldots,n$. يمكن بسهولة أن نثبت أن زمرة الوحدات للحلقة $\text{Hom}_F(V,V)$ هي زمرة التشاكلات الذاتية $\text{Aut}_F V$ للفضاء المتّجه V على F. تسمى هذه الزمرة بالزمرة الخطيّة العامة من الـدرجة n على الحقل F ويرمز لها بالرمز $GL_n(F)$ أو الرمز $GL_F(V)$ وهي نفسها زمرة الوحدات للحلقة $M_n(F)$ ، وكمثال على ذلك انظر التمرين (١ - ١ - ٩).

إنَّ موضوع الزمر الخطيّة يعتبر من الموضوعات المهمة في الجبر وله استخدامات مهمة في الزمر المنتهية والهندسة الجبريّة (Algebraic Geometry) وفي موضوعات رياضيّة أخرى.

تـمـاريـن (٢ - ٢)

١) لتكن M حلقية على حلقة إبدالية بمحايد R ، وليكن r عنصرًا معيّنًا من R. أثبت أنَّ التـطبيق φ من M إلى M المعـرف بالقـاعدة : $\varphi(m)=r\,m$ لكل $m\in M$ يمثل أندومورفزمًا على R من M ، أوجد نواته وصورته.

٢) لتكن M حلقية على الحلقة بمحايد R. عرف الجمع والضرب على $Hom_R(M,M)$ كما يلي:

$$(\eta_1 + \eta_2)(m) = \eta_1(m) + \eta_2(m)$$

$$\eta_1 \eta_2 (m) = \eta_1(\eta_2(m))$$

لكل $\eta_1, \eta_2 \in Hom_R(M,M)$. أثبت أنَّ $Hom_R(M,M)$ تشكِّل حلقة بمحايد [استخدم تمرين (١ - ١ - ٤)].

٣) تسمى الحلقية بسيطة (simple module) إذا لم يوجد فيها حلقية جزئية فعليّة سوى الحلقيّة الصفريّة. إذا كانت M حلقية بسيطة فأثبت أنَّ $End_R M$ حلقة قاسميّة.

٤) أثبت أنَّ $2\mathbf{Z}$ حلقية جزئية على $\mathbf{Z}$ من $\mathbf{Z}$ وأثبت أنَّها تشاكل $\mathbf{Z}$ كحلقيات على $\mathbf{Z}$.

٥) إذا كانت R حلقة تامة، a عنصر غير صفري في R فأثبت أنَّ $R \cong_R Ra$، أي أن R تشاكل Ra كحلقيات على R. أثبت أنَّ $R \cong Ra$ كحلقات إذا وإذا فقط كان a عنصر وحدة في R.

٦) لتكن M حلقية على الحلقة بمحايد R. أثبت أنَّه يمكن اعتبار M حلقية على الحلقة $End_R M$. إذا كانت R إبدالية فأثبت أن كلَّ عنصر منها يُعَيِّن أحد الأندومورفزمات على R للحلقية M.

٧) لتكن M حلقية على الحلقة بمحايد R ولتكن K,L حلقيّتين جزئيّتين من M على R. أثبت أنَّ:

(أ) $K \cap L$ حلقية جزئية على R من M.

(ب) $K+L=\{a+b : a \in K, b \in L\}$ حلقيّة جزئيّة على R من M حيث يعرّف $r(a+b)=ra+rb$ لكل $a+b \in K+L$ ولكل $r \in R$.

(ج) $K+L/K \cong_R L/(L \cap K)$

٨) لتكن M حلقيّة على الحلقة بمحايد R ولتكن K,L حلقتين جزئيّتين من M على R. بافتراض أنَّ $L \supset K$ ، أثبت أنَّ :

$$(M/K) / (L/K) \cong_R M/L$$

٩) لتكن R حلقة بمحايد، M حلقية على R. ولتكن $M_1,M_2,\ldots,M_n$ حلقيات جزئية على R من الحلقية M ، يعرف المجموع المباشر الداخلي للحلقيات $M_1,M_2,\ldots,M_n$ بالطريقة نفسها التي عُرِّف بها في الحلقات. أثبت أنَّ M تكون المجموع المباشر الداخلي للحلقيات الجزئية $M_1,M_2,\ldots,M_n$ إذا وإذا فقط كان كل عنصر $m \in M$ يعبر عنه بطريقة وحيدة على الصيغة التالية :

$$m = \sum_{i=1}^{n} m_i$$

حيث $m_i \in M_i$.

الفصل الثالث

الحلقات الإقليدية وحلقة كثيرات الحدود

مقدمـــة

سنلاحظ في هذا الفصل أن الخصائص الجبرية لحلقة الأعداد الصحيحة والتي سبق أن تعرَّف عليها القارىء في الفصل الأول يمكن أن تعمم على فصل من الحلقات يضم بالإضافة إلى Z حلقات أخرى. يسمى هذا الفصل من الحلقات بالحلقات الإقليدية.

لقد سبق أن تعرَّف القارىء في دراسته قبل الجامعية على كثيرات حدود معاملاتها من إحدى النظم العددية المعروفة. سيتمُّ في هذا الفصل بناء حلقة كثيرات الحدود على حلقة إبدالية بمحايد ولذلك سندرس كثيرات الحدود على أساس أنها عناصر من حلقة تهمنا خصائصها الجبريّة. سنلاحظ أنّ حلقة كثيرات الحدود التي معاملاتها من حقل، لكونها حلقة إقليدية، فإن لها خصائص مطابقة لخصائص الحلقة Z ، سيكون لتلك الحلقة دور أساسي في مناقشاتنا للحقول وامتداد الحقول في الفصل القادم. وفي الختام نودُّ أن نشير إلى أن دراسة حلقة كثيرات الحدود ومثالياتها ستوفر مصدرا لأمثلة كثيرة عن الحلقات والحقول وامتداد الحقول.

الحلقات الإقليديـــة

تعريـــف (٣ ـ ١)

نقول عن الحلقة التامة R إنَّها حلقة إقليدية (Educlidean ring) إذ وجد لكل عنصر غير صفري a في R عدد صحيح غير سالب d (a) بحيث إنَّ :

(١) لكل $a,b\in R^*$ ، فإن $d(a) \leqslant d(ab)$.

(٢) لكل $a,b\in R^*$ فإنه توجد $q,r\in R$ بحيث إنّ :

$a=qb+r$ حيث $r=0$ أو $d(r) < d(b)$.

يسمى d تقويم إقليدس (Euclid evaluation) ويسمى الشرط الثاني خوارزمية إقليدس (Euclid algorithm).

لاحظ أننا لم نعطِ قيمة لـ $d(0)$.

مثـــال (٣ - ١)

ليكن F حقلا، لِنُعرِّف: $d(a)=1$ لكل $a\in F^*$. بالتالي لكل $a,b\in F^*$ فإن $d(a)\leqslant d(ab)$ وكذلك $a=(ab^{-1})b+0$. لذلك فإن شروط الحلقة الإقليدية محققة.

مثـــال (٣ - ٢)

لتكن $d(a)$ القيمة المطلقة للعدد الصحيح a ، من الواضح أنَّ Z تُشَكِّل حلقة إقليدية.

نظرية (٣ - ١)

الحلقة الإقليدية حلقة تامة رئيسة.

البرهـــان

ليكن I مثاليا للحلقة الإقليدية R. إذا كان $I=\{0\}$ فإنَّ I مثالي رئيس. لذلك نفرض أنّ $I\neq\{0\}$ ولنختر العنصر a في I بحيث إنّ $d(a)$ لها أقل قيمة. ليكن b عنصرًا غير صفـري من I. حسب خوارزمية إقليدس فإنَّه يوجد $q,r\in R$ بحيث إنّ $b=qa+r$ حيث $r=0$ أو $d(r)<d(a)$. نلاحظ أنّ $r=b-qa$ وبالتالي $r\in I$. إذا كان r لا يساوي الصفر فإنَّ ذلك يناقض طريقة اختيار العنصر a في I لكون $d(r)<d(a)$ ، لذلك فإن $r=0$ وهذا يؤدي إلى أن $b\in(a)$ ، إذن $I\supset(a)$ وبالتالي فإن $I=(a)$.

مبرهنـة (٣ - ٢)

إذا كانت R حلقة إقليدية، فإن u عنصر وحدة في R إذا وإذا فقط $d(u)=d(e)$ حيث e هو العنصر المحايد للحلقة R.

البرهـان

إذا كانت u عنصر وحدة في R فإن :

$$d(u) = d(ue) \geq d(e) = d(uu^{-1}) \geq d(u)$$

إذن $d(u)=d(e)$.

ليكن $d(u)=d(e)$ ، باستخدام خوارزمية إقليدس فإنَّه يوجد $r,q\in R$ بحيث إنّ $e=qu+r$ حيث $r=0$ أو $d(r)<d(u)$. لما كان d(e) هو أصغر تقويم لعناصر R لأنه لكل $r\in R$ فإن : $d(r)=d(re)\geq d(e)$ ، ولأن $d(u)=d(e)$ فإن $r=0$ لذلـك فإن : $e=qu$ ، وبالتالي فإن u عنصر وحدة في R.

تعريـف (٣ - ٢)

لتكن R حلقة إبداليّة وليكن $a,b\in R$ بحيث إنّ $a\neq 0$. نقول إنّ a تقسم b ، ويرمز لذلك بالرمز $a|b$ ، إذا وجد عنصر c في R بحيث إن $b=ac$ وإلا يقال : إنّ a لا تقسم b.

ملاحظـة (٣ - ١)

يستطيع القارىء أن يتأكد مباشرةً مما يلي :

(١) إذا كان $a|b$ ، $b|c$ فإن $a|c$.

(٢) إذا كان $a|b$ ، $a|c$ فإن $a|b\pm c$.

(٣) إذا كان $a|b$ ، فإن $a|bx$ لكل $x\in R$.

(٤) إذا كان $a|b$ وكان $b|a$ فإن $(b)=(a)$.

تعريـف (٣ - ٣)

لتكن R حلقـة إبـداليّة وليكن $a,b\in R$ ، عندئذ نسمي $d\in R$ القاسم المشترك الأعظم (greatest common divisor) للعنصرين a,b إذا حقق الشرطين التاليين :

(١) $d|a$ ، $d|b$.

(٢) إذا كان $c\in R$ بحيث إنّ $c|a$ ، $c|b$ فإن $c|d$.

وسيرمز للقاسم المشترك الأعظم للعنصرين a,b بالرمز (a,b).

تعريـف (٣ - ٤)

لتكن R حلقة إبداليّة وليكن $a,b\in R$ ، عندئذ نسمي $m\in R$ المضاعف المشترك البسيط (least common multiple) للعنصرين a,b ، إذا حقق الشرطين التاليين:

(١) $a|m$ ، $b|m$

(٢) إذا كان $n\in R$ بحيث إنّ $a|n$ ، $b|n$ فإن $m|n$.

وسيرمز للمضاعف المشترك البسيط للعنصرين a,b بالرمز $l.c.m.(a,b)$

مبرهنـة (٣ - ٣)

لتكن R حلقة إقليدية، عندئذ فإن أي عنصرين $a,b\in R^*$ لهما قاسم مشترك أعظم ولهما مضاعف مشترك بسيط، كما أنّ:

$$(a) + (b) = (d) \quad , \quad (a) \cap (b) = (m)$$

حيث $d = (a,b)$ ، $m=l.c.m.(a,b)$.

البرهـان

حيث إنّ R حلقة تامة رئيسة فإنه يوجد $m,d\in R$ بحيث إنّ $(a)\cap(b)=(m),(a)+(b)=(d)$. نودُّ أن نبرهن أنّ $d=(a,b)$ ، لما كان $a,b\in(d)$ فإن $d|a$ ، $d|b$. ليكن $c\in R$ بحيث إن $c|a$ ، $c|b$. هذا يعني أن $a\in(c)$ ، $b\in(c)$ وبالتالي فإن $(a)+(b)=(d)\supset(c)$ وهكذا فإن $d\in(c)$. أي أن $c|d$ ومنه $d=(a,b)$.

الآن نود أن نبرهن أن $m=l.c.m.(a,b)$. لما كان $m\in(a)\cap(b)$ فإن $m\in(a)$ ، $m\in(b)$ وهذا يعني أن $a|m$ وكذلك $b|m$. ليكن $n\in R$ بحيث إن $a|n$ ، $b|n$ ، ولكن ذلك يعني أن $n\in(a)$ ، $n\in(b)$. إذن $n\in(a)\cap(b)$ وبالتالي $n\in(m)$ ، لذلك فإن $m|n$. وهكذا فإن $m=l.c.m.(a,b)$.

مبرهنة (٣ - ٤)

لتكن R حلقة إقليدية وليكن $a,b\in R^*$. إذا لم يكن b عنصر وحدة في R فإن $d(a)<d(ab)$.

البرهان

ليكن $I=(a)$ مثاليا للحلقة R. من الشرط الأول في تعريف الحلقة الإقليدية نستنتج أن $d(a)\leqslant d(ab)$. إذا كان $b\in R^*$ بحيث إن $d(a)=d(ab)$ ، فإنه بتطبيق خوارزمية إقليدس نحصل على $a=abq+r$ حيث $q,r\in R$ وبحيث إنه إما $d(r)<d(ab)$ أو $r=0$. لما كان $r=a-abq$ فإن $r\in(a)$ وبالتالي $d(r)\geqslant d(a)$ ولكن $d(r)<d(ab)=d(a)$ ، إذن $r=0$. لذلك فإن $a=abq$. باستخدام قانون الاختصار للضرب في الحلقة التامة R نحصل على $bq=1$ ، وهذا يتناقض مع الفرض. إذن $d(a)<d(ab)$.

تعريف (٣ - ٥)

لتكن R حلقة إبدالية بمحايد. نقول إن العنصرين $a,b\in R$ مترافقان (associates) إذا وجد عنصر وحدة u في R بحيث إن $a=bu$ أو نقول إنّ العنصر a مرافق (associate) للعنصر b.

مثال (٣ - ٣)

لقد سبق أن لاحظنا أن زمرة الوحدات لحلقة الأعداد الصحيحة هي $\{-1,1\}$ وبالتالي فإن لأي عدد n في $\mathbf{Z}$ مرافقين n و $-n$.

مثال (٣ - ٤)

حيث إن زمرة الوحدات للحلقة $\mathbf{Z}_8$ هي $\{1,3,5,7\}$ فإن مرافقي 2 في الحلقة $\mathbf{Z}_8$ هما 2,6 بينما مرافقات 3 في الحلقة $\mathbf{Z}_8$ هي 1,3,5,7.

تعريف (٣ - ٦)

إذا كانت R حلقة إقليدية وليكن $\pi\in R$. نقول إن π عنصر أولي (prime element)

في الحلقة R إذا كان π لا يمثّل عنصر وحدة في R ، وفي كل تحليل $\pi=ab$ حيث $a,b\in R$ فإنه إما a أو b عنصر وحدة في R.

مثـال (٣ - ٥)

العدد الأولي في حلقة الأعداد الصحيحة يمثّل عنصرًا أوليًا فيها.

نظرية (٣ - ٥)

إذا كانت R حلقة إقليدية وليكن $a\in R$ فإنّ :

(١) (a) مثالي أولي للحلقة R إذا وإذا فقط كان $a=0$ أو a عنصر أولي في الحلقة R.

(٢) (a) مثالي أعظمي غير تافه للحلقة R إذا وإذا فقط كان a عنصر أولي في الحلقة R.

البرهـان

(١) ليكن (a) مثاليا أوليا للحلقة R ولنفرض أن a عنصر غير صفري في الحلقة R بحيث إنّ $a=bc$ ، $b,c\in R$ إذن $bc\in(a)$ ، ولكن (a) مثالي أولي، إذن إما $b\in(a)$ أو $c\in(a)$. إذا كان $b\in(a)$ فإن $b=ad$ حيث $d\in R$ وبـالتالي فإن $a=adc$ وبتطبيق قانـون الاختصار للضرب نحصل على $dc=1$ لذلك فإن c عنصر وحدة في R. وبالمثل، إذا كان $c\in(a)$ فإن b لابد أن يكون عنصر وحدة في R. لذلك فإن a عنصر أولي في الحلقة R.

إذا كان $a=0$ فإن $(a)=(0)$ والمثالي الصفري لحلقة تامة مثالي أولي، لذلك نفرض أن a عنصر أولي في الحلقة R ونفرض أن $(a)\subset(b)$ حيث $b\in R$ ، لذلك فإن $a=bc$ حيث $c\in R$. ولكن a عنصر أولي، إذن إما b عنصر وحدة أو c عنصر وحدة. إذا كان c عنصر وحدة فإن $ac^{-1}=b$ وبالتالي فإن $b\in(a)$ وهذا يؤدي إلى أن $(a)=(b)$. إذا كان b عنصر وحدة فإن $(b)=R$ لذلك فإن (a) مثالي أعظمي للحلقة R ، ولكن المثالي الأعظمي لحلقة إبدالية بمحايد هو مثالي أولي لذلك فإن (a) مثالي أولي للحلقة R.

(٢) لقد أثبتنا في الفقرة السابقة أنه إذا كان a عنصرا أوليا في الحلقة R فإن (a) مثالي أعظمي للحلقة R. لنفرض الآن أن (a) مثالي أعظمي حيث $a\in R$. لذلك فإن (a) مثالي أولي وباستخدام الفقرة (١) نستنتج أن $a=0$ أو a عنصر أولي، ولكن (a) مثالي غير تافه، لذلك فإن $a\neq 0$ وبالتالي فإن a عنصر أولي.

نتيجـة (١)

لتكن R حلقة إقليدية وليكن $a,b,c\in R$ بحيث إنّ a عنصر أولي، عندئذ فإن $a|bc$ يؤدي إلى أن $a|b$ أو $a|c$.

البرهـان

إذا كان $a|bc$ فهذا يعني أن $bc\in(a)$ ولكن (a) مثالي أولي حسب المبرهنة السابقة لأن a عنصر أولي. إذن إما $b\in(a)$ أو $c\in(a)$ وهذا يؤدي إلى أن $a|b$ أو $a|c$.

نتيجـة (٢)

لتكن R حلقة إقليدية وليكن $a,a_1,a_2,\ldots,a_n\in R$ بحيث إنّ a عنصر أولي، عندئذ فإن:

$$a \mid a_1 a_2 \ldots a_n$$

يؤدي إلى أنّ a تقسم أحد العناصر a_i حيث $1\leqslant i\leqslant n$.

البرهـان

سنثبت النتيجة باستخدام طريقة الاستقراء الرياضي (mathematical induction) على n. إذا كان $n=2$ فإن $a|a_1$ أو $a|a_2$ حسب النتيجة السابقة.

لنفرض الآن أن النتيجة صحيحة لـ $n-1$ من العناصر وليكن $b=a_1a_2\ldots a_{n-1}$، لما كان $a|ba_n$ فإن $a|b$ أو $a|a_n$. إذا كانت $a|b$ فإن ذلك يؤدي حسب فرضية الاستقراء الرياضي إلى أن $a|a_i$ حيث $1\leqslant i\leqslant n-1$. لذلك فإن $a|a_i$ حيث $1\leqslant i\leqslant n$.

نظرية التحليل الوحيد
Unique Factorization Theorem

النظرية

إذا كان R حلقة إقليدية، فإن :

(١) كل عنصر غير صفري في R هو إمّا عنصر وحدة أو حاصل ضرب عدد نهائي من العناصر الأولية من عناصر الحلقة R .

