الجبر الحديث

لطلاب الدراسات التمهيدية والعليا

تأليف

سيرجيت سينج　　كازي زاميرو دين

ترجمة

د. محمود إبراهيم عزوز
د. بروين علي حمادي
أ. حسن جياد سواري

Modern Algebra　Modern Algebra　Modern Algebra　Modern Algebra

مَنْشورَات
جَامِعَة عُمَر المُخْتَار
البَيْضَاء
2022

اسم الكتاب : الجبر الحديث
اسم المترجم : محمود إبراهيم عزوز / بروين علي حمادي / حسن جياد سواري
رقم الإيداع : 2017/106م

دار الكتب الوطنية بنغازي – ليبيا

منشورات

جامعة عمر المختار

البيضاء

الترقيم الدولي

ردمك ISBN 978-9959-79-074-3

محتويات الكتاب

أولاً – فهرس الموضوعات

الموضوع	الصفحة

الفصل الثامن

الهومومورفزمات وغمر الحلقات

الفصل التاسع

حلقة كثيرات الحدود

الفصل العاشر

نظرية التحليل في الساحات التامة

الفصل الحادي عشر

الفضاءات المتجهة

الفصل الثاني عشر
التحويلات الخطيـة

الفصل الثالث عشر
الحقــول

الفصل الرابع عشر
نظرية جالوا

الفصل الخامس عشر
حلقات تحقق شروط السلسلة

الموضوع	الصفحة

الفصل السادس عشر

الصيغ القانونيــة

مقدمة الطبعة الأولى

خلال القرن الحالي حدث نمو سريع للكثير من المصطلحات والمفاهيم في الجبر الحديث ، واقترن الكثير من المصطلحات الجديدة والفروع بهذا المقرر .

هذا النمو السريع يجعل من الصعب على الفرد متابعة جملة هذه الأفكار .

في أي كتاب تمهيدي مثل كتابنا هذا فإنه من الصعب جداً على الشخص أن يلقى نظرة شاملة على التطورات التي تأخذ مساحة على موضوعات الجبر الحديث هذه الأيام وأن كل ما نوقش هنا يمكن اعتباره جزءً كلاسيكياً من الجبر الحديث ، على الرغم من شعورنا بأن هذا الجزء أساسي لكل التطورات التي حدثت في هذا الموضوع .

أهمية الجبر في الهند وقد أدركت في نهاية الخمسينات وفي وقت قريب فإن الكثير من الجامعات بتلك الدولة قررت مقررات في تلك المادة في كل من الدراسات العليا والدراسات التمهيدية لها . وكانت محتويات وتوصيف المقررات تختلف من مكان لآخر .

إنه من الصعوبة أن نقرر بدقة إلى أي مدى يمكن للمقرر التمهيدي في الجبر الحديث أن يكون لمستوى الدراسات العليا أو الدراسات التمهيدية لها لأن الرأي في ذلك يختلف من فرد لآخر .

أي كان ما قدمناه في هذا الكتاب من مادة علمية ، فإننا نشعر أن خبرتنا التدريسية يجب تعلَّم إلى كل هؤلاء الذين يرغبون في متابعة الرياضيات .

هناك الكثير من الموضوعات مثل مسلمات بيانو في النظام العددي وبعض النماذج القانونية من المصفوفات على الحقول والنظريات العامة لنظرية الموديولات الشبكات وفضاءات الضرب الداخلي ... إلخ ، والتي يمكن أن تجد مكاناً مناسباً في أي كتاب تمهيدي للجبر الحديث .

ونضـع في الاعتبـار هـدف وحجـم الكتـاب الـذي يجـب أن يقـدم إلى القـارئ هنا .

لقد قدمنا وبنوع من التوسع النظرية الأساسية للأعداد (متضمنة خوارزمية إقليدس)، كـذلك المصـفوفات علـى الأعـداد المركبـة ، كمـا اسـتخدمنا الكثـير مـن حسـاب التفاضـل والتكامل في بناء الكثير من الأمثلة المتنوعة والتي قدمت في هذا الكتاب .

في الواقع ستكون قراءة هذا الكتاب مفيدة لهؤلاء الذين لديهم بعض المعرفة في الموضوعات التي ذكرت سابقاً .

ونحن في غاية الامتنان من هؤلاء الرياضيين الذين أفادتنا كتبهم وأوراقهم البحثية في مجال الجبر الحديث والتي أثرت معلوماتنا حول الموضوع ، ونشكر بعمق أستاذنا الموقر باتا تشاري بقسم الرياضيات من جامعة دلهي ، والذي كانت مقترحاته وتوجيهاته لها عظيم الأثر على هذا الكتاب .

وجزيل شكرنا لكل الأصدقاء والرفقاء خاصة د. رافيند ركومر الذي قدم لنا الكثير من التوجيهات والمقترحات القيمة . ونؤكد أن أي توجيه أو مقترح سيقدم كذلك أي تعليق أو نقد مؤثر فإننا سنضعه في الاعتبار وسنأخذ به من أجل تطوير هذا الكتاب .

سيرجيت سينج

غازي زمير الدين

مقدمة الطبعة السابعة

هذا الكتاب نقح تنقيحاً شاملاً ، فقد أعيد كتابة عدد كبير من براهين نظرياته ، بهدف زيادة وضوحها ، والكثير من التغييرات حدثت في مسائل المجموعات ، ولقد وردت به بعض المسائل التي أعتقد أنها صعبة ولكنها ممتعة للقارئ العادي وهناك مسائل وضع عليها علامة (*) والتي من وجهة نظرنا تعتبر صعبة للغاية للقارئ العادي ، أما تلك التي أشير إليها بالعلامة (**) فإنه يمكن تجاهلها للعاديين .

ونحن في غاية الامتنان لكثير من الأصدقاء والقراء لتقديرهم ونقدهم البناء لهذا الكتاب والذي حفظ لهذا الكتاب أن يكون مطلوباً على مدى سنوات .

شكرنا الخاص لكل من الأستاذ الدكتور جوبتا ، والأستاذ الدكتور نارانج ، وإلى الدكتور ديكيت ، والدكتور هاربانز لال ، ودكتور جار رام ، ودكتور كانا ، وذلك لتقديمهم المقترحات القيمة حول هذه الطبعة والطبعات السابقة .

إن أي مقترح بهدف تحسينات أكثر سوف يقدر كما ينبغي .

سيرجيت سفنج

مقدمة الطبعة العربية

بسم الله الرحمن الرحيم

الحمد لله رب العالمين ،،، والصلاة والسلام على الرحمة المهداة ، سيدنا وحبيب قلوبنا محمد الصادق الأمين ، وعلى آله الطيبين الطاهرين ، وعلى صحبه أجمعين ، ومن تبع سنته إلى يوم الدين ،،، وبعد :

يؤكد تاريخ العلوم أن الحضارة الحديثة تدين بازدهارها إلى الحضارة العربية الإسلامية وخصوصاً في العصر العباسي ، حيث كانت حركة التأليف والابتكارات .

وعلى الرغم من ذلك فإن المكتبة العربية مازالت تعاني نقصاً كبيراً في الكتب العربية خصوصاً الكتب العلمية . والجامعات العمومية في حاجة ماسة إلى تعريب العديد من الكتب في شتى الاختصاصات ، ويأتي علم الرياضيات على رأس قائمة الاختصاصات التي تعاني هذا الشح .

عليه فقد ارتأينا أن نعرب كتاباً مرجعياً في **الجبر الحديث** لأهمية هذا الموضوع لكل دارس رياضيات ، بل حتى طلاب اختصاصات أخرى تدرس الرياضيات .

وجاء اختيارنا لهذا الكتاب الذي هو بين أيديكم لشموليته ، فالكتاب يتألف من 16 فصلاً يكاد أن يكون مؤلفه قد شمل جميع مواضيع الجبر الحديث .

لقد تم التقيد بالمصطلحات التي شاعت ورسخت في اللغة العربية وتعود عليها الطالب في دراسته الثانوية والجامعية .

نرجو بتقديمنا هذه الترجمة أن نكون قد ساهمنا مساهمة يسيرة في إغناء المكتبة العربية بالكتب القيمة .

وأخيراً نود أن نتقدم بجزيل الشكر والتقدير والعرفان لكل من ساهم في إخراج هذا الكتاب ، ونخص بالشكر كلاً من الدكتور **عبد الرحمن السمان** والدكتور **فؤاد زين العرب** لما بذلاه من جهد جبار في مراجعة هذا الكتاب ولملاحظاتهما الممتازة التي أغنت الكتاب .

وخالص شكرنا وتقديرنا للأخ الفاضل **عبد الكريم جاد الله عزوز** وشقيقته **حنان جاد الله عزوز** من **مركز الهدى للحاسوب** على طباعة هذا الكتاب وإخراجه بهذا الشكل الرائع .

والله ولي التوفيق

المترجمون

1

نـظريـة المجموعـات *Set Theory*

يعتبر مفهوم المجموعة (تقريباً) من المفاهيم الأساسية في الرياضيات ، ففي الواقع نجد أن أغلب الأنظمة الرياضية هي عبارة عن فئات محددة من المجموعات . تلك الأنظمة الرياضية ونظرياتها يمكن بحثها كأجزاء من نظرية المجموعات .

في أي نظام رياضي هناك بعض المصطلحات غير المعرفة والتي يؤول بعضها إلى البعض من خلال بعض العبارات المنطقية المتماسكة والتي يطلق عليها مسلمات أو مبادئ .

وفي نظرية المجموعة فإن مصطلحات المجموعة ، الشيء ، والتساوي ، كذلك (هو عنصر من) كلها غير معرفة .

ونحن هنا لا ننوي مناقشة بديهيات نظرية الأعداد على أساس كونها تطور لنظرية المجموعات فإن ذلك ليس مجال أو هدف هذا الكتاب ، بل أننا (في هذا الكتاب) سوف نبحث تمهيدات نظرية المجموعات والتي نحتاجها مؤخراً خلاله (أي خلال الكتاب) . بالأحرى سنستهدف البديهيات .

نحن لن نطالب هنا بنموذج منطق كامل في براهين مختلف النتائج قيد المناقشة . وإننا ندرك إلى حد كبير أن كلمة المجموعة هي كلمة مرادفة لكلمة تجمع من الأشياء ، وبالنسبة لنا هنا فإنها تعني تجمعاً من الأعداد الصحيحة ، أو تجمعاً من الطلاب في فصل دراسي معين ، أو تجمعاً من الأشياء في منزل ما ، أو تجمعاً من المثلثات في المستوى الكارتيزي ، وهذه أمثلة لبعض المجموعات .

سنشير في هذا الكتاب إلى المجموعات بأحرف كبيرة $A, B, \ldots$ ، أما العناصر فسيتم الإشارة لها بأحرف صغيرة $a, b, c, \ldots$.

تستخدم الرموز C, R, Q, Z, N في العادة للإشارة إلى مجموعة الأعداد الطبيعية ، مجموعة الأعداد الصحيحة ، مجموعة الأعداد النسبية ، مجموعة الأعداد الحقيقية مجموعة الأعداد المركبة على الترتيب .

لتكن A مجموعة ، فإذا كان x عنصراً ينتمي إلى A أو عنصراً ضمن المجموعة A فإننا في هذه الحالة نكتب $x \in A$ ونقول أن x هو عنصر من A ، وإذا كان x عنصراً ليس من عناصر A ، فإننا في هذه الحالة نكتب

$x \notin A$ ونقول أن x لا ينتمي إلى المجموعة A ، على سبيل المثال فإن

$2 \in N$ بينما $\frac{1}{2} \notin N$ في حين أن $\frac{1}{2} \in Q$

إذا كانت A مجموعة كل المثلثات في المستوى الكارتيزي وإذا كان x أي مربع فإن $x \notin A$.

في العادة فإن عناصر المجموعة تحدد من خلال الخاصية العامة $p(x)$ التي تصف المجموعة A .

فإنه من المعتاد إمكانية تحديد الصفة $p(x)$ التي يتصف بها جميع العناصر x التي تقع ضمن A ، في هذه الحالة فإننا نكتب $A = \{x : p(x)\}$

المجموعة التي لا تحتوي أي عنصر تسمى المجموعة الخالية ونرمز لها بالرمز ϕ .

مثال 1

ليكن $p(x) \equiv$ "x عدد طبيعي" ، وحيث أن N هي مجموعة كل الأعداد الطبيعية فإنه يمكننا أن نقول $N = \{x : \text{طبيعي عدد } x\}$

مثال 2

لتكن A مجموعة كل الأعداد الطبيعية التي تمثل مربعاً فإنه يمكننا أن نقول

$A = \{x \mid \exists y \in N, x = y^2\}$

إذا كانت المجموعة A تتكون من العناصر $a_1, a_2, a_3, \ldots, a_n, \ldots$

فإننا عادة نكتب $A = \{a_1, a_2, a_3, .. a_n, \ldots\}$

فعلى سبيل المثال

$A = \{1, 5, 6\}$ تعني أن A تتكون من العناصر $1, 5, 6$ فقط في هذه الحالة $1 \in A, 5 \in A, 6 \in A$

بينما $A \not\in 7, A \not\in 4, A \not\in 3, A \not\in 2$ وهكذا .

تعريف 1.1

يقال للمجموعة A أنها مجموعة جزئية من المجموعة B (رمزياً تكتب $A \subseteq B$) في حالة كون كل عنصر من A عنصراً من B ، بالإضافة إلى ذلك في حالة $A \neq B$ فإنه يقال A مجموعة جزئية فعلية من B وتكتب $A \subset B$.

إذا كانت A مجموعة جزئية من B ، فإننا نقول أيضاً أن A محتواة في B ، أو B تحوي A .

على سبيل المثال $N \subseteq Q \subseteq R \subseteq C$

ومن الواضح من خلال التعريف أنه إذا كانت $B \subseteq C$ و $A \subseteq B$ فإن ذلك يعني أو يؤدي إلى أن $A \subseteq C$ المجموعتان A, B متساويتان في حالة احتوائهما على نفس العناصر . أي أنه في حالة A, B مجموعتان متساويتان فإن $B \subseteq A$ و $A \subseteq B$.

لكون $A \subseteq B$ تعني أن كل عنصر من A هو عنصر في B ، $B \subseteq A$ تعني أن كل عنصر من B عنصر في A وهذا بطبيعة الحال يعني أن A, B بهما نفس العناصر ومن ثم فإن $A = B$.

تعريف 2.1

اتحاد المجموعتين A, B هو المجموعة $A \cup B$ التي تتكون من كل العناصر الموجودة إما في A أو في B . أي أن $A \cup B = \{x : x \in A \text{ or } x \in B\}$

تعريف 3.1

تقاطع المجموعتين A, B هو المجموعة $A \cap B$ التي تتكون من كل العناصر المشتركة في A, B أي أن $A \cap B = \{x : x \in A \text{ and } x \in B\}$

مثال 3

لتكن $A = \{1, 2, 3, 4\}, B = \{3, 4, 2, 5\}$

فإن $A \cup B = \{1, 2, 3, 4, 5\}, A \cap B = \{2, 3, 4\}$

مثال 4

لتكن A مجموعة كل الأعداد الصحيحة الأقل من أو المساوية للصفر ، أي أن

$N \cup A = Z$

نظرية 4.1

لأي مجموعتين A ، B فإن

(i) $A \subseteq B$ إذا كان وفقط إذا كان $A \cap B = A$

(ii) $A \subseteq B$ إذا كان وفقط إذا كان $A \cup B = B$

البرهان

(i) لتكن $A \subseteq B$ إذن أي عنصر x بحيث كان $x \in A$ ، من التعريف فإن $x \in B$ وبناء على ذلك فإن $x \in A \cap B$

وحيث أن وجود x في A أدى إلى وجوده في $A \cap B$ ، فإن هذا يوضح أن

$A \subseteq A \cap B \qquad (1)$

من الواضح (حسب التعريف)

$A \cap B \subseteq A \qquad (2)$

إذن من (1) و (2) ينتج أن $A = A \cap B$

والعكس ، لتكن $A = A \cap B$

وحيث أن $A \cap B \subseteq B$

كذلك $A = A \cap B$ من الفرض ، فإن $A \subseteq B$

وهو المطلوب إثباته

برهان مماثل يلزم لإثبات فقرة (ii)

نحن الآن نذكر علاقات مهمة بين التقاطع والاتحاد ، والتي تعرف بقوانين التوزيع

نظرية 5.1

لأي ثلاث مجموعات A, B, C فإن

(i) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(ii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

البرهان

$$x \in A \cap (B \cup C)$$
$$\Rightarrow x \in A \ , \ x \in B \cup C$$
$$\Rightarrow x \in A \ , \ (x \in B \text{ or } x \in C)$$

وبالتالي إذا كان $x \in B$

فإن $x \in A \cap B \subseteq (A \cap B) \cup (A \cap C)$

يعطي $x \in (A \cap B) \cup (A \cap C)$

وبالمثل إذا كان $x \in C$ ، وحيث أن $x \in A$ ، مرة أخرى نجد أن

$x \in (A \cap B) \cup (A \cap C)$

وها يوصلنا إلى كون

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \qquad (1)$$

والآن

$$x \in A \cap B$$
$$\Rightarrow x \in A, x \in B$$
$$\Rightarrow x \in A, x \in B \cup C$$

لكون

$$B \subseteq (B \cup C) \Rightarrow x \in A \cap (B \cup C)$$

وبالتالي فإن

$$A \cap B \subseteq A \cap (B \cup C) \qquad (2)$$

بالمثل نجد أن

$$A \cap C \subseteq A \cap (B \cup C) \qquad (3)$$

من (2) ، (3) نحصل على

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C) \qquad (4)$$

عليه فإن (1) ، (4) ينتجان $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

ونحن نترك للقراء برهنة (ii) بطريقة مماثلة .

تعريف 6.1

إذا كان لدينا مجموعتين A, B فإن المجموعة الفرق $A - B$ هي المجموعة

$\{x \in A \mid x \notin B\}$

زيادة على ذلك ، إذا كانت B مجموعة جزئية من A فإن $A - B$ يقال لها مكملة B من A .

في بعض الأحيان عندما لا يكون هناك لبس بالنسبة إلى A لأي مجموعة جزئية B من A فإن $A - B$ يشار إليها B' .

مثال (5)

لتكن E مجموعة كل الأعداد الزوجية الطبيعية ، عليه فإن

$N - E$ هي مجموعة كل الأعداد الفردية .

مثال (6)

لتكن
$$A = \{1, 2, 3, 4, 5, 6\}$$
$$B = \{5, 6, 7, 8\}$$

فإن
$$A - B = \{1, 2, 3, 4\}$$
$$B - A = \{7, 8\}$$

من الواضح هنا $A - B$, $B - A$ لا يوجد بينهما أي عنصر مشترك ، عليه فإن

$$(A - B) \cap (B - A) = \phi$$

تعريف 7.1

لأي عنصـرين a, b الـزوج المرتـب (a, b) مـع وجـود a كإحـداثي أول ووجـود b كإحداثي ثاني هو المجموعة المعرفة على النحو التالي $(a, b) = \{\{a\}, \{a, b\}\}$

عليه فإن (a, b) عبارة عن مجموعة مجموعات عناصرها المجموعات $\{a\}, \{a, b\}$.

على سبيل المثال $(1, 2) = \{\{1\}, \{1, 2\}\}, (2, 1) = \{\{2\}, \{2, 1\}\}$

نظرية 8-1

$(a, b) = (c, d)$ إذا كان وفقط إذا كان $a = c, b = d$.

البرهان

باستخدام التعريف

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} \qquad (1)$$

الحالة الأولى عندما $a = b$ ، فإن

$$\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\} \qquad (2)$$

من (1) ، (2) نجد أن

$$\{\{a\}\} = \{\{c\}; \{c, d\}\}$$

$$\Rightarrow \{a\} = \{c\} = \{c, d\} \Rightarrow a = c = d \Rightarrow a = c = d$$

$$\Rightarrow a = b = c = d \,, a = b \qquad (\text{لأن } a = b)$$

عليه فإن

$$a = c, b = d$$

بنفس الطريقة إذا كانت $c = d$ فإن

$$b = d, a = c$$

الحالة الثانية $a \neq b, c \neq d$

حيث أن

$$\{a\} \in \{\{c\}, \{c, d\}\}$$

$$\Rightarrow \{a\} = \{c\}\, or\, \{a\} = \{c, d\}$$

في الحالة الأخيرة $a = c = d$ وهذا تناقض لكون $c \neq d$ ، عليه فإن

$$\{a\} = \{c\}$$

وبالتالي

$$a = c \qquad (3)$$

مرة أخرى فإن (1) ينتج عنها

$$\{a, b\} \in \{\{c\}, \{c, d\}\}$$

$$\Rightarrow \{a, b\} = \{c\}\, or\, \{a, b\} = \{c, d\}$$

في الحالة السابقة تناقض ، ولهذا السبب فإن

$$\{a, b\} = \{c, d\}$$

$$\Rightarrow b \in \{c, d\} \Rightarrow b = c\, or\, b = d$$

في الحالة السابقة $a = b$ نظراً لكون $a = c$ ، وهذا يؤدي مرة أخرى إلى تناقض ، وبطبيعة الحالة ينتج أن

$$b = d \qquad (4)$$

من (4) ، (3) ينتج أن

$$a = c, b = d$$

وبالعكس إذا كان ، $a = c$ و $b = d$ فإن

$$\{a\} = \{c\}, \{a, b\} = \{c, d\}$$

$$\Rightarrow (a, b) = \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} = (c, d)$$

وهكذا يتحقق المطلوب .

الهدف من التعريف السابق كذلك النظرية حول الأزواج المرتبة هو إعطاء معنى لترتيب نسق من العناصر .

فعلى سبيل المثال الأزواج المرتبة $(1, 2), (2, 1)$ مختلفة . من المعروف جيداً في المستوى الكارتيزي بإحداثيات النقطة P يعبر عنها بزوج مرتب (a, b) من الأعداد الحقيقية . حيث يقال أن a إحداثيها السيني بينما b هو إحداثيها الصادي . النقطتان بإحداثيات $(1, 2), (2, 1)$ مختلفتان بينما المجموعتان $\{1, 2\}, \{2, 1\}$ متساويتان لكونهما لهما نفس العناصر .

تعريف 9.1

لتكن A, B مجموعتين ، حاصل الضرب الكارتيزي $A \times B$ يعرف بمجموعة جميع الأزواج المرتبة (a, b) بحيث $a \in A, b \in B$.

حيث أن إحداثيات النقطة في المستوى الكارتيزي عبارة عن زوج مرتب من الأعداد الحقيقية وبالعكس فإن كل زوج مرتب من الأعداد الحقيقية يعبر عن إحداثيات نقطة ما ، عليه فإنه يمكننا القول بأن مجموعة إحداثيات كل النقاط في المستوى الكارتيزي هي $R \times R$.

مثال 7

لتكن $A = \{\alpha, \beta\}, B = \{1, 2, 3\}$

عليه فإن
$$A \times B = \{(\alpha, 1), (\alpha, 2), (\alpha, 3), (\beta, 1), (\beta, 2), (\beta, 3)\}$$
$$B \times A = \{(1, \alpha), (1, \beta), (2, \alpha), (2, \beta), (3, \alpha), (3, \beta)\}$$

ملاحظة

إذا كان للمجموعة A عناصر عددها n عنصر ، فإننا نكتب

$$| A | = n$$

عليه ففي المثال رقم (3) نجد أن

$$| A | = 4 , | B | = 4 , | A \cup B | = 5 , | A \cap B | = 3$$

تمرين 1

إذا كانت المجموعتان A, B بحيث كان $| A | = m, | B | = n$ عليه فإن

$$| A \cup B | = | A | + | B | - | A \cap B | = m + n - | A \cap B |$$

وكحالة خاصة ، إذا كانت A, B منفصلتين فإن $| A \cup B | = m + n$.

الحل

لاحظ أننا عندما نعد العناصر في $A \cup B$ فإن عناصر $A \cap B$ تعد مرتين ، حالما تعد ضمن عناصر A ، وللمرة الثانية تعد ضمن عناصر B وبالتالي فإن النتيجة الأولى تتحقق .

الجزء الثاني ينتج من حقيقة كون $| \phi | = 0$.

تمرين 2

استبيان يوضح أن 63% من الأمريكيين يحبون الجبن ، بينما 76% يحبون التفاح ، ماذا يمكنك القول حول نسبة الأمريكيين الذين يحبون الجبن والتفاح معاً ؟

الحل

افرض أن A هي مجموعة من يحبون الجبن من الأمريكيين بينما B مجموعة هؤلاء الذين يحبون التفاح منهم .

افرض أن تعداد الأمريكيين 100 .

عليه فإن $|A| = 63, |B| = 76$

وحيث أن $|A \cup B| = |A| - |B| - |A \cap B|$

$\Rightarrow |A \cap B| = 139 - |A \cup B|$

ولكن $|A \cup B| \le 100,$

عليه فإن $|A \cap B| \ge 39$

علاوة على ذلك فإن $A \cap B \subseteq A, A \cap B \subseteq B$

وهذا يؤدي إلى $|A \cap B| \le |A|, |A \cap B| \le |B|$

وبالتالي فإن $|A \cap B| \le 63, |A \cap B| \le 76$

أي أن $39 \le |A \cap B| \le 63$

وبالتالي تكون نسبة من يحب من الأمريكيين كلاً من التفاح والجبن معاً تقع بين 39% و 63% .