(٢) إذا كان a عنصرًا غير صفـري ولم يكن عنصر وحدة في R فإن تحليله كحاصل ضرب عدد نهائي من العناصر الأولية من عناصر الحلقة R يكون وحيدًا حسب المفهوم التالي :

إذا كان :

$$a = \pi_1 \pi_2 \dots \pi_n = \pi_1' \dots \pi_m$$

حيث π_i ، π_i' عناصر أولية من عناصر الحلقة فإن $n=m$ وكل π_i مرافق للعنصر π_i' (مع إمكانيّة إعادة الترتيب) لكل $i=1,\dots,n$.

البرهـــان

(١) إثبات وجود التحليل (existence)

لتكن S مجموعة كل العناصر غير الصفريّة التي ليست عناصر وحدة في R والتي لا تحقق شرط النظرية (١). إذا كان S خالية فهذا يعني أنّ الشرط (١) من النظرية صحـيح . لذلـك نفـرض أنّ S مجمـوعـة غير خالـية وأنّ a في S بحـيث إن d(a) هي أصـغـر قيمـة أي أن $d(x) \geq d(a)$ لكـل $x \in S$. بما أنّ $a \in S$ فهـذا يعني أنّ a عنصر غير أولي وبالتالي فإن $a=bc$ بحيث إن c,b لا يمثلان عناصر وحدة في R. حسب المبرهنة (٣ ـ ٤) فإن $d(b)<d(bc)=d(a)$ وكذلك $d(c)<d(a)$ لذلك فإن $b,c \notin S$ وبالتالي فإنّه يمكن كتابة كل منهما كحاصل ضرب عدد نهائي من عناصر الحلقة R الأولية، أي أنّ :

$$b = \pi_1 \pi_2 \dots \pi_s \quad , \quad c = \pi_1' \pi_2' \dots \pi_r$$

حيث إن π_i ، π'_i عناصر أولية من عناصر الحلقة R. لذلك فإن

$$a = bc = \pi_1 \pi_2 \dots \pi_s \pi'_1 \pi'_2 \dots \pi'_r$$

أي أن a هي حاصل ضرب عدد نهائي من العناصر الأولية للحلقة R وهذا يناقض اختيار a ، لذلك فإن S مجموعة خالية .

(٢) برهان وحدانيّة التحليل (uniqueness)

ليكن a عنصرا غير صفري وليس عنصر وحدة في R ونفرض أن

$$a = \pi_1 \pi_2 \dots \pi_n = \pi'_1 \pi'_2 \dots \pi'_m$$

حيث π_i, π'_i عناصر أولية في الحلقة R.

نفرض أنّ $n \leqslant m$ ونستخدم طريقة الاستقراء الرياضي على n في إثبات وحدانيّة التحليل للعنصر a حسب المفهوم الموضّح في منطوق النظرية . إذا كانت $n=1$ فإن :

$$a = \pi_1 = \pi'_1 \pi'_2 \dots \pi'_m$$

لكون π_1 عنصر أولي فإنّنا نستنتج أنّه لقيمة واحدة لـ i فإن π'_i عنصر أولي وأنّ :

$$\pi'_1 \pi'_2 \dots \pi'_{i-1} \pi'_{i+1} \dots \pi'_m$$

عنصر وحدة في R وبالتالي فإن وحدانيّة التحليل صحيحة إذا كانت $n=1$. نفرض أنّ وحدانيّة التحليل صحيحة على عناصر الحلقة التي يكون تحليلها هو حاصل ضرب $n-1$ من العناصر الأوليّة للحلقة . لمّا كانت :

$$a = \pi_1 \dots \pi_n = \pi'_1 \dots \pi'_m$$

فإن $\pi_i | \pi'_1 \dots \pi'_m$ وحسب النتيجة (٢) للمبرهنة (٣ ـ ٥) فإن $\pi_i | \pi'_i$ (قد يكون ذلك مع إمكانيّة إعادة ترتيب) ومنه نستنتج أنّ $\pi'_i = \lambda_i \pi_i$ حيث $\lambda_i \in R$. بما أنّ π_i, π'_i عناصر أولية في R فإن λ_i يجب أن تكون عنصر وحدة في R لذلك فإن π_i مرافق للعنصر π'_i.

الآن نعوض عن قيمة π'_i:

$$a = \pi_1 \pi_2 \dots \pi_n = \pi'_1 \pi'_2 \dots \pi'_{i-1} \lambda_i \pi_i \pi'_{i+1} \dots \pi'_m$$

وحيث إن R إبدالية وحلقة تامة فإننا نختصر π_i من طرفي المعادلة لنحصل على المساواة :

$$\pi_1 \pi_2 \dots \pi_{i-1} \pi_{i+1} \dots \pi_n = \lambda_i \pi'_1 \dots \pi'_{i-1} \pi'_{i+1} \dots \pi'_m$$

ولكن وحدانيّة التحليل تتحقق على $n-1$ من العوامل لذلك فإن $n-1 = m-1$ وبالتالي فإن $n=m$ وكذلك فإن :

$\pi_j'=\lambda_j\pi_j$ لكل $j=1, \ldots, i-1, i+1, \ldots, n$

حيث λ_j عنصر وحدة لكل قيم j أي أن π_j', π_j مترافقان لكل قيم j.

تمـاريـــن (٣ - ١)

١) لتكن R حلقة إقليدية، $a,b,d',m' \in R$ وليكن $d=(a,b)$ ، $m=l.c.m.(a,b)$ أثبت أنّ:

(ا) $d'=(a,b)$ إذا وإذا فقط كان d,d' مترافقين.

(ب) $m'=l.c.m.(a,b)$ إذا وإذا فقط كان m,m' مترافقين.

٢) (ا) أثبت أنّ $\mathbb{Z}[\sqrt{-5}]$ حلقة جزئية من $\mathbb{C}$ حيث: $\sqrt{-5}$

$$\mathbb{Z}[\sqrt{-5}] = \{ a+b\sqrt{-5} : a,b \in \mathbb{Z} \}$$

(ب) أثبت أن نظرية التحليل الوحيد غير صحيحة في $\mathbb{Z}[\sqrt{-5}]$ (إرشاد: اعتبر $6=2\times3=(1+\sqrt{-5})(1-\sqrt{-5})$).

٣) (ا) أثبت أن $\mathbb{Z}[i]$ حلقة جزئية من $\mathbb{C}$ حيث:

$$\mathbb{Z}[i] = \{a + bi : a,b \in \mathbb{Z} \}$$

(ب) أثبت أنّـه إذا كانت $d(a+bi)=a^2+b^2$ فإن $\mathbb{Z}[i]$ تشكّـل حلقـة إقليدية.

تسمى الحلقة $\mathbb{Z}[i]$ حلقة أعداد جاوس (ring of Gaussian integers).

٤) أوجد زمرة الوحدات للحلقة $\mathbb{Z}[i]$.

٥) إذا كان $a+bi$ ليس عنصر وحدة في $\mathbb{Z}[i]$ فأثبت أنّ $a^2+b^2>1$.

٦) أوجد القاسم المشترك الأعظم في $\mathbb{Z}[i]$ للعددين $4-3i$ ، $3+4i$ وكذلك المضاعف المشترك البسيط لهما.

٧) ليكن p عددًا أوليا . افرض أنّه يوجد عدد صحيح c أولي بالنسبة للعدد p بحيث إنه يمكن إيجاد عددين صحيحين x,y يحققان المتساوية $x^2+y^2=cp$. أثبت أنه يوجد عددان صحيحان a,b بحيث إن $p=a^2+b^2$ (إرشاد : افرض أن p عدد أولي في Z[i] واستخدم كون Z [i] حلقة إقليدية لتصل إلى أنّ p عدد غير أولي في Z[i]).

٨) إذا كان p عددًا أوليا من الصيغة 4n+1 فأثبت أنه يمكن حل المتطابقة $x^2\equiv -1 \bmod p$ ، حيث n عدد صحيح ، باستخدام المتطابقة $(p-1)!\equiv -1 \bmod p$.

٩) إذا كان p عددًا أوليا من الصيغة 4n+1 فإن $p=a^2+b^2$ ، حيث a,b,n أعداد صحيحة . تسمى هذه النظرية بنظرية فيرما (Fermat's theorem) .

حلقة كثيرات الحدود

بناء حلقة كثيرات الحدود

لتكن R حلقة إبدالية بمحايد ولتكن S مجموعة كل المتتابعات غير المنتهية من الشكل : $f=(a_0,a_1,a_2,\ldots)$ لعناصر R التي يكون عددا منتهيا فقط من حدودها لا يساوي صفرا . أي أن $(a_0,a_1,a_2,\ldots)\in S$ إذا وإذا فقط وجد عدد صحيح غير سالب N بحيث إن $a_n=0$ لكل $n\geq N$ ولذلك فإن :

$$S=\{(a_0,a_1,\ldots,a_n,0,0,\ldots) : a_i\in R, n\geq 0\}$$

لاحظ أنه إذا كانت $f,g\in S$ وكانت :

$$f=(a_0,a_1,a_2,\ldots) \quad , \quad g=(b_0,b_1,b_2,\ldots)$$

فإن $f=g$ إذا وإذا فقط كانت حدودها المتقابلة متساوية . أي أن $f=g$ إذا وإذا فقط كانت $a_i=b_i$ لكل $i\geq 0$.

لتكن :

$$f=(a_0,a_1,a_2,\ldots) \quad , \quad g=(b_0,b_1,b_2,\ldots)\in S$$

لنعرّف عمليتي الجمع والضرب على S كما يلي :

$$f+g=(a_0+b_0,a_1+b_1,a_2+b_2,\ldots)$$

$$f.g=(c_0,c_1,c_2,\ldots)$$

حيث

$$c_k = \sum_{i+j=k} a_i b_j$$

ولما كان إثبات S حلقة إبدالية محايدها $(1,0,0,\ldots)$ وصفرها $(0,0,\ldots)$ يتطلب حسابات رتيبة تعتمد على الصفات المقابلة للحلقة R فقد تمّ حذفها. سنثبت أنّ R مغمورة في S. لتكن

$$R' = \{(r,0,0,\ldots) : r \in R\}$$

من الواضح أنّه إذا كانت:

$$f = (r,0,0,\ldots) \quad , \quad g = (s,0,0,\ldots)$$

فإن:

$$f - g = (r-s,0,0,\ldots) \quad , \quad fg = (rs,0,0,\ldots)$$

لذلك فإنّ R' حلقة جزئية من S. لنعرّف التطبيق φ من R إلى R' المعرف بالقاعدة:

$$\varphi(r) = (r,0,0,\ldots)$$

نلاحظ أنّ:

$$\begin{aligned}\varphi(r+s) &= (r+s,0,0,\ldots)\\ &= (r,0,0,\ldots) + (s,0,0,\ldots)\\ &= \varphi(r) + \varphi(s)\end{aligned}$$

$$\begin{aligned}\varphi(rs) &= (rs,0,0,\ldots)\\ &= (r,0,0,\ldots)\,(s,0,0,\ldots)\\ &= \varphi(r)\,\varphi(s)\end{aligned}$$

لذلك فإن φ هوموومورفزم من R إلى R'. نفرض أن $r \in R$ بحيث إن:

$$\varphi(r) = (0,0,0,\ldots)$$

لكن $\varphi(r) = (r,0,0,\ldots)$

نستنتج من ذلك أن $r=0$ وبالتالي فإن φ أحادي.

ليكن $(r,0,0,\ldots) \in R'$ ، وبالتالي فإن:

$$\varphi(r) = (r,0,0,\ldots)$$

لذلك فإنّ φ غامر وهكذا فإن $R \cong R'$ وبالتالي R مغمورة في S. سنطبق كل عنصر r في R مع صورته $\varphi(r)$ في R' وبهذه الطريقة نستطيع أن نعتبر أنّ R حلقة جزئية من S. لتكن:

$$x = (0,1,0,0,\ldots)$$

سنستخدم طريقة الاستقراء الرياضي على n في البرهنة على أنّه إذا كانت $n \geq 0$ فإن $x^n=(0,0,\ldots,0,1,0,\ldots)$ أي أن الحد الذي ترتيبه n في المتتابعة x^n هو الواحد وكل حدود المتتابعة الأخرى تساوي صفرًا. إذا كانت $n=1$ فإن الفرضية صحيحة من تعريف x. نفرض أن الفرضية صحيحة لكل $n \geq 1$ ونبرهن أنّها صحيحة لـ $n+1$. بما أنّ: $x^{n+1}=x^n x$ ، لذلك نفرض:

$$x^n = (a_0, a_1, a_2, \ldots) \quad , \quad x = (b_0, b_1, b_2, \ldots)$$

من تعريف عملية الضرب في الحلقة S نلاحظ أنه إذا كانت $i \neq n+1$ فإن $a_h b_k = 0$ لكل $h+k=i$. لأنه في هذه الحالة إما $a_h=0$ أو $b_k=0$. لذلك فإن الحد:

$$c_i = \sum_{h+k=i} a_h b_k = 0$$

لكل $i \neq n+1$. ومن ناحية أخرى نلاحظ أنّ:

$$c_{n+1} = \sum_{h+k=n+1} a_h b_k = a_n b_1 = 1$$

حيث إن الحدود الأخرى $a_h b_k=0$ لأنّه إمّا $h \neq n$ أو $k \neq 1$ وبالتالي فإنّه إمّا $a_h=0$ أو $b_k=0$. وهكذا فإن:

$$x^{n+1} = (0,0,\ldots,0,1,0,\ldots)$$

حيث إن الحد الذي ترتيبه $n+1$ في المتتابعة x^{n+1} هو الواحد وكل حدود المتتابعة الأخرى تساوي صفرًا.

لنفرض أنّ:

$$f = (a_0, a_1, \ldots, a_n, 0,0,\ldots) \in S$$

فإن :

$$\begin{aligned}
f &= (a_0,a_1,\ldots,a_n,0,0,\ldots)\\
&= (a_0,0,0,\ldots)+(0,a_1,0,\ldots)+(0,0,a_2,0,\ldots)+\ldots+(0,0,\ldots,a_n,0,\ldots)\\
&= (a_0,0,0,\ldots)(1,0,0,\ldots)+(a_1,0,0,\ldots)(0,1,0,\ldots)+(a_2,0,0,\ldots)(0,0,1,0,\ldots)\\
&\quad +\ldots+(a_n,0,0,\ldots)(0,0,\ldots,1,0,\ldots)\\
&= a_0+a_1x+a_2x^2+\ldots+a_nx^n\\
&= \sum_{i=0}^{n} a_i x^i
\end{aligned}$$

لذلك فإن أي عنصر f في S نستطيع كتابته بالصيغة التالية :

$$f = \sum_{i=0}^{n} a_i x^i$$

حيث $a_0,a_1,a_2,\ldots,a_n \in R$. وبالتالي إذا كان :

$$f = \sum_{i=0}^{n} a_i x^i \quad , \quad g = \sum_{i=0}^{m} b_i x^i \in S$$

فمن تساوي متتابعتين في S نستنتج أن :

$$\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{m} b_i x^i$$

إذا وإذا فقط كانت $n=m$ وكان $a_i=b_i$ لكل $i=0,1,2,\ldots,n$ وبصفة خاصة

$$\sum_{i=0}^{n} a_i x^i = 0$$

تؤدي إلى أنّ $a_i=0$ لكل $i=0,1,2,\ldots,n$ ، لذلك فقد أثبتنا أن كل عنصر في S نستطيع كتابته بطريقة وحيدة على الصيغة : $\sum_{i=0}^{n} a_i x^i$ حيث $a_i \in R$.

باستخدام خواص الإبدال والدمج والتوزيع في الحلقة S نستنتج أن عمليتي الضرب والجمع الذي سبق أن عرفناهما على S سيكونان كما يلي :

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{m} (a_i + b_i) x^i$$

حيث فرضنا أنّ $m \geq n$ واعتبرنا $a_{n+1}=a_{n+2}=\ldots=a_m=0$

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{i=0}^{n+m} c_i x^i$$

حيث

$$c_i = \sum_{h+k=i} a_h b^k$$

وهذا هو جمع وضرب كثيرات الحدود التي سبق أن تعرض لها القارىء في دراسته قبل الجامعية.

تعريف (٣ - ٧)

لقد حصلنا على الحلقة S بربط العنصر غير المعيّن x (indeterminant) بالحلقة R كما أنّه تم التعبير عن كل عنصر في S ككثيرة حدود معاملاتها من R. لذلك تسمى الحلقة S بحلقة كثيرات الحدود (ring of polynomials) على الحلقة R بمتغيّر x ويرمز لها بالرمز $S=R[x]$.

تعريف (٣ - ٨)

لتكن

$$f = \sum_{i=0}^{n} a_i x^i \in R[x]$$

تسمى العناصر $a_0,a_1,\ldots,a_n$ معاملات (coefficients) كثيرة الحدود f ، a_0 يسمى الحد الثابت (constant term) ، a_n يسمى الدليل أو المعامل القائد (the leading coefficient) والعدد الصحيح n بدرجة (degree) كثيرة الحدود f ويرمز لذلك بالرمز deg f. إذا كان المعامل القائد لكثيرة الحدود يساوي الواحد فإنها تسمى كثيرة الحدود الواحدية (monic polynomial).

ملاحظة (٣ - ٢)

لاحظ أنّ درجة أيّة كثيرة حدود هي عدد صحيح غير سالب ولا توجد درجة لكثيرة الحدود الصفرية كما أن عناصر الحلقة R غير الصفرية هي كثيرات الحدود في R[x] التي درجتها تساوي صفرًا ولذلك تسمى كثيرات الحدود الثابتة (constant polynomials).

تعريـف (٣ - ٩)

لتكن R حلقة إبدالية بمحايد ولتكن $R[x_1]$ حلقة كثيرات الحدود على R بمتغير x_1. نستطيع أن نُكَوِّن حلقة كثيرات الحدود $(R[x_1])[x_2]$ على الحلقة $R[x_1]$ بمتغير x_2 ويرمز لهذه الحلقة $R[x_1,x_2]$ وتسمى حلقة كثيرات الحدود على R بمتغيرين x_1,x_2. وهكذا نستطيع أن نُعَرِّف حلقة كثيرات الحدود $R[x_1,x_2,\ldots,x_n]$ بالمتغيرات $x_1,x_2,\ldots,x_n$.

مبرهنـة (٣ - ٦)

لتكن R حلقة تامة ولتكن f,g عناصر غير صفرية في R[x] ، عندئذ فإنّ

$$\deg fg = \deg f + \deg g$$

البرهـان

لتكن

$$f = \sum_{i=0}^{n} a_i x^i \quad , \quad g = \sum_{i=0}^{m} b_i x^i$$

بحيث إن $a_n \neq 0$ ، $b_m \neq 0$ ، بالتالي فإنّ $\deg f=n$ ، $\deg g=m$.

من تعريف الضرب نلاحظ أنّ :

$$fg = \sum_{i=0}^{n+m} c_i x^i \qquad \text{حيث} \qquad c_i = \sum_{h+k=i} a_h b_k$$

لما كان $c_{n+m}=a_n b_m$ لا يساوي صفرًا لأنه حاصل ضرب عنصرين غير صفريّين في حلقة تامة لذلك فإن المعامل القائد لكثيرة الحدود fg هو c_{n+m} وبالتالي فإن $\deg fg=n+m$. أي أن :

$$\deg fg = \deg f + \deg g$$

مثـال (٣ - ٦)

لتكن

$$f = 1 + 3x \quad , \quad g = 1 + 2x^2 \in \mathbb{Z}_6[x]$$

نلاحظ أنّ

$$fg=(1+3x)(1+2x^2)=1+3x+2x^2+2.3x^3=1+3x+2x^2$$

لذلك فإن $\deg fg=2$ ، وهكذا فإنّ $\deg fg<\deg f+\deg g$ ولذلك فإنّ المبرهنة السابقة ليست صحيحة على حلقة كثيرات الحدود التي معاملاتها من حلقة يوجد بها قواسم للصفر.

نتيجـــة

إذا كانت R حلقة تامة فإن R[x] حلقة تامة .

البرهـــان

لتكن $f,g\in R[x]$ ولتكن معاملاتها ودرجاتها حسب ما هو موضح في إثبات المبرهنة السابقة، ولنفرض أنّ $fg=0$ وهذا يعني أنّ معاملات fg تساوي صفرًا وبشكل خاص فإنّ $c_{n+m}=0$. ولكن هذا يناقض أن $\deg fg=m+n$ ، إذن $fg\neq 0$ وبالتالي فإن R[x] حلقة تامة .

مبرهنـــة (٣ - ٧)

إذا كانت R' حلقة إبدالية بمحايد، وإذا كانت R حلقة جزئية من R' لها المحايد نفسه وكان $a\in R'$ فإنّه يوجد هوموم‌ورفزم من R[x] إلى R' صورته R[a].

البرهـــان

يستطيع القارىء بسهولة أن يتأكد من أن التطبيق المعرّف بالقاعدة $\varphi(f)=f(a)$ يشكِّل هوموم‌ورفزما من R[x] إلى R'. وحيث إن $\operatorname{Im}\varphi=\{f(a):f\in R[x]\}$ ، لذلك :

$$\operatorname{Im}\varphi=\left\{\sum_{i=0}^{n}a_i a^i : a_i\in R\ ,\ n\in\mathbb{N}\cup\{0\}\right\}$$

لذلك فإنّ $R[a]\supset\operatorname{Im}\varphi$ ومن ناحية أخرى $\operatorname{Im}\varphi$ تحوي R وكذلك $\operatorname{Im}\varphi$ تحوي a لأنّ $\varphi(x)=a$ ولكن R[a] هي أصغر حلقة تحوي R وتحوي a ، إذن $\operatorname{Im}\varphi\supset R[a]$ وبالتالي فإن $\operatorname{Im}\varphi=R[a]$.

تعريـــف (٣ - ١٠)

إذا كانت R حلقة إبدالية بمحايد وإذا كانت f كثيرة حدود غير ثابتة فى R[x] فإنّنا

نقول إنّ f قابلة للتحليل (reducible) على R إذا وجد $f_1,f_2\in R[x]$ بحيث إنّ $f=f_1f_2$ ، $\deg f_1$ ، $\deg f_2>0$ وإلا نقول إنّ f غير قابلة للتحليل (irreducible) على R. أي أنّه إذا كان $f=f_1f_2$ فإنـه إما $\deg f_1=0$ أو $\deg f_2=0$. سنلاحظ أنّ كثيرات الحدود غير القابلة للتحليل على حقل ستلعب الدور نفسه الذي تلعبه العناصر الأولية في الحلقة الإقليدية.

مثـال (٣ ـ ٧)

نلاحظ أنّ $x^2+1\in\mathbb{R}[x]$ غير قابلة للتحليل على حقل الأعداد الحقيقية بينما إذا اعتبرنا $x^2+1\in\mathbb{C}[x]$ فإنها قابلة للتحليل على حقل الأعداد المركبة حيث إن: $x^2+1=(x-i)(x+i)$ ، $\deg(x+i)>0$ ، $\deg(x-i)$. وهذا يوضّح أنّ صفة قابلية التحليل على حلقة أو عدمها لكثيرة حدود ليست صفة خاصة بكثيرة الحدود فقط ولكنها أيضًا تعتمد على الحلقة التي تنتمي لها معاملات كثيرة الحدود.

حلقة كثيرات الحدود على حقل

سنعتبر ابتداءً من الآن موضوع دراستنا هو حلقة كثيرات الحدود F[x] حيث F حقل. نلاحـظ أن F[x] حلقـة تامـة حسب نتيجـة المبرهنـة (٣ ـ ٦)، لذلك نستطيـع أن نعتـبر F[x] حلقـة جزئية من حقـل قواسمهـا الذي يسمى حقل الدوال النسبية (field of rational functions) في المتغير x ويرمز له بالرمز F(x).

نظرية خوارزمية القسمة Division algorithm theorem

إذا كانت f,g كثيرات حدود غير صفرية في الحلقة F[x] فإنّه توجد كثيرتي حدود وحيدتان $q,r\in F[x]$ بحيث إن:

$$f = g\,q + r$$

حيث $r = 0$ أو $\deg r < \deg g$.

البرهـان

إثبات الوجـود (existence)

إذا كانت $\deg f=n$ أصغر من $\deg g=m$ فإن النظرية صحيحة باعتبار $q=0$

r=f لذلك نفرض أن n≥m. سنبرهن النظرية باستخدام طريقة الاستقراء الرياضي على n. إذا كانت n=0 فإن m=0. لتكن g=μ,f=λ عندئذ فإن : f=(λμ⁻¹)g+0.

الآن نفرض أن النظرية صحيحة إذا كانت deg f أقل من أو تساوي n − 1 ونودُّ أن نبرهن أنها صحيحة لـ n. لتكن :

$$f = \sum_{i=0}^{n} a_i x^i \quad , \quad g = \sum_{i=0}^{m} b_i x^i$$

حيث $n \geq m,\ b_m \neq 0,\ a_n \neq 0$ ، ضع :

$$f_1 = f - a_n b_m^{-1} x^{n-m} g$$

لذلك فإنّ $\deg f_1 \leq n-1$ ، ولكن النظرية صحيحة على n−1 ، وهكذا فإنّه توجد $q_1, r \in F[x]$ بحيث إن $f_1 = gq_1 + r$ حيث r=0 أو deg r<deg g.

$$f - a_n b_m^{-1} x^{n-m} g = gq_1 + r$$

ضع $q = q_1 + a_n b_m^{-1} x^{n-m}$ فإننا نحصل على f=gq+r حيث $q, r \in F[x]$ ، r=0 أو deg r<deg g.

إثبات الوحدانية *(uniqueness)*

لتكن $f = gq_1 + r_1 = gq_2 + r_2$ حيث $q_1, q_2, r_1, r_2 \in F[x]$ ، $r_1 = 0$ أو $\deg r_1 < \deg g$ ، $r_2 = 0$ أو $\deg r_2 < \deg g$.

نودُّ أن نبرهن أن $q_1 = q_2$ ، $r_1 = r_2$. لمّا كان $gq_1 + r_1 = gq_2 + r_2$ فإن $g(q_1 - q_2) = r_2 - r_1$ وبالتالي فإن :

$$\deg g + \deg (q_1 - q_2) = \deg (r_2 - r_1)$$

ومن ذلك نستنتج أن $\deg (r_2 - r_1) \geq \deg g$ ولكن $\deg r_2$ ، $\deg r_1$ وهذا تناقض، لذلك فإن $r_1 = r_2$ وبالتالي $q_1 = q_2$.

مبرهنـــة (٣ ـ ٨)

زمرة الوحدات للحلقة F[x] هي F^*.

البرهـــان

نفرض أنّ $f\in F[x]/F$ عنصر وحدة في F[x]. لذلك فإنّه توجد $g\in F[x]$ بحيث $fg=1$. وهـذا يؤدي إلى أن $\deg fg=0$. وهذا تناقض لأن $\deg fg\geq \deg f$ ، $\deg f\geq 1$. وهكذا فإن كل العناصر الموجودة في F[x]/F ليست عناصر وحدة، لذلك فإن عناصر الوحدة في F[x] محتواة في F^* ولكن F^* محتواة في زمرة الوحدات للحلقة F[x] وبالتالي فإن F^* هي زمرة الوحدات للحلقة F[x].

نظرية (٣ ـ ٩)

F[x] حلقة إقليدية .

البرهـــان

من نتيجـة المبرهنة (٣ ـ ٦) نستنتج أنّ الحلقة F[x] حلقة تامة ولنعرِّف تقويم إقليدس d(f) لكل $0\neq f\in F[x]$ بأنّه يساوي $\deg f$.

نلاحظ أن :

(١) لكل كثيرتي حدود $f,g\in F[x]$ غير صفريتين فإن $\deg f\leq \deg fg$

(٢) خوارزمية إقليدس تتحقق من خلال نظرية خوارزمية القسمة في F[x].

لذلك فإن F[x] حلقة إقليدية .

لذلك فإن جميع النظريات التي تنطبق على الحلقة الإقليدية والتي ذكرت في البند السـابق ستنطبق على حلقة كثيرات الحدود F[x] على حقل F ، ولحاجتنا إليها هنا، سنتـولى ذكـرها. وقد يكون مفيدًا للقارىء أن يحاول إثبات هذه النتائج باستخدام طريقة البرهان في البند السابق على حلقة كثيرات الحدود على حقل.

نظرية (٣ ـ ١٠)

F[x] حلقة تامة رئيسة .

مبرهنـة (٣ - ١١)

يوجد قاسم مشترك أعظم d ومضاعف مشترك بسيط m لأي كثيرتي حدود غير صفريتين $f,g\in F[x]$ كما أن

$$(m) = (f) \cap (g) \qquad (d) = (f) + (g)$$

نظرية (٣ - ١٢)

إذا كان $I=(g)$ مثاليًّا للحلقة $F[x]$ فإن :

(i) I مثالي أولي للحلقة $F[x]$ إذا وإذا فقط كان $g=0$ أو g غير قابلة للتحليل على F.

(ii) I مثالي أعظمي غير تافه للحلقة $F[x]$ إذا وإذا فقط كان g غير قابلة للتحليل على F.

نظرية التحليل الوحيد

إذا كانت f كثيرة حدود غير ثابتة في الحلقة $F[x]$ فعندئذ يكون :

(i) توجد كثيرات حدود $g_1,g_2,\ldots,g_n\in F[x]$ غير قابلة للتحليل على F بحيث إن $f=g_1g_2\ldots g_n$.

(ii) يكون التحليل المذكور في الفقرة (i) وحيدا حسب المفهوم التالي :

إذا كان

$$f = h_1 h_2 \ldots h_m$$

حيث $h_1,h_2,\ldots,h_m$ كثيرات حدود غير قابلة للتحليل على F فإن $n=m$ ويوجد $\lambda_1,\lambda_2,\ldots,\lambda_n\in F^*$ بحيث إن $h_i=\lambda_i g_i$ لكل $i=1,2,\ldots,n$ (قد يكون ذلك بعد إعادة ترتيب).

ملاحظـة (٣ - ٣)

ليكن F حقلاً جزئيًّا من حقل K. من الواضح أنّ $F[x]$ حلقة جزئية من $K[x]$. لذلك فإن أيّة كثيرة حدود f على F يمكن اعتبارها ككثيرة حدود على K ولكنّها إذا كانت غير قابلة للتحليل على F فإنّها قد تكـون قابلة للتحليل على K كما لاحـظنا في مثال (٣ - ٧). وبصفة خاصة إذا كانت :

$$f = g_1 g_2 \ldots g_n$$

تحليل f إلى عوامل غير قابلة للتحليل على F ، فإن تحليل f على K ليس من الضروري أي يكون تحليل f على F حيث إن بعض g_i التي تظهر في تحليل f على F قد تكون قابلة للتحليل على K. ويمكن أن نحصل على تحليل f على K بالتعويض في :

$$f = g_1 g_2 \cdots g_n$$

عن g_i بعواملها غير القابلة للتحليل على K التي نحصل عليها من تحليل g_i حسب نظرية التحليل الوحيد.

ملاحظـة (٣ ـ ٤)

يمكن إثبات أنّ زمرة الوحدات للحلقة F[x] هي F^* مباشرةً باستخدام المبرهنة (٣ ـ ٢) التي تنص على أنّه إذا كانت R حلقة إقليدية فإن u عنصر وحدة في R إذا وإذا فقط كان d (u)= d (e).

جذور كثيرات الحدود على حقل

تعريـف (٣ ـ ١١)

ليكن F حقلاً جزئيًّا من حقل K ، ولتكن $f\in F[x]$ نقول إنَّ $a\in K$ جذر (root) لكثيرة الحدود f إذا كان f(a)=0.

مبرهنـة (٣ ـ ١٣)

إذا كان F حقلا جزئيا من حقل K وكان $f\in F[x]$ فإن $a\in K$ جذر لكثيرة الحدود f إذا وإذا فقط كان $(x - a) | f$.

البرهـان

إذا كان $a\in K$ بحيث إن $(x-a)|f$ فإن $f=(x-a)q$ حيث $q\in K[x]$ وهكذا فإن :

$$f(a) = (a-a)q(a) = 0.q(a) = 0$$

أي أن a جذر لكثيرة الحدود f.

ليكن $a\in K$ جذرًا لكثيرة الحدود f. باستخدام نظرية خوارزمية القسمة، نستنتج أنّه يوجد $q,r\in K[x]$ بحيث إنَّ :

$$f = (x-a)q + r$$

حيث $r=0$ أو $\deg r<1$ أي أن $r\in K$. نلاحظ أن :

$$f(a) = (a-a)q(a) + r$$

$$0 = 0 + r$$

ومنه نستنتج أن $r=0$ وبالتالي : $(x-a)|f$.

ملاحظـة (٣ - ٥)

ليكن F حقـلاً جزئيًا من حقـل K ، $f\in F[x]$ و $\deg f<1$. نستنتج من المبرهنة السابقة أنّه إذا كان $a\in K$ جذرًا لكثيرة الحدود f فإنّ f قابلة للتحليل على K ولكن العكس ليس صحيحًـا ، فكثيرة الحدود $x^4+2x^2+1=(x^2+1)^2$ كثيرة حدود قابلة للتحليل على حقل الأعداد الحقيقية $\mathbb{R}$ ولكن لا يوجد لها جذر في $\mathbb{R}$. ولكن إذا كانت درجة كثيرة الحدود f تساوي اثنين أو ثلاثة وكانت قابلة للتحليل على K فإنّه يوجد لها جذر في K لأنّ أحد عوامل تحليلها درجته تساوي الواحد، أي من الصيغة $ax+b$ حيث $a,b\in K$ وبالتالي يكون $-a^{-1}b$ جذرًا لها في K.

مبرهنـة (٣ - ١٤)

إذا كان F حقلاً جزئيًا من حقل K ، $f\in F[x]$ ،وكانت $a_1,\dots,a_n$ عناصر مختلفة من K فإن $a_1,\dots,a_n$ جذور لكثيرة الحدود f إذا وإذا فقط كان $(x-a_1)(x-a_2)\dots(x-a_n)|f$.

البرهـان

لتكن $a_1,a_2,\dots,a_n$ جذورًا لكثـيرة الحـدود f ولنـبرهن أنّ $(x-a_1)\dots(x-a_n)|f$ باستخدام طريقة الاستقراء الرياضي على n. إذا كان $n=1$ فإن $x-a_1|f$ حسب المبرهنة السابقة . نفرض أنّ النتيجة صحيحة لـ $n-1$ ونبرهن أنّها صحيحة لـ n ، لذلك فإنّ : $(x-a_1)\dots(x-a_{n-1})|f$ وبالتالي $f=(x-a_1)\dots(x-a_{n-1})q$ حيث $q\in K[x]$. كذلك فإن :

$$0 = f(a_n) = (a_n-a_1)(a_n-a_2)\dots(a_n-a_{n-1})q(a_n)$$

حيث إنّ $a_1,\dots,a_n$ عنـاصر مختلفة من الحقل K فإن $\Pi_{i=1}^{n-1}(a_n-a_i)$ عنصر غير صفري في K ، ولكن K حقـل وبـالتالي حلقة تامة، لذلك فإن $q(a_n)=0$ وهذا يعني حسب

المبرهنة السابقة أن $(x-a_n)|q$ ، وهكذا فإن $q=(x-a_n)q_1$ حيث $q_1 \in K[x]$ وبالتالي :

$$f = (x-a_1) \dots (x-a_{n-1})q$$
$$= (x-a_1) \dots (x-a_{n-1})(x-a_n)q_1$$

وهذا يؤدي إلى أن : $(x-a_1)\dots(x-a_n)|f$

العكس واضح .

ملاحظـة (٣ - ٦)

ليكن F حقلاً جزئيًا من حقل K ، $f \in F[x]$ و $a_1,\dots,a_n \in K$. إذا كانت $a_1,\dots,a_n$ جذورًا مختلفة لكثيرة الحدود f فإنه حسب المبرهنة السابقة $(x-a_1)\dots(x-a_n)|f$ وبالتالي :

$$\deg f \geq \deg \Pi_{i=1}^{n} (x-a_i)$$

ولكن حسب المبرهنة (٣ - ٦) فإن :

$$\deg \Pi_{i=1}^{n} (x-a_i) = n$$

إذن $\deg f \geq n$. بالتالي نستنتج من المبرهنة السابقة أن كثيرة الحدود $f \in F[x]$ التي إذا فرضنا أنّ درجتها تساوي n يكون لها على الأكثر n من الجذور المختلفة في F أو في أي حقل يحوي F .

تعريـف (٣ - ١٢)

ليكن F حقـلاً جزئيًا من حقـل K ، $f \in F[x]$ نقـول إن $\alpha \in K$ جذر مكـرر (multiple root) لكثيرة الحدود f إذا كان $(x-\alpha)^m|f$ حيث m عدد صحيح أكبر من الواحد.

مبرهنـة (٣ - ١٥)

إذا كان F حقلاً جزئيًا من الحقل K ، $f \in F[x]$ كثيرة حدود غير قابلة للتحليل على F ، $\alpha \in K$ جذر لكثيرة الحدود f ، فإن α جذر مكرر لكثيرة الحدود f إذا وإذا فقط كان α جذرا لكثيرة الحدود f' حيث f' هي مشتقة (derivative) f.

البرهـان

ليكن α جذرًا مكـررًا لكثـيرة الحـدود f. إذن يوجـد عدد صحيح m أكبر من الواحد بحيث إن $f=(x-\alpha)^m q$ حيث $q\in K[x]$ وهكذا فإن :

$$f' = m(x-\alpha)^{m-1} q + (x-\alpha)^m q'$$

وحيث إن $m-1>0$ فهذا يعني أن $(x-\alpha)|f'$ وبالتالي فإن α جذر لكثيرة الحدود f'.

نفـرض أن $f'(\alpha)=0$. حيث إن α جذر لكثـيرة الحـدود f فإنـه حسب المبرهنة (٣ - ١٣) $f=(x-\alpha)q$ حيث $q\in K[x]$ وهكذا فإن :

$$f' = q + (x-\alpha)q'$$

ولكن $f'(\alpha)=0$ إذن $q(\alpha)=0$ وبـالتالي $(x-\alpha)|q$. أي أن $q=(x-\alpha)q_1$ حيث $q_1\in K[x]$ ، وهكذا فإن :

$$f = (x-\alpha)^2 q_1$$

وبالتالي فإن α جذر مكرر لكثيرة الحدود f.

مثـال (٣ - ٨)

لتكن $g=x^2-7\in \mathbb{Q}[x]$. نلاحظ أن جذري g وهما $\pm\sqrt{7}$ لا ينتميان إلى $\mathbb{Q}$ ، ولأنّ درجة g تساوي إثنين لذلك فإن g غير قابلة للتحليل على $\mathbb{Q}$ [انظر الملاحظة (٣ - ٥)]. بما أن g غير قابلة للتحليل على $\mathbb{Q}$ فإن (g) يمثّل مثاليًا أعظميًا للحلقة $\mathbb{Q}[x]$ ، وبالتالي فإن $\mathbb{Q}[x]/(g)$ حقل .