تمرين 3

مجموعتان X, Y تكونان متساويتين إذا كان وفقط إذا كان

$X \cup Y = X \cap Y$

الحل

في حالة $X = Y, X \cup Y = X, X \cap Y = X$

وبالتالي فإن $X \cup Y = X \cap Y$

وبالعكس ، فإذا كان $X \cup Y = X \cap Y$

فإن $X \subseteq X \cup Y = X \cap Y \subseteq Y$

و $Y \subseteq X \cup Y = X \cap Y \subseteq X$

وبالتالي ينتج أن $X = Y$

تمرين 4

لأي ثلاث مجموعات A, B, C

فإن $A - (B \cup C) = (A - B) \cap (A - C)$

و $A - (B \cap C) = (A - B) \cup (A - C)$

وهذا ما يعرف بقانون دي مورجان للمكملات .

الحل

$x \in A - (B \cup C) \Rightarrow x \in A, x \notin (B \cup C)$

$\Rightarrow (x \in A \text{ such that } x \notin B) \text{ and } (x \in A \text{ such that } x \notin C)$

$\Rightarrow x \in A - B, x \in A - C \Rightarrow x \in (A - B) \cap (A - C)$

عليه فإن $A - (B \cup C) \subseteq (A - B) \cap (A - C)$

وبالعكس إذا كان $y \in (A - B) \cap (A - C) \Rightarrow y \in A - B, y \in A - C$

$\Rightarrow (y \in A \text{ and } y \notin (B \cup C) \Rightarrow y \in A - (B \cup C)$

عليه فإن $(A - B) \cap (A - C) \subseteq A - (B \cup C)$

وبالتالي ينتج أن $A - (B \cup C) = (A - B) \cap (B - C)$

أما بالنسبة للجزء الثاني $x \in A - (B \cap C) \Rightarrow x \in A \text{ but } x \notin (B \cap C)$

يؤدي إلى ، إما $(x \in A \text{ but } x \notin B)$ أو $(x \in A \text{ but } x \notin C)$

$\Rightarrow x \in (A - B) \text{ or } x \in (A - C) \Rightarrow x \in (A - B) \cup (A - C)$

وبذلك فإننا نحصل على $A - (B \cap C) \subseteq (A - B) \cup (A - C)$

وبالعكس إذا كان $y \in (A - B) \cup (A - C)$

يـــؤدي إلى ، إمـــا $y \in A - B$ أو $y \in A - C$ وهـــذا بـــدوره يـــؤدي إلى $y \in A$ و $y \notin B$ أو $y \in A$ و $y \notin C$ وبالتالي فإن

$$y \in A \quad \text{و} \quad y \notin (B \cap C) \Rightarrow y \in A - (B \cap C)$$

$$\therefore \quad (A - B) \cup (A - C) \leq A - (B \cap C)$$

ونتيجة لذلك فإننا نحصل على $A - (B \cap C) = (A - B) \cup (A - C)$

تمرين 5

لتكن A, X, Y ثلاث مجموعات بحيث كان $A \cap X = A \cap Y$

وكان $A \cup X = A \cup Y$

فإن $X = Y$

الحل

لقد أوضحنا أن

$$X \subseteq Y$$

$X \subseteq Y$ سوف يتبع أو ينتج من تماثل الشروط المعطاة .

نفرض أن $x \in X$

فهناك حالتين

الحالة الأولى $x \in A$

الآن $x \in X \Rightarrow x \in A \cap X = A \cap Y$

$$\Rightarrow x \in Y$$

الحالة الثاني $x \notin A$

وحيث أن $x \in X \Rightarrow x \in A \cup X = A \cup Y$

$$\Rightarrow x \in A \cup Y \text{ و } x \notin A$$

$\Rightarrow x \in Y$

في كلتا الحالتين $x \in X$ يؤدي إلى كون $x \in Y$ وبالتالي ينتج أن $X \subseteq Y$

تمارين

1- لأي ثلاث مجموعات A, B, C أثبت أن

(i) $A \cup (B \cup C) = (A \cup B) \cup C$

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

2- أثبت أن المجموعة الخالية جزئية من كل مجموعة .

3- لتكن $A = (1, 2, 3)$ أجب عما يأتي

– ما هي عناصر A .

– كم مجموعة جزئية للمجموعة A ، أوجد كلاً منها (الإجابة 8) .

– لتكن $B = (3, 4, 5)$ هل B مجموعة جزئية من A .

أوجد $A - B$ ، $B - A$.

4- لتكن $A_1, A_2, \ldots, A_n$ مجموعات عددها n يعرف الاتحاد منها $A_1 \cup A_2 \cup \ldots \cup A_n$ تخليقياً على النحو التالي

$$A_1 \cup A_2 \ldots \cup A_n = (A_1 \cup A_2 \ldots \cup A_{n-1}) \cup A_n$$

وبنفس الطريقة يعرف $A_1 \cap A_2 \cap \ldots \cap A_n$

برهن ما يأتي :

(i) $(A_1 \cup A_2) \cup A_3 = (A_1 \cup A_3) \cup A_2 = A_1 \cup A_2 \cup A_3$

(ii) $(A_1 \cap A_2) \cap A_3 = (A_1 \cap A_3) \cap A_2 = A_1 \cap A_2 \cap A_3$

5- المجموعة A لها n عنصراً والمجموعة B لها m عنصراً ، ماذا يمكننا القول حول أكبر عدد أو أصغر عدد من العناصر يمكن للمجموعة $A - B$ أن تحتويه ؟

6- لأي مجموعتين A, B برهن أن $A - B$, $B - A$ غير منفصلتين بمعنى أنه لا يوجد بينهما عنصر مشترك .

7- لأي ثلاث مجموعات A, B, C برهن ما يأتي

(i) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

(ii) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

(iii) $(A \times C) - (B \times C) = (A - B) \times C$

8- إذا كانت A, B مجموعتين لهما m, n من العناصر على الترتيب ، وضح أن $A \times B$ لها $m.n$ عنصراً .

9- لتكن $A = \{1, 2, 5, 6\}, B = \{1, 2, 3\}$

حدد

$$(A \times B) \cup (B \times A), (A \times B) \cap (B \times A), (A \times B) - (B \times A)$$

10-مجموعة كل المجموعات الجزئية للمجموعة A تسمى مجموعة القوة للمجموعة A ويرمز لها بالرمز $P(A)$.

إذا كان A بها n عنصراً فوضح أن $P(A)$ بها 2^n من العناصر .

11- A, B, C ثلاث مجموعات بحيث كان $|A| = m, |B| = n, |C| = P$ وضح أن

$$|A \cup B \cup C| = m + n + P - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

12-في معركة ما فقد 70% من المقاتلين أحد عيونهم ، كما فقد 80% منهم أحد آذانهم ، وفقد 75% منهم أحد ذراعيه ، وفقد 85% منهم أحد ساقيه ، وفقد x% منهم الأربعة أعضاء معاً . أوجد أقل قيمة ممكنة للمتغير x . (إجابة : 10)

13-في استبيان استهدف 100 طالب حول دراستهم اللغات المختلفة وجد أن 28 منهم يدرسون الأسبانية ، و 30 منهم يدرسون الألمانية ، و 42 منهم يدرسون الفرنسية ، كما وجد أن 8 منهم يدرسون الأسبانية والألمانية معاً ، و 10 منهم يدرسون الأسبانية والفرنسية ، و 5 منهم يدرسون الألمانية والفرنسية ، و 3 منهم يدرسون اللغات الثلاث .

- كم عدد من لا يدرس أي لغة .

– كم عدد من يدرس الفرنسية كلغتهم فقط . (إجابة (30) ii (20)i)

14-لتكن $X \cup Y = X$ لكل المجموعات X . أثبت أن $Y = \phi$.

15-إذا كانت كل من P, Q, R مجموعات جزئية من A ، وكانت المكملات النسبية (′) بالنسبة إلى A برهن ما يأتي

i- $P \subseteq Q$ إذا كان وفقط إذا كان $P \cap Q' = \phi$

ii- $P \subseteq Q$ إذا كان وفقط إذا كان $P' \cup Q = A$

iii- $P \subseteq Q$ إذا كان وفقط إذا كان $P \cap Q' \subseteq P'$

iv- $P \subseteq Q$ إذا كان وفقط إذا كان $P \cap Q' \subseteq Q$

v- $P \subseteq Q$ إذا كان وفقط إذا كان $P \cap Q' \subseteq R \cap R'$

16- A, B مجموعتان أي العبارات التالية صحيحة وأيها خاطئة ؟ علل إجابتك

(i) $P(A \cap B) = P(A) \cap P(B)$

(ii) $P(A \cup B) = P(A) \cup P(B)$

(iii) $P(A - B) = P(A) - P(B)$

الإجابة (i) صحيحة ، (ii) خاطئة ، (iii) خاطئة .

17-لتكن X, Y, S, T أربع مجموعات ، بحيث كان

$$X \cup Y = T \cup S \ , \ X \cap Y = T \cap S = \phi$$

أثبت أن $X = \phi$ إذا كان وفقط إذا كان

$$T = (X \cap S) \cup (Y \cap T)$$

2– العلاقات والرواسم

نحن ومن خلال السياق اليومي لكلامنا نتحدث عن العلاقات التي تحدث بين اثنين أو مجموعة أشياء ، فعلى سبيل المثال

(i) العدد 2 يقسم العدد (4) .

(ii) أكبار كان والداً لجيهانجير .

(iii) العدد 6 أكبر من العدد (4) .

ثلاثة أمثلة لعلاقة تحدث في السياق اليومي . في هذه الأمثلة نجد أن هناك نوع من الارتباطات بين زوج من الأشياء قد حدث ، وبالتالي فإن هذه الأمثلة تعبر عن بعض العلاقات بين أزواج من الأشياء ، ويمكن للفرد أن يفكر في علاقة بين مجموعة من الأشياء . هذه الفكرة غير الواضحة للارتباط البديهي يمكن أن تركب مع التعريف الأساسي للعلاقة ، وبالأحرى فنحن نعرف العلاقة على النحو التالي

تعريف 1-10

لتكن X, Y مجموعتان غير خاليتين تعرف أي مجموعة جزئية من $X \times Y$ على أنها علاقة ثنائية من X إلى Y . والعلاقة أيضاً تسمى تطابقاً .

إذا كانت $X = Y = S$ فإن المجموعة الجزئية من $S \times S$ تسمى علاقة ثنائية في S .

في هذا الكتاب سيكون اهتمامنا فقط بالعلاقات الثنائية وبالتالي فإنه عندما نقول علاقة ، فإن ذلك يعني علاقة ثنائية .

إذا كانت T علاقة من A إلى B و $(a, b) \in T$ ، فإننا نكتب aTb ونقول أن a يحقق العلاقة T مع b . وإذا كان $(a, b) \notin T$ فإننا نقول أن a ليس لديه العلاقة T مع b .

وبناء على التعريف فإننا نجد أنه في أي مجموعة S يوجد عدد من العلاقات بمقدار عدد المجموعات الجزئية من $S \times S$ من بين هذه فإن العلاقات المتكافئة والتي ستناقش في نهاية هذا الفصل لها أهمية قصوى .

تعريف 11-1

لتكن X, Y مجموعتين غير خاليتين ، فإن المجموعة الجزئية T من حاصل الضرب الكارتيزي $X \times Y$ يقال لها راسم من X إلى Y إذا كان لكل $x \in X$ يوجد عنصر واحد فقط $y \in Y$ بحيث كان $(x, y) \in T$. الراسم يعرف أيضاً بأنه دالة .

لأي عنصر $x \in X$ إذا كان $(x, y) \in T$ في هذه الحالة يقال أن y قيمة x بواسطة T أو صورة x تحت T أو يقال أن y تناظر x تحت T ونكتب ذلك هكذا $y = T(x)$. إذا كان T راسماً من X إلى Y في هذه الحالة يسمى X نطاق T (dom T) كما يقال للمجموعة

$\{y \in Y \mid x \in X \text{ لبعض } y = T(x)\}$ يقال لها في هذه الحالة بمدى T (range$T$) النطاق المصاحب للراسم T $(\text{Co} - \text{dom}\, T)$.

ملاحظة

الرمز $f : X \to Y$ سوف يشير إلى أن f راسم من X إلى Y .

تعريف 12-1

ليكن f راسماً من المجموعة X إلى المجموعة Y عندئذ

(i) يقال أن f راسم أحادي إذا كان لكل $x_1, x_2 \in X$ فإن $f(x_1) = f(x_2)$ يؤدي إلى أن $x_1 = x_2$.

(ii) إذا كان نطاق f هو Y يقال في هذه الحالة أن الراسم f فوقي (onto) .

(iii) إذا كان f أحادي وفوقي ، ففي هذه الحالة يقال أن f تناظر أحادي (1-1 cor ponden) .

نظرية 1-12 (a)

الراسمان f, g من المجموعة X إلى المجموعة Y متساويان إذا كان وفقط إذا كان $f(x) = g(x)$ لكل $x \in X$.

البرهان

نفرض أن $f = g$

لتكن $x \in X \,, (x, f(x)) \in f$

وحيث أن $f = g$ فإن $(x, f(x)) \in g$ وهذا يعطينا $f(x) = g(x)$

وبالعكس فإذا كان $f(x) = g(x)$ لكل $x \in X$.

لتكن $(a, b) \in f$ فإن $b = f(a) = g(a)$

وهذا يعطينا أن $(a, b) \in g$

عليه فإن $f \subseteq g$

وبنفس الطريقة يمكن أن نبرهن أن $g \subseteq f$ ، وعليه فإن $g = f$

ملاحظة

الراسم الأحادي يسمى injection ، وأيضاً الراسم الفوقي يسمى surjection ، والتقابل الأحادي يسمى أيضاً bijection .

مثال 8

لتكن X مجموعة غير خالية ، يعرف بها الراسم $i: X \to X$ على النحو التالي :

$$i(x) = x \quad \forall \quad x \in X$$

وفي مفهوم الأزواج المرتبة $i = \{(x, x) \mid x \in X\}$

i في هذه الحالة يسمى الراسم المحايد في X .

مثال 9

ليكن $f : Z \to Z \quad , \quad X = Y = Z$

على النحو التالي $f(x) = 2x \quad : \forall \quad x \in Z$

وحيث أنه لكل $x_1, x_2 \in Z$ ، فإذا كان $f(x_1) = f(x_2)$

$$2x_1 = 2x_2 \Rightarrow x_1 = x_2 \qquad \therefore$$

أي أن f راسم أحادي . والآن مدى الراسم f يساوي

$$\{f(x) \mid x \in Z\} = \{2x \mid x \in Z\}$$

ويساوي مجموعة كل الأعداد الصحيحة الزوجية .

عليه فإن مدى $f \neq Z$ وبالتالي f ليس فوقياص .

مثال 10

لتكن $X = Z \times Z$ ، الراسم $f : Z \times Z \to Z$ معرف على النحو التالي

$$f(n, m) = n + m \quad \forall (n, m) \in Z \times Z$$

أي أن f راسم فوقي وكذلك لأنه لكل $n \in Z$

فإنه لدينا $f(0, n) = 0 + n = n$

وأن (مـدى f) $n \in$ ، لـذلك فـإن نطـاق f يسـاوي Z ، بينمـا نجـد f لـيس أحـادياً

لأن $f(1, 3) = 1 + 3 = 4 = 2 + 2 = f(2, 2)$

ولكن $(1, 3) \neq (2, 2)$

مثال 11

لتكن $X = \{x_1, x_2, x_3, x_4\}, Y = \{\alpha, \beta\}$

الراسم $f : x \to X$ معرف بالصورة

$$f(x_1) = \alpha , f(x_2) = \beta , f(x_3) = \alpha , f(x_4) = \alpha$$

f يكون فوقياً ولكنه ليس أحادياً .

الراسم $g : X \to Y$ المعرف على النحو

$$g(x_1) = \alpha , g(x_2) = \beta , g(x_3) = \alpha , g(x_4) = \alpha$$

فإن مدى الراسم g هو $\{\alpha\}$ ، ونلاحظ أن $\{\alpha\} \neq Y$ لذلك فإن g ليس راسماً فوقياً وأيضاً ليس راسماً أحادياً .

تعريف 13.1

إذا كان $g : Y \to Z , f : X \to Y$

راسمين ، في هذه الحالة فإن تركيبهما gof (ويطلق عليه أيضاً حاصل ضرب g, f) هو راسم من X إلى Z بحيث يكون لكل عنصر $x \in X$

$$(gof)(x) = g(f(x))$$

هنا في تركيب gof نقول أنه لأي عنصر $x \in X$ فإن f يعمل على x أولاً ، وبعد ذلك g يعمل على $f(x)$.

وقبل أن نواصل مناقشة خواص الرواسم فإننا نتوقف لتقديم بعض الأمثلة حول تركيب الرواسم .

مثال 12

ليكن $X = \{a, b, c\}, Y = \{x, y, z, u\}, S = \{\alpha, \beta, \gamma\}$

وكان الراسم $f : X \to Y$ معرف على النحو التالي

$$f(a) = x , f(b) = y , f(c) = z$$

وكان الراسم $g : Y \to S$ معرف على النحو التالي

$g(x) = \alpha \, , g(y) = \beta \, , g(z) = \gamma \, , g(u) = \alpha$

فإن $gof : X \to S$

بحيث كان
$$(gof)(a) = g(f(a)) = g(x) = \alpha$$
$$(gof)(b) = g(f(b)) = g(y) = \beta$$
$$(gof)(c) = g(f(c)) = g(z) = \gamma$$

وحيث أن صورتي أي عنصرين مختلفتين تحت تأثير gof مختلفتان ، لذلك فإن gof أحادي ، كما أن مدى gof يساوي S ، أي أن gof فوقي . وبالتالي فإن gof تناظري مع العلم بأنه لا f ولا g تناظري ، بل إن g ليس أحادياً .

مثال 13

ليكن $X = Y = Z$

وكان $, \; g : Z \to Z \; f : Z \to Z$

معرفان على النحو التالي $f(x) = -x \, , g(x) = x + 2 \qquad \forall x \in X$

فإنه لأي عنصر $x \in X$ فإن
$$(gof)(x) = g(f(x)) = g(-x) = -x + z \, ,$$
$$(fog)(x) = f(g(x)) = f(x + 2) = -(x + 2)$$

وحيث أن $-x + 2 \neq -(x + 2) \qquad \forall x$

فإنه ينتج أن $fog \neq gof$

نظرية 14.1

ليكن $f : U \to V \, , g : V \to X \, , h : X \to Y$

أي ثلاثة رواسم ، فإن

(a) $ho(gof) = (hog)of$

(b) إذا كان كل من f ، g أحادي فإن gof يكون أحادي أيضاً .

(c) إذا كان كل من f ، g فوقي فإن gof يكون فوقي أيضاً .

(d) إذا كان $j:V \to V\,,\, i:U \to U$ راسمان محايدان فإن $foi = f$ كذلك $jof = f$

البرهان

نفرض أن $u \in U$

(a) من التعريف نجد أن

$$\left[ho(gof)\right](u) = h\left[(gof)\,(u)\right] = h\left[g(f(u))\right]$$

كذلك نجد أن

$$\left[(hog)\,of\right](u) = (hog)\,(f(u)) = h\left[g(f(u))\right]$$

أي أن
$$\left[ho\,(gof)\right](u) = \left[(hog)\,of\right](u) \qquad \forall u \in U$$

$$\therefore \qquad ho\,(gof) = (hog)\,of$$

(b) نفرض أن $u_1, u_2 \in U$ فيكون

$$\begin{aligned}(gof)\,(u_1) = (gof)\,(u_2) &\Rightarrow g(f(u_1)) = g(f(u_2))\\ &\Rightarrow f(u_1) = f(u_2)\\ &\Rightarrow u_1 = u_2\end{aligned}$$

لأن f راسم أحادي . وبالتالي ينتج أن gof أحادي .

(c) لكي نثبت أن gof فوقياً فإنه يكفي أن نثبت أن كل عنصر من X يمثل صورة لعنصر من U تحت تأثير الراسم gof .

اعتبر أن $x \in X$

وحيث أن g فوقي فإنه $\exists v \in V$ يكون $g(v) = x$.

والآن حيث أن $f:U \to V$ فوقي ، فإنه $\exists u \in U$ يكون $f(u) = r$.

عليه فإن
$$(gof)\,(u) = g(f(u)) = g(v) = x$$

أي أن gof يكون فوقياً .

(d) والآن لأي عنصر $u \in U$

بما أن i راسم محايد في U ، فإن

$$i(u) = u \Rightarrow f(i(u)) = f(u) \Rightarrow (foi)(u) = f(u) \Rightarrow foi = f$$

لأي عنصر $u \in U$.

حيث أن $j, f(u) \in V$ راسم محايد في V ، فإن

$$j(f(u)) = f(u)$$

وبالتالي فإن

$$(jof)(u) = f(u)$$

$$\therefore \quad jof = f$$

وبالتالي نحصل على المطلوب . □

في النظرية السابقة ، إذا كان كل من f, g تقابل أحادي ، ومن خلال الفقرتين $(b), (c)$ فإن gof يكون أيضاً تقابل . وبالتالي فإننا يمكن أن نحصل على

نتيجة 15-1

إذا كان كل من $f : U \to V, g : V \to X$ تقابلاً أحادياً ، فإن $gof : U \to X$ يكون أيضاً تقابلاً أحادياً . □

تعريف 16-1

لتكن X أي مجموعة ، فإذا كان هناك راسم أحادي وفوقي من X إلى X نفسها فإنه يسمى تحويل غير منفرد أو تبديل للمجموعة X .

سوف يرمز $S(x)$ لمجموعة جميع تباديل المجموعة X . والآن لدينا الآتي :

نظرية 17-1

إذا كانت X مجموعة غير خالية و $f, g, h \in S(x)$ فإن :

(a) $f \circ g \in S(x)$

(b) $(f \circ g) \circ h = f \circ (g \circ h)$

(c) إذا كان $i : x \to X$ الراسم المحايد على X ، فإن $i \circ f = f = f \circ i$

(d) يوجد $f' \in S(x)$ بحيث $f \circ f = f' \circ f = i$

البرهان

(a) بما أن f و g تبديلان أحاديان ، وهما فوقيان أيضاً ، فحسب الجزئين (b) و (c) من نظرية 1-14 نحصل على أن $g \circ f$ أحادي ، كما أنه فوقي ، عليه $g \circ f \in S(x)$.

(b) ينتج من جزء (a) نظرية 1-14 .

(c) ينتج من جزء (d) نظرية 1-14 .

(d) عرف $f' : x \to X$ كالآتي : اعتبر $x \in X$ ، بما أن $f : x \to X$ فوقي فيوجد $y \in X$ بحيث $f(y) = x$ ولأن f أحادي فإن y وحيد .

عرف $f'(x) = y$ ، أي أن لأي $x, y \in X$ نعرف $f'(x) = y$ إذا وفقط إذا كان $x = f(y)$.

اعتبر $x_1, x_2 \in X$ ، وافرض أن $f'(x_1) = y_1$ ، $f'(x_2) = y_2$. عليه فإن $f(y_1) = x_1$ و $f(y_2) = x_2$

$$f'(x_1) = f'(x_2) \Rightarrow y_1 = y_2 \Rightarrow f(y_1) = f(y_2) \Rightarrow x_1 = x_2$$

لذلك فإن f' تبديل أحادي . بما أن لعنصر $x \in X$ إذا كان $f(x) = y$ فإنه وحسب تعريف $f'(y) = x$ نحصل على أن $x \in \text{range}\, f'$. وهكذا فإن $X \subseteq \text{range}\, f'$ وبالتالي $X = \text{range}\, f'$. إذاً f' تبديل على X أي $f' \in S(x)$. الآن لأي $x, y \in X$ ، $f(x) = y$ إذا وفقط إذا كان $f'(y) = x$ هذا يعطي

$$(f' \circ f)(x) = f'(f(x)) = f'(y) = x = i(x)$$

و $(f \circ f')(y) = f(f'(y)) = f(x) = y = i(y)$

إذاً $f \circ f' = f' \circ f = i$ وهذا يثبت النظرية . □

نظرية 18-1

ليكن $f : x \to y$ راسماً لأي مجموعة جزئية A من x المجموعة $\{f(a) \mid a \in A\}$ وهي مجموعة جزئية في y ، تسمى صورة A تحت f ويرمز بالرمز $f(A)$.

لأي مجموعة جزئية B من y المجموعة $\{x \in X \mid f(x) \in B\}$ وهي مجموعة جزئية من x تسمى الصورة العكسية للمجموعة B ويرمز لها $f^{-1}(B)$.

والآن نذكر النتيجة الآتية بدون إثبات ويترك ذلك للقراء .

نظرية 19-1

اعتبر الراسم $f : x = y$ ، لأي مجموعات جزئية A_1, A_2 من x و B_1, B_2 من y .

(a) $f(\phi) = \phi$

(b) $A_1 \subseteq A_2$ يؤدي إلى أن $f(A_1) \subseteq f(A_2)$

(c) $f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$

(d) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$

(e) $f^{-1}(y) = X$

(f) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$

(g) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$

(h) $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$. □

مثال 14

ليكن $y = \{\alpha, \beta\}, x = \{1, 2, 3\}$ عرف $f : x \to y$ بحيث $f(1) = \alpha$ ، $f(2) = \alpha$ ، $f(3) = \beta$.