مثـال (٣ - ٩)

لتكن $g=x^3+x^2+1\in \mathbb{Z}_2[x]$. نلاحظ أن عنـاصر $\mathbb{Z}_2$ لا تشكّـل جذورا لكثـيرة الحدود g ، ولأن درجتها 3 ، فإنه حسب الملاحظة (٣ - ٥) فإن g غير قابلة للتحليل على $\mathbb{Z}_2$ لذلك فإن (g) مثالي أعظمي للحلقة $\mathbb{Z}_2[x]$ وبالتالي فإن $\mathbb{Z}_2[x]/(g)$ حقل .

ملاحظـة (٣ - ٧)

ليكن F حقلاً ولتكن $f\in F[x]$. باستخدام المبرهنة (٣ - ٦) يمكن الاستنتاج أن عدد جذور f في F (بعضها قد يكون مكررًا) يساوي على الأكثر درجة f. سوف نثبت في

الفصل القادم أنّه يمكن تمديد F إلى حقل يحوي كل جذور f.

حلقة كثيرات الحدود على حقل الأعداد النسبية

تعريـف (٣ - ١٣)

يقال عن كثيرة الحدود

$$f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$$

إنّها كثيرة حدود بدائية (primitive polynomial) إذا كان القاسم المشترك الأعظم للمعاملات $a_0, a_1, \ldots, a_n$ يساوي الواحد.

مبرهنـة (٣ - ١٦)

إذا كانت f,g كثيرتي حدود بدائيّتين فإن f g كثيرة حدود بدائيّة.

البرهـان

لتكن

$$f = \sum_{i=0}^{n} a_i x^i \quad , \quad g = \sum_{i=0}^{m} b_i x^i \in \mathbf{Z}[x]$$

ولنفرض أنّ المبرهنة غير صحيحة. لذلك نفرض أنّ معاملات f g يجب أن تقبل القسمة على عدد أكبر من الواحد وبالتالي تقبل القسمة على عدد أولي وليكن p. لما كانت f بدائيّة فإن p لا تقسم بعض المعاملات a_i. ليكن a_j المعامل الأوّل من معاملات f الذي لا يقبل القسمة على p ، وبالطريقة نفسها ليكن b_k المعامل الأول من معاملات g الذي لا يقبل القسمة على p. ليكن معامل x^{j+k} في كثيرة الحدود f g هو c_{j+k} وبالتالي فإن $c_{j+k}=a_jb_k+d+e$ حيث إن :

$$d = a_{j+1} b_{k-1} + a_{j+2} b_{k-2} + \ldots + a_{j+k} b_0$$

$$e = a_{j-1} b_{k+1} + a_{j-2} b_{k+2} + \ldots + a_0 b_{j+k}$$

من طريقة اختيار b_k نستنتج أن $p|b_{k-1}, b_{k-2}, \ldots$ ولذلك $p|d$ وكذلك من طريقة اختيار a_j نستنتج أن $p|a_{j-1}, a_{j-2}, \ldots$ ولذلك $p|e$. حيث إن p يقسم كل معاملات f g ، لذلك فإن p يقسم c_{j+k} ، ونتيجة لذلك فإن p يقسم a_jb_k ولكن هذا يناقض كون p لا يقسم a_j ولا يقسم b_k.

مأخوذة جـاوس (Gauss's lemma)

كل كثيرة حدود بدائيّة غير قابلة للتحليل على Z تكون غير قابلة للتحليل على $\mathbb{Q}$.

البرهـان

لنفرض أن f كثيرة حدود بدائيّة غير قابلة للتحليل على Z ، ونفرض أن f=gh حيث $g,h \in \mathbb{Q}[x]$ و $\deg g,\ \deg h \geq 1$. بالتخلص من المقامات في معاملات g,h وإخراج العوامل المشتركة نستطيع كتابة $f=(a/b)\lambda\mu$ ، حيث a,b أعداد صحيحة ، λ,μ كثيرات حدود بدائيّة على Z ولهما درجات g,h على الترتيب . لذلك فإن $bf=a\lambda\mu$ لمّا كانت λ,μ كثيرتي حدود بدائيّتين فإنه حسب المبرهنة السابقة فإن $\lambda\mu$ كثيرة حدود بدائيّة . ولكن f كثيرة حدود بدائيّة أيضًا ، لذلك فإن a=b وبالتالي $f=\lambda\mu$ ، وهذا يناقض كون f غير قابلة للتحليل على Z . لذلك فإن f غير قابلة للتحليل على $\mathbb{Q}$.

من الصعوبة بمكان التأكد من كون كثيرة حدود معينة قابلة للتحليل على $\mathbb{Q}$ ، وتوجد طرائق قليلة لتسهيل ذلك إحداها معيار ايسنستاين التالي .

معيار ايسنستاين (Eisenstein criterion)

إذا كان p عددًا أوليًّا وكانت :

$$f = \sum_{i=0}^{n} a_i x^i \in \mathbf{Z}[x]$$

حيث معاملات f تحقق الشروط التالية :

(أ) $p \mid a_0, a_1, \ldots, a_{n-1}$

(ب) p^2 لا يقسم a_0

(ج) p لا يقسم a_n

فإن f غير قابلة للتحليل على Z .

البرهـــان

لتكن $f=gh$ حيث

$$g = \sum_{i=0}^{r} b_i x^i \quad , \quad h = \sum_{i=0}^{s} c_i x^i \in \mathbf{Z}[x]$$

من تعريف حاصل ضرب كثيرتي حدود نستنتج أنّ $a_0=b_0c_0$. لما كانت $p|a_0$ فإن $p|b_0$ أو $p|c_0$ ، وحيث إن p^2 لا يقسم a_0 فإن p لا يمكن أن يقسم كلا من b_0,c_0. لنفرض أنّ $p|b_0$ لا يقسم c_0. لمّا كان p لا يقسم a_n ، فليس كل المعاملات $b_0,b_1,\ldots,b_r$ تقبل القسمة على p. ليكن b_k المعامل الأول الذي لا يقبل القسمة على p ، حيث $k\leq r<n$. لذلك فإن p يقسم كلاّ من: $b_0,b_1,\ldots,b_{k-1}$.

$$a_k = b_k c_0 + b_{k-1} c_1 + \ldots + b_0 c_k$$

وكذلك $p|a_k$ و $p|b_0,b_1,\ldots,b_{k-1}$. لذلك فإن $p|b_kc_0$ ، ولكن p لا يقسم c_0 ، وبالتالي فإن $p|b_k$ وهذا تناقض. لذلك فإن f غير قابلة للتحليل على $\mathbf{Z}$.

لتكن $f=\mathbf{Z}[x]$ تحقق شروط معيار ايسنستاين. نلاحظ أنّ $f=dg$ حيث g كثيرة حدود بدائيّة، d هو القاسم المشترك الأعظم لمعاملات f. لما كانت g تحقق شروط معيار ايسنستاين لذلك فهي غير قابلة للتحليل على $\mathbb{Z}$ ولكنها بدائيّة، إذن g غير قابلة للتحليل على $\mathbb{Q}$ حسب مأخوذة جاوس لذلك فإن f غير قابلة للتحليل على $\mathbb{Q}$ وهكذا نكون قد برهنّا النتيجة التالية:

نتيجـــة

إذا كانت $f\in \mathbf{Z}[x]$ كثيرة حدود تحقق شروط معيار ايسنستاين، فإن f غير قابلة للتحليل على $\mathbb{Q}$.

مثـــال (٣ - ١٠)

باستخدام معيار ايسنستاين نستنتج أن كثيرة الحدود

$$x^m - p \in \mathbf{Z}[x]$$

حيث p عدد أولي، $m>1$ ، غير قابلة للتحليل على $\mathbb{Q}$ وبالتالي فإن العدد $\sqrt[m]{p}$ دائما عدد غير نسبي.

مثال (٣ - ١١)

لتكن $f=x^3-4\in \mathbb{Q}[x]$. نستطيع أن نختبر كون f غير قابلة للتحليل على $\mathbb{Q}$ باستخدام الملاحظة (٣ - ٥) لأنّ درجتها تساوي ثلاثة ولأنه يمكن تحليلها وبالتالي استنتاج أنّ جذورها لا تنتمي إلى $\mathbb{Q}$. كما نستطيع استخدام معيار ايسنستاين كما يلي:

إذا كانت $x=y+1$ فإن $f=y^3+3y^2+3y-3\in \mathbb{Q}[y]$ وهذه غير قابلة للتحليل على $\mathbb{Q}$ باستخدام معيار ايبنستاين.

مثال (٣ - ١٢)

ليكن p عددًا أوليًّا ولنعتبر كثيرة الحدود

$$f = x^{p-1} + x^{p-2} + \ldots + 1 \in \mathbb{Q}[x]$$

لتكن $x=y+1$. يكفي أن نثبت كما في المثال السابق أنّ $f(y+1)$ غير قابلة للتحليل على $\mathbb{Q}$. حيث إن :

$$(x^p - 1) = (x - 1)(x^{p-1} + x^{p-2} + \ldots + 1).$$

$$f(y + 1) = ((y + 1)^p - 1) / ((y + 1) - 1)$$

$$= ((y + 1)^p - 1) / y$$

حيث إن

$$(y + 1)^p = y^p + \sum_{i=1}^{p-1} \binom{p}{i} y^i + 1$$

وحيث إنه لكل $1\leqslant i\leqslant p-1$ فإن $\binom{p}{i}$ يقبل القسمة على p ولا يقبل القسمة على p^2 ، لذلك فإن :

$$f(y+1) = (y^p + p\,y^{p-1} + \ldots + p\,y) / y = y^{p-1} + p\,y^{p-2} + \ldots + p$$

الآن نطبق معيار ايسنستاين لنستنتج أن $f(y+1)$ غير قابلة للتحليل على $\mathbb{Q}$ وبالتالي f غير قابلة للتحليل على $\mathbb{Q}$.

تمارين (٣ - ٢)

١) لتكن R حلقة إبدالية بمحايد ولتكن $f\in R[x]$ بحيث إن حدها الثابت عنصر وحدة في R. أثبت أن f لا يمكن أن تكون قاسما للصفر في $R[x]$.

٢) أثبت أن $D[x_1,\ldots,x_n]$ حلقة تامة إذا كانت D حلقة تامة .

٣) لتكن R حلقة إبدالية بمحايد وليكن I مثاليا للحلقة R. أثبت أن مجموعة كل كثيرات الحدود التي يكون حدّها الثابت صفرًا ومعاملاتها الأخرى عناصر من I تشكّل مثاليا في R[x]

٤) أثبت أن F[x,y] حلقة غير رئيسة، حيث F حقل (إرشاد: اعتبر المثالي (y)+(x)).

٥) أثبت أن Z[x] حلقة غير رئيسة (إرشاد: اعتبر المثالي (2)+(x)).

٦) أثبت أن نظرية خوارزمية القسمة ليست صحيحة على Z[x].

٧) لتكن R حلقة إبدالية بمحايد. أثبت أنّه يوجد هوموم ورفزم غامر من R[x] إلى R وأنّ Ker φ=(x).

٨) أعطِ مثالا لمثالي أولي للحلقة Z[x] غير أعظمي وأعط مثالاً لمثالي أعظمي للحلقة Z[x].

٩) ليكن F حقلاً. أثبت أن (x) مثالي أولي ولكنّه ليس أعظميا للحلقة F[x,y]، أعط مثالاً لمثالي أعظمي للحلقة F[x,y].

١٠) أوجد كل كثيرات الحدود غير القابلة للتحليل على Z_2 والتي درجتها أقل أو تساوي خمسة.

١١) عيّن كل كثيرات الحدود غير القابلة للتحليل على Z_3 والتي درجتها تساوي اثنين.

١٢) أعط مثالا عن حقل لانهائي مميزه عدد أولي.

١٣) أثبت أن $x^3-1001x^2-1$ غير قابلة للتحليل على Q.

١٤) أثبت أن $x^{17}-13x^{16}-26x^2+39$ غير قابلة للتحليل على $\mathbb{Q}$.

١٥) إذا كانت $f,g,d',m' \in F[x]$ كثيرات حدود غير صفرية، وإذا كان d هو القاسم المشترك الأعظم لكثيرتي الحدود f,g وكان m المضاعف المشترك البسيط لهما. فإن:

(i) d' قاسم مشترك أعظم لـ f,g إذا وإذا فقط كان d,d' مترافقين.

(ii) m' مضاعف مشترك بسيط لـ f,g إذا وإذا فقط كان m,m' مترافقين.

١٦) أثبت باستخدام مأخوذة جاوس أن الحلقة $\mathbb{Z}[x]$ حلقة تحليل وحيد.

امتداد الحقول

مقدمة

سنقوم في هذا الفصل ببناء أو تمديد حقل اعتمادًا على حقل جزئي منه حيث سيمدنا ذلك بطريقة لمعرفة التركيب الجبري لحقل اعتمادًا على حقل جزئي إذا أمكن تمديد الحقل الجزئي إلى الحقل الأساسي كما سنلاحظ أن امتداد الحقول سيكون مصدرا لأمثلة ملموسة عن الحقول، والأهم من ذلك كله فإن امتداد الحقول يشكّل الأساس للأفكار الجميلة لنظرية جالوا (Galois theory) في إيجاد جذور كثيرات الحدود على حقل والتي لها دور مهم في وصول موضوع الجبر إلى ما هو عليه الآن.

نستطيع أن نتعرف على الدور المهم الذي لعبه حقل الأعداد المركّبة (التخيلية) $\mathbb{C}$ في رياضيات القرن الماضي من كون أن الحقيقة التي تنص على أن أية كثيرة حدود على $\mathbb{C}$ تنشر فيه (جذورها كلها في $\mathbb{C}$) كانت تسمى حينذاك النظرية الأساسية في الجبر، وبالرغم من أن النظرية مازالت تحمل المسمى نفسه حاليًا لكن ذلك ناتج عن احترام الماضي لأن $\mathbb{C}$ لا تلعب دورًا أساسيًا في موضوع الجبر، حيث توجد لدينا حقول مهمة مميزها عدد أولي (هذه الحقول لها تطبيقات مهمة، مثلا في نظرية الأعداد) ولا يمكن غمرها في $\mathbb{C}$. سندرس في هذا الفصل كجزء من امتداد الحقول موضوع حقول الانشطار وهي الحقول التي تنشر فيها كثيرات الحدود والتي معاملاتها من حقل، كما سندرس الحقول المنتهية والتي تمثل مصدر أمثلة ملموسة عن امتداد الحقول.

الامتداد البسيط للحقول

تعريـف (٤ - ١)

ليكن F حقلاً . نقول إنّ الحقل K امتداد (extension) للحقل F إذا كان K يحوي F ودرجة امتداد (degree of extension) K على F هي بعده كفضاء متّجه على F ويرمز لذلك بالرمز [K:F].

تعريـف (٤ - ٢)

ليكـن K امتـدادًا للحقـل F وليكـن $a\in K$. نقـول إنّ a عنصر جبري (algebraic element) على الحقل إذا كان a جذرًا لكثيرة حدود على F وإلّا نقول a متسامٍ (transcendental) على F.

تعريـف (٤ - ٣)

ليكن K امتـدادًا للحقل F. نقول إنّ K امتداد جبري (algebraic extension) للحقـل F إذا كان كل عنصر في K جبري على F وإلا يسمى امتـدادًا متسـاميًا (transcendental extension) للحقل F ، لذلك نقول عن الامتداد K للحقل F إنه متسامٍ إذا وجد عنصر واحد من K متسامٍ على F.

مثـال (٤ - ١)

العدد الحقيقي $\sqrt{2}$ عنصر جبري على حقل الأعداد النسبية $\mathbb{Q}$ لأنّه جذر لكثيرة الحدود $x^2-2\in\mathbb{Q}[x]$.

مثـال (٤ - ٢)

العدد المركب $i=\sqrt{-1}$ عنصر جبري على $\mathbb{Q}$ لأنه جذر لكثيرة الحدود $x^2+1\in\mathbb{Q}[x]$.

ملاحظـة (٤ - ١)

سنـركّـز في دراستنـا على الامتـداد الجبري لحقل ونشير فقط إلى أنّ العددين الحقيقيّين e,π عنصران متساميان على $\mathbb{Q}$ وبالتالي $\mathbb{R}$ امتداد متسامٍ على $\mathbb{Q}$ ، وإذا رغب القارىء في التعرف على برهان أن e,π عنصران متساميان على $\mathbb{Q}$ يستطيع أن يراجع صفحة (٢٦٨) في المرجع رقم [٧].

نظرية (٤ - ١)

إذا كان K امتدادًا للحقل F، $a\in K,F$ فإنّه إمّا $F(a)\cong F(x)$ أو $F(a)\cong F[x]/(g)$ حيث $g\in F[x]$ غير قابلة للتحليل على F ، والعنصر a جذر لها.

البرهـان

نعتبر الهوموموفزم الذي سبق أن درسناه في الفصل السابق $\phi:F[x]\to K$ المُعرَّف بالقاعدة:

$$\phi(f) = f(a)$$

حيث أثبتنا في المبرهنة (٣ ـ ٧) أنّ $\text{Im}\ \phi=F[a]$ وباستخدام النظرية الأولى في التشاكل نحصل على:

$$F[x] / \text{Ker}\ \phi \cong \text{Im}\ \phi$$

نميّز الحالتين التاليتين:

(١) عندما يكون العنصر a متساميًا على F ، أي أنّه لا توجد كثيرة حدود $f\in F[x]$ يكون a جذرًا لها، وبالتالي فإن $\text{Ker}\ \phi=\{0\}$ ولذلك فإن $F[x]\cong F[a]$. باستخدام النظرية (٢ ـ ٤) نستنتج أن $F(x)\cong F(a)$.

(٢) عندما يكون العنصر a جبريًّا على F. في هذه الحالة $\text{Ker}\ \phi\neq(0)$ ولكن F[x] حلقة تامة رئيسة، لذلك فإن $\text{Ker}\ \phi=(g)$ ، حيث $g\in F[x]$. بما أن F[a] حلقة جزئية من حقل فإنها حلقة تامة ولذلك فإن (g) مثالي أولي، انظر النظرية (١ ـ ٢٠)، وحيث إن $g\neq 0$ لذلك فإن g غير قابلة للتحليل على F حسب النظرية (٣ ـ ١٢)، وبالتالي فإن (g) مثالي أعظمي للحلقة F[x]. وهذا يؤدي إلى أن F[x]/(g) حقل، حسب النظرية (١ ـ ٢٠)، وبالتالي فإن F[a] حقل، أي أن $F[a]=F(a)$.

نتيجـة

إذا كان K امتدادًا للحقل F وإذا كان a,b عنصرين متساميين على F فإن $F(a)\cong F(b)$.

البرهـان

حسب إثبات النظرية السابقة فإن $F(a)\cong F(x)$ وكذلك $F(b)\cong F(x)$ وبالتالي فإن $F(a)\cong F(b)$.

تعريـف (٤ ـ ٤)

إذا كان K امتدادًا للحقل F ، وكان $a\in K$ عنصرًا جبريًّا على F فإن F(a) يسمى امتـدادًا جبريًّا بسيطًا (simple algebraic extension) للحقل F ، ويسمى a العنصر البدائي (primitive element) للامتداد الجبري البسيط ويسمى F(a) امتدادًا متساميًا بسيطًا (simple transcendental extension) للحقل F إذا كان a عنصرًا متساميًا على الحقل F.

ملاحظـة (٤ ـ ٢)

ليكن K امتدادًا للحقل F ، $a\in K$ عنصر جبري على F ، $\text{Ker}\ \phi=(g)$ حيث ϕ هو الهـومـومـورفزم المعرّف في إثبات النظرية السابقة، $g\in F[x]$ كثيرة حدود غير قابلة للتحليل على F بحيث يكون a جذرًا لها. لقد سبق أنّ استنتجنا من النظرية (٣ ـ ١) أن (g) لها أقل تقويم d(g) من بين كل عناصر $\text{Ker}\ \phi$ ، أي أن درجة g أقل درجة من بين كل كثيرات الحدود التي تنتمي إلى $\text{Ker}\ \phi$ ، لهذا تسمى كثيرة حدود صغرى للعنصر a على F. ومن ناحية أخرى فإن زمرة الوحدات للحلقة F[x] حسب المبرهنة (٣ ـ ٨) هي F^* ، لذلك إذا كانت $\lambda\in F^*$ فإن λg تنتمي إلى (g) ولها نفس درجة g ، وهكذا فإن $\text{Ker}\ \phi=(\lambda g)$ ، وبالتالي فإنّنا نحصل على عدد من كثيرات الحدود الصغرى للعنصر a بقدر عناصر F^*. لذلك حتى نجعل كثيرة حدود صغرى للعنصر a وحيدة يحتاج أن نفـرض أنها واحـدية وتـسـمـى في هذه الحـالـة كثـيرة الحـدود الـصـغـرى (the minimal polynomial) للعنصر a على F وتسمى درجتها بدرجة a على F.

نظريـة (٤ - ٢)

إذا كان K امتدادا للحقل F ، $a\in K$ عنصر جبري على F ، n درجة a على F ، فإن العناصر $1,a,a^2,\dots,a^{n-1}$ تُشكِّل أساسًا للحقل F(a) على الحقل F كفضاء متجه على F.

البرهـان

حيث إن F(a)=F[a] حسب إثبات النظرية (٤ - ١) فإن :

$$F(a)=\left\{\sum_{i=0}^{m} a_i\, a^i : a_i \in F\ ,\ m \in \mathbb{N}\cup\{0\}\right\}$$

ليكن $f(a)=\sum_{i=0}^{m} a_i a^i$ عنصرا من F(a) ، $f=\sum_{i=0}^{m} a_i x^i$ ، g كثيرة الحدود الصغرى للعنصر a على F. باستخدام مبرهنة خوارزمية القسمة نستنتج أنّه توجد $q,r\in F[x]$ بحيث إن $f=g\,q+r$ حيث r=0 أو deg r<deg g ، لتكن $g=\sum_{i=0}^{n} b_i x^i$ ، حيث إن deg r<deg g. لنفرض أن $r=\sum_{i=0}^{n-1} \alpha_i x^i$ بالتالي فإن :

$$f(a) = g(a)\,q(a) + r(a) = 0q(a) + r(a) = r(a)$$

إذن f(a)= r(a) ومنه نجد أنّ كل عنصر في F(a) مُولَّد من قبل العناصر

$$1,\ a,\ a^2,\ \dots,\ a^{n-1}$$

لنفرض جدلاً أن العناصر $1,a,a^2,\dots,a^{n-1}$ غير مستقلة خطيًّا، أي توجد عناصر $\alpha_0,\alpha_1,\dots,\alpha_{n-1}$ في F ليست كلها أصفارًا وبحيث إنّ :

$\sum_{i=0}^{n-1} \alpha_i a^i=0$ وهذا يعني أن a جذر لكثيرة الحدود $f=\sum_{i=0}^{n-1} \alpha_i x^i$ ، لذلك فإن $f\in(g)$ حيث إن g كثيرة الحدود الصغرى للعنصر a على F ، ومنه نجد أن f=g h ، حيث $h\in F[x]$ وبالتالي فإن :

$$\deg f = \deg g + \deg h$$

أي أنّ deg f≥deg g=n ، وهذا تناقض لأن deg f≤n-1. لذلك فإن :

$$\alpha_0 = \alpha_1 = \alpha_2 = \dots = \alpha_{n-1} = 0$$

إذن $1,a,a^2,\dots,a^{n-1}$ مستقلة خطيًّا على الحقل F.

بناء حقول الامتداد

ليكن K امتـدادًا للحقـل F. لقـد قمنـا بتمـديد F بربـطه أو إقـرانـه بعنصر a من K لنحصل على امتداد (extension by adjoining an element to a field) بسيط لحقل F داخل K ذي صفات معيّنة، فمثلا لو كان E امتدادًا جبريًّا للحقل F فإنه لا يوجد بداخله امتداد متسامٍ بسيط، وكذلك إذا كان $g\in F[x]$ فقد لا يوجد امتداد جبري بسيط للحقل F داخل K ناتج عن ربط F بجذر لكثيرة الحدود g حيث إنّه قد لا يوجد في K أي جذر لكثيرة الحدود g. لذلك سنوضح في المبرهنتين القادمتين كيفية بناء امتداد متسامٍ بسيط أو بناء امتداد لحقل F يحوي جذرًا لكثيرة حدود غير قابلة للتحليل على الحقل F.

مبرهنـة (٤ - ٣)

إذا كان F حقلاً فإنه يوجد له امتداد متسامٍ بسيط.

البرهـان

إذا كان F(x) حقل جميع الدوال النسبية لمتغيّر x على حقل F، أي حقل القواسم للحلقة التامّة F[x]، فإن F(x) امتداد متسامٍ بسيط للحقل F، انظر إثبات المبرهنة (٤ - ١) (١).

نظريـة (٤ - ٤)

إذا كان F حقلاً، $g\in F[x]$ كثيرة حدود غير قابلة للتحليل على F فإنه يوجد امتداد للحقل F يحوي جذرًا لكثيرة الحدود g.

البرهـان

لما كانت g كثيرة حدود غير قابلة للتحليل على F فإن (g) مثالي أعظمي للحلقة F[x] وبالتالي فإن $K=F[x]/(g)$ يشكّل حقلا. لنعتبر الهومومورفزم الطبيعي ϕ من F[x] إلى K. لمّا كان F حقـلاً وكـذلـك حلقة جزئية من F[x]، فإن قصر ϕ على F يعطينا

هومومورفزما أحاديًا (انظر تمرين ١ - ٢ - ١٤)، ولذلك فإن F يشاكل $\Phi(F)$ وبالتالي فإن F مغمور في K ، وهكذا نستطيع أن نعتبر F حقلًا جزئيًا بتطبيق كل عنصر $\lambda \in F$ مع صورته $\bar{\lambda}=\lambda+(g)$. لنفرض أنّ :

$$a = x + (g)$$

من الواضح أنّ a عنصر من K. لتكن :

$$g = \sum_{i=0}^{n} a_i x^i$$

حيث إن كل عنصر λ في F يُعبَّر عنه بـ $\lambda+(g)$ الذي يقع في صورة F ، لذلك فإنّنا نعبّر عن $\bar{g}$ كما يلي :

$$\bar{g} = \sum_{i=0}^{n} (a_i + (g))\, x^i$$

نلاحظ أنّ

$$\bar{g}(a) = \sum_{i=0}^{n} (a_i + (g))\, a^i$$

$$= \sum_{i=0}^{n} (a_i + (g))\, (x + (g))^i$$

$$= \sum_{i=0}^{n} (a_i + (g))\, (x^i + (g)) = \sum_{i=0}^{n} a_i x^i + (g)$$

$$= g + (g) = (g)$$

وبالتالي فإنه يمكن اعتبار a جذر لكثيرة الحدود g وهو عنصر من K.

مثـال (٤ - ٣)

اعتبر كثيرة الحدود $g=x^2+x+1 \in \mathbf{Z}_2[x]$. لما كانت درجة g تساوي اثنين ولا يوجد من بين عناصر $\mathbf{Z}_2$ من يكون جذرا لها، فإن g غير قابلة للتحليل على $\mathbf{Z}_2$[انظر الملاحظة (٣ - ٥)]، لذلك فإن $K=\mathbf{Z}_2[x]/(g)$ حقل، وحسب إثبات النظرية السابقة فهو يحوي العنصر $a=x+(g)$ الذي يمثل جذرًا لكثيرة الحدود g. من النظرية (٤ - ١) (٢) نستنتج

أنّ $K = Z_2(a)$ باعتبار Z_2 حقل جزئي من K لأنّه مغمور فيه. كذلك من النظرية (٤ - ٢) نلاحظ أنّ $1,a$ تُشكّل أساسا للحقل K على F. أي أن:

$$K = \{\lambda_0 + \lambda_1 a : \lambda_0, \lambda_1 \in Z_2\}$$
$$= \{0, 1, a, 1 + a\}$$
$$= \{0, 1, a, a^2\}$$

لأن $a^2+a+1=0$ وبالتالي $a^2=a+1$. لاحظ أنّ $K^*=<a>$ ، أي أنّها زمرة دائرية رتبتها ثلاثة، كما أنّ تحليل g على K هو:

$$g = (x + a)(x + a + 1)$$

مثـال (٤ - ٤)

اعتبر كثيرة الحدود $g=x^2+1 \in Z_3[x]$. لمّا كانت درجة g تساوي اثنتين ولا يوجد من بين عناصر Z_3 من يكون جذرًا لـ g ، فإن g غير قابلة للتحليل على Z_3 ، لذلك فإن $K= Z_3[x]/(g)$ حقل يحوي العنصر $a=x+(g)$ الذي يمثل جذرًا لكثيرة الحدود g. من النظريات السابقة نستنتج أنّ $K=Z_3(a)$ باعتبار أنّ Z_3 حقل جزئي من K لأنه مغمور فيه، كما أن $1,a$ تُشكّل أساسًا للحقل K على Z_3 ، أي أن

$$K = Z_3(a) = \{\lambda_0 + \lambda_1 a : \lambda_0, \lambda_1 \in Z_3\}$$
$$= \{0, 1, 2, a, 2a, 1 + a, 1 + 2a, 2 + a, 2 + 2a\}$$

كما أن تحليل x^2+1 على K هو:

$$g = (x + a)(x + 2a)$$

لاحظ أنّ

$$(1+a)^4 = (1+a)^3 (1+a) = (1+a^3)(1+a) = (1-a)(1+a)$$
$$= 1 - a^2 = 1 = -1$$

لذلك فإن رتبة $(1+a)$ لا يمكن أن تكون اثنتين أو أربعة. ولما كانت رتبة $(1+a)$ تقسم رتبة K^* ، فإن رتبة $(1+a)$ تساوي ثمانية وبالتالي فإن $K^*=<1+a>$.

سنبرهن في بند الحقول المنتهية أنّه إذا كان K حقلاً منتهيًا، فإن K^* زمرة دائرية وهذا يوضح ما لاحظناه في المثالين السابقين من كون K^* زمرة دائرية.

مثـال (٤ - ٥)

اعتبر كثيرة الحدود $g=x^2-2 \in \mathbb{Q}[x]$. لما كانت درجة g تساوي اثنتين ولا يوجد لها جذر في $\mathbb{Q}$ لأن جذريها $\pm\sqrt{2}$ فإن g غير قابلة للتحليل على $\mathbb{Q}$ ولذلك فإن $K=\mathbb{Q}[x]/(g)$ حقل يحوي العنصر $a=x+(g)$ الذي يمثل جذرا لكثيرة الحدود g. من النظريات السابقة نستنتج أنّ $K=\mathbb{Q}(a)$ كما أنّ $1,a$ تشكّل أساسًا للحقل K على $\mathbb{Q}$. لمّا كان $a^2=2$. فإن $a=\pm\sqrt{2}$ لذلك $1,\sqrt{2}$ تشكّل أساسًا للحقل $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(a)$ على $\mathbb{Q}$ وبالتالي فإن :

$$\mathbb{Q}(\sqrt{2}) = \{\lambda_0 + \lambda_1 \sqrt{2} : \lambda_0, \lambda_1 \in \mathbb{Q}\}$$

كما أن تحليل g على $\mathbb{Q}(\sqrt{2})$ هو:

$$g = (x - \sqrt{2})(x + \sqrt{2})$$

مثـال (٤ - ٦)

اعتبر كثيرة الحدود $g=x^2+1 \in \mathbb{R}[x]$. لمّا كانت درجة g تساوي اثنتين وجذراها $i,-i$ لا ينتميان إلى $\mathbb{R}$ ، فإن g غير قابلة للتحليل على $\mathbb{R}$. لذلك فإن $K=\mathbb{R}[x]/(g)$ حقل وهو يحوي العنصر $a=x+(g)$ الذي يمثل جذرًا لكثيرة الحدود g. من النظريات السابقة نستنتج أنّ $K=\mathbb{R}(a)$ كما أنّ $1,a$ تشكّل أساسًا للحقل K على $\mathbb{R}$. حيث إن $a^2=-1$ فإن $a=\pm i$ ، لذلك فإن $1,i$ تشكّل أساسًا للحقل $K=\mathbb{R}(i)$ على $\mathbb{R}$ ، أي أنّ :

$$\mathbb{R}(i) = \{\lambda_0 + \lambda_1 i : \lambda_0, \lambda_1 \in \mathbb{R}\}$$

كما أنّ تحليل g على $\mathbb{R}(i)$ هو

$$g = (x - i)(x + i)$$

من الـواضـح أنّ $\mathbb{R}(i)=\mathbb{C}$ ، وهكـذا استـطعنا أن نعمل امتدادًا للحقل $\mathbb{R}$ حتى نحصل على حقل الأعداد المركّبة .

مبرهنـة (٤ - ٥)

إذا كان K ، $\bar{K}$ امتـدادين للحقلين F ، $\bar{F}$ على التـوالي، وكان τ_0 تشاكلاً من الحقـل F إلى الحقـل $\bar{F}$ وكان $F(a)$ ، $\bar{F}(\bar{a})$ امتدادين جبريّين بسيطين، ولنفرض أنّ a جذر لكثـيرة حدود g غير قابلة للتحليل على F، $\bar{a}$ جذر لكثـيرة الحـدود $\bar{g}$ التي هي

صورة g تحت تأثير τ_0 (أي أنّه إذا كانت $g=\sum a_i x^i$ فإن $\bar{g}=\sum \tau_0(a_i)x^i$) من الممكن تمديد τ_0 إلى تشاكل τ_1 من F(a) إلى $\bar{F}(\bar{a})$ بحيث إن τ_0 يرسل a إلى $\bar{a}$.

البرهـان

نستطيع تمديد τ_0 إلى تشاكل τ من F[x] إلى $\bar{F}[x]$ حيث τ معرّف بالقاعدة:

$$\tau\left(\sum_{i=0}^{m} a_i x^i\right)=\sum_{i=0}^{m} \tau_0(a_i)\, x^i$$

بما أنّ τ تشاكل من F[x] إلى $\bar{F}[x]$ فإن $\bar{g}$ غير قابلة للتحليل على F لأن $\bar{g}=\tau(g)$، ولأن g غير قابلة للتحليل على F. باستخدام المبرهنة (١ ـ ١٤) نحصل على

$$\psi : F[x] / (g) \cong \bar{F}[x] / (\bar{g})$$

ولكن من المبرهنة (٤ ـ ١):

$$\phi : F(a) \cong F[x] / (g)$$

وكذلك

$$\bar{\phi} : \bar{F}(\bar{a}) \cong \bar{F}[x] / (\bar{g})$$

ليكن

$$\tau_1 = \bar{\phi}\, \psi\, \phi$$

من الواضح أنّ τ_1 تشاكل من F(a) إلى $\bar{F}(\bar{a})$، كما أن:

$$\tau_1(a) = \bar{\phi}\, \psi\, \phi(a) = \bar{\phi}\, \psi\, (x + (g))$$
$$= \bar{\phi}\, (x + (\bar{g})) = \bar{a}$$

الامتـداد المنتهي للحقـول

تعريـف (٤ ـ ٥)

ليكن K امتـدادًا للحقل F ولتكن $a_1,\ldots,a_n \in K$. الحقل $F(a_1,\ldots,a_n)$ هو أصغر حقـل يحوي F ويحـوي العنـاصر $a_1,\ldots,a_n$ ونستطيع تعريفه بأنّه تقاطع جميع الحقول الجزئية من K التي تحوي F وتحوي العناصر $a_1,a_2,\ldots,a_n$. يمكن الحصول على

$F(a_1,a_2,\ldots,a_n)$ باستخدام الامتداد البسيط $F(a_1)$ ثم نعمل امتدادًا بسيطًا آخرًا على الحقل $F(a_1)$ لنحصل على الحقل $F(a_1,a_2)=(F(a_1))(a_2)$ ونتابع هكذا حتى نحصل على الحقل $F(a_1,\ldots,a_n)$.

تعريف (٤ - ٦)

ليكن K امتدادًا للحقل F. نقول إنّ K امتداد منته (finite extension) للحقل F إذا كانت درجة امتداد K على F منتهية أي أنه إذا كان $\dim_F K$ منتهٍ.

مبرهنة (٤ - ٦)

إذا كان K امتدادًا منتهيًا للحقل F فإن K امتداد جبري للحقل F.

البرهان

إذا كان $[K:F]=n$ ، وكان $a\in K$ ، فإن $1,a,\ldots,a^n$ غير مستقلة خطيًّا على F وبالتالي فإنّه يوجد $\alpha_0,\alpha_1,\ldots,\alpha_n\in F$ لا تساوي الصفر في آن واحد بحيث إن :

$$\sum_{i=0}^{n}\alpha_i a^i = 0$$

وهذا يعني أن a جذر لكثيرة الحدود :

$$\sum_{i=0}^{n}\alpha_i x^i$$

أي أن a عنصر جبري على F ، ولكن a عنصر اختياري من K ، إذن K امتداد جبري للحقل F.

نتيجة

إذا كان K امتدادًا جبريًّا بسيطًا للحقل F فإن K امتداد جبري للحقل F.

البرهان

إذا كان $K=F(a)$ ، وكانت $f\in F[x]$ كثيرة الحدود الصغرى للعنصر a على F ، فإن

$[K:F]=\deg f$ (انظر النظرية (٤ ـ ٢)). وهذا يعني أنّ درجة امتداد K على F منتهية وبالتالي فإن K امتداد جبري للحقل F لأنه امتداد منتهٍ.

مبرهنـــة (٤ ـ ٧)

إذا كان K امتدادًا منتهيًا للحقل F وكان L امتدادًا منتهيًا للحقل K فإن:

$$[L : F] = [L : K]\,[K : F]$$

وبالتالي فإن L امتداد منتهٍ للحقل F.

البرهـــان

لتكن $[L:K]=m$ ، $[K:F]=n$ ولنتخذ الأساسين $\alpha_1,\ldots,\alpha_m$ ، $\beta_1,\ldots,\beta_n$ للحقل L على K وللحقل K على F على التوالي. ليكن $x\in L$ فإنّنا نستطيع أن نعبّر عن x بطريقة وحيدة كما يلي:

$$x = \sum_{i=1}^{m} a_i\,\alpha_i$$

حيث $a_i\in K$ ولكن a_i نعبّر عنه بطريقة وحيدة كما يلي:

$$a_i = \sum_{j=1}^{n} b_{ij}\,\beta_j$$

حيث $b_{ij}\in F$ لذلك فإن:

$$x = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\,\beta_j\,\alpha_i$$

أي أنّ العناصر $\alpha_i\beta_j$ (حيث $i=1,\ldots,m$ ، $j=1,\ldots,n$) تولد الحقل L على F.

لكي نثبت أنّها مستقلة خطيًّا نفرض أن:

$$\sum_{j=1}^{m}\sum_{i=1}^{n} c_{ij}\,\alpha_i\,\beta_j = 0$$

حيث إن $c_{ij}\in F$ إذا كانت

$$\gamma_i = \sum_{j=1}^{n} c_{ij}\,\beta_j$$

فإن $\gamma_i \in K$ وحيث إن $\alpha_1,\ldots,\alpha_m$ مستقلة خطيًا على K ، لذلك فإن $\gamma_i = 0$ لكل $i=1,\ldots,m$

لكن $\beta_1,\ldots,\beta_n$ مستقلة خطيًا على F، لذلك فإن $c_{ij} = 0$ لكل $i=1,\ldots,m$ ولكل $j=1,\ldots,n$ ،

، وهذا يثبت أن العناصر $\alpha_i\beta_j$ (حيث $i=1,\ldots,m$ ، $j=1,\ldots,n$) تُشكّل أساسا للحقل L على الحقل F ، لذلك فإن :

$$[L : F] = m\,n = [L : K]\,[K : F]$$

نتيجـــة (١)

إذا كان K امتدادًا للحقل F ، وإذا كانت $a_1,\ldots,a_n \in K$ عناصر جبريّة على F ، فإن $F(a_1,\ldots,a_n)$ امتداد منته للحقل F وبالتالي جبري .