اعتبر $A_1 = \{1\}$ ، $A_2 = \{2\}$ فإن $f(A_1) = \{f(1)\} = \{\alpha\} = f(A_2)$. عليه $f(A_1) \cap f(A_2) = \{\alpha\}$ من ناحية أخرى $A_1 \cap A_2 = \phi$ يؤدي إلى أن $f(A_1) \cap f(A_2) = f(\phi) = \phi$ ، عليه فإن $f(A_1 \cap A_2) \neq f(A_1) \cap f(A_2)$.

ليكن $B_1 = \{\alpha\}$ ، $B_2 = y = \{\alpha, B\}$ ، بما أن $f(1) = \alpha = f(2)$ نحصل على أن $f^{-1}(B_1) = \{1, 2\}$ من ناحية أخرى $f^{-1}(B_2) = \{1, 2, 3\}$ عليه $f^{-1}(B_1) \subseteq f^{-1}(B_2)$ ولكن $f^{-1}(B_1) \neq f^{-1}(B_2)$.

نظرية 1-19 (a)

لتكن $f : x \to y$ دالة أحادية وفوقية . عندئذ توجد دالة $g : y \to y$ بحيث لأي $y \in Y$ ، $g(y) = x, x \in Y$ حيثما كان $f(x) = y$.

البرهان

بما أن f دالة فوقية ، لأي $y \in Y$ ويوجد $x \in X$ بحيث $y = f(x)$ هذا حسب التعريف يؤدي إلى أن $g(x) = x \in X$. لذا فإن g علاقة من X إلى Y ، ولكي نبرهن أن g دالة افرض أن y_1 و y_2 عنصران في Y . بحيث $y_1 = y_2$ ، $g(y_1) = x_1$ و $g(y_2) = x_2$ لبعض $x_1, x_2 \in X$.

مرة ثانية تعريف g يعطي أن $f(x_1) = y_1 = y_2 = f(x_2)$. بما أن f أحادية ، نحصل مباشرة أن $x_1 = x_2$ ، إذا g دالة من Y إلى X . □

تعريف 19-1 (b)

إذا كانت $f : X \to Y$ دالة أحادية وفوقية ، فيقال عنها أنها الة قابلة للعكس .

ملاحظة

مـن نظريـة 19-1 (a) توجـد دالـة $g : Y \to Y$ معرفـة حسـب $g(y) = x$ طالمـا $f(x) = y$ حيـث $x \in X$ ، $y \in Y$ ، الدالـة g تسـمى معكـوس f . في النظريـة التاليـة نبين أن معكوس دالة قابلة للعكس وحيد إضافة إلى ذلك فهو أحادي وفوقي .

نظرية 19-1 (c)

لأي دالة قابلة للعكس $f : X \to Y$ فإن المعكوس وحيد .

البرهان

افـرض g و h معكوسـان للدالـة $f : X \to Y$ ، مـن التعريـف لأي $y \in Y$ فـإن $g(y) = x$ حيـث $x \in X$ وطالمـا كـان $f(x) = y$ و $h(y) = x_1$ حيـث $x_1 \in X$ طالمـا كان $f(x_1) = y$ عليه $f(x) = f(x_1)$.

وحيـث أن f دالـة أحاديـة نحصـل علـى أن $x = x_1$ إذاً $g(y) = h(y)$ بالتـالي $g = h$. □

اصطلاح

إذا كان f دالة قابلة للعكس فإن معكوسها يرمز بالرمز f^{-1} .

النظرية التالية تمدنا بتعريف مكافئ لتعريف دالة قابلة للعكس .

نظرية 19-1 (d)

الدالـة $f : X \to Y$ قابلة للعكس إذا وفقـط إذا توجـد دالـة $g : X \to Y$ بحيث $g - f = i_x$ ، $f \circ g = i_y$ حيث i_x المحايد على X و i_y المحايد على Y .

البرهان

افرض $f : X \to Y$ له معكوس . حسب تعريف (1-19 b) توجد $g : Y \to X$ بحيث $g(y) = x$ وطالما كان $f(x) = y$ حيث $x \in X$ ، $y \in Y$.

الآن لأي $x \in X$ $$g = f(x) = g[f(x)] = g(y) = x$$

ولأي $y \in Y$ $$f \circ g(y) = f[g(y)] = f(x) = y$$

إذاً $g \circ f = i_x$ و $f \circ g = i_y$.

بالعكس افرض $g : Y \to X$ دالة بحيث $g \circ f = i_x$ و $f \circ g = i_y$.

ليكن $x_1, x_2 \in Y$ بحيث $f(x_1) = f(x_2)$ فإن

$$g[f(x_1)] = g[f(x_2)] = (g \circ f)(x_1) = (g \circ f)(x_2)$$
$$\Rightarrow i_x(x_1) = i_x(x_2) \Rightarrow x_1 = x_2$$

أي أن f دالة أحادية .

وأخيراً إذا كان $y \in Y$ ، فإن $y = i_y(y)$ يعطي $y = [f \circ g](y) = f[g(y)]$ لأن $g(y) \in X$ فإن f دالة فوقية . بالتالي فإن f لها معكوس من تعريف 1-19 (b) . □

أحياناً مدى الدالة يعتبر أكثر أهمية من الدالة نفسها . في تلك الحالة نغير المصطلحات ونستخدم مصطلحاً جديداً وهو مصطلح العائلة ، والذي يعرف كالآتي .

تعريف 1-20

لتكن I و X مجموعتين . عندئذ الدالة $f : I \to X$ تسمى عائلة وكل عضو في I يسمى دليل . المجموعة I تسمى مجموعة الدليل ومدى f تسمى مجموعة مفهرسة (مفهرسة بواسطة I) .

لكل $f(i), i \in I$ يطلق عليه الحل رقم (i) من العائلة f .

إذا كانت : $f : I \to X$ عائلة فإنه لكل $i \in I$ فإنه من المتفق عليه بأن نشير إلى $f(i)$ عن طريق الرمز f_i ، كذلك فإننا نقول أن $\{f_i\}_{i\in I}$ عائلة . إذا كان مدى f مجموعة من المجموعات فإننا نقول أن f عائلة من المجموعات . ومن ثم فعندما نقول أن $\{S_\alpha\}_{\alpha\in \mathrm{A}}$ عائلة من المجموعات الجزئية أو المفهرسة من المجموعة A ، هذا يعني أن هناك دالة f من A إلى المجموعة X من المجموعات بحيث $f(\alpha) = S_\alpha$ لكل α ضمن A أو تنتمي إليها .

تعريف 21.1

لتكن $\{S_a\}_{a\in A}$ عائلة من المجموعات فإن اتحاد هذه العائلة يكون المجموعة $U_{\alpha\in \mathrm{A}} S_\alpha$ والمكونة من كل تلك العناصر x التي تنتمي على الأقل إلى مجموعة واحدة S_α . أما التقاطع لهذه المجموعة فهي المجموعة $\cap_{\alpha\in \mathrm{A}} S_\alpha$ والتي تتكون من كل تلك العناصر x المشتركة بين جميع المجموعات S_α .

مثال 15

لتكن

$$A_1 = \{\alpha, \beta\},\ A_2 = \{\alpha, \beta, \gamma\},\ A_3 = \{\alpha, \gamma\},\ A_4 = \{\alpha, \beta, \delta\},$$
$$I = \{1, 2, 3, 4\},\ X = \{\alpha, \beta, \gamma, \delta\}$$

$f : I \to P(X)$ دالة معرفة على النحو :

$$f(1) = A_1\ ,\ f(2) = A_2\ ,\ f(3) = A_3\ ,\ f(4) = A_4$$

في هذه الحالة يمكننا القول أن f هي عائلة المجموعات المفهرسة بواسطة I . ويمكننا أن نكتب $f = \{A_i\}_{i\in I}$.

اتحاد هذه العائلة هو :

$$\{\alpha, \beta, \gamma, \delta\} = A_1 \cup A_2 \cup A_3 \cup A_4$$

ويكون التقاطع لهذه العائلة هو $\{\alpha\}$ ، ومرة أخرى فإننا نلفت الانتباه إلى العلاقات العامة .

تعريف 22.1

لتكن R علاقة معرفة في المجموعة X ، فإن

(a) R تسمى عاكسة إذا كان : $(x, x) \in R$ لكل عنصر $x \in X$.

(b) R تسمى متماثلة إذا كان لكل $x, y \in X$ ، $(x, y) \in R$ فإن $(y, x) \in R$.

(c) R تسمى متعدية إذا كان : $(x, y) \in R , (y, z) \in R$ يؤدي إلى أن $(x, z) \in R$ لكل $x, y, z \in X$.

(d) R تسمى لاتناظرية إذا كان لكل : $x, y \in X$ ، $(x, y) \in R$ و $(y, x) \in R$ يؤدي إلى أن $x = y$.

تعريف 23.1

أي علاقة R في المجموعة X تسمى علاقة تكافؤ إذا كانت منعكسة ومتعدية ومتماثلة .

تعريف 24.1

أي علاقة R في المجموعة X تسمى ترتيب جزئي إذا كانت R منعكسة ولاتناظرية ومتعدية .

ملاحظة

الترتيب الجزئي دائماً يشار إليه بالعلاقة $\leq$.

وإذا كان $a \leq b$ ولكن $a \neq b$ في هذه الحالة فإننا نكتب $a < b$.

مثال 16

العلاقة الاعتيادية لتساوي عنصرين في المجموعة S هي علاقة تكافؤ في S .

مثال 17

لتكن X مجموعة كل الخطوط في المستوى الكارتيزي . إن علاقة التوازي المعرفة في المجموعة X هي علاقة تكافؤ وذلك لأنه إذا كان : $a, b, c \in X$ ثلاثة مستقيمات من هذه المجموعة فإن :

1- المستقيم a يوازي نفسه : $a \,//\, a$ فالعلاقة عاكسة .

2- إذا كان $a \,//\, b$ فإن $b \,//\, a$ أي أن العلاقة متماثلة .

3- إذا كان $a \,//\, b$ ، $b \,//\, c$ فإن $a \,//\, c$ علاقة متعدية ، أي أن :

$$a \,//\, b, b \,//\, c \Rightarrow a \,//\, c$$

مثال 18

ليكن n عدد صحيح موجب وثابت .

لأي عددين صحيحين a, b ، فإننا نعرف $a \equiv b \pmod{n}$ ، إذا كان وفقط إذا كان n تقسم ناتج الطرح $a - b$.

إن ذلك يفيد مباشرة بأنه لأي ثلاثة أعداد صحيحة a, b, c فإن :

(i) $a \equiv a \pmod{n}$

(ii) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

(iii) $a \equiv b \pmod{n},\ b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

ومن ثم فإن العلاقة $\equiv$ على مجموعة الأعداد الصحيحة الموجبة Z علاقة تكافؤ ، وهذه العلاقة معروفة بعلاقة التطابق مقياس n أو معيار n .

مثال 19

لأي عددين : $a, b \in N$ حيث N مجموعة الأعداد الطبيعية نعرف $a \leq b$ إذا كان وفقط إذا كان a يقسم b .

إذن فإنه لأي ثلاثة أعداد طبيعية a, b, c :

(i) حيث أن $a = 1.a$ فإن ذلك يؤدي إلى أن a يقسم نفسه أي a يقسم a عليه فإن $a \leq a$.

(ii) $a \leq b$ ، $b \leq a$ فإن ذلك يؤدي إلى أن a يقسم b ، وكذلك b يقسم a وهذا يعني أن $a = b$.

(iii) $a \leq b$ ، $b \leq c$ فإن ذلك يؤدي إلى أن a يقسم b كذلك فإن b يقسم c وهذا بطبيعة الحال يؤدي إلى كون a يقسم c أي أن $a \leq c$.

عليه فإن العلامة $(\leq)$ المعرفة سابقاً هي عاكسة ولاتناظرية ومتعدية في مجموعة الأعداد الطبيعية N وبالتالي فإن $(\leq)$ تمثل ترتيب جزئي في N .

واستناداً إلى $(\leq)$ الترتيب الجزئي المعرف على N فإنه يلاحظ أن 2 لا تقسم 3 كما أن 3 لا تقسم 2 ، وحسب التعريف فإن $3 \not\leq 2$ ، $2 \not\leq 3$.

تعريف 25.1

لتكن $\sim$ علاقة تكافؤ على المجموعة غير الخالية X ، لأي عنصر a ، $a \in X$ أي فصل التكافؤ للعنصر a بالنسبة للعلاقة $\sim$ هو المجموعة :

$$a / \sim = \{b \in X : a \sim b\}$$

حيث لا يكون هناك لبس في علاقة التكافؤ $\sim$ في المجموعة X سوف نشير إلى فصل التكافؤ $a / \sim$ بالرمز $Cl(a)$.

نظرية 26.1

لتكن $\sim$ علاقة تكافؤ على المجموعة X .

لأي $a, b \in X$

(i) $a \in Cl(a)$.

(ii) إما : $Cl(a) \cap Cl(b) = \phi$ أو $Cl(a) = Cl(b)$. وهذا يعني أن أي فصلي تكافؤ للعلاقة R إما أن يكونا منفصلين أو يكونا متساويين .

(iii) X تمثل اتحاد فصول التكافؤ $Cl(a)$.

البرهان

(i) من التعريف : $Cl(a) = \{b \in X : a \sim b\}$ ، حيث أن $a \sim a$ من الانعكاس ، فإننا نحصل على : $a \in Cl(a)$.

(ii) حيث أن : $Cl(a) \cap Cl(b) \neq \phi$ ، فإنه يوجد على الأقل عنصر x بحيث :

$$x \in Cl(a) \cap Cl(b)$$
$$\Rightarrow a \sim x , b \sim x$$
$$\Rightarrow a \sim x , x \sim b \qquad \text{(من التماثل)}$$
$$\Rightarrow a \sim b \qquad \text{(من التعدي)} \qquad (1)$$

لتكن $y \in Cl(b)$ وبالتالي فإن $b \sim y$ ، نستخدم (1) تعدي ~ فنحصل على

$$a \sim y$$

وهذا يعني أن $y \in Cl(a)$

$$\therefore \quad Cl(b) \subseteq Cl(a)$$

وبالمثل بتغيير دور a, b فإننا نحصل على $Cl(a) \subseteq Cl(b)$

$$\therefore \quad Cl(a) = Cl(b)$$

(iii) نفرض أن : $Y = U_{a \in X}\ Cl(a)$

من الواضح أن : $Y \subseteq X$

حيث أن لكل عنصر a بحيث $a \in X$ ، فإن $a \in Cl(a$

$$\Rightarrow a \in Y$$

وبالتالي فإن $X \subseteq Y$

$$\therefore \quad X = Y$$

وهذا يبرهن النظرية . □

في النظرية السابقة رأينا أن علاقة التكافؤ في مجموعة X تحلل X إلى فصول تكافؤ غير منفصلة ، وبصورة عامة أي مجموعة معطاة X ، فإن أي مجموعة (F) لمجموعات جزئية غير خالية من X تسمى تجزيئاً للمجموعة X في حالة كون تقاطع كل زوج من عناصر F المختلفة $= \phi$ (أي يمثل مجموعتين منفصلتين) وكانت X تمثل اتحاد جميع عناصر F .

وعلى ذلك فإنه لو أخذنا : $F = \{Cl(a) \mid a \in X\}$

في النظرية السابقة ، فإننا نرى أن F تجزئ X .

ومن هنا فإن كل علاقة تكافؤ في المجموعة X تحدد تجزيئاً لها . والآن نبرهن العكس .

نظرية 27.1

لتكن $F = \{S_\alpha\}_{\alpha \in \mathrm{A}}$ تجزيئاً للمجموعة X ، فإنه توجد علاقة تكافؤ في X ، بحيث تكون F مجموعة كل فصول التكافؤ تحت تلك العلاقة .

البرهان

أي عنصرين a, b بحيث كان $a, b \in X$ فإن $a \sim b$ إذا كان وفقط إذا كان في نفس المجموعة S_α وبالتالي فإنه لكل ثلاثة عناصر a, b, c في X نجد أن

(i) الانعكاس : من التعريف $X = US_\alpha$ ، يوجد $\alpha \in A$ حيث $a \in S_\alpha$ لهذا ومن التعريف فإن $a \sim a$.

(ii) التماثل : $a \sim b \Rightarrow \exists \alpha \in \mathrm{A}$ بحيث يكون

$$a, b \in S_\alpha \Rightarrow b, a \in S_a \Rightarrow b \sim a$$

(iii) التعدي : $a \sim b, b \sim a \Rightarrow \exists\, \alpha, \beta \in \mathrm{A}$

بحيث كان : $b, c \in S_\beta$ و $a, b \in S_\alpha$ في حالة $\alpha \neq \beta$. من التعريف فإن $S_\alpha \cap S_\beta = \phi$

ومن ناحية أخرى $b \in S_\alpha \cap S_\beta$

وبالتالي فإن $\alpha = \beta$

وبناء على ذلك $a, c \in S_\alpha, a \sim c$

$\therefore$ ~ هي علاقة تكافؤ في X .

نعتبر أي مجموعة S_α و $\alpha \in S_\alpha$. الآن $Cl(a) = \{b \in X \mid a \sim b\}$

حيث أن $a \sim b$ إذا كـان وفقـط إذا كـان a, b كلاهما في نفـس العنصـر مـن F ، فـإذا كـان $a \in S_\alpha$ نجـد أن $b \in S_\alpha$ وبالتـالي فـإن $Cl(a) = S_\alpha$ أو بالتـالي فـإن كـل S_α يمثـل فصـل تكافؤ .

وبالعكـس حيـث أنـه لأي عنصـر b حيـث $b \in X, b \in S_\beta$ لـبعض β $\beta \in A$ وبالتالي نجد $Cl(b) = S_\beta$ ، وعلى ذلك فإن F هي مجموعة كل فصول التكافؤ تحت ~ . وهكذا يكمل البرهان .

تعريف a-27.1

يقـال للمجمـوعتين X, Y أنهمـا متكافئتـان إذا تحقـق وجـود تقابـل أحـادي بـين X, Y .

ملاحظة

إذا كانت X, Y متكافئتان فإننا نكتبهما $X \sim Y$.

مثال a-19

المجموعة Z تكافئ المجموعة "E" مجموعة الأعداد الزوجية الصحيحة ، حيث الدالة

$$f : Z \to E$$

المعرف على النحو $f(x) = 2x , x \in Z$

هي تقابل أحادي .

تعريف b-27.1

يقال للمجموعة X أنها غير منتهية إذا كانت تكافئ مجموعة جزئية منها ، ويقال أن X منتهية إذا كانت خالية أو تكافئ المجموعة $\{1, 2, \ldots, n\}$ حيث n عدد صحيح ، $n > 0$.

مثال b.19

المجموعة Z غير منتهية لكون E مجموعة جزئية فعلية منها و $f : Z \rightarrow E$ المعرفة على النحو $f(x) = 2x$

لكل $x \in Z$ ، وهي تقابل أحادي .

المجموعة $\{a, b, c, d\}$ مجموعة منتهية حيث الراسم :

$$g : \{a, b, c, d\} \rightarrow \{1, 2, 3, 4\}$$

معرف على النحو التالي $g(a) = 2, g(b) = 1, g(e) = 3, g(d) = 4$

وهو يمثل تقابل أحادي .

تعريف c-27.1

يقال للمجموعة X أنها قابلة للترقيم (denumerable) إذا كانت تكافئ N ، (مجموعة الأعداد الطبيعية) .

تعريف d-27.1

يقال أن المجموعة X قابلة للعد إذا كانت تكافئ مجموعة جزئية من N . عليه كل مجموعة قابلة للترقيم هي قابلة للعد في حين المجموعة القابلة للعد ليس بالضرورة أن تكون قابلة للترقيم .

تعريف e-27.1

إذا كانت : $f : X \to Y$ دالة وكانت T مجموعة جزئية من X ، فإن الدالة : $g : T \to Y$ تسمى مقصور أو قيد f إلى T إذا كان

$$g(t) = f(t) \quad \text{لكل} \quad t \in T$$

ونشير لذلك بالرمز f_T .

تمارين محلولة

تمرين 1

لتكن A, B مجموعتان كل منهما تحوي n عنصراً ، وضح أن عدد التقابلات الأحادية من A إلى B هو $n!$.

الحل

نطبق الاستنتاج الرياضي في n .

في حالة $n = 1$ ، $B = \{b_1\}, A = \{a_1\}$

فإنه يوجد تقابل واحد : $f : A \to B$ يعرف على أساس $f(a_1) = b_1$. افرض $n > 1$ ولتكن النظرية صحيحة لكل المجموعات التي تحوي $n - 1$ عنصراً .

لتكن $B = \{b_1, b_2, \ldots, b_n\}$, $A = \{a_1, a_2, \ldots, a_n\}$

وليكن f تقابل أحادي من A إلى B .

نفرض أن : $f(a_1) = b_1$ لبعض i ، $1 \le i \le n$ ، ولما كانت f تقابل أحادي من A إلى B ، f_y أيضاً تقابل أحادي من المجموعة الجزئية $Y = A - \{a_1\}$ إلى $B - \{b_1\}$ وبالتالي فإن عدد التقابلات الأحادية من A إلى B والذي يأخذ a_1 إلى b_i يساوي عدد التقابلات الأحادية من $A - \{a_1\}$ إلى $B - \{b_i\}$ ، ومن فرضية الاستنتاج الرياضي .

$\therefore$ يكون عدد التقابلات الأحادية من A إلى B والتي تأخذ a_1 إلى b_i مساوياً $(n-1)!$ عندما i تأخذ من 1 إلى n ، a_1 يمكن أن يرتبط بأي من $b_1, b_2, \ldots, b_i, \ldots, b_n$ الارتباطات الثنائية الثنائي من A إلى B يكون $n(n-1)! = n!$ وهو المطلوب إثباته .

تمرين 2

لتكن X_i مجموعة غير منتهية ، فإن كل مجموعة تحوي X هي أيضاً مجموعة غير منتهية .

الحل

حيث أن X مجموعة غير منتهية ، فإنه يوجد مجموعة جزئية فعلية Y من X ، ويوجد تناظر أحادي $f : Y \to X$

لتكن T مجموعة تحوي X .

معرف بها $g : T \to Y \cup (T - X)$ على النحو $g(t) = f(t)$ عندما $t \in X$ و $g(t) = t$ عندما $t \in T - X$. من الواضح أن g أحادية ، كذلك فوقية .

وحيث أن Y مجموعة جزئية فعلية من X ، فإنه يوجد عنصر $y \in X$ ولكنه أي y غير موجد في Y ، أي أن $y \notin Y$.

الآن $y \in T$ ، لكن $y \notin T - X$ ، إذن $Y \cup (T - X)$ مجموعة جزئية فعلية من T .

ونتيجة لذلك فإن T مجموعة غير منتهية .

تمرين 3

إذا كان B مجموعة جزئية من A وكانت $f : A \to B$ دالة أحادية ، فإنه يوجد تقابل أحادي بين B, A .

الحل

إذا كانت $A = B$ فإن i_A هو التقابل الأحادي المطلوب .

والآن لتكن $A \neq B$ فإننا نعرف $f^0 = i_A$ ولأي عدد صحيح

$$f^k = f^{k-1}(f)\,, k \geq 1$$

بوضع $C = \{a \in A \mid \exists n \in Z, n \geq 0, \exists x \in A - B; a = f^n(x)\}$

والآن لأي $y \in A$ نعرف $g(y) = f(y)$ إذا كان $y \in C$.

من الواضح أن : $A - B \subseteq C$.

لكل z في C يوجد فقط عدد صحيح غير سالب n كذلك عنصر واحد x في $A - B$ بحيث يكون $z = f^n(x)$

لتكن $t \in f(C)$ وبالتالي فإن $t \in f(C)$ لبعض العناصر $c \in C$ ، وبالتالي أيضاً $c = f^k(x)$ لبعض الأعداد الصحيحة $x \in A - B\,, k \geq 0$

إذن : $t = f^{k-1}(x) \Rightarrow t \in C$ عليه فإن $f(C) \subseteq C$.

والآن لكل $u \in A$ إما أن $u \in B$ أو $u \in A - B$ في حالة $u \in A - B$ و $u \in C, g(u) = f(u) \in B$.

في حالة $u \in B$ فإنه إما $u \in C$ أو $u \notin C$ وفي كلا الحالتين وبتعريف g $g(u) \in B$ ، ومن التفسير أو البناء فإن g أحداية .

مرة أخرى لتكن : $b \in B$.

في حالة $b = g(b)\,, b \notin C$.

وفي حالة $b \in C$ ، لبعض $x \in A - B$ ، $b = f^s(x)$ ، s لا يمكن أن تكون صفر وإلا فإن $b = x \in A - B$ ، وهذا غير منطقي . إذاً $s \geq 1$ ، $b = f\left[f^{s-1}(x)\right] = g\left[f^{s-1}(x)\right]$ وبالتالي فإن g هي تناظر أو تقابل أحادي .

تمرين 4

(نظرية شرودر – برنشتين) :

لتكن A, B مجموعتين بحيث كانت $A \sim X$ لبعض $X \subseteq B$, $B \sim Y$ لبعض $Y \subseteq A$ فإن $A \sim B$.

الحل

نفرض أن $f : A \to X$ تناضر أحادي ، و $g : B \to Y$ تناظر أحادي .