البرهـــان

نستخدم طريقة الاستقراء الرياضي على n في إثبات هذه النتيجة . إذا كان $n=1$ فإن $F(a_1)$ امتـداد منته للحقل F حسب النظرية (٤ ـ ٢) . نفرض أنّ $F(a_1,\ldots,a_{n-1})$ امتداد منته للحقل F ونودُّ إثبات أنّ $F(a_1,\ldots,a_n)$ امتداد منته للحقل F. لمّا كان $F(a_1,\ldots,a_n)$ امتدادًا منتهيًا للحقل $F(a_1,\ldots,a_{n-1})$ ، والحقل $F(a_1,\ldots,a_{n-1})$ امتدادًا منتهيًا للحقل F ، لذلك فإن $F(a_1,\ldots,a_n)$ امتداد منته للحقل F حسب المبرهنة السابقة وبالتالي فإنه امتداد جبري للحقل F.

نتيجـــة (٢)

إذا كان L امتدادًا جبريًّا للحقل K وكان K امتدادًا جبريًّا للحقل F ، فإن L امتداد جبري للحقل F.

البرهـــان

ليكن $a \in L$. نودُّ أن نثبت أنّ a عنصر جبري على الحقل F. لمّا كان الحقل L امتدادًا جبريًّا للحقل K ، فإن a عنصر جبري على الحقل K. لتكن :

$$f = \sum_{i=0}^{n} a_i\,x^i$$

كثيرة حدود على K بحيث يكون a جذرًا لها ولنضع $M=F(a_0,\ldots,a_n)$ حيث $a_0,\ldots,a_n\in K$. لمّا كان a عنصرًا جبريًا على الحقل M ، فإن M(a) امتداد جبري بسيط للحقل M وبالتالي امتداد منته حسب النظرية (٤ ـ ٢)، ولكن M امتداد منته للحقل F حسب النتيجة (١)، إذن M(a) امتداد منته للحقل F حسب المبرهنة السابقة . وهكذا فإن M(a) امتداد جبري للحقل F [انظر المبرهنة (٤ ـ ٦)] وبالتالي فإن a عنصر جبري على F ، ولكن a عنصر اختياري من L لذلك فإن L امتداد جبري للحقل F.

نتيجـــة (٣)

إذا كان K امتدادًا للحقل F ، وإذا كانت A مجموعة كل العناصر الجبرية في K على الحقل F ، فإن A حقل جزئي من K يحوي F.

البرهـــان

لما كان كل عنصر a في الحقل F هو عنصر جبري على F لأنّه جذر لكثيرة الحدود $x-a\in F[x]$ ، فإن F محتوى في A. لكي نبرهن أنّ A حقل جزئي من K يكفي أن نبرهن أنه إذا كانت $a,b\in A$ فإن $ab,a-b\in A$ وإذا كانت $a\neq 0$ فإن $a^{-1}\in A$. نعتبر الامتداد F(a,b) للحقل F ، هذا الامتداد امتداد منته للحقل F حسب النتيجة (١) وبالتالي فهو امتداد جبري للحقل F ، لذلك فإن $A\supset F(a,b)$. بما أن $a,b\in F(a,b)$ ، فإن $ab,a-b\in F(a,b)$. كذلك إذا كانت $a\neq 0$ فإن $a^{-1}\in F(a,b)$ ، لذلك فإن $ab,a-b\in A$ وكذلك إذا كانت $a\neq 0$ فإن $a^{-1}\in A$. وهكذا فإن A حقل جزئي من K يحوي F.

ملاحظـــة (٤ ـ ٣)

ليكن K امتدادًا للحقل F ولتكن $S=\{a_1,\ldots,a_n\}$ مجموعة جزئية من K ، كون S مجموعة منتهية لا يعني أن $F(a_1,\ldots,a_n)$ امتداد منته للحقل F. فمثلا لو كان العنصر a متساميا على F فإن F(a) يشاكل حقل الدوال النسبية F(x) وبالتالي فإن F(a) امتداد غير منته للحقل F.

الإغلاق الجبري لحقل

تعريف (٤ - ٧)

ليكن K امتدادا للحقل F. الحقل الجزئي من K الذي يحوي جميع العناصر في K الجبرية على F يسمى الإغلاق الجبري (algebraic closure) للحقل F في K ويرمز له بالرمز $\bar{F}$..

إذا كان $\bar{\bar{F}}$ الإغلاق الجبري للحقل $\bar{F}$ في K وإذا كان $x\in\bar{\bar{F}}$ فإن x عنصر جبري على $\bar{F}$ ، ولكن $\bar{F}$ امتداد جبري على F ، لذلك فإن x عنصر جبري على F حسب النتيجة (٢) للمبرهنة (٤ - ٧) وبالتالي فإن $x\in\bar{F}$. وهذا يعني أن $\bar{\bar{F}}\supset\bar{F}$ ولكن $\bar{F}\supset F$ ، إذن $\bar{\bar{F}}=\bar{F}$..

مثال (٤ - ٧)

ليكن A حقل الأعداد المركّبة الجبرية على حقل الأعداد النسبية $\mathbb{Q}$. يسمى الحقل A حقل الأعداد الجبريّة، وهو الإغلاق الجبري لحقل الأعداد النسبية $\mathbb{Q}$ في حقل الأعداد المركّبة $\mathbb{C}$.

تعريف (٤ - ٨)

نقول عن الحقل إنه مغلق جبريا (algebrically closed) إذا كان هو الامتداد الجبري الوحيد لنفسه، أو بطريقة أخرى هو الحقل الذي تكون أية كثيرة حدود معاملاتها منه وذات درجة أكبر من الصفر لها جذر فيه.

تعريف (٤ - ٩)

نقول عن الحقل K إنّه الإغلاق الجبري (algebraic closure) للحقل F إذا كان K امتدادًا جبريًا للحقل F وكان K مغلقًا جبريًا.

ملاحظـة (٤ - ٤)

نودُّ أن نشير إلى ما يسمى النظرية الأساسية في الجبر (fundamental theorem of Algebra) وهي الحقيقة التي تنص على أنّ حقل الأعداد المركّبة $\mathbb{C}$ مغلق جبريًا. لن ندخل في تفاصيل إثبات هذه النظرية لأنّه يحتاج إلى أفكار ليست ضمن منهاج الكتاب، والقارىء الذي يود الاطلاع على الإثبات يستطيع أن يراجع صفحة ٢٩٣ في المرجع رقم [٧].

مثـال (٤ - ٨)

حقل الأعداد المركّبة هو الإغلاق الجبري لحقل الأعداد الحقيقية لأنّه امتداد جبري بسيط له حيث إن $\mathbb{C} = \mathbb{R}(i)$ [انظر المثال (٤ - ٦)] كما أنّ $\mathbb{C}$ مغلق جبريًا، ولكن $\mathbb{C}$ لا يشكل الإغلاق الجبري لحقل الأعداد النسبية $\mathbb{Q}$ لأنّه ليس امتدادا جبريا للحقل $\mathbb{Q}$ حيث إن $e,\pi \in \mathbb{C}$ عنصران متساميان على $\mathbb{Q}$.

تمارين (٤ - ١)

١) أثبت أن $1+\sqrt{2}$ ، $\sqrt{2}=\sqrt{3}$ ، $\sqrt{1+\sqrt[3]{2}}$ ، $\sqrt{\sqrt[3]{2-i}}$ عناصر جبرية على $\mathbb{Q}$.

٢) وضّح فيما إذا كانت العناصر $\alpha \in \mathbb{C}$ جبرية أو متسامية على الحقل F:

(أ) $\alpha = i \, , F = \mathbb{Q}$

(ب) $\alpha = \sqrt{\pi} \, , F = \mathbb{Q}(\pi)$

(جـ) $\alpha = \sqrt{\pi^2} \, , F = \mathbb{Q}(\pi^3)$

(د) $\alpha = \sqrt{\pi} + 1 \, , F = \mathbb{Q}(\pi^2)$

(هـ) $\alpha = \sqrt{2} + \sqrt[3]{\pi} \, , F = \mathbb{Q}(\pi)$

٣) ليكن p عددًا أوليًّا، $K = \mathbf{Z}_p(x)$ ، $F = \mathbf{Z}_p(x^p)$ حيث x متغيّر

(أ) هل x عنصر جبري على $\mathbf{Z}_p$؟

(ب) هل x عنصر جبري على F ؟

(ج) هل x عنصر جبري على K ؟

(د) هل K امتداد جبري للحقل F ؟

٤) ليكن $E=F(u)$ ، حيث u عنصر جبري على F ودرجته عدد فردي. أثبت أنّ درجة u^2 على F عدد فردي وأثبت أنّ $F(u)=F(u^2)$.

٥) ليكن $E=F(\alpha)$ ، حيث α عنصر متسامٍ على F ، وليكن $K \supset F$ حقلاً جزئيًا من E. أثبت أنّ α عنصر جبري على K.

٦) أثبت أنّ $\sqrt{2}+\sqrt[3]{5}$ عنصر جبري على $\mathbb{Q}$ درجته تساوي 6.

٧) أثبت أنّ $g=x^3+x^2+1$ كثيرة حدود غير قابلة للتحليل على $\mathbf{Z}_2$، ثم أثبت أنّ $K = \mathbf{Z}_2[x]/(g)$ حقل عدد عناصره ثمانية عناصر. أوجد أساسه على $\mathbf{Z}_2$ وأثبت أنّ K^* دائرية.

٨) ليكن $\omega=-\frac{1}{2}+\frac{1}{2}\sqrt{3}i$ حيث $i=\sqrt{-1}$ ، أثبت أنّ ω جبري على $\mathbb{Q}$. أوجد أساس $\mathbb{Q}(\omega)$ على $\mathbb{Q}$ ودرجة امتداده.

٩) أثبت أنّ $\mathbb{Q}(\sqrt{3},\sqrt{7}) = \mathbb{Q}(\sqrt{3}+\sqrt{7})$.

١٠) ليكن K امتدادًا للحقل F ، $a,b=K$ عنصران جبريان على F ودرجاتهما على F هما n,m على الترتيب حيث $(m,n)=1$. أثبت أن $F(a,b)$ امتداد درجته m n على F.

١١) ليكن $\omega \in \mathbb{C}$ حيث إن $\omega^p=1$ ، $\omega\neq1$. أثبت أن $[\mathbb{Q}(\omega):\mathbb{Q}]=p-1$. (إرشاد: استخدم مثال (٣ ـ ١٢)).

١٢) ليكن p عددًا أوليًا:
(ا) أثبت أنه توجد كثيرة حدود غير قابلة للتحليل درجتها اثنتين على Z_p
(ب) استخدم كثيرة الحدود في (ا) لتبني حقل رتبته p^2.
(جـ) لاحظ أن كل كثيرتي حدود تحققان الفقرة (ا) ينتج عنهما حقلان حسب الفقرة (ب)، أثبت أن هذين الحقلين متشاكلان.

١٣) أثبت أنّ الإغلاق الجبري للحقل $\mathbb{Q}$ في $\mathbb{C}$ يساوي الإغلاق الجبري للحقل $\mathbb{Q}(\sqrt{2})$ في $\mathbb{C}$.

١٤) أوجد Aut K إذا كان:
(ا) $K = \mathbb{Z}_2[x]/(x^2+x+1)$.
(ب) $K = \mathbb{Z}_3[x]/(x^2+1)$.

حقول الانشطـــار

تعريـــف (٤ - ١٠)

إذا كان F حقلا وكانت $f \in F[x]$ وكان K أصغر امتداد جبري يحوي F وتنشر أو تنشطر فيه (splitts) كثيرة الحدود f ، فإن K يسمى حقل الانشطار (splitting field) لكثيرة الحدود f على F ، لذلك إذا كان تحليل f على K هو:

$$f = \lambda(x-a_1)(x-a_2)\dots(x-a_n)$$

حيث $\lambda \in F$. فإن $K=F(a_1,\dots,a_n)$ وبالتالي فإن K مولد من قبل جذور f على الحقل F ، أي أنه أصغر امتداد جبري للحقل F يحوي كل جذور كثيرة الحدود f.

مثـــال (٤ - ٩)

اعتبر كثيرة الحدود $f=x^2-2 \in \mathbb{Q}[x]$. لمّا كانت:

$$f = (x-\sqrt{2})(x+\sqrt{2})$$

فإن جذري f وهما $\sqrt{2}, -\sqrt{2}$ ينتميان إلى الحقل $\mathbb{Q}(\sqrt{2})$، لذلك فإن $\mathbb{Q}(\sqrt{2})$ هو حقل الانشطار لكثيرة الحدود f على الحقل $\mathbb{Q}$.

مثـال (٤ - ١٠)

اعتبر كثيرة الحدود $f=x^2+1 \in \mathbb{R}[x]$ ، لما كانت

$$f = (x + i)(x - i)$$

فإن جذري f وهما $i, -i$ ينتميان إلى الحقل $\mathbb{R}(i) = \mathbb{C}$ وبالتالي فإن $\mathbb{C}$ هو حقل الانشطار لكثيرة الحدود f على الحقل $\mathbb{R}$.

تعريـف (٤ - ١١)

ليكن K_1, K_2 امتدادين للحقل F. نقول عن التشاكل ϕ من الحقل K_1 إلى الحقل K_2 إنّه تشاكل (F-isomorphism) على الحقل F إذا كان ϕ يثبت كل عنصر من F أي أنّ $\phi(x)=x$ لكل $x \in F$.

ملاحظـة (٤ - ٥)

التشاكل المذكور في التعريف السابق يمكن اعتباره تشاكلاً بين فضاءين متجهين K_1, K_2 على الحقل F.

نظريـة (٤ - ٨)

إذا كان F حقلا، $f \in F[x]$ عندئذ :

(i) يوجد حقل انشطار لكثيرة الحدود f على F.

(ii) أي حقلي انشطار لكثيرة الحدود f على F هما حقلان متشاكلان على F.

البرهـان

(i) إثبات وجود حقل الانشطار

باستخـدام نظريـة التحليل الـوحيد لتحليل f في $F[x]$ إلى عواملهـا غير القـابلة للتحليل نستنتج أنّ :

$$f = \lambda f_1 f_2 \dots f_r$$

حيث $\lambda \in F$ ، وحيث $f_1, f_2, \dots, f_r$ كثيرات حدود غير قابلة للتحليل على F. إذا كانت درجة كل من كثيرات الحدود f_i تساوي الواحد فإن F هو حقل الانشطار لكثيرة الحدود f على F ، لذلك نفرض أن درجة إحدى العوامل ولتكن $\deg f_1$ أكبر من الواحد. نستطيع أن نصنع امتدادا للحقل F بربطه أو إقرانه بالعنصر a_1 الذي هو جذر لكثيرة الحدود f_1 ويكون تحليل f في $F(a_1)[x]$ كما يلي :

$$f = \mu(x - a_1)\, g_1 g_2 \dots g_s$$

حيث $\mu \in F(a_1)$ وحيث $g_1, g_2, \dots, g_s$ كثيرات حدود غير قابلة للتحليل على $F(a_1)$. إذا كانت درجة كل من g_i تساوي الواحد فإن $F(a_1)$ يحوي جميع جذور f ، لذلك نفرض أنّ درجة أحد عوامل f في $F(a_1)[x]$ ولتكن $\deg g_1$ أكبر من الواحد. نستطيع أن نعمل امتدادا للحقل $F(a_1)$ بربطه أو إقرانه بالعنصر a_2 الذي هو جذر لكثيرة الحدود g_1 ونحصل على الحقل $F(a_1, a_2)$ وسيكون تحليل f في $F(a_1, a_2)[x]$ كما يلي :

$$f = \gamma(x - a_1)(x - a_2)\, h_1 \dots h_t$$

حيث $\gamma \in F(a_1, a_2)$ وحيث $h_1, \dots, h_t$ كثيرات حدود غير قابلة للتحليل على $F(a_1, a_2)$. إذا كانت درجة كل من h_i تساوي الواحد فإن $F(a_1, a_2)$ هو حقل الانشطار لكثيرة الحدود f على F وإلا نستمر بتمديده بالطريقة السابقة نفسها. نلاحظ أنّ كل امتداد بربط أو إقران الحقل بجذر لكثيرة حدود غير قابلة للتحليل من عوامل f سيعطينا عاملا خطيًّا واحدًا على الأقل من النوع $(x - a_i)$ ، لذلك بعد عدد منته من المرات من تمديد الحقل بربطه أو إقرانه بعنصر نصل إلى الحقل $F(a_1, \dots, a_n)$ الذي يحتوي على كل جذور f وبالتالي فإنه حقل الانشطار لكثيرة الحدود f على F.

(ii) إثبات وحدانية الانشطار

لكي نطبق طريقة الاستقراء الرياضي سنبرهن نتيجة أكثر أهمية وهي كما يلي :

ليكن τ_0 تشاكلا من الحقل F إلى الحقل $\bar{F}$ ولتكن $f \in F[x]$ صورة f تحت تأثير تمديد τ_0 إلى $F[x]$ [انظر منطوق المبرهنة (٤ - ٥)]. إذا كان K ، $\bar{K}$ حقلي الانشطار

لكثيرة الحدود f على F ولكثيرة الحدود $\bar{f}$ على $\bar{F}$ على الترتيب فإنه يمكن تمديد التشاكل τ_0 إلى تشاكل من K إلى $\bar{K}$.

إذا كان $F=\bar{F}$ وكانت τ_0 هي التشاكل المحايد من F إلى $\bar{F}$ فإن النتيجة المذكورة أعلاه تعطينا وحدانيّة حقل الانشطار لكثيرة الحدود تحت سقف التشاكل (up to isomorphism) على الحقل F.

البرهان

سنبرهن النتيجة باستخدام طريقة الاستقراء الرياضي على عدد الجذور، وليكن n ، لكثيرة الحدود f الموجودة خارج الحقل F. إذا كانت $n=0$ ، فإن F تحوي جميع جذور f ، أي أن f تنشر في F كحاصل ضرب عوامل خطيّة في F[x]. لذلك فإن $K=F$ ، $\bar{K}=\bar{F}$ ، τ_0 هي التشاكل المطلوب، سنفرض الآن فرضية الاستقراء الرياضي التالية:

إذا كان τ_1 تشاكلاً بين الحقلين $L,\bar{L}$ وكانت $g\in L[x],\bar{g}\in\bar{L}[x]$ حيث $\bar{g}$ صورة g تحت تأثير تمديد التشاكل τ_1 إلى L[x] ، إذا كان $K,\bar{K}$ حقلي الانشطار لـ $g,\bar{g}$ على $L,\bar{L}$ على الترتيب بحيث إن عدد جذور g خارج L هو أقل من n ، فإنه يمكن تمديد التشاكل τ_1 إلى تشاكل من K إلى $\bar{K}$..