الآن $gf : A \to Y$ دالة أحادية لأن $X \subseteq B$ بما أن $Y \subseteq A$ و $gf : A \to Y$ أحادية ومن التمرين (3) فقد حصلنا على تناظر أحادي : $h : A \to Y$ ، وبالتالي فإن $g^{-1}h : A \to B$ دالة أحادية وفوقية ، إذن : $A \sim B$.

تمرين 5

مجموعة الأعداد الطبيعية x ، $0 < x < 1$ غير محدودة .

الحل

نفرض أن $X = \{x : 0 < x < 1\}$

مجموعة قابلة للترقيم ، عليه فإن $X \sim N$ ، وبالتالي فإن $N \sim X$.

لتكن $f : N \to X$ تناظر أحادي .

لتكن :

$$f0 = C_{11}C_{12}C_{13}\ldots$$
$$f0 = C_{21}C_{22}C_{23}\ldots$$
$$f0 = C_{31}C_{32}C_{33}\ldots$$

وبصفة عامة فإن :

$$f(k) = 0C_{k1}C_{k2}C_{k3}$$

لأي $k \geq 1$ ، حيث C_{Ji} يشير إلى العلامة العشرية في i للرقم $f(j)$.

لنعتبر العدد الحقيقي $0d_1, d_2, d_3, ...$

والتي لكل $i = 1, 2, 3, ...$ يكون $d_i \neq 0, d_i \neq C_{ii}$ و $d_i \neq g$

حيث أن f فوقية . فإنه يوجد عدد صحيح $n \geq 1$ بحيث يكون

$$0.d_1 d_2 d_3 \ldots = f(n) = 0.C_{n1} C_{n2} C_{n3} \ldots$$

ومن ناحية أخرى فإنه إذا عبرنا بكسرين عشريين عن عدد واحد فإنهما لابد أن يكونا متطابقين ، إلا إذا كان الرقم 0 قد تكرر في أحد الكسرين ابتداء من منزلة معينة وفي الآخر الرقم 9 يكون مكرراً كذلك من منزلة معينة . فمثلاً

$$0.120000 \ldots = 0.11999 \ldots$$

وبما أن هذه الحالة مستثناة من الفرض الذي يقول أن $d_i \neq 0$ و $d_i \neq g$ ، ومع ذلك فإن لدينا $d_i = C_{ni}$ لكل $i = 1, 2, ...$ ، وعلى وجه الخصوص $d_n = C_{nn}$ وهذا يناقض $d_i \neq C_{ii}$.

ومن ثم فإن f لا تكون فوقية ، ونتيجة لذلك فإن X غير قابلة للترقيم .

تمرين 6

$R \sim X$ حيث $X = \{x : 0 < x < 1\}$

الحل

عرف : $f : X \to R$ على النحو التالي :

$$f(x) = \frac{2x - 1}{1 - |2x - 1|}$$

حيث $|2x - 1| = 2x - 1$ عندما $x \geq \frac{1}{2}$

و $|2x - 1| = 1 - 2x$ عندما $x \leq \frac{1}{2}$

في الحالة الأولى ، عندما :

(لأن $0 < x < 1$) $, 1 - |2x - 1| = 2 - x = 2(1 - x) > 0$

في الحالة الثانية $1 - |2x - 1| = 2x > 0$

في الحالتين المقام موجب .

لتكن $f(x) = f(y)$

فيكون $\dfrac{2x - 1}{1 - |2x - 1|} = \dfrac{2y - 1}{1 - |2y - 1|}$

والذي يعطي أن $2x - 1$ ، $2y - 1$ موجبان أو سالبان معاً .

لتكن $x, y \geq \dfrac{1}{2}$

$$\begin{aligned} f(x) = f(y) &\Rightarrow \frac{2x - 1}{2 - 2x} = \frac{2y - 1}{2 - 2y} \\ &\Rightarrow (2x - 1)(1 - y) = (2y - 1)(1 - x) \\ &\Rightarrow x = y \end{aligned}$$

في حالة $x, y \leq \dfrac{1}{2}$

$$\begin{aligned} f(x) = f(y) &\Rightarrow \frac{2x - 1}{2x} = \frac{2y - 1}{2y} \\ &\Rightarrow x = y \end{aligned}$$

وبالتالي فإن f أحادية .

لكي تثبت أن f فوقية فإننا نتابع ذلك كما يلي :

لتكن : $y \in R$ ، فإذا كانت $y \leq 0$.

فإن $\dfrac{1}{2(1 - y)} \leq \dfrac{1}{2}$

و $f\left[\dfrac{1}{2(1 - y)}\right] = y$

علاوة على ذلك فإذا كانت : $y \geq 0$.

فإن
$$\frac{2y+1}{2(1+y)} \geq \frac{1}{2}$$

و
$$f\left[\frac{2y+1}{2(1+y)}\right] = \frac{\frac{2y+1}{1+y} - 1}{2 - \frac{2y+1}{1+y}} = \frac{\frac{y}{1+y}}{\frac{1}{1+y}} = y$$

ومن ثم فإن
$$X \sim R$$

وبالتالي
$$R \sim X$$

تمرين 7

المجموعة R غير قابلة للعد .

الحل

إذا كانت R قابلة للعد ، فإن R تكون مكافئة لمجموعة جزئية Y من N .

إذا كانت $Y = N$ فمن تمرين (6) ، $X \sim N$ وهذا يتعارض مع نتيجة التمرين (5) .

لتكن $Y \subset N$ ومن ثم لأن $R \subseteq N \sim N$ ، وتوافقاً مع نظرية (شرودر – برنشين) فسوف نحصل على أن $R \sim N$ والتي تكون مرة أخرى معارضة للتمرينين 6, 5 .

تمارين

1- لتكن T, S مجموعتين ولهما عدد من العناصر n, m على الترتيب ، كم علاقة تتحقق من S إلى T . (الإجابة : 2^{m-2}) .

2- لتكن T, S مجموعتين لهما n, m من العناصر على الترتيب ، وضح أن هناك عدد من الرواسم $= n^m$ تتحقق من S إلى T .

3- $f : X \to Y$ هو راسم فوقي ، وكانت X منتهية ، وضح أن عدد العناصر Y لا يمكن أن يكون أكبر عدد عناصر X .

4- لتكن المجموعتان

$$X = \{1, 2, 3, 4\}, Y = \{\alpha, \beta, \gamma\}$$

ولتكن

$$f_1 = \{(1, \alpha), (2, \alpha), (3, \beta), (4, \gamma)\}$$
$$f_2 = \{(1, \alpha), (1, \beta), (2, \alpha), (3, \beta), (4, \beta)\}$$
$$f_3 = \{(1, \beta), (2, \beta), (3, \beta), (4, \gamma)\}$$
$$f_4 = \{(1, \alpha), (2, \beta), (3, \gamma)\}$$

أجب على الآتي :

(i) أي من تلك f_i, s رواسم من X إلى Y ؟ وما هو نطاقهما ؟

(ii) أي من تلك الرواسم يعتبر فوقياً ؟

(iii) إذا كانت بعض من f_i ليست رواسم ، فما هو السبب .

5- لتكن

$$f : X \to Y$$

راسماً عرف في X $x_1 \sim x_2$ إذا كان وفقط إذا كان $f(x_1) = f(x_2)$ ، وضح أن $\sim$ تكون علاقة تكافؤ في X .

6- لتكن : $f : X \to Y, g : Y \to Z$ دالتين بحيث كان gof أحادياً وفوقياً .
وضح أن f أحادياً و g فوقياً . واعط أمثلة توضح أن f ليس من الضروري أن يكون فوقياً ، كذلك g ليس من الضروري أن يكون أحادياً ، بينما gof يكون أحادياً وكذلك فوقياً .

7- لتكن X مجموعة كل الرواسم من المجموعة A إلى مجموعة الأعداد الحقيقية R لأي $f, g \in X$ نعرف $f \le g$ إذا كان وفقط إذا كان $f(a) \le g(a)$ لكل $a \in A$.
وضح أن $\le$ هي ترتيب جزئي في X .

8- ليكن $f : A \to B, g : B \to C$ تقابلين ، أثبت أن

$$(gof)^{-1} = f^{-1}og^{-1}$$

9- لأي مجموعة X المجموعة

$$\Delta = \{(x, x) : x \in X\}$$

تسمى المجموعة القطرية للمجموعة $X \times X$ لأي علاقة R على X ، فإن معكوس R هو العلاقة $R^{-1} = \{(y, x) \mid (x, y) \in R\}$

برهن الآتي :

(i) العلاقة R في X تكون عاكسة إذا كان وفقط إذا كان $\Delta \subseteq R$

(ii) العلاقة R في X تكون متماثلة إذا كان وفقط إذا كان $R = R^{-1}$

10- من المعروف أن الراسم : $f : X \to Y$ هو علاقة أعطى مثلاً لعلاقة $f : X \to Y$ والتي لا تمثل راسماً .

11- لتكن F مجموعة من المجموعات ، لأي $A, B \in F$ نعرف $A \le B$ إذا كان وفقط إذا كان A مجموعة جزئية من B .

وضح أن $\leq$ هي ترتيب جزئي في F ، (هذا الترتيب الجزئي يسمى علاقة احتواء) .

12- لتكن X مجموعة جميع الخطوط ، لأي $a, b \in X$ نعرف $a \sim b$ إذا كان وفقط إذا كان a عمودياً على b ، وضح أن $\sim$ علاقة تماثل ولكنها ليست عاكسة ولا متعدية.

13- لتكن X مجموعة كل المصفوفات المربعة من السبعة $n \times n$ على تحت الأعداد الحقيقية لأي $A \in X$ ليكن $| A |$ رمزاً محدداً تلك المصفوفة لأي مصفوفتين $A, B \in X$ ، فإننا نعرف $A \sim B$ إذا كان وفقط إذا كان $| A | = | B |$ ، وضح أن $\sim$ علاقة تكافؤ في X .

14- لتكن $X = \{1, 2, 3\}$:

(i) أوجد جميع العلاقات في X .

(ii) أوجد جميع علاقات التكافؤ في X .

(iii) أوجد جميع الترتيبات الجزئية في X .

(iv) أوجد جميع العلاقات في X العاكسة وغير المتماثلة وغير المتعدية .

(v) أوجد كل العلاقات في X المتماثلة وغير العاكسة وغير المتعدية .

(vi) أوجد كل العلاقات في X المتعدية وغير العاكسة وغير المتماثلة .

(vii) أوجد كل العلاقات في X غير المتعدية وغير العاكسة وغير المتماثلة .

15- ليكن $f : X \to Y$ راسماً أثبت ما يأتي :

(i) لأي $B \subseteq Y$ و $ff^{-1}(B) \subseteq B$ ، و $ff^{-1}(B) = B \; \forall B \leq Y$ إذا كان وفقط إذا كان f فوقياً .

(ii) لأي مجموعة جزئية A من X ، $A \subseteq f^{-1}f(A)$ وعلاوة على ذلك $A = f^{-1}f(A)$ لكل $A \subseteq X$ إذا كان وفقط إذا كان f راسماً أحادياً .

(iii) $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ يتحقق لكل المجموعات الجزئية A_1, A_2 من X إذا كان وفقط إذا كان f أحادياً .

(iv) لأي مجموعة جزئية A' من X لتكن A المتممة لها في X فإن $f(A') \supseteq f(A')$ حيث $f(A)$ مكملة $f(A)$ في Y لكل $A \subseteq X$ إذا كان وفقط إذا كان f فوقياً و $f(A') \subseteq f(A)'$ إذا كان وفقط إذا كان f أحادياً .

16- أثبت ما يلي :

(i) علاقة التكافؤ بين المجموعات تكون علاقة تكافؤ .

(ii) إذا كان A, B, A', B' أربعة مجموعات بحيث كان $A \cap B = A' \cap B' = \phi$ ، $B \sim B'$ و $A \sim A'$ فإن $A \cup B \sim A' \cup B'$ وأن $A \times B \sim A' \times B'$.

(iii) لأي مجموعتين A, B لتكن A^B تمثل مجموعة كل الرواسم من B إلى A ، وضح أن : $A \sim B', B \sim B'$ تنتج أن $A^B \sim A'^{B'}$.

(iv) وضح أنه لا يمكن أبداً أن تكون مجموعة A مكافئة لمجموعة القوة لها .

17- أثبت ما يلي :

(i) أي مجموعة جزئية من مجموعة قابلة للعد هي أيضاً قابلة للعد .

(ii) وضح أن الراسم : $f : Z \to N$ بحيث كان $f(n) = 2n \; \forall n \geq 1, f(n) = -2n + 1 \; \forall n \leq 0$ هو تقابلاً أحادياً واستنتج أن Z قابلة للترقيم .

(iii) عرف $f : N \times N \to N$ بحيث كان $f(n, m) = 2^n.3^m$ وضح أن f راسم أحادي وباستخدام (i) وضح أن $N \times N$ قابلة للترقيم .

(iv) لتكن $\{E_i\}_{i \in N}$ عائلة قابلة للعد من المجموعات قابلة للعد بين أن اتحادها يشكل مجموعة [استخدم (iii)] .

(v) وضح أن Q مجموعة قابلة للترقيم .

(vi) وضح أن مجموعة كل الأعداد الحقيقية غير قابلة للعد ، في الحقيقة $R \sim P(N)$ $P(N)$ مجموعة قوى N .

18- لتكن $\{S_\alpha\}_{\alpha \in \Delta}$ و $\{T_\beta\}_{\beta \in \Gamma}$ أي عائلتين من المجموعات ، برهن ما يلي :

(i) $(\cup_{\alpha \in \Delta} S_\beta) \cup (\cap_{\beta \in \Gamma} T_\beta = \cup_{\alpha, \beta}(S_\alpha \cap T_\beta)$ وهذا يعتبر تعميماً لقانون التوزيع .

19- لتكن : $f : X \to Y, g : Y \to Z, h : Z \to X$ ثلاث دوال بحيث كان كل من hgf, gfh أحادياً وكانت fhg فوقية . برهن أن كلاً من f, g, h تقابل أحادي .

20- إذا كانت المجموعة S تحوي n عنصراً ، كان $\alpha : S \to S$ و $\beta : S \to S$ بحيث كان : $| \alpha(S) | = | \beta(S) | = n - 1$. برهن أنه توجد تباديل f و g في S بحيث يكون $\beta = f \alpha g$.

21- ليكن k أي عدد صحيح بحيث كان $1 \le k \le n$ ولتكن X مجموعة تحوي k عنصراً ، Y مجموعة تحوي n عنصراً ، برهن أن عدد الرواسم الأحادية من X إلى Y يساوي $\frac{n!}{(n-k)!}$.

22- ليكن m عدداً صحيحاً بحيث كان $1 \le m \le n$ وليكن $\sigma_n(m)$ عدد الرواسم الفوقية من مجموعة بها n عنصراً إلى مجموعة بها m عنصراً . وضح أن $\sigma_n(m) = m^n - \sum_{k=1}^{m-1} C_n^m \sigma_n(k)$ واستنتج أن :

$$\sigma_n(m) = \sum_{k=0}^{m-1} (-1)^k C_{m-k}^m (m-k)^n = \sum_{j=1}^{m} (-1)^{my} C_s^m j^n$$

23- ليكن $g_{n,k}$ عدد المرتبات k $(a_1, a_2, \ldots, a_k)$ من الأعداد الطبيعية بحيث كان : $a_1 + a_2 + \ldots + a = n$

(a) وضح أن $g_{n,k} = 1$ و $g_{n,k} = \sum_{i=0}^{n} g_{i,k-1}$ لكل $n \in N$ وكل $k \geq 2$.

(b) وضح أن لكل $n \geq 1$ وكل $k > 2$ فإن :

$$g_{n,k} = g_{n-1,k} + g_{n,k-1}$$

(c) استنتج أن لكل :

$$g_{n,k} = {}^{n+k-1}C_{k-1} \qquad : \qquad k \in N, n \in N$$

24- يقال أن الدالة $f : A \to B$ يسارية الحذف (قابلة للحذف يساراً) إذا كان لكل مجموعة C ولأي راسمين h, g من C إلى A بحيث كان $fg = fh$ يؤدي $g = h$ ، أثبت أن الدالة $f : A \to B$ يسارية الحذف إذا كان وفقط إذا كان f أحدياً .

[إرشاد : اجعل f يسارية الحذف ، واجعل $X = \{a\}$ وعرف $\lambda : X \to A$ بحيث كان $\lambda(x) = a\ \forall x \in X$ ، وكذلك $\mu = X \to A$ بحيث يكون : $\mu(x) = b\ \forall x \in X$ وضح أن $f\lambda = f\mu$] .

25- الدالة $f : A \to B$ يقال أنها يمينية الحذف (قابلة للحذف يميناً) إذا كان لأي مجموعة C ولأي راسمين k, g من B إلى C بحيث كان $gf = hf$ يؤدي إلى $g = h$ أثبت أن الدالة $f : A \to B$ فوقية إذا كان وفقط إذا كان f يميني الحذف.

[إرشاد : اعتبر f يمينية الحذف .

ضع $X = \{B - f(A)\} \cup \{\phi\}$ حيث ϕ المجموعة الخالية .

عـــرف : $\lambda : B \to X$ عـــن طريـــق $\lambda(b) = \phi$ عنـــدما $b \in f(A)$ ، وأن $\lambda(b) = B - f(A)$ عندما $b \in B - f(A)$.

وعلى ذلك عرف : $\mu : B \to X$ بواسطة $\mu(b) = \phi$ لكل $b \in B$ ، وضح أن $\lambda f = \mu f$] .

3- التركيبات الثنائية (العمليات الثنائية)

بعدما ناقشنا العلاقة والراسم ، فإننا نقدم مفهوم التركيبة الثنائية في المجموعة ، ولنبدأ باعتبار المجموعة Z (أي مجموعة الأعداد الصحيحة) ، سوف نجد أن هناك ثلاثة عمليات معرفة تعريفاً كاملاً في المجموعة Z وبالتحديد هي عمليات الجمع والضرب والطرح والتي من خلالها نجد أن لكل زوج مرتب (m, n) من عناصر Z تتحدد العناصر $m - n, m \,.\, n, m + n$ على الترتيب من Z ويمكن النظر إلى الجمع والضرب والطرح كثلاث رواسم في $Z \times Z$ إلى Z والتي تحدد لكل عنصر (m, n) في $Z \times Z$ العناصر $m + n$ ، $m \,.\, n$ و $m - n$ على الترتيب في Z . ويستطيع الشخص أن ينشئ الكثير من الرواسم الأخرى بين $Z \times Z$ إلى Z . كل هذه الرواسم تعتبر أمثلة من التركيبات الثنائية والتي نعرفها على النحو التالي :

تعريف 28.1

X مجموعة معطاة ، أي راسم من $X \times X$ إلى X يطلق عليه تركيب ثنائي في X .

لتكن f تركيباً ثنائياً في X . من خلال تعريف f على أنها راسم من $X \times X$ إلى X . فإذا أعطينا $(a, b) \in X \times X$ ، $f(a, b) \in X$ ولداعي الراحة نكتب $a * b$ للتعبير عن $f(a, b)$ ، حيث * هو رمز ثابت ومناسب وسوف نقول أن "*" تركيب ثنائي في X . ومن ثم فإنه لكل $(a, b) \in X \times X$ ، "*" تحدد عنصراً $a * b$ (بالطبع وحيد) من X . التركيبة الثنائية * تسمى جمع أو ضرب أو تركيبة دائرة وفقاً لما نكتبه "+" أو "." أو "0" للرمز * . إذا كان $a, b \in X$ وكان $a \neq b$ نحن نعرف أن $(a, b) \neq (b, a)$ ولذلك فإنه وبصورة عامة فليس ضرورياً أن الزوج (a, b) ، والزوج (b, a) تتساوى صورتي تحت تأثير التركيبة الثنائية في X * . بمعنى آخر فإنه ليس ضرورياً أن تكون التركيبة الثنائية "*" في X

محققة للعلاقة ، $a * b = b * a$ لكل a, b في X . بعض من الأمثلة سوف نناقشها بعد ذكر بعض التعريفات ، تبرر الملاحظة التي أشرنا إليها سابقاً .

تعريف 29.1

لتكن "*" تركيبة ثنائية في X ، فإنه

(i) يقال أن العملية الثنائية "*" تبديلية إذا كان
$a * b = b * a$ لكل $a, b \in X$.

(ii) يقال أن العملية الثنائية "*" تنسيقية إذا كان
$a * (b * c) = (a * b) * c$ لكل : $a, b, c \in X$.

(iii) يقال للعنصر e من X أنه محايد يساري من X بالنسبة للعملية "*" إذا كان $e * a = a$ لكل عنصر $a \in X$.

(iv) يقال لعنصر f من X أنه محايد يميني من X بالنسبة للعملية "*" إذا كان $a * f = a$ لكل عنصر $a \in X$.

(v) إذا كان العنصر i من X محايداً يسارياً محايداً يمينياً معاً ، فإننا نطلق عليه اسم محايد X .

(vi) إذا كان e محايداً في X تحت العملية "*" وكان $a \in X$ فإن العنصر $a' \in X$ يطلق عليه معكوس يساري أو يميني للعنصر a تبعاً لكون
$a' * a = e$ أو $a * a' = e$.

وإذا كان العنصر a'' يمثل كلاً من المعكوس اليميني واليساري للعنصر a ، فإنه يطلق عليه معكوس a ونقول أن a عنصراً قابلاً للعكس أو له معكوس .

نظرية 30.1

إذا كانت "*" عملية ثنائية معرفة في X ، فإن ما يلي يتحقق :

(i) إذا كان للمجموعة X محايد أيمن ومحايد أيسر فإنهما يكونان متساويين .

(ii) إذا كان للمجموعة X محايد (من الجهتين اليمنى واليسرى) فإنه وحيد .

البرهان

(i) لتكن e و f محايدان أحدهما أيسر والآخر أيمن (على الترتيب) للمجموعة X .

وبالتالي فإن $e * f = f$ لكون e محايد أيسر .

وكذلك فإن $e * f = e$ لكون f محايد أيمن .

وبالتالي فإننا نستنتج أن $e = f$.

(ii) بالنسبة للجزء الثاني ، نفرض أن e_1, e_2 محايدان في المجموعة X وحيث أن e_1 محايد أيسر و e_2 محايد أيمن ، واستناداً على برهان الجزء الأول فإن $e_1 = e_2$.

مثال 20

لأي ثلاثة أعداد صحيحة m, n, p نعلم أن :

(i) $m + n = n + m$

(ii) $m + (n + p) = (m + n) + p$

(iii) $m + 0 = m = 0 + m$

(iv) $m + (-m) = 0 = (-m) + m$

وأن $-m$ عدد صحيح أيضاً .

هنا (i) ، (ii) توضحان أن عملية الجمع هي عملية ثنائية تبديلية وتنسيقية في مجموعة الأعداد الصحيحة Z . (iii) توضح أن الصفر (0) هو العنصر المحايد لعملية الجمع في المجموعة Z (iv) توضح أنه لكل : $m \in Z$ فإن $-m$ معكوساً له تحت عملية الجمع .

مثال 21

لأي ثلاثة أعداد صحيحة m, n, p نعلم أن :

(i) $m \,.\, n = n \,.\, m$

(ii) $m \,.\, (n \,.\, p) = (m \,.\, n) \,.\, p$

(iii) $m \,.\, 1 = m = 1 \,.\, m$

وهـذا يوضـح أن عمليـة الضـرب العادية في مجموعـة الأعـداد الصـحيحة Z تبديليـة وتنسـيقية وأن "1" العدد واحد هو العنصر المحايد في المجموعة Z بالنسبة لعملية الضرب .

مـن المعـروف أنـه لأي عـدد صـحيح m يختلـف عـن $1, -1$ فإنـه يوجـد عـدد غـير صحيح n بحيث كـان : $m \,.\, n = 1$ ، وبالتالي فإن m ليس له معكوس في مجموعة الأعداد الصحيحة Z تحت عملية الضرب العادية .

مثال 22

نحن نعلم أنه لأي عددين صحيحين m, n فإن $m - n$ هو أيضاً صحيح ، وبالتالي فإن عملية الطرح هي عملية ثنائية في مجموعة الأعداد الصحيحة Z . الآن : $2, 3, 5 \in Z$ وأن :

(i) $2 - 3 \neq 3 - 2$

(ii) $2 - (3 - 5) \neq (2 - 3) - 5$

(iii) $2 - 0 = 2 \neq 0 - 2$

(i) ، (ii) توضـحان أن عمليـة الطـرح ليسـت تبديليـة وليسـت تنسـيقية . وحيـث أنـه لأي عـدد صـحيح k فـإن $k - 0 = k$ ، وبالتـالي فـإن 0 هـو محايـد أيمـن للمجموعـة Z تحت عمليـة "-" ، لكـن (iii) توضـح أن 0 لـيس محايـداً أيسـر تحـت عمليـة "-" ، وبالتـالي فـإن عمليـة الطـرح لهـا محايـد أيمـن في المجموعـة Z ولا يوجـد لهـا محايـد أيسـر في نفـس المجموعة .

مثال 23

لتكن X أي مجموعة تحوي على الأقل ثلاثة عناصر ، ولتكن $S(X)$ تشير إلى مجموعة كل التباديل للمجموعة X .

النظرية 17.1 توضح أن محصلة التركيبة "0" تنسيقية . الراسم المحايد i في X هو المحايد ، وكل عنصر من $S(X)$ قابل للعكس (أي له معكوس) .