إذا كان:

$$f = f_1 f_2 \dots f_r$$

تحليل f إلى عوامل غير قابلة للتحليل في F[x] ، فإن التحليل المناظر لكثيرة الحدود $\bar{f}$ في $\bar{F}[x]$ هو

$$\bar{f} = \bar{f}_1 \bar{f}_2 \dots \bar{f}_r$$

بما أنّ تمديد τ_0 إلى F[x] هو تشاكل من F[x] إلى $\bar{F}[x]$ فإن $\bar{f}_1,\dots,\bar{f}_r$ عوامل غير قابلة للتحليل في $\bar{F}[x]$. لمّا كنّا نعتبر $n>0$ ، فإنّنا سنفرض أنّ درجة أحد عوامل f أكبر من الواحد وليكن f_1 وبالتالي فإن درجة $\bar{f}_1$ أكبر من الواحد. لنفرض أن $a,\bar{a}$ جذرا $f_1,\bar{f}_1$ على الترتيب. سنكوّن الامتداد $L=F(a)$ والامتداد $\bar{L}=\bar{F}(\bar{a})$. نستطيع حسب

المبرهنة (٤ - ٥) تمديد τ_0 إلى تشاكل τ_1 من L إلى $\bar{L}$. نستطيع اعتبار f,$\bar{f}$ كثيرتي حدود في L[x],$\bar{L}$[x] على الترتيب، لذلك فإن عدد جذور f خارج L أقل من n. باستخدام فرضية الاستقراء الرياضي نستنتج أنه يمكن تمديد τ_1 إلى تشاكل من K إلى $\bar{K}$..

مثـال (٤ - ١١)

لاحظنا في المثال (٤ - ٣) أنّه إذا كان a جذرًا لكثيرة الحدود $g=x^2+x+1\in \mathbf{Z}_2[x]$ فإن $a^2=a+1$ هو الجذر الآخر، لذلك فإن $\mathbf{Z}_2(a)$ يحوي جميع جذور g ويحوي الحقل $\mathbf{Z}_2$، وبالتالي فهو حقل الانشطار لكثيرة الحدود g على $\mathbf{Z}_2$.

مثـال (٤ - ١٢)

لتكن $f=x^3+x+1\in \mathbf{Z}_2[x]$. لمّا كانت عناصر $\mathbf{Z}_2$ لا تمثل جذورًا لكثيرة الحدود f ولأنّ درجتها تساوي ثلاثة، فإن f غير قابلة للتحليل على $\mathbf{Z}_2$[الملاحظة (٣ - ٥)].

لقد سبق أن لاحظنا أنه إذا كان α جذرًا لكثيرة الحدود f فإن $L=\mathbf{Z}_2(\alpha)$ امتداد جبري بسيط للحقل $\mathbf{Z}_2$ يحوي الجذر α[النظرية (٤ - ١)]، كما نلاحظ أن α^2,α^4 جذران آخران لكثيرة الحدود f لأنّ:

$$(\alpha^2)^3+\alpha^2+1=(\alpha^3)^2+\alpha^2+1=(\alpha^3+\alpha+1)^2=0$$
$$(\alpha^4)^3+\alpha^4+1=(\alpha^3)^4+\alpha^4+1=(\alpha^3+\alpha+1)^4=0$$

باستخدام $\alpha^3+\alpha+1=0$ نستنتج أن α^2,α^4 عنصران مختلفان من الحقل L. لذلك فإن α,α^2,α^4 جذور مختلفة لكثيرة الحدود f وكلها موجودة في L ، وهكذا فإن L هو حقل الانشطار لكثيرة الحدود f على $\mathbf{Z}_2$ لأنه يحوي $\mathbf{Z}_2$ ويحوي جميع جذور f.

نلاحظ أنّ درجة امتداد الحقل L على $\mathbf{Z}_2$ هي درجة كثيرة الحدود f التي تساوي ثلاثة [النظرية (٤ - ٢)] لذلك فإن عدد عناصر L تساوي $2^3=8$ حيث إن:

$$L=\{\lambda_0+\lambda_1\alpha+\lambda_2\alpha^2:\lambda_0,\lambda_1,\lambda_2\in\mathbf{Z}_2\}$$
$$=\{0,1,\alpha,\alpha^2,1+\alpha,1+\alpha^2,\alpha+\alpha^2,1+\alpha+\alpha^2\}$$

سنثبت في موضوع الحقول المنتهية أنّه إذا كانت f كثيرة حدود غير قابلة للتحليل على $\mathbf{Z}_p$ وكانت درجتها r وكان α جذرا لها فإن $\mathbf{Z}_p(\alpha)$ هو حقل الانشطار لكثيرة الحدود f على $\mathbf{Z}_p$ علما بأن جذور f هي :

$$\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{r-1}}$$

مثـال (٤ - ١٣)

سننشىء في هذا المثال الحقل $\mathbb{Q}(\sqrt{2},\sqrt{3})$ على $\mathbb{Q}$. نلاحظ أن $\pm\sqrt{2},\pm\sqrt{3}$ هي جذور $x^2-3, x^2-2 \in \mathbb{Q}[x]$ على الترتيب، كما نشير إلى أنّ x^2-2 غير قابلة للتحليل على $\mathbb{Q}$ لأن درجتها على $\mathbb{Q}$ تساوي اثنتين ولأن جذريها لا ينتميان إلى $\mathbb{Q}$ [الملاحظة (٣ - ٥) أو انظر المثال (٣ - ١٠)]، لذلك يمكن حسب النظرية (٤ - ١) أن نحصل على :

$$F = \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2-2)$$

وبالتالي فإن F امتداد جبري بسيط للحقل $\mathbb{Q}$ درجته تساوي اثنتين وأساسه على $\mathbb{Q}$ هو $1,\sqrt{2}$ ، لذلك فإن :

$$F = \{\lambda_0 + \lambda_1\sqrt{2} : \lambda_0, \lambda_1 \in \mathbb{Q}\}$$

بما أن جذري (x^2-3) هما $\pm\sqrt{3}$ وبالتالي غير موجودين في F ولأن درجة (x^2-3) على F هي اثنتان، لذلك فإنّ (x^2-3) غير قابلة للتحليل على F ، وهكذا حسب النظرية (٤ - ١) فإن :

$$F(\sqrt{3}) \cong F[x]/(x^2-3)$$

كما أن درجة امتداد $F(\sqrt{3})$ على F هي اثنتان والمجموعة $\{1,\sqrt{3}\}$ تُشكّل أساسًا للحقل $F(\sqrt{3})$ على الحقل F [النظرية (٤ - ٢)]، لذلك فإن :

$$F(\sqrt{3}) = \{\mu_0 + \mu_1\sqrt{3} : \mu_0, \mu_1 \in F\}$$

باستخدام المبرهنة (٤ - ٧) نستنتج أنّ :

$$[F(\sqrt{3}) : \mathbb{Q}] = [F(\sqrt{3}) : F][F : \mathbb{Q}]$$
$$= 2 \times 2 = 4$$

كما أنّ عناصر الأساس للحقل $F(\sqrt{3})$ على $\mathbb{Q}$ هي $1,\sqrt{2},\sqrt{3},\sqrt{2}\sqrt{3}=\sqrt{6}$ وبالتالي فإن :

$$F(\sqrt{3}) = \{\lambda_0+\lambda_1\sqrt{2}+\lambda_2\sqrt{3}+\lambda_3\sqrt{6} : \lambda_0,\lambda_1,\lambda_2,\lambda_3 \in \mathbb{Q}\}$$

حيث إن $F(\sqrt{3})$ يحوي الحقل $\mathbb{Q}$ ويحوي جميع جذور $f=(x^2-3)(x^2-2)$ فإنّه حقل الانشطار لكثيرة الحدود f على الحقل $\mathbb{Q}$.

مثـال (٤ ـ ١٤)

سنجد حقل الانشطار لكثيرة الحدود $g=x^3-2 \in \mathbb{Q}[x]$ على $\mathbb{Q}$ ودرجة امتداده وأساسه على $\mathbb{Q}$ باعتباره فضاء متّجها. يعلم القارىء من دراسته قبل الجامعية وباستخدام طريقة المميّز في تحليل كثيرات الحدود أن:

$$x^3-2=(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$$
$$=(x-\sqrt[3]{2})(x+\omega\sqrt[3]{2})(x+\omega^2\sqrt[3]{2})$$

حيث $\omega=\frac{-1+\sqrt{3}i}{2}$. ليكن $F=\mathbb{Q}(\sqrt[3]{2})$. لمّا كانت جذور g لا تنتمي إلى $\mathbb{Q}$ ودرجتها ثلاثة فإن g غير قابلة للتحليل على $\mathbb{Q}$ [الملاحظة (٣ ـ ٥) أو مثال (٣ ـ ١٠)]، وبالتالي فإن F امتداد جبري بسيط للحقل $\mathbb{Q}$ [النظرية (٤ ـ ١)] درجته ثلاثة وأساس F على $\mathbb{Q}$ كفضاء متجه [النظرية (٤ ـ ٢)] هو:

$$1, \sqrt[3]{2}, \sqrt[3]{4}$$

وبالتالي فإن:

$$F=\{\lambda_0+\lambda_1\sqrt[3]{2}+\lambda_2\sqrt[3]{4} : \lambda_0,\lambda_1,\lambda_2 \in \mathbb{Q}\}$$

لمّا كان F حقلاً جزئيًا من حقل الأعداد الحقيقية فإن F لا يحوي الجذرين المركّبين (التخيلين) الآخرين لكثيرة الحدود g. اعتبر الحقل $F(\omega)$، من الواضح أن $F(\omega)$ يحوي الجذرين المركبين لكثيرة الحدود g وكذلك $F(\omega)=F(\alpha)$ حيث $\alpha=\sqrt{3}\,i$. لما كان $\alpha^2=-3$، لذلك فإن α هو جذر لكثيرة الحدود $f=x^2+3$ وهي غير قابلة للتحليل على F لأنّ جذريها $\pm\alpha$ غير موجودين في F ودرجتها على F تساوي اثنتين، لذلك فإن $F(\alpha)$ يُشكّل امتدادًا جبريًا بسيطًا للحقل F كما أنّ أساسه كفضاء متّجه على F هو $1,\alpha$ وبالتالي فإن:

$$F(\alpha)=\{\mu_0+\mu_1\alpha : \mu_0,\mu_1 \in F\}$$

لما كان $F(\alpha)$ يحوي جميع جذور f ويحوي الحقل F فإنه حقل الانشطار لكثيرة الحدود f على الحقل F. باستخدام المبرهنة (٤ ـ ٧)، نستنتج أنّ:

$$[F(\alpha) : \mathbb{Q}] = [F(\alpha) : F][F : \mathbb{Q}]$$
$$= 2 \times 3 = 6$$

أي أنّ درجة امتداد $F(\alpha)$ على $\mathbb{Q}$ هي ستة، كما أن عناصر أساسه على $\mathbb{Q}$ هي :

$$1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{3}\,i, \sqrt[3]{2}\sqrt{3}\,i, \sqrt[3]{4}\sqrt{3}\,i$$

وبالتالي فإن :

$$F(\alpha) = \{\lambda_0 + \lambda_1 \sqrt[3]{2} + \lambda_2 \sqrt[3]{4} + \lambda_3 \sqrt{3}\,i + \lambda_4 \sqrt[3]{2}\sqrt{3}\,i$$
$$+ \lambda_5 \sqrt[3]{4}\sqrt{3}\,i : \lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5 \in \mathbb{Q}\}$$

بما أن $F(\alpha)$ هو أصغر حقل يحوي $\mathbb{Q}$ ويحوي جميع جذور g ، لذلك فإن $F(\alpha)$ هو حقل الانشطار لكثيرة الحدود g على الحقل $\mathbb{Q}$.

مثـال (٤ ـ ١٥)

لتكن $\alpha=\sqrt{2}+i$ ، سنجـد كثـيرة الحدود g التي يكون $\mathbb{R}(\alpha)$ حقل انشطار لها على الحقـل $\mathbb{R}$. نلاحظ أنّ $\alpha-\sqrt{2}=i$ وبالتالي $(\alpha-\sqrt{2})^2=-1$ ، أي أنّ α جذر لكثيرة الحـدود $g=x^2-2\sqrt{2}\,x+3$. لما كان $\sqrt{2}-i$ هو الجـذر الآخـر لكثيرة الحدود g فإنها غير قابلة للتحليل على الحقـل $\mathbb{R}$ لأنّ درجتهـا تساوي اثنتين وجذراها لا ينتميان إلى $\mathbb{R}$ [المـلاحـظة (٣ ـ ٥)]. هذا من ناحية ومن ناحية أخرى فإن $\mathbb{R}(\alpha)$ يحوي الحقل $\mathbb{R}$ ويحـوي جميع جذور g لذلك فهو يمثّل حقل انشطار لكثيرة الحدود g على الحقل $\mathbb{R}$. لما كان $\alpha, \sqrt{2} \in \mathbb{R}(\alpha)$ ، فإن $i=\alpha-\sqrt{2} \in \mathbb{R}(\alpha)$ وبـالتالي فإن $\mathbb{C} = \mathbb{R}(i) \supset \mathbb{R}(\alpha)$ ، ولكن $\mathbb{C} \supset \mathbb{R}(\alpha)$ ، إذن $\mathbb{C} = \mathbb{R}(\alpha)$.

مثـال (٤ ـ ١٦)

سنجـد الآن كثـيرة حدود g والتي يكون $\mathbb{Q}(\alpha)$ حقل انشطار لها على $\mathbb{Q}$ حيث $\alpha=\sqrt{2}+i$. نلاحظ أنّ $\alpha^2=1+2\sqrt{2}\,i$ وبـالتـالي فإنّ $(\alpha^2-1)^2=-8$ ، لذلـك فإن α هو جذر لكثيرة الحدود $g=x^4-2x^2+9$. يستطيع القارىء بسهولة أن يستنتج أنّ جذور g الأخرى هي :

$$-\sqrt{2}+i\,,\ \sqrt{2}-i\,,\ -(\sqrt{2}+i)$$

وبالتالي فإن :

$$g = (x - \sqrt{2} - i)(x + \sqrt{2} + i)(x - \sqrt{2} + i)(x + \sqrt{2} - i)$$
$$= (x^2 - 2\sqrt{2}x + 3)(x^2 + 2\sqrt{2}ix + 3)$$

لذلك فهي كثيرة حدود غير قابلة للتحليل على $\mathbb{Q}$ ، وهذا يؤدي إلى أن g تمثل كثيرة الحدود الصغرى للعنصر α على $\mathbb{Q}$ [النظريـــة (٤ - ١)]. لذلك فإن درجة امتداد $\mathbb{Q}(\alpha)$ على $\mathbb{Q}$ هي أربـعةوعناصر الأساس له على $\mathbb{Q}$ هي $1,\alpha,\alpha^2,\alpha^3$ [النظـريـة (٤ - ٣)]. وبالتالي فإن :

$$\mathbb{Q}(\alpha) = \{\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3 : \lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}\}$$

نلاحظ أنّ $\alpha^3+\alpha=6i$ حيث إن $\alpha^3=5i-\sqrt{2}$.

لذلك فإن $i \in \mathbb{Q}(\alpha)$ ، ولكن $\alpha-i=\sqrt{2}$ ، إذن $\sqrt{2} \in \mathbb{Q}(\alpha)$ وبالتالي فإن كل جذور g تنتمي إلى $\mathbb{Q}(\alpha)$ ، وبما أن $\mathbb{Q}(\alpha)$ يحوي $\mathbb{Q}$ إذن $\mathbb{Q}(\alpha)$ هو حقل الانشطار لكثيرة الحدود g على $\mathbb{Q}$.

الحقــول المنتهيــة

تعريــف (٤ - ١٢)

الحقل المنتهي أو حقل جالوا (Galois field) هو حقل عدد عناصره منته.

مثــال (٤ - ١٧)

الحقل Z_p هو حقل منته، حيث p عدد أولي.

مبرهنــة (٤ - ٩)

أي حقل منته F تكون رتبته p^r ، حيث p عدد أولي، r عدد صحيح موجب.

البرهــان

لما كان F حقــلا منتهيًا فإن مميّز F يســاوي عددا أوليا p ، وبــالتــالي فإن

Z_p حقل جزئي من F. نستطيع أن نعتبر F كفضاء متجه، ولكون F حقل منته فإن بعده كفضاء متجه على Z_p منته وليكن r ، وبالتالي فإن $|F|=p^r$.

نظريـــة (٤ - ١٠)

إذا كان p عددًا أوليًا وإذا كان r عددًا صحيحًا موجبًا فإنه يوجد حقل F رتبته p^r.

البرهـــان

اعتبر كثيرة الحدود $f=x^{p^r}-x\in Z_p[x]$ وليكن K حقل الانشطار لكثيرة الحدود f على Z_p. نلاحظ أنّ $f'=-1$ ، لذلك فإنه لا يوجد جذور مشتركة بين f, f' وهذا يؤدي إلى أن كل جذور f مختلفة [المبرهنة (٣ - ١٥)]، لذلك فإن عددها p^r لتكن $\xi_1,\xi_2,\ldots,\xi_{p^r}$ جذورًا لـ f ولنفرض أنّ $F=\{\xi_1,\xi_2,\ldots,\xi_{p^r}\}$ إذا كانت $a,b\in F$ فإن :

$$(a+b)^{p^r}=a^{p^r}+b^{p^r}$$

[انـظر التمـرين (٢ - ١ - ٨)]. لما كانت $a,b\in F$ فهي جذور لكثيرة الحدود f وبالتالي فإن $a^{p^r}=a,\ b^{p^r}=b$ لذلك فإن :

$$(a-b)^{p^r}=a^{p^r}-b^{p^r}=a-b$$

كذلك :

$$(a\,b)^{p^r}=a^{p^r}\,b^{p^r}=a\,b$$

لذلـك فإن $a\,b,\ a-b\in F$. إذا كان a عنصرًا غير صفـري في F فإن a^{-1} موجـود في K ، لذلك فإن :

$$(a^{-1})^{p^r}=(a^{p^r})^{-1}=a^{-1}$$

أي أنـه إذا كان a عنصرا غير صفـري في F فإن $a^{-1}\in F$. وهكـذا فإن F حقل جزئي من K. ولكـون F حقـلاً منتهيًا مميّزه p لذلـك فإن Z_p حقـل جزئي من F ، وبالتالي فإن F يحوي Z_p وجميع جذور f محتواة في F لذلك فإن $K=F$.

نتيجـــة (١)

أيّ حقل منته F رتبته p^r هو حقل الانشطار لكثيرة الحدود $f=x^{p^r}-x$ على Z_p.

البرهـــان

من الواضح أنّ Z_p حقل جزئي من F. حيث إن زمرة الوحدات للحقل F هي F^* لذلك فإنه لكل $x \in F^*$:

$$x^{p^r-1} = 1$$

وهكذا فإن :

$$x^{p^r} = x$$

لكل $x \in F^*$. ولما كانت العلاقة الأخيرة صحيحة أيضًا للصفر فإن :

$$x^{p^r} = x$$

لكل $x \in F$ وهكذا فإن أي عنصر في F هو جذر لكثيرة الحدود f ، لذلك فإن F هو حقل الانشطار لكثيرة الحدود f على Z_p لأنّه يحوي جذور f ويحوي Z_p .

نتيجـــة (٢)

أي حقلين منتهيين لهما عدد العناصر نفسه هما حقلان متشاكلان .

البرهـــان

ليكـــن F,F′ حقـلين منـتـهـيين بحـيث $|F'|=|F|=p^r$ ، حيث p عدد أولي، r عدد صحيح موجب. حسب النتيجـة السـابقة فإن F.F′ هما حقلا انشطار لكثيرة الحدود $x^{p^r}-x$ على Z_p لذلك فهما متشاكلان .