ليكن a, b, c ثلاثة عناصر مختلفة من X ، والدوال $g : X \to X, f : X \to X$ معرفة على النحو التالي :

$f(x) = x \, , f(b) = a \, , f(a) = b$ لكل $x \in X$ ومختلفاً عن a, b .

$g(x) = x$ ، $g(c) = a$ ، $g(b) = c$ ، $g(a) = b$ لكل : $x \neq a, b, c$ ، فتكون :

$f, g \in S(X)$.

والآن : $(gof)(a) = g[f(a)] = g(b) = c$

وأن : $(fog)(a) = f[g(a)] = f(b) = a$

عليه فإن : $(fog)(a) \neq (gof)(a)$

وبالتالي ينتج أن : $fog \neq gof$

ومن ثم فإن تركيب الدوال في $S(X)$ عملية غير تبديلية .

مثال 24

لتكن M_2 مجموعة كل المصفوفات المربعة من الرتبة 2×2 والتي عناصرها أعداد نسبية لأي مصفوفتين : $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ $\quad B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

فإن حاصل الجمع العادي كذلك حاصل الضرب $A + B = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}$

$$AB = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

معرفان وموجودان في M_2 .

وبالتالي فإن الجمع المعتاد للمصفوفات كذلك حاصل الضرب لها عمليتان ثنائيتان في M_2 .

من خلال الخواص المعروفة للمصفوفات فإننا نعلم أن الجمع في M_2 تبديلي وتنسيقي كما أن المصفوفة $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ تمثل العنصر المحايد للجمع .

والمصفوفة $$-A = \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix}$$

تمثل المعكوس الجمعي للمصفوفة A .

وبنفس الطريقة فإن عملية الضرب هي تنسيقية كما أن المصفوفة $$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

هي العنصر المحايد في عملية الضرب .

والمصفوفة التي لها معكوس في عملية الضرب هي المصفوفات غير الشاذة أو غير المنفردة .

وحيث أنه ضرب المصفوفتين $$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

يعطي أن $$AB \neq BA$$

فإن عملية الضرب ليست تبديلية .

جداول التركيب للمجموعات المنتهية

لتكن X مجموعة غير خالية ومنتهية ولتكن * عملية ثنائية معرفة في X .

جدول التركيب العملية * يمكن بناؤه على النحو التالي :

لتكن $$X\{x_1 , x_2 , \dots , x_n\}$$

فإننا نكتب العناصر : $x_1, x_2, \dots, x_n$ للمجموعة X في صف أفقي ، وكذلك في عمود رأسي. وبعد ذلك ضع في الأسفل العنصر $x_i * x_j$ عند تقاطع الصف الذي دليله i

$(1 \le i \le n)$ والعمـود الـذي يليـه j $(1 \le j \le n)$ وبالتـالي سنحصـل علـى الجـدول التالي :

$*$	x_1	x_2	x_3	$\dots$	x_i	$\dots$	x_j	$\dots$	x_n
x_1	$x_1 * x_1$	$x_1 * x_2$	$x_1 * x_3$	$\dots$	$x_1 * x_i$	$\dots$	$x_1 * x_j$	$\dots$	$x_1 * x_n$
x_2	$x_2 * x_1$	$x_2 * x_2$	$x_2 * x_3$	$\dots$	$x_2 * x_i$	$\dots$	$x_2 * x_j$	$\dots$	$x_2 * x_n$
x_3	$x_3 * x_1$	$x_3 * x_2$	$x_3 * x_3$	$\dots$	$x_3 * x_i$	$\dots$	$x_3 * x_j$	$\dots$	$x_3 * x_n$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
x_i	$x_i * x_1$	$x_i * x_2$	$x_i * x_3$	$\dots$	$x_i * x_i$	$\dots$	$x_i * x_j$	$\dots$	$x_i * x_n$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
x_j	$x_j * x_1$	$x_j * x_2$	$x_j * x_3$	$\dots$	$x_j * x_i$	$\dots$	$x_j * x_j$	$\dots$	$x_j * x_n$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
x_n	$x_n * x_1$	$x_n * x_2$	$x_n * x_3$	$\dots$	$x_n * x_i$	$\dots$	$x_n * x_j$	$\dots$	$x_n * x_n$

مثال 25

لتكن $X = \{0, 1, 2, 3\}$ ، و * عملية معرفة في X على النحو التالي :

لأي $a, b \in X$ فـإن $a * b = c$ حيـث c أصـغر باقـي موجـب ينـتج عنـدما $a + b$ يـتم قسمتهما على العدد 4 ، على سبيل المثال :

$$1 * 3 = 0\,,\, 2 * 3 = 1\,,\, 3 * 3 = 2$$

والوارد فيما بعد هو جدول تركيب العملية الثنائية * في X .

*	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

مثال 26

لتكن : $X = \{0,1,2,3\}$ لأي $a, b \in X$ فإن * تعرف على النحو التالي $a * b = b$ فمثلاً $3 = 2 * 3 = 2 , 3 * 2 = 3$.

الجدول التالي يوضح العملية الثنائية * :

*	0	1	2	3
0	0	0	0	0
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3

والآن نعود إلى صديقتنا القديمة مجموعة الأعداد الصحيحة Z .

لتكن E مجموعة كل الأعداد الزوجية الصحيحة ، وبالتالي فإن $E \subset Z$. من المعروف أنه إذا كان n, m عددين صحيحين زوجيين فإن $m + n$ أيضاً عدد صحيح زوجي . وبصورة أخرى فإنه لأي $m, n \in E$ فإن $m + n \in E$ ، وبالتالي نقول أن المجموعة E جزئية من Z ومغلقة تحت عملية الجمع في Z .

والآن نعرف المجموعة الجزئية المغلقة بالنسبة لعملية ثنائية .

تعريف 1-31

لتكن X مجموعة غير خالية ، * عملية ثنائية في X ، المجموعة الجزئية H من X يقال عنها أنها مغلقة تحت العملية الثنائية * ، إذا كان $a * b \in H$ لكل $a, b \in H$.

لتكن X مجموعة غير خالية معرف عليها عملية ثنائية * وكانت A مجموعة جزئية من X مغلقة تحت العملية الثنائية * لأي $a, b \in A$ ، $a * b \in A$ ، فإننا نحصل على

راسم أو دالة $f : A \times A \to A$ بحيث كان $f(a,b) = a * b$ لكل $a, b \in A$. وبالتالي فمن بالتعريف تكون f عملية ثنائية في A . هذه العملية الثنائية f في A يقال عنها حادثة بواسطة * ، وببساطة يطلق عليها عملية ثنائية حادثة .

مثال 27

المجموعة E لكل الأعداد الصحيحة الزوجية مجموعة جزئية من Z مغلقة تحت عملية الجمع .

مثال 28

لتكن K مجموعة كل الأعداد الصحيحة الفردية . K مجموعة جزئية من Z ، بينما نجد أن مجموع أي عددين صحيحين فرديين يساوي عدد صحيح زوجي .

وبالتالي فإذا كان $n \in K, m \in K$ فإن $m + n \notin K$ وبالتالي فأن K ليست مغلقة تحت عملية الجمع . في الوقت الذي تعتبر فيه K مجموعة جزئية من Z مغلقة تحت عملية الضرب .

مثال 28 يوضح أنه إذا كانت هناك أكثر من عملية ثنائية معرفة في مجموعة X ، فإن أي مجموعة A من X قد تكون مغلقة تحت عملية ثنائية واحدة في الوقت الذي قد لا تكون مغلقة بالنسبة للعملية الثنائية الأخرى .

تمارين

1- إذا كانت A مجموعة بها n عنصر ، فكم يكون عدد العمليات الثنائية الممكنة في A .

2- لأي عـددين : $a, b \in Q$ تعرف * على النحـو التـالي : $a * b = \frac{ab}{2}$ ، وضـح أن Z ليست مغلقة تحت * ، بينما E مجموعة كل الأعداد الصحيحة الزوجية تكون مغلقة تحت * .

3- لأي عددين صحيحين m, n نعرف * على النحو : $m * n = m + n + 1$ ، وضح ما يأتي :

(i) E مجموعة كل الأعداد الصحيحة الزوجية ليست مغلقة بالنسبة إلى * .

(ii) K مجموعة كل الأعداد الصحيحة الفردية مغلقة بالنسبة إلى * .

(iii) * تكـون تنسـيقية وتبديليـة وهنـاك محايـد لتلـك العمليـة في مجموعـة الأعـداد الصـحيحة Z وأن كـل عنصر مـن Z قابـل للعكـس (أي لـه معكـوس بالنسبة للعملية *) .

4- لـتكن M_2 مجموعـة كـل المصـفوفات المربعـة 2×2 علـى الأعـداد النسـبية ، لأي $A, B \in M_2$ نعرف

$$A \circ B = \frac{AB + BA}{2}$$

برهن ما يأتي :

(i) $\circ$ عملية تبديلية .

(ii) للمصـــــــــــــفوفات $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

$$(A \circ B) \circ C \neq A \circ (B \circ C)$$

أي أن $\circ$ ليست تنسيقية .

(iii) $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ هو العنصر المحايد بالنسبة إلى "$\circ$" .

5- لأي مصفوفتين A, B في M_2 نعرف $A * B = \dfrac{AB - BA}{2}$

برهن ما يأتي :

(i) لأي : $A \in M_2$ ، $A * A = 0$ حيث $\circ$ هي المصفوفة الصفرية .

(ii) للمصفوفات $A, B, C \in M_2$

$$A * (B * C) + B * (C * A) + C * (A * B) = 0$$

(iii) لا يوجد عنصر محايد في M_2 بالنسبة إلى * .

(iv) لأي : $A, B, C \in M_2$

$$A * (B + C) = A * B + A * C$$
$$(B + C) * A = B * A + C * A$$

(v) وضح أن * ليست تبديلية وليست تنسيقية .

6- لتكن $Z[i]$ مجموعة كل الأعداد المركبة التي على الصورة $a + bi$ حيث a, b عددان صحيحان ، وضح ما يأتي :

(i) $Z[i]$ مغلقة تحت عمليتي الجمع العادية والضرب للأعداد المركبة . $Z[i]$ لها محايد بالنسبة لعملية الجمع ولها محايد بالنسبة لعلمية الضرب ، وضح أن هذين المحايدين مختلفين .

(ii) أوجد كل العناصر من $Z[i]$ التي لها معكوس تحت عملية الضرب .

7- لأي مجموعتين A, B ، فإن المجموعة : $(A - B) \cup (B - A)$ تسمى الفرق التناظري أو التماثلي للمجموعتين A, B ، ويرمز له بالرمز $A \Delta B$. لتكن X أي مجموعة وكانت $P(X)$ مجموعة قوى X برهن ما يأتي :

(i) لأي $A, B \in P(X)$, $A \Delta B \in P(X)$ لأي عدد $A, B, C \in P(X)$.

(ii) $A \Delta B = B \Delta A$.

(iii) $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.

(iv) $A \Delta B = A$ إذا كان وفقط إذا كان $B = \phi$ (قانون برويسكي) .

(v) $A \Delta A = \phi$.

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

[إرشـــــاد للحالـــــة (iii) $(A \Delta B) \Delta C = [A - (B \cup C)] \cup [B - (C \cup A)] \cup$
$[C - (A \cup B)] \cup [A \cap B \cap C]$] .

8- لأي مجموعات A_1, A_2, B_1, B_2 برهن أن

$$(A_1 \cup A_2) \Delta (B_1 \cup B_2) \subseteq (A_1 \Delta B_1) \cup (A_2 \Delta B_2)$$

9- وضح أنه لا يوجد نظام ثنائي بعنصر محايد ومعكوس من الطرفين في حالة عدم تحقيق قانون التنسيق في ثلاثي مرتب .

10- مجموعة A بها n عنصر . كم عدد العمليات الثنائية التبديلية التي يمكن أن تتحقق في A . (جواب : $n^{\frac{n^2+n}{2}}$)

4– بعض النتائج الأولية حول نظرية الأعداد

في الأبواب التالية سنحتاج دائماً لنتائج معينة في نظرية الأعداد ، ولأن معظم هذه النتائج لا تدرس في الجبر الأساسي لذلك نعطي خلاصة مختصرة لنظرية الأعداد التي سنحتاجها في الكتاب .

ملاحظة

خلال هذا القسم كل الحروف اللاتينية الصغرى تشير إلى الأعداد الصحيحة .

تعريف 32.1

يقال أن العدد غير الصفري b يقسم a إذا كان $a = bk$ لبعض k .

اصطلاح : إذا كان b يقسم a فإننا نعبر عن ذلك كتابة b / a .

ملاحظة

جميع العبارات التالية متكافئة .

b تقسم b, a قاسم للعدد b, a عامل للعدد a ، a مضاعف للعدد b .

نظرية 33.1

ليكن a عدداً صحيحاً غير صفرياً فإن :

(i) $a \mid 0$

(ii) $a \mid a$

(iii) إذا كان $a \mid b$ ، فإن $a \mid bc$ لكل c

(iv) إذا كان $a \mid b$ و $a \mid c$ ، فإن $a \mid (bx + c)$ بجمع x, y

(v) إذا كان $a \mid b$ و $b \mid c$ $(b \neq 0)$ ، فإن $a \mid c$

(vi) إذا كان $a \mid b$ و $b \mid a$ $(b \neq 0)$ فإن $a = \pm b$

البرهان

(i) $a.0=0$

(ii) $a=a1$

(iii) $a \mid b \Rightarrow b=ak \Rightarrow bc=a(kc) \Rightarrow a \mid bc$ (لبعض k)

(iv) $a \mid b \Rightarrow b=ak$ (لـبعض k) $a \mid c \Rightarrow c=al$ (لـبعض l) بالتـالي فـإن $a \mid b$ و $a \mid c$ يؤدي إلى أن $b=ak, c=al$ ، هذا يعطي

$$bx+cy=akx+aly=a(kx+ly) \Rightarrow a \mid (bx+cy)$$

(v) $a \mid b, b \mid c \Rightarrow b=ak, c=bl \Rightarrow c=a(kl)$ وذلك لبعض l, k . هذا يعني أن $a \mid c$.

(vi) $a \mid b \Rightarrow b=ak$ (لـــبعض k) $b \mid a \Rightarrow a=bl$ (لـــبعض l) ، بالتـــالي $b=ak=blk \Rightarrow lk=1$ إذاً $k=\pm 1$ وعليه $a=\pm b$. □

وقبل أن نبدأ النظرية التالية ، سنعيد إلى الأذهان قاعدة الترتيب الجيد .

قاعدة الترتيب الجيد

كـل مجموعـة غـير خاليـة مـن الأعـداد الصـحيحة والمحـدودة مـن أسـفل يحـدها مـن أصسفل أصغر العناصر قيمة .

النظريـة التاليـة هـي إحـدى النتـائج الأوليـة لنظريـة الأعـداد ، والشـائع معرفتهـا علـى أسـاس تقسـيم نظـام العـد العـربي العشـري أو في بعـض الأحيـان يعـرف علـى أنـه نظـام العـد الإقليدي .

نظرية 34.1

إذا كـان a, b عـددان صـحيحان $b \neq 0$ فإنـه يوجـد عـددان صـحيحان q, r بحيث يكـــون $a=bq+r$ و $0 \leq r < \mid b \mid$ ، وكـــذلك إذا كـــان $a=bq_1+r_1$ وكانـــت $0 \leq r_1 < \mid b \mid$ فإن $r=r_1$ كما أن $q=q_1$.

البرهان

لتكن $S = \{a - |b|s : s \in Z, a - |b|s \geq 0\}$

حيث أن $|a||b| \geq |a| - a$

فإننا نحصل على $a + |a||b| \geq 0$

ولأن $s = -|a|$ $a + |b||a| = a - |b|s \geq 0$

وهذا يعطي $a - |b|s \in S$

وبالتالي فإن S ليست خالية .

وباستخدام قاعدة الترتيب الجيد فإن S لها عنصر أصغر ، وليكن r .

وبالتالي فإن $r = a - |b|t$

لبعض $t \in Z$.

من الواضح أن $r \geq 0$

ونحن مطالبون بإثبات أن $r < |b|$

ولذلك نفرض أن $r \geq |b|$

فيكون $0 \leq r - |b| < r$

ومن ناحية أخرى فإننا نجد $r - b = a - |b|(1 + t)$

وهنا يعطينا أن $r - |b| \in S$

وهذا يعارض أن r عنصر أصغر في S ، ومن هنا فإن $0 \leq r < |b|$

وبالتالي يكون لدينا

$$a = |b|t + r \quad \text{مع} \quad 0 \leq r < |b| \qquad (1)$$

إذا كانت : $b > 0$ و $b = |b|$ ، فبوضع $q = t$ في (1) ، فإننا نحصل على

$a = bq + r$

إذا كانت : $b < 0$ و $-b = | b |$ فإنه بوضع $q = -(t)$ فإننا نحصل على

$a = bq + r$

والآن نبرهن وحدانية r, q .

لذلك نفرض أن $a = bq' + r', q', r' \in Z, 0 \le r' < | b |$

فإننا نحصل على $bq + r = bq' + r'$

وبالتالي فإن $b(q - q') = r' - r$

إذا كان $q \ne q' . | b(q - q') | \ge | b |$

ولكن $| r' - r | \le \max (r, r') < | b |$

وهذا يوصلنا إلى تناقض .

وبالتالي فإن $q = q'$ ، وكذلك $bq + r = bq + r'$

وعليه فإن $r = r'$ ، وهذا يبرهن النظرية . □

تعريف 35.1

يقال للعدد الصحيح الموجب c أنه عامل مشترك أكبر (ع.م.أ) و (HCF) لعددين a, b إذا كان .

(i) $c | a, c | b$

(ii) إذا كان $d | b, d | a$ فإن $d | c$

تعريف 36.1

يقال للعدد الصحيح الموجب g أنه مضاعف مشترك أصغر لعددين صحيحين غير صفريين a, b إذا كان (م.م.أ) .

(i) $a | g, b | g$

(ii) إذا كان $b \mid h, a \mid h$ فإن $h \mid g$

(HCF) أو (ع.م.أ) للعددين a, b يرمز له بالرمز (a, b)

(LCM) أو (م.م.أ) للعددين a, b يرمز له بالرمز $[a, b]$

ملاحظة هامة

إذا كان هناك ع.م.أ للعددين الصحيحين a, b فإنه يكون وحيداً ، لأننا إذا افترضنا أن c' ع.م.أ آخر للعددين a, b فمن الفقرة (ii) من التعريف 35.1 نجد أن

نظرية 33.1

$$\begin{aligned} c' \mid c, \quad c \mid c' &\Rightarrow c = \pm c' \\ &\Rightarrow c = c' \end{aligned}$$

وكلا العددين c, c' موجبين .

بالمثل نستطيع أن نثبت أن م.م.أ لعددين a, b هو عدد وحيد .

مثال 29

6 هو أعلى عامل مشترك أكبر بين 12, 18 .

كل عوامل العدد 12 هي $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

بينما كل عوامل العدد 18 هي $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$

ومن الواضح أن $6 \mid 12, 6 \mid 18$

وأيضاً فإن كل عامل مشترك للعددين 12 ,18 هو عامل للعدد 6 .

مثال 30

العدد 36 هو مضاعف مشترك أصغر للعددين 12, 18 ، فمن الواضح أن

$18 \mid 36, 12 \mid 36$

إذا كانت $h \mid 12, h \mid 18$ ، فإن $h \mid 4, h \mid 9$

وبالتالي فإن $h \mid 36 = 4.9$ (انظر نتيجة 2 نظرية 1-39 لأن $(4,9) = 1$) .

النظرية التالية توضح وجود العامل المشترك الأكبر لكل زوج من الأعداد الصحيحة غير الصفرية .

نظرية 37.1

كل زوج من الأعداد الصحيحة غير الصفرية a, b لها عامل مشترك أكبر .

البرهان

لتكن $X = \{ta + ub : t, u \in Z\}$

من الواضح أن $a = 1.a + 0.b \in X$ ، وبالتالي فإن X تحتوي على الأقل عدداً صحيحاً واحداً مغايراً للصفر .

وزيادة على ذلك إذا $\alpha = ta + ub \in X$

عدد صحيح سالب فإن $-\alpha = (-t)\, a + (-u)\, b$

عدد صحيح موجب في X .

وبالتالي فإن X تكون مجموعة جزئية غير خالية من الأعداد الصحيحة بها على الأقل عدد صحيح موجب .

وباستخدام قاعدة الترتيب الجيد فإنه يوجد $c = xa + yb$ أصغر عدد موجب وصحيح ينتمي إلى المجموعة X .

والمطلوب منا الآن هو إثبات أن $c = (a, b)$

ومن خوارزمية القسمة فإن لأي $ka + lb \in X$ يكون $ka + lb = cg + r$

حيث $0 \le r < c$.

في حالة $r \ne 0$ نجد أن

$$r = ka + lb - cq = ka + lb - (xaq + ybq) = (k - xq)\, a + (l - yq)\, b$$

يكون عدداً موجباً ينتمي إلى X .

عندما $r < c$ فإننا نحصل على تناقص بالنسبة لاختيار c .

وبالتالي فإن $r = 0$.

بمعنى آخر : $c \mid ka + lb$ أي أن c عامل لكل عنصر من المجموعة X .

لأن $a = 1a + 0b, b = 0a + 1b$

عناصر من X ، فإننا نحصل على كون $c \mid a, c \mid b$.

افرض الآن : $d \mid a$ و $d \mid b$ فإن $d \mid (xa + yb)$ ، (نظرية 1-33) وبالتالي $d \mid c$ أي أن $c = (a, b)$.

تعريف 38.1

العددان الصحيحان غير السالبين b, a يقال أنهما أوليان لبعضهما البعض ، أو أوليان نسبياً إذا كان $(a, b) = 1$.

مثال 31

4 ,9 أوليان نسبياً لكون عوامل 4 هي $\pm 1, \pm 2, \pm 4$ بينما تلك الخاصة العدد 9 فهي $\pm 1, \pm 3, \pm 9$ ، وبالتالي فإن العامل المشترك الأكبر بين 4 ,9 هو 1 .

نظرية 39.1

العددان الصحيحان غير السالبين a, b أوليان نسبياً إذا كان وفقط إذا وجد x, y بحيث كان $ax + by = 1$ (محايد بيزوت) .

البرهان

ليكن : $(a, b) = 1$ ، وبالتالي فباستخدام نظرية 1-37 يكون $1 = ax + by$ ، لبعض x, y .

وبالعكس ليكن : $ax + by = 1$ لبعض x, y . نفرض أن $c = (a, b)$ ، فإن $c \mid a, c \mid b$. وباستخدام نظرية 33.1 فإن $c \mid (ax + by) \Rightarrow c \mid 1$ ولأنه $c > 0$ فإن هذا يعطي $c = 1$ وبالتالي فإن $(a, b) = 1$. □

نتيجة 1

إذا كان $a \mid bc$ و $(a, b) = 1$ فإن $a \mid c$.

البرهان

لأن $(a, b) = 1$ فإن $ax + by = 1$ لبعض x, y ونحصل على $acx + bcy = c$.

الآن $a \mid a$ ، $a \mid b$ ، عليه حسب نظرية 1-33 فإن $a \mid [a(cx) + (bc)y]$ أي أن $a \mid c$. □

نتيجة 2

إذا كان $a \mid b, c \mid b, (a, c) = 1$ فإن $ac \mid b$.

البرهان

لأن $(a, c) = 1$ فإن $ax + cy = 1$ لبعض x, y .

والآن $a \mid b \Rightarrow b = ak$ لبعض k ، وبالتالي فإننا نجد أن $akx + kcy = k$ أي أن $bx + kcy = k$ ، لأن $c \mid c, c \mid b$ فإن $c \mid (xb + kyc)$ (نظرية 1-33) ، وهذا يؤدي إلى كون $c \mid k$ أو $k = cd$ لبعض d ، إذاً $b = ak = acd \Rightarrow ac \mid b$. □

تعريف 1-40

أي عدد صحيح : $P > 1$ يقال عنه أنه أولي (عدد أولي) إذا كانت عوامله هي فقط $\pm P$ و ± 1 .

مثال 32

2, 3, 5, 7, 11, 13, 17, 19 كلها أعداد أولية ، بينما 4, 6, 8, 10 ليست أعداد أولية .

تعريف 1-41

أي عدد صحيح $n > 1$ يقال أنه مركب إذا كان غير أولياً . وبتعبير آخر فإن العدد الصحيح : $n > 1$ يطلق عليه مركب إذا كان بالإمكان تحليل n إلى $a.b$ بحيث كان $b > 1, a > 1$.

نظرية 1-42

إذا كان P عدد أولي فإنه لأي عدد صحيح n ، إما $(n, P) = 1$ أو $(n, P) = P$.

البرهان

نفرض أن $(n, P) = d$ ، وبالتالي فإن $d \mid n, d \mid P$.

d عدد موجب وأن العوامل الموجبة الوحيدة للعدد P هي 1 و P . وبالتالي تحققت النظرية . □

نتيجة

إذا كان P عدد أولي بحيث كان $p \mid ab$ في هذه الحالة إما $P \mid a$ أو $P \mid b$.

البرهان

باستخدام النظرية السابقة ، إذا كان $P \nmid a$ فإن $(P, a) = 1$ ، وبتطبيق نتيجة 1 من النظرية 39.1 فإننا نجد أن $P \mid b$. □

والآن نقدم ما يسمى بالنظرية الأساسية لعلم الحساب .

نظرية 43.1 (النظرية الأساسية في علم الحساب)

إذا كان n عدداً صحيحاً موجباً أكبر من 1 ، فإنه يمكن كتابة n بصورة وحيدة على الشكل $P_1^{k_1} . P_2^{k_2} \dots P_t^{k_t}$

حيث : $P_1 > P_2 > P_3 > \dots > P_t$ ، كلها أعداد أولية ، وأنه لجميع قيم i ، $1 \le i \le t$ فإن k_i كلها أعداد صحيحة أكبر من 0 .

البرهان

بالاستنتاج الرياضي على n . وقبل كل شيء نبرهن أن n إما أن يكون عدد أولي أو يكون حاصل ضرب أعداد أولية ، عندما $n = 2$ فإنه من الواضح أن المطلوب تحقق . وبالتالي نفرض أن $n > 2$ ولكي نطبق الاستنتاج الرياضي فإننا نجعل كل عدد صحيح m بحيث كان $2 \le m < n$ إما أن يكون عدد أولي أو حاصل ضرب الأعداد أولية .

إذا كانت $n = P$ عدد أولي فإننا نتوقف وقد وصلنا إلى المطلوب ، وإلا نعتبر $n = ab$ لبعض الأعداد الصحيحة الموجبة a, b وكلاهما أصغر من n . وبالتالي فإن $2 \le a, b < n$ ، وبواسطة افتراض الاستنتاج الرياضي

$$a = P_1 P_2 .. P_s$$

و

$$b = q_1 q_2 \dots q_n$$

لبعض الأعداد الأولية q_i, P_i وهكذا فإن

$$n = P_1 . P_2 \dots P_s . q_1 . q_2 \dots q_i$$

هو حاصل ضرب أعداد أولية .

وعند التعبير عن n على كونه حاصل ضرب مجموعة من الأعداد الأولية بواسطة تجميع الأعداد الأولية المتساوية معاً . يمكن لنا كتابته n على الصورة

$$n = P_1^{k_1} . P_2^{k_2} \dots P_i^{k_i} \qquad (1)$$

لبعض الأعداد الأولية $P_1 > P_2 > \dots > P_i$ والأعداد الصحيحة الموجبة $1 \le i \le t , k_i$.

ونطبق الاستنتاج الرياضي على t لنثبت أن التعبير السابق لـ n هو وحيد ، وبالتالي نفرض أيضاً أن :

$$n = q_1^{s_2} . q_2^{s_2} \dots q_u^{s_u} \qquad (2)$$

لبعض الأعداد الأولية $q_1 > q_2 > q_3 > \dots > q_u$ ، والأعداد الصحيحة الموجبة s_i .

الآن $P_1 \mid n$ تعطينا $P_1 \mid q_1^{s_1} . q_2^{s_2} \dots q_u^{s_u}$. تطبيقاً للنظرية 1-42 $P_1 \mid q_i^{s_i}$ لبعض i . هذا في النهاية يعطينا $P_1 \mid q_i$ ، وبالتالي فإن $P_1 \le q_i$ ، وبنفس الطريقة $q_1 \le P_j$ لبعض j .

وبالتالي فإن $q_1 \le P_1, P_1 \le q_1$ يعطينا $P_1 = q_1$.

نفرض أن $s_1 < k_1$ نجد أن $P_1^{s_1} = q_1^{s_1}$ من (1) و (2) فإننا نحصل على

$$n = P_1^{k_1} . P_2^{k_2} \dots P_i^{k_i} = q_2^{s_2} . q_3^{s_3} \dots q_u^{s_u}$$

ولأن $k_1 - s_1 > 0$ فإننا نحصل على $P_1 \mid n$ ، وبالتالي من خلال $n = q_2^{s_2} . q_3^{s_3} \dots q_u^{s_u}$ فإننا نحصل على $P_1 \mid q_i$ لبعض $i \ge 2$. ومن ناحية أخرى $q_i < q_1 = P_1$ ، ومن ثم فإن P_1 لا يمكن أن تقسم q_1 . وهذا يؤدي على تناقض ، بالتالي $s_1 \not< k$ بالمثل $k_1 \not< s$. عليه $k_1 = s_1$. إذن (1) ، (2) يعطيان :

$$h = P_2^{k_2} . P_3^{k_3} \dots P_i^{k_i} \qquad (3)$$

$$= q_2^{s_2} . q_3^{s_3} \dots q_u^{s_u} \qquad (4)$$

وحيث أنه في (3) يوجد عدد $(t - 2)$ من الأعداد الأولية المختلفة فإننا نحصل باستخدام الاستنتاج أن الافتراضان (3) ، (4) تعبيران متشابهان . وهذا يعني أن $t - 1 = s - 1$ ، (وبالتالي $t = s$) حيث $P_i = q_i, k_i = s_i$ $2 \le i \le t$ ، وهذا يبرهن النظرية .

إذا كانت $c = P_2^{k_2} \dots P_t^{k_t} = q_2^{s_2} \dots q_r^{s_r} = 1$ فإن $k_2 = \dots = k_t = s_2 = \dots = s_r = 0$
وهذا مرفوض لكون كل $k_i > 0, s_j > 0$.
إذن $c > 1$. من الواضح أن $c < n$. بالتالي وعن طريقة افتراض الاستنتاج :
$r - 1 = t - 1$ و $k_i = s_r$ و $P_i = q_i$ لكل $2 \le i \le r - 1$ وبالتالي $r = t$
$k_j = s_j, P_i = q_j$ لكل $1 \le j \le r$ وبالتالي فقد برهنت النظرية . □

نتيجة

مجموعة الأعداد الأولية ليست منتهية .

البرهان

نفرض أن مجموعة الأعداد الأولية منتهية ، وبالتالي يمكن وضعها في تناظر أحادي مع المجموعة $\{1, 2, 3, \dots, n\}$ ، لبعض عدد طبيعي n .
ليكن $f(i) = P_i$ لكل $1 \le i \le n$ ، بالتالي فإن $\{P_1, P_2, \dots P_n\}$ هي مجموعة كل الأعداد الأولية .
والآن اعتبر العدد الصحيح $P_1 P_2 P_3 \dots P_n + 1$.
وحيث أن $P_1 . P_2 . P_3 \dots P_n + 1 > 1$ ، وبتطبيق النظرية السابقة فإنه يوجد عدد أولي q بحيث كان $q \mid (P_1\ P_2\ P_3 \dots P_n + 1)$ ، والآن فإن كل الأعداد الأولية يجب أن تكون ضمن عناصر المجموعة $\{P_1, P_2, \dots P_n\}$ ، وبالتالي $q = P_i$ لبعض $1 \le i \le n$ ، وهذا يؤدي على كون $q \mid P_1 P_2 \dots P_n$ كنتيجة لذلك $q \mid 1$ ، والذي يتنافى مع المنطق ، وبالتالي فإن رأينا قد ثبت . □

تعريف 1-44

لأي عدد صحيح $n \ge 1$ ، عدد كل الأعداد الصحيحة i و $1 \le i \le n$ بحيث كان $(n, j) = 1$ تسمى φ دالة أويلر (أو دالة توتينت) ويرمز لها بالرمز $\varphi(n)$.

مثال 33

$\varphi(1) = 1 , \varphi(2) = 1 , \varphi(3) - 2 , \varphi(4) = 2$

لحساب $\varphi(12)$ فإننا نعتبر $1, 2, 3, 4, 5, \ldots, 12$ بداية بالعدد (1) ، فإننا نلاحظ أن :

$(1, 12) = 1 , (2, 12) = 2 , (3, 12) = 3 , (4, 12) = 4 , (5, 12) = 1 ,$
$(6, 12) = 6 , (7, 12) = 1 , (8, 12) = 4 , (9, 12) = 3 , (10, 12) = 2$
$(11, 12) = 1 , (12, 12) = 12$

وبالتالي فإن فقط الأعداد $1, 5, 7, 11$ تحقق شرط التعريف .

إذن $\varphi(12) = 4$.

فيما يلي نعطي صيغة تجعل حساب $\varphi(n)$ سهل لكل $n > 1$.

نظرية 1-45

إذا كانت : $P_1, P_2, \ldots, P_k$ عوامل أولية مختلفة للعدد n فإن :

$$\phi(n) = n\left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)\ldots\left(1 - \frac{1}{P_k}\right)$$

البرهان

نستطيع أن نكتب : $n = P_1^{t_1} . P_2^{t_2} \ldots P_k^{t_k}$

لبعض الأعداد الأولية : $P_1 > P_2 > \ldots > P_k$

وللأعداد الموجبة الصحيحة t_i ، $1 \le i \le k$ حيث $(r, n) = 1, 1 \le r \le n$ إذا كان وفقط إذا كان $P_1, P_2, \ldots, P_2$ أي منهم لا يشكل عاملاً للعدد r .

$\therefore$ العدد $\varphi(n)$ يعتبر من الأعداد الصحيحة ويقع بين $n, 1$ والتي لا يكون أي منها له P_i عاملاً .

لأي $m \ge 2$ وأي من العوامل الأولية المختلفة $q_1, q_2, \ldots, q_i$ من m ضع $\varphi_{q_i \cdot q_2 \ldots q_i}(m)$ يساوي عدد الأعداد الصحيحة الموجبة $\le m$ ولا يقبل القسمة على أي من q_j , $1 \le j \le i$. من الواضح أن :

$$\varphi(n) = \varphi_{P_1, P_2 \ldots k_2(n)} \qquad (1)$$

باستخدام الاستنتاج الرياضي على i ، فإننا نبرهن أن :

$$\phi_{q_1, q_2, \ldots, q_i}(m) = \left[1 - \frac{1}{q_1}\right]\left[1 - \frac{1}{q_2}\right]\ldots\left[1 - \frac{1}{q_i}\right] \qquad (2)$$

الآن الأعداد الصحيحة الموجبة $\le m$ والقابلة للقسمة على q_1 هي :

$$q_1, 2q_1, \ldots \left[\frac{m}{q_1}\right] q_1$$

هذه عددها $\frac{m}{q_1}$.

وبالتالي فإن الباقي $\left[1 - \frac{1}{q_1}\right] m = m - \frac{m}{q_1}$ هو عدد صحيح موجب $\le m$ وهي غير قابلة للقسمة على q_1 .

ونتيجة لذلك فإن $\varphi(m) = m\left(1 - \frac{1}{q_1}\right)$.

وبالتالي فإن (2) تتحقق للعدد $i = 1$ ولأي عدد صحيح موجب m .

ولنطبق الاستنتاج الرياضي ، افرض أنه لبعض $i = s$ ، (2) تتحقق لأي عدد صحيح موجب m . ولتكن : $q_1, q_2, \ldots q_{s+1}$ هو $(s + 1)$ من العوامل الأولية المختلفة للعدد m (لاحظ أن m يمكن أن يكون لها عوامل أولية أكثر) وبالتالي :

$$\phi q_1, q_2, \ldots, q_s^{(m)} = m\left(1 - \frac{1}{q_2}\right)\ldots\left(1 - \frac{1}{q_2}\right) \qquad (3)$$

لتكن X مجموعة الأعداد الصحيحة الموجبة $\le m$ والتي لا تقبل القسمة على أي من q_i , $1 \le i \le s$.

وبالتالي فإن (3) تحدد العدد $|X|$ من عناصر المجموعة X . بعض عناصر X ربما يقبل القسمة على q_{s+1} .

الآن الأعداد الصحيحة الموجبة $\le m$ وقابلة القسمة على q_{s+1} هي :

$$q_{s+1}, 2q_{s+1}, \ldots \left[\frac{m}{q_{s+1}}\right] q_{s+1}$$

العنصر من X سيكون قابلاً للقسمة على q_{s+1} فقط إذا كان على الصورة $d.q_{s+1}$ ، $1 \le d \le \frac{m}{q_{s+1}}$ ، وكانت d غير قابلة القسمة على أي من q_i , $1 \le i \le s$. وبالتالي فإن عدد عناصر X الغير قابلة للقسمة على q_{s+1} مساوٍ للعدد u من الأعداد الصحيحة الموجبة $d \le \frac{m}{q_{s+1}}$ الغير قابلة للقسمة على أي من q_i ، $1 \le i \le s$ ، وبالتالي :

$$\phi_{q_1, q_2, \ldots, q_{s+1}^{(m)}} = \phi_{q_1, q_2, \ldots, q_s^{(m)}} - u \qquad (4)$$

ومن ناحية أخرى خلال فروض الاستنتاج الرياضي فإن (3) تعطي :

$$u = \varphi_{q_1, q_2, \ldots, q_s}\left(\frac{m}{q_{s+1}}\right)$$

$$= \frac{m}{q_{s+1}}\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\ldots\left(1 - \frac{1}{q_s}\right) \qquad (5)$$

باستخدام (3) ، (4) ، (5) فإننا نحصل على :

$$\varphi_{q_1, q_2, \ldots, q_{s+1}^{(m)}} = m\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\ldots\left(1 - \frac{1}{q_{s+1}}\right)$$

وبالتالي فإن (2) تتحقق لكل i .

إذن (1) ، (2) يعطيان :

$$\varphi(n) = \varphi_{P_1, P_2, \ldots P_k^{(n)}} = n\left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)\ldots\left(1 - \frac{1}{P_k}\right)$$

وهذا يبرهن النظرية . □

نتيجة

إذا كان a, b عددان صحيحان ≥ 1 بحيث كان $(a, b) = 1$ فإن $\varphi(ab) = \varphi(a) . \varphi(b)$.

البرهان

إذا كان أي من a أو b يساوي (1) فإن النتيجة واضحة التحقق حيث $\varphi(1) = 1$.

وبالتالي ليكن $a > 1$ كذلك $b > 1$ فإن $b = q_1^{\beta_1} \dots q_s^{\beta_s}, a = P_1^{\alpha_1} \dots P_k^{\alpha k}$

حيث لكل $1 \le i \le k$ و $1 < j \le s$ ، P_i, q_i أعداد أولية ، $\alpha_i > 0$ و $\beta_j > 0$ لأن $(a, b) = 1$ ، $P_1, P_2, \dots P_k, q_1, q_2, \dots, q_s^1$ كلها أعداد أولية مختلفة .

الآن : $a . b = P_1^{\alpha_1} \dots P_k^{\alpha_k} . q_1^{\beta_1} \dots q_s^{\beta_s}$

وبتطبيق النظرية السابقة نجد أن :

$$\phi(ab) = P_1^{\alpha_1} \dots P_k^{\alpha_k}\ q_1^{\beta_1} \dots q_s^{\beta_s}\left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)\dots\left(1 - \frac{1}{P_k}\right)$$
$$\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\dots\left(1 - \frac{1}{q_s}\right)$$
$$= P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k}\left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)\dots\left(1 - \frac{1}{P_k}\right)$$
$$\times\ q_1^{\beta_1} . q_2^{\beta_2} \dots q_s^{\beta_s}\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\dots\left(1 - \frac{1}{q_s}\right) = \phi(a)\phi(b)$$

مثال 34

$36 = 2^2 . 3^2$ وبالتالي فإن : $\phi(36) = 36\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12$ ، وبصورة مباشرة يستطيع أن يتأكد بأن :

1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35

وهي أعداد أولية نسبياً للعدد 36 وهي أقل من 36 .

ملاحظة

النتيجة السابقة ليست صحيحة في حالة $(a, b) \neq 1$ ، فعلى سبيل المثال اجعل $b = 6, a = 4$ وبالتالي فإن $ab = 24, \phi(a) = \phi(4) = 2, \phi(b) = \phi(6) = 2$

وأن $\phi(ab) = \phi(24) = 8$

ولكن $8 \neq 2 \times 2$

نظرية 46.1

إذا كانت $d \geq 1 , n \geq 1$ فإن $\sum_{d|n} \phi(d) = n$

البرهان

إذا كانت $n = 1$ فإن العامل الوحيد الموجب للعدد 1 هو 1 وبالتالي فإننا نحصل على

$$\sum_{d|n} \phi(d) = \phi(1) = 1 = n$$

إذا كانت $n > 1$ نفرض أن $n = P_1^{\alpha_1} , \alpha_1 > 0$

العوامل الموجبة للعدد n هي فقط $1, P_1, P_1^2, \ldots, P_1^{\alpha_1}$ وبالتالي فإن :

$$\sum_{d|n} \phi(d) = \phi(1) + \phi(P_1) + \phi(P_1^2) + \ldots \phi(P_r^{\alpha_1})$$

$$= 1 + P_1\left(1 - \frac{1}{P}\right) + P_1^2\left(1 - \frac{1}{P_1}\right) + \ldots + P_1^{\alpha_1}\left(1 - \frac{1}{P_1}\right)$$

$$= 1 + (P_1 - 1) + (P_1^2 - P_1^1 + \ldots (P_1^{\alpha_1} - P_1^{\alpha_1})$$

$$= P_1^{\alpha_1} = n$$

إذا كانت : $n = P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_k^{\alpha_k}$ بحيث كان $\alpha_k > 0$ واجعل النتيجة صحيحة لكل الأعداد الصحيحة ≤ 1 ولها $k - 1$ من الأعداد الأولية المختلفة كعوامل .

نستطيع أن نكتب $n = q \, . \, P_1^{\alpha_1}$ بحيث كان $q = P_2^{\alpha_2} \ldots P_k^{\alpha_k}$ ، من الواضح أن : $(q, P_1) = 1$.

والآن العوامل الموجبة للعدد n تكون على الصورة $d, dP_1 , dP_1^2, \ldots, dP_1^{\alpha_1}$

وبالتالي فإن :

$$\sum_{d|n}\phi(d)\sum_{d|q}\phi(d)+\sum_{d|q}\phi(dP_1)+\ldots+\sum_{d|q}\phi(dP_1^{\alpha_1})$$
$$=\sum_{d|q}\phi(d)+\sum_{d|q}\phi(d)\,.\,\phi(P_1)+\ldots+\sum_{d|q}\phi(d)\,.\,\phi(P_1^{\alpha_1})$$
$$=\sum_{d|q}\phi(d)+\phi(P_1)\sum_{d|q}\phi(d)+\ldots+\phi(P_1^{\alpha_1})\sum_{d|q}\phi(d)$$
$$=\{1+\phi(P_2)+\ldots\phi(P_1^{\alpha_1})\}\sum_{d|q}\phi(d)$$
$$=P_1^{\alpha_1}q$$ (من فروض الاستنتاج الرياضي)
$$=n$$

تمارين محلولة

تمرين 1

إذا كانت a, b, c أعداد طبيعية فإن :

$$\max\{\min\{a,b\},\min\{a,c\}\}=\min\{a,\max\{b,c\}\}$$

الحل

إذا كان a هو الأصغر بين a, b, c فإن $LHS=\max\{a,a\}=a$

والآن : $a\le c, a\le b$ يؤدي إلى $a\le\max\{b,c\}$ ، وبالتالي $RHS=a$.

ومن ثم فإن النتيجة تحققت في هذه الحالة .

إذا كان a هو الأكبر بين a, b, c فإن $LHS=\max\{b,c\}$

مرة ثانية : $a\ge b, b\ge c$ يؤدي إلى : $a\ge\max\{b,c\}$ ، وبالتالي :

$$\min\{a,\max\{b,c\}\}=\max\{b,c\}$$

ومن ثم فإن النتيجة تحققت في هذه الحالة أيضاً ، وبالتالي فإنه يتم مناقشة حالتين فقط عندما $c \le a \le b$ وعندما $b \le a \le c$ ، وبسبب التماثل في c, b من حيث النتيجة المراد برهنتها ، فإنه يكتفى أن نناقش الحالة $b \le a \le c$.

$$LHS = \max\{b, a\} = a$$
$$RHS = \min\{a, c\} = a$$

وبالتالي فإن النتيجة تتحقق لكل $a, b, c \in N$

تمرين 2

إذا كان $a, b, c \in N$ فإن $\left(a, [b, c]\right) = [(a, b), (a, c)]$ ، وبمعنى آخر فإن عملية HCF تكون توزيعية على عملية LCM .

الحل

في حالة $a = 1$, $LHS = [1, 1]$ و $RHS = 1$.

في حالة $b = 1$ فإن $LHS = [1, (a, c)] = (a, c)$, $RHS = (a, c)$

إن حالة $c = 1$ شبيهة بتلك التي فيها $b = 1$ وبالتالي نفترض أن كل من a, b, c أكبر من الواحد . يمكننا كتابة

$$a = P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_s^{\alpha_s}$$
$$b = P_1^{\beta_1} P_2^{\beta_2} \ldots P_s^{\beta_s}$$
$$c = P_1^{\gamma_1} P_2^{\gamma_2} \ldots P_s^{\gamma_s}$$

حيث لكل $1 \le i \le s$, $\alpha_i, \beta_i, \gamma_i$ كلها أعداد صحيحة غير سالبة .

لتكن $\delta_i = \min\{\alpha_i, \beta_i\}$ ، $\theta_i = \min\{\alpha_i, \gamma_i\}$ ، $h_i = \max\{\delta_i, \theta_i\}$ ، $\phi_i = \max\{\beta_i, \gamma_i\}$ ، $\psi_i = \min\{\alpha_i, \phi_i\}$.

لأن $(a, b) = P_1^{\delta_1} P_2^{\delta_2} \ldots P_s^{\delta_s}$ ، (أثبتها !) :

$$(a, c) = P_1^{\theta_1} P_2^{\theta_2} \ldots P_s^{\theta_s}, [b, c] = P_1^{\phi_1} P_2^{\phi_2} \ldots P_s^{\phi_s}$$

$(a,[a,c]) = P_1^{\psi_1} \dots P_s^{\psi_s}$ كذلك $[(a,b),(a,c)] = P_1^{h_1} P_2^{h_2} \dots P_s^{h_s}$ ، وبالتالي فإننا نحتاج إلى برهان أن $\hbar_i = \psi_i$ لكل i . وبأسلوب آخر يجب إثبات أن

$$\max[\min\{\alpha_i, \beta_i\}, \min\{\alpha_i, \gamma_i\}] = \min\{\alpha_i, \phi_i\} = \min\{\alpha_i, \max\{\beta_i, \gamma_i\}\}$$

لكل $1 \le i \le s$.

ولكن هذا ما برهناه في تمرين (1) .

تمرين 3

إذا كان a, b عددان صحيحان موجبان بحيث كان : $(a,b) = c$ و $[a,b] = d$ فإن : $ab = cd$.

الحل

حيث أن $(a,b) = c$ فإن $a = kc$ ، $b = lc$

$$(a,b) = c, a = kc, b = lc$$

ندعي أن $(l,k) = 1$. إذا كان $(l,k) = d'$ فإن : $d' \mid k, d' \mid l$

وبالتالي فإن $d'c \mid b, d'c \mid a$

ولكن من تعريف HCF (العامل المشترك الأعلى) فإن هذا يؤدي إلى : $d'c \mid c$ أو $c = d'cu$ لبعض u .

وبتعبير آخر $d'u = 1$ فإن $d' = 1$ وبالتالي فإن ادعائنا قد تحقق .

الآن اعتبر lkc . من الواضح أن $a \mid lkc$ و $b \mid lkc$. افرض $a \mid x$ و $b \mid x$ بالتالي فإن :

$$x = aw = by \Rightarrow kcw = lcy \Rightarrow kw = ly$$

ولكن $(l,k) = 1$ إذن $l \mid w$ وهذا يعطينا $w = lm$ أو $x = alm = lkcm$

أي أن $lkc \mid x$

كنتيجة $lkc = [a,b]$ ، ومن خلال وحدانية المضاعف المشترك الأصغر فإننا نحصل على $d = lkc$ أو $cd = (kc)(lc) = ab$.

تمرين 4

وضح أنه إذا كانت $m \geq 2$ فإن مجموع كل الأعداد الصحيحة الموجبة التي أصغر من m والأولية نسبياً بالنسبة للعدد m هو $\frac{1}{2} m\phi\,(m)$

الحل

نفرض أن $x_1, x_2, \ldots, x_{\phi(m)}$ هي $\phi(m)$ للأعداد الصحيحة الموجبة $\leq m$. والأولية بالنسبة للعدد m . لأي i و $1 \leq i \leq \phi(m)$ ، $1 \leq x_i \leq m$ يعطينا $1 \leq m - x_i < m$ لأي عدد صحيح موجب d ، m / d و $d \mid (m - x_i)$ يعطينا $d \mid [m - (m - x_i)]$ أي أن $d \mid x_i$ وبالتالي $d = 1$ ونتيجة لذلك : $m - x_i \in x = \{x_1, x_2, \ldots x_{\phi(m)}\}$

وحيث أنه لأي $i \neq j$ ، $x_i \neq x_j$ يعطينا $m - x_i \neq m - x_j$.

فإننا نحصل على $m - x_i$ هي كل عناصر X . وبالتالي فإن

$$(m - x_1) + (m - x_2) + \ldots + (m - x_{\phi(m)} = x_1 + x_2 + \ldots x_{\phi(m)}$$

ونتيجة لذلك فإن $m\phi(m) = 2(x_1 + x_2 + \ldots + x_{\phi(m)}$

وبالتالي فإن $x_1 + x_2 + \ldots + x_{\phi(m)} = \frac{1}{2} m\phi(m)$

تمارين

1- إذا كان : $a = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k}$, $b = P_1^{\beta_1} P_2^{\beta_2} \dots P_k^{\beta_k}$ حيث P_i هي أعداد أولية مختلفة وأن كل $\alpha_i \geq 0 , \beta_i \geq 0$ هي أعداد صحيحة ، برهن أن :

(i) $(a, b) = P_1^{\delta_1} P_2^{\delta_2} \dots P_k^{\delta_k}$ حيث $\delta_i = \min\{\alpha_i, \beta_i\}$ لكل i .