سنحتاج المبرهنة التالية من نظرية الزمر:

مبرهنـــة (٤ ـ ١١)

إذا كانت G زمرة إبداليّة منتهية بحيث يكون للمعادلة $x^n=1$ عدد n من الحلول على الأكثر في G لكل عدد صحيح موجب n ، فإن G زمرة دائريّة .

البرهـــان

لتكن رتبـة G تسـاوي n ولتكن G′ زمـرة دائـريّة رتبتهـا n. إذا كانت G زمرة

غير دائريّة فإنه يوجد قاسم فعلي d للعدد n بحيث تكون عدد عناصر G التي رتبتها d أكثر من عدد عناصر G' التي رتبتها d وإلاّ فإنه يجب أن يكون عدد عناصر الزمرة G التي رتبتها n بقدر أو أقل من عدد عناصر الزمرة الدائريّة G' التي رتبتها n. لتكن λ,λ' عدد العناصر التي رتبتها d في G,G' على التوالي، بالتالي فإن $\lambda>\lambda'$. لما كانت G' زمرة دائرية فإن جميع العناصر التي رتبتها d وعددها λ' في G' تُولّد الزمرة الجزئية نفسها والتي رتبتها d ، ولكن $\lambda>\lambda'$ ، إذن عناصر G التي رتبتها d يجب أن تُولّد على الأقل زمرتين جزئيّتين H_1,H_2 رتبة كل منهما d. لذلك فإن $x^d=1$ لكل $x\in H_1\cup H_2$ ، ولكن $|H_1\cup H_2|>d$ وهذا يناقض الفرض، لذلك فإن G زمرة دائرية.

نتيجة (١)

إذا كانت G زمرة جزئية منتهية من زمرة الوحدات لحقل، فإن G زمرة دائرية.

البرهان

بما أن للمعادلة $x^n=1$ عدد n من الحلول على الأكثر في أي حقل، حيث n عدد صحيح موجب، فإن G زمرة دائرية.

نتيجة (٢)

زمرة الوحدات لحقل منتهٍ زمرة دائرية.

نتيجة (٣)

الحقل المنتهي له حقل جزئي وحيد ذو رتبة معينة.

البرهان

يمكن برهنة النتيجة باستخدام المبرهنة في نظرية الزمر التي تنص على «أن كل زمرة جزئية من زمرة دائرية منتهية G تكون وحيدة كزمرة جزئية من G ذات رتبة معينة».

ملاحظـة (٤ - ٦)

ليكن $n = mk$ ، لما كانت

$$y^k - 1 = (y-1)(y^{k-1} + y^{k-2} + \dots + y + 1)$$

فإن $p^m - 1 | p^n - 1$ وذلـك بفـرض $y = p^m$. لتكن $p^n - 1 = k(p^m - 1)$ ، بوضـع $y = x^{p^{m-1}}$ فـإن $x^{p^m - 1} - 1 | x^{p^n - 1} - 1$ وبالتالي فإن :

$$x^{p^m} - x \mid x^{p^n} - x$$

مبرهنـة (٤ - ١٢)

إذا كان K حقلاً منتهيًا رتبته p^n ، حيث p عدد أولي، n عدد صحيح موجب، فإن K يحوي حقلاً جزئيًا رتبته p^m إذا وإذا فقط كان $m|n$.

البرهـان

ليكن F حقلاً جزئيًا من K رتبته p^m حيث p عدد أولي . نستطيع اعتبار K كفضاء متّجه على F وبالتالي فإن بعده على F منته وليكن r ، لذلك فإن $\dim_F K = r$ وأيضًا $|K| = |F|^r$ وبالتالي $p^n = p^{mr}$ ، وهذا يعني أنّ $n = mr$.

ليكن $n = m\,r$ ، حسب الملاحظة السابقة فإن :

$$x^{p^m} - x \mid x^{p^n} - x$$

نلاحظ أنّ حقل الانشطار لكثيرة الحدود $x^{p^n} - x \in \mathbf{Z}_p[x]$ على $\mathbf{Z}_p$ هو K [النتيجة (١) للنظريـنة (٤ - ١٠)] وهو يحوي جميع جذور $x^{p^m} - x$ وبالتالي يحوي حقل انشطارها على $\mathbf{Z}_p$، لكن حقل انشطار $x^{p^m} - x$ هو حقل رتبته p^m ، لذلك فإن K يحوي حقلاً جزئيًا رتبته p^m.

مثـال (٤ - ١٨)

إذا كان F حقلاً منتهيًا رتبته p^{40} ، حيث p عدد أولي، فإن رتب جميع الحقول الجزئية الفعليّة منه هي :

$$p, p^2, p^4, p^5, p^8, p^{10}, p^{20}$$

أي أنّ القواسم الفعليّة للعدد 40 هي التي تحدد الحقول الجزئيّة الفعليّة من الحقل الذي رتبته p^{40}.

نتيجـة

إذا كان الحقلان $G\,F(p^m)$.$G\,F(p^n)$ حقلين جزئيّين من حقل منته L فإن

$$G\,F(p^m) \cap G\,F(p^n) = G\,F(p^d)$$

حيث $d=(m.n)$. $G\,F(p^r)$ ترمز لحقل منته (حقل جالوا) رتبته p^r.

البرهـان

ليكـن $F=G\,F(p^n)$.$K=G\,F(p^m)$ ولـيكـن $K\cap F=G\,F(p^s)$. نلاحظ أن $K\cap F$ حقل جزئي من F وحقل جزئي من K وبالتالي فإن s n وكذلك s m وهكذا فإن s d ، وهذا يؤدي إلى أن $G\,F(p^d)\supset K\cap F$ ، من ناحية أخرى d|n ، d|m يعني أن $G\,F(p^d)$ محتواة في F ومحتواة في K ، لذلك فإن $K\cap F\supset G\,F(p^d)$ وبالتالي فإن :

$$K \cap F = G\,F(p^d)$$

مثـال (٤ - ١٩)

لتكن $f=x^6+x^4+x+1$. لإيجاد حقل الانشطار لكثيرة الحدود f على Z_2 نلاحظ أنّ

$$f = (x + 1)(x^5 + x^4 + 1)$$
$$= (x + 1)(x^2 + x + 1)(x^3 + x + 1)$$

وبالتالي فإن حقل الانشطار لكثيرة الحدود f على Z_2 هو حقل الانشطار لكثيرة الحدود $g=x^5+x^4+1$ على Z_2. لتكن $g_1=x^2+x+1$. $g_2=x^3+x+1$ ، لقـد لاحـظنـا في مثـال (٤ - ١١) أنّ $F=Z_2(\alpha)$ هو حقل الانشطار لكثيرة الحدود g_1 على Z_2 وأن $F=G\,F(2^2)$ ، حيث α هو جذر لـ g_1. كما لاحظنا في مثال (٤ - ١٢) أن حقل الانشطار لكثيرة الحدود g_2 على Z_2 هو $K=G\,F(2^3)$ ، وبالتالي فإن $K\cap F=Z_2$ (انظر النتيجة السابقة)، وهذا يعني أنّ F لا يحوي أي جذر لكثيرة الحدود g_2. لما كانت درجة g_2 على F تساوي ثلاثة لذلك فهي غير قابلة للتحليل على F حسب الملاحظة (٣ - ٥). لنعمل الآن امتدادًا

للحقل F بربطه بأحد جذور g_1 وليكن β. باستخدام الطريقة نفسها في مثال (٤ - ١٢) نستنتج أن $\beta^{-1}.\beta^{-2}.\beta^{-3}$ تمثل جذور g_1 ، ولكنّها محتواة في $F(\beta)$ ، لذلك فإن $F(\beta)$ هو حقل الانشطار لكثيرة الحدود g_1 على F وهكذا فإن $Z_1(\alpha.\beta)$ هو حقل الانشطار لكثيرة الحدود g على Z_1. وبالتالي فهو يمثل حقل الانشطار لكثيرة الحدود f على Z_1.

مبرهنة (٤ - ١٣)

إذا كان $F=G\,F(p^n)$ وإذا كانت $f=x^{p^m}-x$ فإن عدد جذور f في F هو p^d حيث $d=(m.n)$.

البرهان

ليكن L حقل الانشطار لكثيرة الحدود f على F وليكن K حقل الانشطار لكثيرة الحدود f على Z_p. من نتيجة النظرية (٤ - ١٠) نستنتج أنّ $K=G\,F(p^m)$. لما كان F.K حقلين جزئيّين من L ، فإن $K\cap F=G\,F(p^d)$ حسب النتيجة السابقة. لما كانت عناصر K هي جذور f ، فإن عدد جذور f في F هو عدد عناصر $K\cap F$ ، وهكذا فإن عدد جذور f في F هو p^d.

مبرهنة (٤ - ١٤)

لأيّ حقل منته F ولأيّ عدد صحيح موجب r ، فإنه توجد كثيرة حدود $f\in F[x]$ ذات درجة r وغير قابلة للتحليل على F.

البرهان

ليكن $K=G\,F(p^{nr})$ امتداداً للحقل $F=G\,F(p^n)$. بما أنّ K حقل منته، فإن $K^*=<\alpha>$. لما كان $F(\alpha)$ يحوي K^* وبالتالي K ، فإن $K=F(\alpha)$. نلاحظ أنّ α جذر كثيرة الحدود $x^{p^{nr}}-x\in Z_p[x]$. لذلك فإن α عنصر جبري على Z_p وبالتالي عنصر جبري على F وهكذا فإن K امتداد جبري بسيط للحقل F بربطه بالعنصر α. باستخدام المبرهنة (٤ - ١) نستنتج أنّ:

$$K \cong F[x] / (f)$$

حيث f هي كثيرة الحدود الصغرى للعنصر α على F ودرجتها تساوي درجة امتداد K على F ، أي تساوي r.

نتيجة

أي حقل منته يمكن تمديده إلى امتداد جبري بسيط وبالتالي لا يمكن أن يكون مغلقًا جبريًا.

نظرية (٤ - ١٥)

إذا كان $F=G\,F(p^r)$ فإن زمرة التشاكلات الذاتية Aut F زمرة دائرية رتبتها r .

البرهان

لقد سبق أن أثبتنا أن التطبيق ϕ المعرف بالقاعدة $\phi(x)=x^p$ من الحقل F إلى F ، يمثّل تشاكلاً ذاتيًا للحقل F (انظر تمرين ٢ - ١ - ٨). كما نلاحظ أنه لكل $x\in F$ فإن :

$$\phi^r(x)=\phi^{r-1}\,\phi(x) = \phi^{r-1}(x^p) = \phi^{r-2}(x^{p^2}) = \ldots = x^{p^r}$$

ولكن $x^{p^r}=x$ لكل $x\in F$ [انظر إثبات المبرهنة (٤ - ١٠)]، لذلك فإن :

$$\phi^r(x) = x$$

لكل $x\in F$ ، وبالتالي فإن $\phi^r=i\,d_F$. اعتبر الزمرة الجزئية من Aut F المولّدة من قبل ϕ ، نودُّ أن نبرهن أن رتبتها تساوي r. نفرض أنّ :

$$\phi^i = \phi^j \quad . \quad 1 \leq i, j \leq r$$

وهذا يعني أن :

$$x^{p^i} = x^{p^j}$$

لكل $x\in F$ ، لذلك فإن كل عناصر الحقل F هي جذور لكثيرة الحدود :

$$x^{p^i}\,(x^{p^j-p^i} - 1)$$

على فرض أنّ $i<j$ ، وبالتالي فإن كل عناصر F^* هي جذور لكثيرة الحدود :

$$x^{p^j-p^i}-1$$

وهذا تناقض لأنّ $p^j-p^i<p^r-1$ لذلك فإن :

$$\phi, \phi^2, \ldots, \phi^r = i\,d_F$$

هي عناصر مختلفة من Aut F وبالتالي فإن رتبة ϕ تساوي r. الآن نودُّ أن نثبت أنّ رتبة Aut F أقل من أو تساوي r. حيث F حقل منته فإن F^* زمرة دائرية. لتكن $F^*=<\alpha>$ ، وبالتالي فإن $F=\mathbf{Z}_p(\alpha)$. لتكن f هي كثيرة الحدود الصغرى للعنصر α على $\mathbf{Z}_p$. بما أنّ درجة امتداد F على $\mathbf{Z}_p$ تساوي r ، لذلك فإن درجة f تساوي r. لنفرض أنّ

$$f=\sum_{i=0}^{r} a_i x^i$$

حيث $a_i \in \mathbf{Z}_p$ ولنفرض أنّ $\varphi \in$ Aut F. بما أنّ φ يثبّت العنصر المحايد، فإنه يثبّت عناصر $\mathbf{Z}_p$. لما كان α جذرًا لكثيرة الحدود f ، فإن :

$$0=f(\alpha)=\sum a_i \alpha^i$$

وبالتالي فإن :

$$\begin{aligned} 0=\varphi(0)=\varphi(f(\alpha))=\varphi(\sum a_i \alpha^i)&=\sum \varphi(a_i)\,\varphi(\alpha^i)\\ &=\sum a_i\,(\varphi(\alpha))^i\\ &=f(\varphi(\alpha)) \end{aligned}$$

لذلك إذا كانت $\varphi \in$ Aut F فإن $\varphi(\alpha)$ جذر آخر لكثيرة الحدود f. لما كان تأثير φ يتحدد على F بتأثيره على العنصر البدائي α ، فإن عدد التشاكلات الذاتيّة للحقل F لا يمكن أن تزيد عن جذور f التي عددها على الأكثر r ، لذلك فإن :

$$|\text{Aut } F| \leq r$$

وبالتالي فإن : $\text{Aut } F=<\phi>$.

نتيجـة

إذا كانت f كثيرة حدود غير قابلة للتحليل على الحقل $\mathbf{Z}_p$ ودرجتها r ، فإن الحقل $F=\mathbf{Z}_p[x]/(f)$ هو حقل الانشطار لكثيرة الحدود f على $\mathbf{Z}_p$.

البرهـــان

لما كانت درجة امتداد F على Z_p هي درجة كثيرة الحدود f [النظرية (٤ - ٢)] والتي تساوي r ، لذلك فإن $F=G\ F(p^r)$. لقد سبق أن لاحظنا في إثبات النظرية (٤ - ٤) أن $a=x+(f)$ هو أحد الجذور لكثيرة الحدود f في الحقل F وبالتالي فإن $Z_p(a)=F$. إذا كان $\varphi \in Aut\ F$ فإن $\varphi(a)$ جذر آخر لكثيرة الحدود f (انظر إثبات النظرية السابقة). لما كان تأثير φ على F يتحدد بتأثيره على العنصر البدائي a للحقل F ، لذلك فإن كل تشاكل ذاتي φ في Aut F يعطينا جذرًا لكثيرة الحدود f في الحقل F ، وحيث إن رتبة Aut F تساوي r ، لذلك فإنه يوجد عدد r جذر من جذور f في F. لكن درجة f تساوي r ، إذن كل جذور f في الحقل F ، وهكذا فإن F هو حقل الانشطار لكثيرة الحدود f على Z_p.

تمـاريـــن (٤ ـ ٢)

١) لتكن $f=x^2+\alpha x+\beta \in F[x]$ ، حيث F حقل. إذا كان K أي امتداد للحقل F يحوي جذرًا لـ f ، فأثبت أنّ K يحوي حقل الانشطار لكثيرة الحدود f على الحقل F.

٢) أنشىء الحقل $\mathbb{Q}(\sqrt{5},\sqrt{7})$ على الحقل $\mathbb{Q}$ وأوجد درجة امتداده على $\mathbb{Q}$ وأساسه كفضاء متّجه على $\mathbb{Q}$. ما هي كثيرة الحدود التي يكون لها $\mathbb{Q}(\sqrt{5},\sqrt{7})$ حقل انشطار على $\mathbb{Q}$. هل $\mathbb{Q}(\sqrt{5},\sqrt{7})=\mathbb{Q}(\sqrt{5}+\sqrt{7})$ ؟

٣) أنشىء الحقل $\mathbb{Q}(\sqrt{5}+\sqrt{2})$ على الحقل $\mathbb{Q}$ وأوجد درجة امتداده على $\mathbb{Q}$ وأساسه كفضاء متّجه على $\mathbb{Q}$. ما هي كثيرة الحدود التي يكون لها $\mathbb{Q}(\sqrt{3}+\sqrt{2})$ حقل انشطار على $\mathbb{Q}$.

٤) أوجد حقل الانشطار ودرجة امتداده على $\mathbb{Q}$ لكثيرات الحدود التالية :

(أ) x^4+1

(ب) x^4-2

(جـ) x^6+1

(د) x^4-5x^2+6

٥) أوجد حقل الانشطار لكثيرة الحدود x^p-1 على $\mathbb{Q}$ حيث p عدد أولي [استخدم المثال (٣ - ١٢)].

٦) ليكن $F=GF(p^r)$ ، α العنصر الابتدائي للحقل F على $\mathbf{Z}_p$ ، f كثيرة الحدود الصغرى للعنصر α على $\mathbf{Z}_p$ وليكن $\alpha=\alpha_1,\alpha_2,\ldots,\alpha_r$ جذور f. أثبت أن :

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_r \\ \alpha_1^p & \alpha_2^p & \ldots & \alpha_r^p \end{pmatrix}$$

عبارة عن تبديل دائري (cyclic permutation) على مجموعة الجذور $\{\alpha_1,\alpha_2,\ldots,\alpha_r\}$.

٧) أثبت أنّ $(p-1)!\equiv -1 \bmod p$ ، حيث p عدد أولي، تسمى هذه بنظرية ولسون (Wilson's theorem) (إرشاد: لاحظ أنّ الحقل $\mathbf{Z}_p$ هو حقل الانشطار لكثيرة الحدود x^p-x على $\mathbf{Z}_p$).

٨) ليكن $K=GF(p^{nr})$ ، $F=GF(p^n)$ حقلاً جزئيًّا من K. أثبت أنّ زمرة التشاكلات الذاتيّة للحقل K التي تثبّت كل عنصر من عناصر F ، ويرمز لها بالرمز $Aut_F K$ ، هي زمرة دائرية رتبتها r.

٩) ليكن $F=GF(p^n)$ ، $f\in F[x]$ كثيرة حدود غير قابلة للتحليل على F درجتها r. أثبت أنّ $K=F[x]/(f)$ هو حقل انشطار كثيرة الحدود f على F.

١٠) ليكن $K=GF(p^n)$ ، وليكن $\varphi_i(x)=x^{p^i}$ لكل $x\in K$. ضع $F=\{x\in K:\varphi_i(x)=x\}$.
(ا) أثبت أنّ F حقل جزئي من K وأوجد رتبته .
(ب) أوجد $Aut_F K$ وما هي رتبتها .

المراجع

References

[١] Burton, D.M. *Introduction to modern abstract Algebra*. Reading, Massachusetts: Addison - Wesley, 1967.

[٢] ———. *A first course in rings and ideals*. Reading, Massachusetts: Addison - Wesley, 1970.

[٣] Halmos, P. *Naive set theory*. New York: Springer - Verlag, 1960.

[٤] Hartley, B. and Hawkes, T.O. *Rings, Modules and Linear Algebra*. London, New York: Chapman and Hall, 1991.

[٥] Herstein, I.N. *Topics in Algebra*. New York: John Wiley and sons, 1977.

[٦] Hungerford, T.W. *Algebra*. New York: Springer - Verlag, 1984.

[٧] Jacobson, N. *Algebra*, Vol. 1. San Francisco: W.H. Freeman and Company, 1985.

[٨] Kochendorffer, R. *Introduction to Algebra*. The Netherland: Wolters - Noordhoff, 1972.

[٩] Lang, S. *Algebra*. Reading, Massachusetts: Addison - Wesley, 1984.

[١٠] Maclane, S. and Birkhoff, G. *A survey of modern Algebra*. New York: Macmillan, 1977.