(ii) $[a, b] = P_1^{\gamma_1} P_2^{\gamma_2} \dots P_k^{\gamma_k}$ حيث $\gamma_i = \max\{\alpha_i, \beta_i\}$ لكل i .

2- a, b معلومة بتطبيق خوارزمية إقليدس ، و $0 \leq r_2 \leq r_1$ و $b = q_1 r_1 + r_2$ ، $a = q_0 b + r_1$ ، $0 \leq r_1 \leq | b |$

$$r_1 = q_2 r_2 + r_3, 0 \leq r_3 < r_2, \dots, r_k = q_{k+1} r_{k+1} + r_{k+2}, \quad 0 \leq r_{k+2} \leq r_{k+1}$$

حيث الأعداد الصحيحة r_k تناقصية وكلها غير سالبة ، يوجد أول عدد صحيح n بحيث كان $r_{n+1} = 0$.

أثبت أن : $r_n = (a, b)$ (نعتبر هنا أن $r_0 = | b |$) .

3- إذا كان $\left(\frac{a}{c}, \frac{b}{c} \right) = 1$ $c > 0, c \mid a, b \mid c,$ فإن $c = (a, b)$ ، برهن ذلك .

4- إذا كانت $a, b, c \in N$ ، وضح أن : $([a, b], [a, c]) = [a, (b, c)]$

5- وضح أنه إذا كان a, b أعداد صحيحة موجبة بحيث كان $(a, b) = 1$ فإن $(a + b, a - b)$ إما يساوي 1 أو 2 .

6- برهن أن : $n > 1$ هو عدد أولي إذا كان وفقط إذا كان لأي a إما $(a, n) = 1$ أو $n \mid a$.

7- $a, b, c \in N$ بحيث كانت $a^2 + b^2 = c^2$ وضح أن $a = 2kmn$, $b = k(m^2 - n^2)$, $c = k(m^2 + n^2)$ لبعض $k, m, n \in N$ بحيث كان $m > n$ وأن m, n مختلفة التماثل ، (بمعنى أنه إما m فردي و n زوجي أو m يكون زوجي و n فردي) .

2

الزمر Groups

مقدمة

في الفصل السابق درسنا مفهوم العلاقات والرواسم والعمليات الثنائية . وفي هذا الفصل سوف نعد أنفسنا لدراسة نظام جبري يطلق عليه الزمرة . وقبل أن نعرف الزمرة ، دعنا نحدد أو نقرر أن الزمرة هي عبارة عن نظام يتكون من مجموعة غير خالية G وعملية ثنائية معرفة في G وتحقق بعض المبادئ أو المسلمات . الأهمية لمفهوم الزمرة ينجم من كون أن هناك عدد كبير من الأنظمة الجبرية تشكل زمر . وهذه سوف يتم توضيحها من خلال أمثلة يتم عرضها بعد تعريف الزمرة . ونحن نأمل في جعل الملاحظة حول لعب نظرية الزمر جزءاً مؤثراً في تطور الهندسة ، ونظرية الأعداد في الأوقات الحالية .

1- تعريف وأمثلة

تعريف 1.2

الزمرة : النظام : $< G , * >$ حيث G مجموعة غير خالية و $*$ عملية ثنائية معرفة على G يسمى زمرة إذا حقق البديهيات أو المسلمات التالية :

1- **قانون التنسيق** : $a * (b * c) = (a * b) * c \ \forall a, b, c \in G$.

2- **وجود المحايد** : يوجد عنصر $e \in G$ يسمى محايد ، بحيث كان :
$$a * e = a = e * a \ \forall a \in G$$

3- **وجـود المعكـوس** : لكـل عنصـر $a \in G$ يوجـد عنصـر $a^{-1} \in G$ يسـمى معكوس a بحيث كان : $a * a^{-1} = e = a^{-1} * a$.

بالإضـافة إلى الشـروط الثلاثـة السـابقة ، فـإن الشـرط التـالي إذا تحقـق تسـمى الزمرة تبديلية أو أبيلية .

4- **قانون التبديل** : $a * b = b * a \quad \forall a, b \in G$.

الزمرة $< G , * >$ والتي لا يتحقق فيها الشرط أو المسلمة (4) تسمى زمرة غير أبيليـة . إذا كانـت المجموعـة G منتهيـة فـإن $< G , * >$ تسـمى زمـرة منتهيـة ، وإذا كان غير ذلك فإنها تسمى زمرة غير منتهية .

لـبعض الأغـراض المحـدودة فـإن المفـاهيم المبسـطة لشـبه الزمـرة أو نصـف الزمـرة يعتـبر هامة ، وبالتالي فإننا نعرف شبه الزمرة .

تعريف 2.2

النظام الرياضي $< G , * >$ المكون من مجموعة غير خالية G وعملية ثنائية $*$ معرفة على G يسمى شبه زمرة (أو نصف زمرة) إذا حقق الشرط أو المسلمة التالية :

1- **قـانون التنسـيق** : $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$ مـع التشـابه الجزئـي للزمر ، يمكننا أن نتحدث حول شبه الزمر المنتهية ، وشبه الزمر الغير منتهية وشبه الزمر الأبيلية وغير الأبيلية ، نلاحظ أن الزمرة دائماً هي في الأصل شبه زمرة ، بينما العكس ليس صحيحاً على العموم كما سنوضح خلال الأمثلة فيما بعد .

في وصف زمرة معينة على الشخص أن يحدد العملية الثنائية والمجموعة G والتي فيها تتحقـق العمليـة الثنائيـة . لقـد تم في الفصـل السـبق توضـيح أنـه مـن الممكـن تعريـف أكثـر مـن عملية ثنائية على المجموعة G . وبالتالي فإن المجموعة الواحدة يمكـن أن تجزأ إلى العديـد مـن الزمـر المختلفـة . ومـع ذلـك إذا كـان في الزمـرة $< G , * >$ لا يوجـد احتمـال حـول أي لـبس

بالنسبة للعملية الثنائية سوف نشير ببساطة إلى المجموعة G على كونها زمرة . إذا أردنا أن نكون مهمتين بالعملية ، فإننا سوف نقول أن المجموعة G هي زمرة تحت تأثير العملية * .

أمثلة من الأعداد

مثال 1

كما أوضحنا في الفصل الأول ، الجزء الثالث أن عملية الجمع العادية + المعرفة على مجموعة الأعداد الصحيحة Z هي تبديلية وتنسيقية وأن الصفر عنصر محايد في عملية الجمع ، وأنه لكل عنصر : $a \in Z$ فإن $-a$ المعكوس الجمعي للعنصر a وبالتالي فإن $< Z , + >$ هي زمرة أبيلية ، والأكثر من ذلك فإن $< Z , + >$ هي زمرة غير منتهية لكون Z مجموعة غير منتهية .

مثال 2

لتكن Z' مجموعة كل الأعداد الصحيحة الغير سالبة . حيث أن مجموع الصحيحين الغير سالبين هو غير سالب ، Z' مغلقة تحت عملية الجمع "+" . الجمع في Z' تبديلي وتنسيقي والصفر 0 عنصر محايد بالنسبة للمجموعة Z' . وبالتالي فإن $< Z' , + >$ هو شبه زمرة أبيلية بعنصر محايد . وهي غير منتهية باعتبار أن Z' مجموعة غير منتهية . الآن ولأي عنصر $a\ (\neq 0)$ في Z' لا يوجد عدد صحيح غير سالب b (بمعنى أنه لا يوجد b في Z') بحيث كان $a + b = 0$. وبالتالي فإن Z' هو شبه زمرة وليست زمرة .

مثال 3

لتكن Q^* مجموعة كل الأعداد النسبية الغير صفرية . حاصل ضرب عددين نسبيين غير صفريين هو عدد نسبي غير صفري ، بالتالي فإن Q^* مغلقة تحت عملية الضرب . لأي $r, s, t \in Q^*$ ، من المعروف أن :

$$r(st) = (rs)t \qquad \text{(i)}$$
$$1.r = r.1 = r, \quad 1 \in Q^* \qquad \text{(ii)}$$
$$r \,.\, \frac{1}{r} = 1, \quad \frac{1}{r} \in Q^* \qquad \text{(iii)}$$
$$rs = sr \qquad \text{(iv)}$$

وبالتالي فإن Q^* هي زمرة أبيلية تحت عملية الضرب .

Q^* زمرة غير منتهية .

مثال 4

في خطوات مماثلة كتلك التي اتبعت في مثال رقم (3) يمكن للشخص أن يوضح أن المجموعة R^*, C^* الغير صفرية من الأعداد الحقيقية R والغير صفرية من الأعداد المركبة C أنها تشكل زمر أبيلية تحت عملية الضرب . كلاً منهما زمرة غير منتهية .

مثال 5

ليكن n عدد صحيح موجب و G هي مجموعة الأعداد المركبة ، وعناصرها الجذور النونية للواحد الصحيح ، حيث أن هناك n جذر ، فإن G لها n عنصراً . G تعتبر زمرة أبيلية منتهية تحت عملية الضرب .

مثال 6

لتكن : $S = \{0, 1, 2, \ldots, n-1\}$ حيث n عدد صحيح موجب . للعددين : $a, b \in S$ تعرف العملية $a * b$ على أساس أصغر عدد صحيح غير سالب c نحصل عليه كباقي ، عندما $a + b$ يتم قسمته على العدد n (فعلى سبيل المثال : $S = \{0, 1, 2, 3, 4\}, n = 5$ فإن : $2 * 4 = 1$ ، $3 * 2 = 0$ ... وهكذا) ، العملية $*$ عملية ثنائية في S وتسمى الجمع بمقياس أو معيار n و $a * b = r$ يؤدي على كون

$a + b - r$ يقبل القسمة على n . وسنبين أن S تكون زمرة تحت هذه العملية الثنائية .
لتكن $a, b, c \in S$.

(i) التنسيق :

لتكن $a * b = d$, $(a * b) * c = d * c = r$ وحيث أن d هو هو أصغر عدد غير سالب متبقي حصلنا عليه عندما $a + b$ قسم على العدد n فيكون لدينا $a + b = d + kn$ لبعض قيم k الصحيحة . وبالمثل $d + c = r + k_1 n$ لبعض قيم k_1 الصحيحة . وبالتالي فإن :

$$(a + b) + c = d + kn + c = r + (k_1 + k)\, n, 0 \leq r < n$$

المعادلة الأخيرة توضح أن r هو أصغر باقي غير سالب نحصل عليه من قسمة $a + (b + c)$ بالعدد n .

بنفس الطريقة ، إذا كان $a * (b * c) = s$ فإن s يكون أصغر باقي غير سالب حصلنا عليه من قسمة $a * (b * c)$ بالعدد n ومن ناحية أخرى $(a + b) + c = a + (b + c)$. بالتالي فإن أصغر البواقي الغير سالبة r, s لابد وأن تكون متساوية .

إذن $(a * b) * c = a * (b * c)$.

(ii) وجود العنصر المحايد

لأي $a \in S$ فإننا نهدف إلى إثبات أن $a * 0 = a$. حيث أن $0 \leq a < n$ ، $0 + a = a + 0 = 0n + a$ تعطينا a أصغر باقي غير سالب نحصل عليه نتيجة قسمة a بالعدد n وبالتالي $a * 0 = 0 * a = a$ وبالتالي فإن 0 هو العنصر المحايد في S .

(iii) وجود المعكوس

لأي $a \in S$ إذا كان $a = 0$ فإن $0 = 0 * 0$ ، وفي حالة $a \neq 0$ فإنه ولأن $0 < n - a < n$ ، $n - a \in S$ وبالإضافة إلى ذلك فإن :

$$(n - a) + a = a + (n - a) = 1n + 0$$

وهذا يعطينا $(n - a) * a = a * (n - a) = 0$ ، وبالتالي فإن $n - a$ يعتبر معكوس a تحت العملية * .

إذن S تشكل زمرة تحت * . ويمكن توضيح أن $< S , * >$ زمرة أبيلية .

اصطلاح

$a + b \equiv c \pmod n$ حيث $a, b, c \in Z$ و n عدد صحيح موجب يعني به n تقبل القسمة على $a + b - c$.

مثال 7

لتكن :

$$S = \{x \in Z \ : \ 1 \leq x \leq n \ \text{ and } \ (x, n) = 1\}$$

* عملية معرفة على S كما يلي :

لكل $a, b \in S$ ، $a * b$ هو أصغر عدد صحيح موجب يتحقق كباقٍ عندما $a . b$ يقسم على n هذا يسمى الضرب بمقياس n . من الواضح أن $a * b = b * a$.

أولاً نوضح أن * عملية ثنائية في S .

ليكن $a * b = c$. الآن c لا يمكن أن يكون صفر وإلا فإن n / ab سيكون لا معنى له باعتبار $(a, n) = 1$ و $(b, n) = 1$ وبالتالي : $1 \leq c < n$. زيادة على ذلك إذا كان $(c, n) \neq 1$ فإنه يوجد عدد أولي P بحيث كان p / c و p / n . وهذا يعطينا p / ab ، وعندما $a * b = c$ فإن ذلك يؤدي إلى كون : $ab = c + kP$ لعدد الصحيح k ، وباعتبار P أولي فإنه إما p / a أو p / b . بالتالي فإنه إما P يقسم العامل المشترك الأعلى بين n, a أو العامل المشترك الأعلى بين n, b وهو من المستحيل لأن $(a, n) = 1$ و $(b, n) = 1$

. وبالتالي $(c, n) = 1$. ومن هذا المنطلق فإن $c \in S$. هذا يثبت تأكيدنا بأن $*$ عملية ثنائية معرفة على S .

هذه العملية تسمى الضرب بمقياس n .

(i) التنسيق

إذا كان :

$$(a * b) * c = r_1 * c = r_2 \ , \ a * b = r_1$$

يعني أن : $r_1 c = r_2 + k_2 n$ لعدد صحيح k_2 .

الآن : $ab = r_1 + k_1 n$ لعدد صحيح k_1 وكذلك $r_1 c = r_2 + k_2 n$.

وهذا يؤدي إلى كون :

$$(ab - k_1 n)\, c = r_2 + k_2 n$$
$$\Rightarrow abc = r_2 + (k_2 + k_1 c)\, n$$

وستكون محصلة ذلك كون r_2 هو أصغر باقي غير سالب تم الحصول عليه من قسمته $(ab)\,c$ بواسطة n .

وبنفس الطريقة إذا كان :

$$a * (b * c) = r_3$$

فإن r_3 هو أصغر باقي غير سالب تم الحصول عليه نتيجة قسمة $a(bc)$ بواسطة n . ولكن $(ab)\,c = a\,(bc)$ وبالتالي فإن $r_2 = r_3$ إذن $(a * b) * c = a * (b * c)$.

(ii) وجود المحايد

من الواضح أن $1 \in S$ وأنه : $\forall a \in S$ فإن $1 * a = a * 1 = a$ وبالتالي فإن 1 هو العنصر المحايد في S .

(iii) وجود المعكوس

ليكن $a \in S$. إذن $(a, n) = 1$ وبالتالي يوجد عددين صحيحين x, y بحيث كان:

$$ax + ny = 1$$

من ناحية أخرى ومن خوارزمية القسمة $0 \le r < n , x = qn + r$

فإن

$$1 = ax + ny = a(qn + r) + ny = ar + ny = ar + n\,(aq + y) \quad (1)$$

افترض $d = (r, n)$ ، وحيث أن d / n و d / r فإن المعادلة السابقة تعطينا أن $d / 1$ وبناء على ذلك $d = 1$ وبالتالي فإن $r \in S$. مرة أخرى (1) تعطينا : $ar = n(-aq - y) + 1$ أي أن 1 هو أصغر باقي غير سالب تم الحصول عليه نتيجة قسمة ar بواسطة n .

من هنا فإن $a * r = 1$ ولما كانت هذه العملية تبديلية فإنه يتحقق لدينا أيضاً $r * a = 1$ ، وبالتالي فإن $r = a^{-1}$ في S . ويكون $< S , * >$ زمرة أبيلية . وبناء على ذلك فإن $(r, n) = 1$ وبالتالي $r \in S$.

وعلى ذلك فإن $< S , * >$ زمرة . ويمكن أن نتحقق من كونها أبيلية .

اصطلاح

المقصود بكتابتنا $ab = c \,(\text{mod})$ (مقياس n) أن $ab - c$ قابلة القسمة على n .

ملاحظات

1- من الملاحظ أنه خلال برهان أن :

$$(a * b) \ne c = a * (b * c)$$

فإننا لم نستخدم a, b, c على أساس كونهم أعداد صحيحة أصغر من n ، وأولية بالنسبة إليه. وبالتالي فإن "*" تكون تنسيقية بصورة عامة .

2- كحالة خاصة ، إذا اعتبرنا $n = P$ عدد أولي ، فإن كل الأعداد الصحيحة :
$1, 2, \dots, P-1$ كلها أولية بالنسبة إلى P وكلها أصغر من P .
في هذه الحالة فإن $< S , * >$ يطلق عليها زمرة الأعداد الصحيحة تحت عملية الضرب بمقياس P .

مثال من المتجهات

مثال 8

المجموعة V لكل المتجهات في المستوى ، والتي تبدأ من نقطة الأصل 0 هي زمرة أبيلية غير منتهية تحت عملية جمع المتجهات .

في هذه الزمرة فإن المتجه الصفري $\bar{0}$ هو محايد الجمع ، ولكل متجه $\bar{a}$ فإن $-\bar{a}$ هو المعكوس الجمعي للمتجه $\bar{a}$.

أمثلة من المصفوفات

مثال 9

لأي عدد موجب n ، المجموعة G_n لكل المصفوفات المربعة $n \times n$ على الأعداد المركبة تشكل زمرة أبيلية منتهية تحت عملية جمع المصفوفات كعملية ثنائية . المصفوفة الصفرية تعتبر المحايد الجمعي ، ولكل $A \in C_n$ فإن $-A$ تعتبر المعكوس للمصفوفة A .

مثال 10

لتكن G مجموعة المصفوفات التالية :

$$\pm\begin{Bmatrix} 1 & 0 \\ 0 & 1 \end{Bmatrix} \;,\; \pm\begin{Bmatrix} i & 0 \\ 0 & -i \end{Bmatrix} \;,\; \pm\begin{Bmatrix} 0 & i \\ i & 0 \end{Bmatrix} \;,\; \pm\begin{Bmatrix} 0 & 1 \\ -1 & 0 \end{Bmatrix}$$

حيث $i = \sqrt{-1}$. إنه يمكن وبسهولة إثبات أن كل المصفوفات الغير منفردة ، وأن المجموعة G مغلقة تحت عملية الضرب للمصفوفات ، فإن G تكون زمرة تحت هذه العملية . G هي زمرة منتهية وليست تبديلية (أثبت ذلك) .

مثال لزمرة التحويلات

مثال 11

لتكن S مجموعة غير خالية ، ولتكن $A(S)$ مجموعة كل التباديل الممكنة في S . لقد برهنا في نظرية 1-17 أنه لكل $f, g \in A(s)$ ، فإن fog يعني راسماً من S إلى S . معرفاً على أساس : $(fog)(s) = f[g(s)]$ لكل : $s \in S$ ، وبالتالي فإن $A(s)$ لها الخصائص التالية :

لكل $f, g, h \in A(s)$.

(i) $fog \in A(s)$

(ii) $f \circ (goh) = (f \circ g) \circ h$.

(iii) يوجد $i \in A(s)$ بحيث كان : $f \circ i = f = i \circ f$.

(iv) لكل $f \in A(s)$ يوجد $f \in A(s)$ بحيث كان $f \circ f' = i = f' \circ f$.

وبالتالي فإن العملية "$\circ$" هي عملية ثنائية في $A(s)$ ، وبالتالي أصبحت $A(s)$ زمرة تحت هذه العملية .

إذا كانت S بها n عنصراً فإن $A(s)$ بها $n!$ عنصراً وأن $A(s)$ زمرة منتهية . زيادة على ذلك إذا كانت S بها 3 أو أكثر من العناصر — كما هو موجود في مثال 23 الفصل الأول — فهناك $f, g \in A(s)$ بحيث $f \circ g \neq g \circ f$ ، ونتيجة لذلك فإن $A(s)$ ليست زمرة أبيلية عندما يكون S بها أكثر من عنصرين . في حالة كون S مجموعة غير منتهية فإن $A(s)$ تكون زمرة غير منتهية وغير أبيلية .

تمارين

1- لتكن Q^+ مجموعة الأعداد النسبية الموجبة ، $*$ معرفة على Q^+ على النحو التالي : لكل $a, b \in Q$ فإن $a * b = \frac{ab}{3}$ ، برهن أن $< Q^+ , * >$ زمرة أبيلية .

2- لتكن S مجموعة كل الأعداد الحقيقية ماعدا -1 ,$*$ معرفة على S وذلك على النحو التالي : $a * b = a + b + ab$ لكل : $a, b \in S$ ، وضح أن $< S , * >$ هي زمرة أبيلية .

3- أعط مثالاً حول زمرة غير أبيلية تختلف عن تلك التي أعطيت في هذا الكتاب سابقاً.

4- لتكن R^* مجموعة كل الأعداد الحقيقية ما عدا 0 ,$*$ معرفة على R^* على النحو التالي : $a * b = | a | b$ ، حيث $| a |$ تشير إلى القيمة المطلقة للعدد a . وضح أن :

(i) $*$ تنسيقية في R^* .

(ii) يوجد محايد أيسر للعملية $*$.

كذلك معكوس أيمن لكل عنصر في R^* . هل $< R^* , * >$ زمرة ؟ اعط سبباً لتأكيد إجابتك .

[إرشاد : 1 ,-1 كلاهما محايد أيسر بالإشارة إلى بند 2**]** .

5- اعط أمثلة عن أنظمة $< G , * >$ حيث G مجموعة غير خالية $*$ عملية ثنائية معرفة في G ، بحيث :

(i) $< G , * >$ يحقق كل من : $G - 1, G - 2$ ولا يحقق $G - 3$.

(ii) $< G, * >$ يحقق كل من : $G-3, G-1$ ولا يحقق $G-2$.

(iii) $< G, * >$ يحقق كل من : $G-3, G-2$ ولا يحقق $G-1$.

[**إرشاد** : في حالة (iii) اعتبر : $G = \{e, a, b\}$, $*$ معرفة في G وباستخدام الجدول التالي :

$*$	e	a	b
e	e	a	b
a	a	e	a
b	b	b	e

في هذا المثال $*$ ليست تبديلية . هل يمكنك إيجاد مثال مشابه تكون فيه $*$ تبديلية ؟ .

6- حدد أي الأنظمة الرياضية التالية تعتبر زمر . اذكر الأسباب لماذا لا تكون البقية الباقية ليست زمرة :

(i) مجموعة G لكل المصفوفات غير المنفردة $n \times n$ على مجموعة الأعداد المركبة مع عملية ضرب المصفوفات .

(ii) مجموعة الأعداد الطبيعية N تحت عملية الجمع .

(iii) مجموعة الأعداد الحقيقية R تحت عملية الضرب .

(iv) المجموعة : $G = \{1, a, b, c\}$ تحت العملية الثنائية المعرفة وفق جدول العملية التالي :

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

[يعرف ذلك بالزمرة الرباعية لكلاين] .

(v) المجموعة $G = \{\alpha, \beta, \gamma, \delta\}$ تحت العملية الثنائية المعرفة من خلال جدول العملية التالي :

	α	β	γ	δ
α	α	β	γ	δ
β	α	β	γ	δ
γ	α	β	γ	δ
δ	α	β	γ	δ

(vi) المجموعة G لكل الجذور النونية للواحد بحيث n تتغير من 1 إلى ∞ تحت عملية الضرب .

(vii) المجموعة $G = \{(m, n) \mid m, n \in Z; m \neq 0 \text{ or } n \neq 0\}$. مع العملية $*$ المعرفة في G على النحو التالي :

$$(a, b) * (c, d) = (ac - bd, ad + bc)$$

(viii) المجموعة E لكل الأعداد الصحيحة الزوجية مع عملية الجمع .

(ix) المجموعة E لكل الأعداد الصحيحة الزوجية مع العملية الثنائية $*$ المعرفة على النحو التالي :

$$a * b = 2a + 2b$$

(x) المجموعة K لكل الأعداد النسبية على الصورة $\frac{p}{q}$ حيث q عدد صحيح فردي ، مع عملية الجمع العادية للأعداد النسبية .

7- في التمرين رقم (6) حدد أي منها :

(i) زمرة أبيلية .

(ii) زمرة غير أبيلية .

(iii) شبه زمرة وليست زمرة .

(iv) كل الأنظمة التي لا تمثل شبه زمرة .

8- إذا كانت مجموعة المصفوفات $n \times n$ على الأعداد المركبة تشكل زمرة مع عملية ضرب المصفوفات ، بين أنه إما أن يكون جميع عناصر المجموعة من المصفوفات غير المنفردة أو تكون جميعها منفردة .

2– تمهيد

في هذا الجزء سنناقش الخصائص الأساسية للزمرة والتي تعتبر في الحقيقة حجر الأساس في بناء التطور الساحر أو نظرية الزمر بعمق . دعنا نسترجع مصطلحنا عندما نقول G هي زمرة ، عمليتها الثنائية يرمز بالضرب ولأي $a, b \in G$ فإنه يشار إليها بواسطة $a . b$.

نظرية 3.2

إذا كانت G زمرة فإن :

(1) العنصر المحايد للزمرة G وحيد .

(2) كل $a \in G$ له معكوس وحيد في G .

(3) لكل $a \in G$ فإن $(a^{-1})^{-1} = a$.

(4) لجميع $a, b \in G$ فإن $(ab)^{-1} = b^{-1}a^{-1}$.

ملاحظة

قبل أن نتابع برهان النظرية ، دعنا أولاً نحاول أن نفهم إلى أي حقيقة نريد أن نبرهنها ، ما هي الأهمية لها أو المغزى منها . دعنا نستعيد مرة أخرى أن عنصر : $e \in G$ يطلق عليه محايد للزمرة G في حالة $\forall a \in G \quad a . e = a = e . a$. المسلمة $G - 2$. G في تعريف الزمرة G فقط يؤكد وجود محايد e . لم يؤكد أنه يوجد محايد واحد فقط في G . وبالتالي فقد يتوقع الشخص أنه ربما يوجد عنصر آخر $f \in G$ بحيث كان $\forall a \in G \quad af = a = fa$ جزء 1 من هذه النظرية يؤكد مثل هذه الحالة ليست محتملة . وبالمثل فإن المسلمة $G - 3$ في تعريف الزمرة تحدد أنه للعنصر a المعطى يوجد على الأقل

عنصر واحد $G \ni a^{-1}$ بحيث $a^{-1}.a = e = a.a^{-1}$ حيث e هو محايد للزمرة G ولكنها لم تحدد أن هذا العنصر وحيد .

في الجزء 2 برهنا أن كل عنصر له معكوس وحيد . بعد الجزء الأول والجزء الثاني من النظرية يتضح أنه من السهولة أن تتبلور الفكرة وراء هدفنا من برهان الجزء الثالث والجزء الرابع من النظرية السابقة .

البرهان

1- ليكن e, f محايدان موجودان في G . وبالتالي فإن $ef = f$ على أساس أن e محايد ، وأيضاً $ef = e$ على أساس أن f محايد . وهذا يعني أن $e = f = ef$.
هذا يبرهن وحدانية المحايد .

2- ليكن العنصر $G \ni a$ له معكوسان ، ولنقل x, y في G . وبالتالي فإن $xa = e = ax$ ، كذلك فإن $ya = e = ay$ وهذا يعطينا أن :

$$x = xe = x(ay) = (xa)y = ey = y$$

وبالتالي فإن معكوس a وحيد .

3- حيث أنه لكل $G \ni a$ ، $aa^{-1} = e = a^{-1}a$ فإنه ينتج من تعريف المعكوس أن $(a^{-1})^{-1} = a$.

4- الآن :

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= \left[a\,(bb^{-1})\right]\,a^{-1}\\ &= (ae)a^{-1} = aa^{-1} = e\end{aligned}$$

كذلك فإن :

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}\left[a^{-1}(ab)\right]\\ &= b^{-1}\left[(a^{-1}a)b\right]\\ &= b^{-1}(eb) = b^{-1}.b = e\end{aligned}$$

وينتج أن $(ab)^{-1} = b^{-1}a^{-1}$

نظرية 4.2 (قوانين الحذف)

لتكن G زمرة فإنه لكل $a, b, c \in G$

(قانون الحذف الأيسر) $ab = ac \Rightarrow b = c$

(قانون الحذف الأيمن) $ba = ca \Rightarrow b = c$

البرهان

$$\begin{aligned} ab = ac &\Rightarrow a^{-1}(ab) = a^{-1}(ac) \\ &\Rightarrow (a^{-1}a)\, b = (a^{-1}a)\, c \\ &\Rightarrow eb = ec \\ &\Rightarrow b = c \end{aligned}$$

بنفس الطريقة فإن :

$$\begin{aligned} ba = ca &\Rightarrow (ba)a^{-1} = (ca)a^{-1} \\ &\Rightarrow b = c \end{aligned}$$

ملاحظة 1

من الضروري التأكيد على كون العامل المشترك في ناتجي ضرب متساويين في الزمرة يمكن اختصاره فقط في حالة ظهوره في نفس الجهة . في الحقيقة فإن لثلاثة عناصر a, b, c : في زمرة G : $a\,.\,b = c\,.\,a$ ربما لا يؤدي إلى $b = c$ بصورة عامة .

لتوضيح ذلك اعتبر : $S = \{1, 2, 3\}$ والزمرة $A(s)$. كل من : $f : S \to S$ ، $g : S \to S$ معرفتان على النحو التالي :

$$g(1) = 2\,,\, g(2) = 1\,,\, g(3) = 3 \quad ; \quad f(1) = 2\,,\, f(2) = 3\,,\, f(3) = 1$$

من الواضح أن $f, g \in A(s)$. نترك للقارئ إثبات أن $f \circ g = g \circ (f \circ f)$ ولكن $f \neq f \circ f$.

ملاحظة 2

في شبه الزمرة قوانين الحذف قد لا تتحقق كما هو واضح في المثال التالي :

مثال 12

المجموعة S من جميع المصفوفات المربعة 2×2 على الأعداد الصحيحة هي شبه زمرة تحت عملية الضرب .

الآن $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

ثلاث عناصر بحيث كان $AB = AC$ ولكن $B \neq C$.

ملاحظة 3

هناك شبه زمر ليست زمر ولكنها تحقق قوانين الحذف . ويمكن توضيحها فيما يلي:

مثال 13

المجموعة N هي شبه زمرة أبيلية تحت عملية الجمع . من المعروف جيداً أنه لأي ثلاث أعداد صحيحة موجبة a, b, c :

$$a + b = a + c \Rightarrow b = c$$

ولكن هذا النظام ليس زمرة .

نظرية 5.2

أي شبه زمرة منتهية تحقق قانونا الحذف هي زمرة .

البرهان

لتكن S شبه زمرة منتهية تحقق قانونا الحذف . لتكن :

$$S = \{a_1, a_2, a_3, \ldots, a_n\} \qquad (1)$$

اعتبر أي : $a_1 \in S$ فإن :

$$a_1a_i, a_2a_i, a_3a_i, \ldots, a_na_i \qquad (2)$$

كلها مختلفة ، حيث أنه لأي j, i $(1 \le i, j \le n)$.

(قانون الحذف الأيمن) $a_i a_l = a_j a_l \Rightarrow a_i = a_j$

وبالتالي فإن العناصر الواردة في (2) كلها ضمن عناصر (1) وربما في ترتيب آخر . وبالتالي إذا أعطينا أي $a_i \in S$ يوجد $a_j \in S$ بحيث

$$a_i = a_j a_l \quad (3)$$

وعلى وجه الخصوص يوجد $a_k \in S$ بحيث كان $a_l = a_k a_l$ وبالتالي فإن :

$$a_i a_l = a_i(a_k a_l) = (a_i a_k)\, a_l$$

وبالتـالي وباسـتخدام قـانون الحـذف الأيمـن في S ، $a_i = a_i a_k$ لكـل i . وبـنفس الطريقـة وباعتبار العناصر : $a_l a_1, a_l a_2, a_l a_3, \dots, a_l a_n$ وباستخدام قانون الحذف الأيسر يمكننا إيجاد عنصر a_t بحيث كان $a_t a_i = a_i$ لكل i .

وبالتالي فقد حصلنا على $a_k = a_t a_k = a_t$

و $a_k a_i = a_i = a_i a_k$ لكـــل $i = 1, 2, 3, \dots, n =$ ، فيكـــون a_k العنصـــر المحايـــد في S .

دعنا نكتب e بدلاً من a_k متخذين $i = k$ في رقم (3) يمكننا القول أنه يوجد a_m بحيث كان : $e = a_k = a_m a_l$. وبطريقة مشابهة ، وباعتبار العناصر :

$$a_i a_1, a_i a_2, \dots, a_i a_n$$

يمكننا إيجاد عنصر a_u بحيث كان : $a_l a_u = e$

بالتالي فإن $a_u = e a_u = (a_m a_k)\, a_u = a_m(a_l a_u) = a_m e = a_m$

وكذلك $a_m a_l = e = a_l a_m$

وبالتالي $a_l^{-1} = a_m$

ونستنتج أن كل عنصر في S له معكوس في S .

وبالتالي فإنه في S لكل $a, b, c \in S$

(i) $a(bc) = (ab)c$ (S شبه زمرة) .

(ii) يوجد $e \in S$ بحيث كان : $ae = a = ea \quad \forall a \in S$.

(iii) لأي عنصر $a \in S$ يوجد $a \in S$ بحيث كان : $aa^{-1} = e = a^{-1}a$ ، وبالتالي فإن S زمرة .

وهذا يبرهن النظرية . □

الآن إذا كانت G أي زمرة منتهية فبتطبيق نظرية 4.2 فإن G تحقق قوانين الحذف، وبأخذ هذا في الاعتبار سيكون لدينا ما يلي :

نظرية 6.2

شبه زمرة منتهية G تكون زمرة إذا كان وفقط إذا كان G تحقق قانونا الحذف . □

ملاحظة

لاحظ أنه في مثال 13 ، $< N , + >$ شبه زمرة غير منتهية مع قوانين الحذف ، ولكن $< N , + >$ ليست زمرة ، هذا يعني أن النظرية السابقة لا يمكن تعميمها على شبه الزمر الغير منتهية .

نظرية 7.2

إذا كان a, b في زمرة G ، المعادلتان : $ax = b$ و $ya = b$ لهما حل وحيد لكل من y, x في G .

البرهان

حيث أن $a(a^{-1}b) = (aa^{-1})\, b = eb = b$ فإن $x = a^{-1}b$ حل للمعادلة $ax = b$ في G .

بـنفس الطريقـة $y = ba^{-1}$ هـو حـل للمعادلـة $ya = b$ في G . وحدانيـة الحـل تأتي نتيجـة استخدام قوانين الحذف في G . □

نظرية 8.2

مجموعـة غـير خاليـة G مـع عمليـة ثنائيـة يشـار إليهـا بالضـرب تكـون زمـرة إذا كـان وفقط إذا كان :

(1) لكل $a, b, c \in G$: $a(bc) = (ab)\,c$

(2) لأي $a, b \in G$ فإن المعادلتان $ax = b$ و $ya = b$ لهما حلول في G .

البرهان

فقط إذا الجزء

لـتكن G زمـرة ، مـن تعريـف الزمـرة فـإن رقـم (1) يتحقـق في G ورقـم (2) تأتي مـن نظرية 2-7 .

"إذا" if الجزء

لـتكن G مجموعة غير خالية مع عملية ضرب ثنائية تحقق (1) وكذلك (2) . لكـي نوضـح أن G زمـرة فإننـا نحتـاج فقـط إلى توضـيح أن G تحتـوي محايـد وكـل عنصـر مـن G لـه معكوس .

(i) وجود المحايد

اعتـبر $a \in G$ وبالتـالي ومـن خـلال رقـم (2) المعادلـة $ax = a$ لهـا حـل في G . وبالتالي فإنه يوجد عنصر $e \in G$ بحيث كان $ae = a$.

الآن لتكن $b \in G$ ومن خلال رقم (2) يوجد : $y \in G$ ، بحيث كان : $b = ya$.

إذن : $$be = (ya)\,e = y(ae) = ya = b$$

أي أن لكل : $b \in G$ ، $be = b$.

بنفس الطريقة حيث أن المعادلة : $ya = a$ لها حل في G فإنه يوجد $f \in G$ بحيث كان $fb = b, fa = a$ لكل $b \in G$. بصفة خاصة $fe = f$ حيث $be = b$ لكل $b \in G$

وأيضاً $fe = e$ لأن $fb = b$ لكل $b \in G$.

ينتج أن $e = f$ وبالتالي نحصل على $be = b = eb$ لكل $b \in G$ ، ومن ثم فإن e يعتبر المحايد في G .

(ii) وجود المعكوس

لتكن $a \in G$ من رقم (2) يوجد $a', a'' \in G, a'', a'$ ، بحيث كان $a''a = e, aa' = e$ فإن $$a' = ea' = (a''a)\,a' = a''(aa') = a''e = a''$$

وبالتالي فقط حصلنا على $$a'a = e = aa'$$

إذن : $a' = a^{-1}$ موجود في G .

بالتالي ومن خلال (i) و (ii) فإن G تعتبر زمرة . □

هذه النظرية تعطي وصفاً للزمرة ، وعليه فإنه يمكننا بالتعاقب أن نعرف الزمرة على النحو التالي :

تعريف 9.2

نظام رياضي $< G, . >$ حيث G مجموعة غير خالية و "." عملية ثنائية (يشار إليها بالضرب) يطلق عليها زمرة إذا كانت تحقق الشروط أو المسلمات التالية :

لكل : $a, b, c \in G$.

(1) $a(bc) = (ab)c$.

(2) المعادلتان : $ax = b$ و $ya = b$ لهما حلول في G .

ملاحظة

من ناحية أخرى إذا G شبه زمرة ، وإذا أعطينا لكل $a, b \in G$ فقط المعادلة $ax = b$ لها حل في G فإن G ربما لا تكون زمرة . وهذا ما يوضحه المثال التالي .

مثال 14

لتكن G أي مجموعة بها على الأقل عنصران . b, a معطيان في G ومعرف فيها أن $ab = b$.

i- لتكن : $a, b, c \in G$ بالتالي $a.(b.c) = a.c = c$ ، وأيضاً $(a.b).c = b.c$ وبالتالي فإن $(a.b).c = a.(b.c)$.

ii- حيث أن $ab = b$ فإن $x = b$ هو حل المعادلة $ax = b$.

اعتبر عنصرين مختلفين a, b في G فإن $b.b = b, a.b = b$

وينتج من ذلك أن $b.b = a.b$

ولكن $a \neq b$ وبالتالي فإن G لا تحقق قانونا الاختصار . وبالتالي فإن G ليست زمرة . □

نظرية 10.2

مجموعة غير خالية G تكون زمرة تحت عملية ثنائية يشار إليها بالضرب إذا وفقط إذا تحقق ما يأتي :

(1) $\forall a, b, c \in G \quad a(bc) = (ab)c$.

(2) يوجد عنصر : $e \in G$ بحيث كان : $\forall a \in G \quad ae = a$.

(3) لكل $a \in G$ يوجد $a' \in G$ بحيث كان $aa' = e$.

البرهان

"فقط إذا" تتأتى من التعريف 1.2 للزمرة .

"إذا" نفرض أن G مجموعة غير خالية معرف بها عملية ثنائية تحقق (3) ,(2) ,(1) .

لتكن $a \in G$ من خلال (3) فإنه يوجد $a' \in G$ بحيث كان $aa' = e$ مرة أخرى من (3) فإنه يوجد $a'' \in G$ بحيث كان $a'a'' = e$.

الآن :

$$\begin{aligned} a'a &= (a'a)\, e = (a'a)\,(a'a'') = a'\left[a\,(a'a'')\right] \\ &= a'\left[(aa')\,a''\right] \\ &= a'(ea'') = (a'e)\,a'' \\ &= aa'' \\ &= e \end{aligned}$$

بالتالي فإن

$$aa' = e = a'a$$

وزيادة على ذلك فإن

$$ea = (aa')\,a = a\,(a'a) = ae = a$$

وبالتالي

$$ae = a = ae$$

وعليه فإن G تكون زمرة . □

بنفس الطريقة يمكننا أن نبرهن ما يلي :

نظرية 11.2

مجموعة غير خالية G تكون زمرة تحت عملية معرفة بها يشار إليها بالضرب إذا وفقط إذا كانت تحقق ما يلي :

1- $\forall a, b, c \in G \quad a\,(bc) = (ab)\,c$.

2- يوجد عنصر $e \in G$ بحيث كان $ea = a \quad \forall a \in G$.

3- لكل عنصر $a \in G$ يوجد عنصر $a' \in G$ بحيث كان $a'a = e$. □

النظريتان 10.2 ، 11.2 يزودانا التعريفين البديلين التاليين للزمرة .

تعريف 12.2

نظام رياضي $< G , \bullet >$ حيث G مجموعة غير خالية و "$\bullet$" عملية ثنائية معرفة على G يطلق عليه زمرة في حالة تحقيق البديهيات التالية :

1- $\forall a, b, c \in G \quad a . (b . c) = (a . b) . c$.

2- يوجد عنصر $e \in G$ بحيث كان $a . e = a \quad \forall a \in G$.

3- لكل $a \in G$ يوجد $a' \in G$ بحيث كان $a . a' = e$.

تعريف 13.2

نظام رياضي $< G , \bullet >$ حيث G مجموعة غير خالية و "$\bullet$" عملية ثنائية معرفة على G يطلق عليه زمرة في حالة تحقيقه للبديهيات التالية :

لكل $a, b, c \in G$

1- $a . (b . c) = (a . b) . c$.

2- يوجد عنصر $a \in G$ بحيث كان : $e . a = a$.

3- لكل $a \in G$ يوجد $a' \in G$ بحيث كان $a' . a = e$.

التعريف 12.2 يطلق عليه التعريف الأيمن للزمرة "ذو الجهة اليمنى" . أما التعريف 13.2 فيطلق عليه التعريف الأيسر للزمرة "ذو الجهة اليسرى" .

يجب أن يلاحظ أن شبه الزمرة G لربما G تحوي محايد أيسر وكل عنصر : $a \in G$ ربما معكوس أيمن ولكن G ربما لا تكون زمرة . وهذا يوضح من خلال المثال التالي :

مثال 15

لتكن G شبه زمرة المتضمنة في مثال (14) وليكن e أي عنصر مثبت في G . بالتالي ومن خلال التعريف :

(i) $ea = a \quad \forall a \in G$. إذن e هو محايد أيسر .

(ii) لكل $a \in G$ حيث $ae = e$ فإن e هو معكوس أيمن للعنصر a بالنسبة إلى e .

وعليه فإن G لها محايد أيسر e وكل عنصر من G له معكوس أيمن في G ولكننا علمنا أن G ليست زمرة . نحن نترك للقراء إنشاء مثال مشابه لشبه الزمرة التي لها محايد أيمن ولها معكوس أيسر لكل عناصرها ، ولكن لا تصلح أن تكون زمرة .

تمارين محلولة

تمرين 1

إذا كان في زمرة G ، $xy^2 = y^3x$ و $yx^2 = x^3y$ وضح أن $x = y = e$ حيث e هو العنصر المحايد في G .

الحل

$$xy^2 = y^3x \Rightarrow x = y^3xy^{-2}$$
$$x^2 = xy^3xy^{-2} = xy^2yxy^{-2} = y^3xyx^{-2}$$
$$x^2y = y^3xyxy^{-1} \qquad (1)$$

الآن

$$yx^2 = x^3y \Rightarrow yx^2 = xy^3xyxy^{-1}$$
$$\Rightarrow x^2 = y^{-1}xy^3xyxy^{-1}$$
$$\Rightarrow x^2y = y^{-1}xy^3xyx \qquad (2)$$

من (2) ، (1) نحصل على

$$y^3xyxy^{-1} = y^{-1}xy^3xyx \Rightarrow y^4xyx = xy^3xyxy$$
$$\Rightarrow y^4xyx = xy^2yxyxy = y^3xyxyxy$$

$\Rightarrow (yx)^2 = (xy)^3$ (3)

بتبديل x مع y في (3) فنحصل على

$(xy)^2 = (yx)^3$ (4)

والآن (3) ، (4) معاً يؤديان إلى : $(xy)^2 = (yx)^3 = (yx)^2(yx) = (xy)^3(yx)$

$\Rightarrow e = xy^2x = x^{-2} = y^2$

علاوة على ذلك $xy^2 = y^3x \Rightarrow xx^{-2} = yx^{-2}x$

$\Rightarrow x^{-1} = yx^{-1} \Rightarrow y = e$

أخيراً $yx^2 = x^3y \Rightarrow ex^2 = x^3e \Rightarrow x = e$

تمرين 2 (إسبيل)

G زمرة ، يوجد عددان صحيحان موجبان أوليان بالنسبة إلى بعضهما البعض m, n بحيث كان $a^mb^m = b^ma^m$ و $a^nb^n = b^na^n$ ، لكل $a, b \in G$. برهن أن G أبيلية .

الحل

حيث أن $(m, n) = 1$ فإننا نجد أن $mx + ny = 1$ ، لبعض $x, y \in Z$.

الآن :

$$
\begin{aligned}
(a^mb^n)^{mn} &= a^m(b^na^m)^{mx_1}b^n \\
&= a^m(b^na^m)^{mx}(b^na^m)^{-1}b^n \\
&= (b^na^m)^{mn}a^ma^{-m}b^{-n}b^n \\
&= (b^na^m)^{mx} \qquad (1)
\end{aligned}
$$

بنفس الطريقة يمكننا إثبات أن :

$(a^mb^n)^{ny} = (b^na^m)^n y$ (2)

من (1) ، (2) نحصل على $a^mb^n = (a^mb^n)^{mx+ny}$

$$= (b^n a^m)^{mx+ny} = b^n a^m \qquad (3)$$

أخيراً $ab = a^{mx+ny} b^{mx+ny}$

$= a^{mx}(a^{ny} b^{mx})\, b^{ny}$

من (3) $= a^{mx} b^{mx} a^{ny} b^{ny}$

من الفرض $= b^{mx} a^{mx} b^{ny} a^{ny}$

من (3) $= b^{mx+xy} a^{mx+ny}$

$= ba$

وبالتالي فإن G أبيلية .

تمرين 3

S هي شبه زمرة منتهية . أثبت أنه يوجد $e \in S$ بحيث كان : $e^2 = e$.

الحل

لتكن $x \in S$ ، حيث أن S منتهية فإن $x, x^2, x^3, \ldots$ كلها لا يمكن أن تكون مختلفة . وبالتالي فإنه يوجد أعداد صحيحة $m > n$ بحيث كان $x^m = x^n$. هذا يعطينا $x^{n+k} = x^n$ ، حيث $k = m - n$.

الآن : $x^{n+k} = x^n x^{n+k} = x^{2k}$. وباستخدام قاعدة الاستنتاج الرياضي يمكن أن نبرهن أن $x^{mn+k} = x^{mn}$ لأي $m \in N$.

أيضاً $x^{mn+2k} x^{mn+k} \,.\, x^k = x^{mn} x^k = x^{mn+k} = x^{mn},$

$x^{mn+33} = x^{mn+2k} \,.\, x^k = x^{mn+k} = x^{mn}$

وهكذا .

مرة أخرى وباستخدام قاعدة الاستنتاج الرياضي فإنه يمكن أن نبرهن أن :

$x^{mn+lk} = x^{mk}$

لأي $l \in N$. بصفة خاصة فإننا نحصل على $x^{kn+nk} = x^{kn}$ أي أن $x^{2kn} = x^{nk}$ ولكن $x^{nk} = e$.

ضع $x^{nk} = e$.

تمرين 4

G زمرة و $a \in G$ و عرف عملية ثنائية $*$ على G بحيث $< G, * >$ زمرة و a العنصر المحايد لها .

الحل

نعرف $*$ في G على النحو التالي $x * y = xa^{-1}y$ لكل $x, y \in G$.

(1) $*$ تنسيقية : ليكن $x, y, z \in G$:

$$(x * y) * z = (xa^{-1}y) * z = (xa^{-1}y)\, a^{-1}z = xa^{-1}ya^{-1}z$$

مرة أخرى

$$x * (y * z) = x * (ya^{-1}z) = xa^{-1}(ya^{-1}z) = xa^{-1}ya^{-1}z$$

وبالتالي فإن

$$(x * y) * z = x * (y * z)$$

(2) لأي $x \in G$:

$x * a = xa^{-1}a = xe = x$ ، حيث e عنصر محايد في G ، بنفس الطريقة $a * x = aa^{-1}x = ex = x$ إذن a هو محايد G .

(3) لتكن $x \in G$ ، وبالتالي فإن :

$$x * (ax^{-1}a) = xa^{-1}(ax^{-1}a) = xx^{-1}a = ea = a$$

بالإضافة إلى

$$(a^{-1}xa) * x = (ax^{-1}a)\, a^{-1}x = ax^{-1}x = ae = a$$

إذن

$$x^{-1} = ax^{-1}a$$

ونتيجة لذلك فإن $< G , * >$ هو زمرة مع a كمحايد لها .

تمرين 5

أثبت أن المعادلة : $x^2ax = a^{-1}$ لها حل لـ x في زمرة G إذا كان وفقط إذا كان a هو مكعب لعنصر في G .

الحل

نفرض أن $x^2ax = a^{-1}$ قابلة للحل في G وبالتالي يوجد $c \in G$ بحيث كان $c^2ac = a^{-1}$ وهذا يعطينا :

$$caca = c^{-1} \Rightarrow cacac = e \Rightarrow cacaca = ea = a \Rightarrow (ca)^3 = a$$

وبالعكس لتكن $e = b^3$ لعنصر b في G . إذن $x = b^{-3}$ هي حل للمعادلة $x^2ax = a^{-1}$ ، لأن $x^3ax = b^{-4}b^3b^{-2} = b^{-3}$ بينما $a^{-1} = b^{-3}$.

تمرين 6

شبه زمرة S يقال عنها أنها منتظمة إذا كان لكل : $y \in S$ يوجد $a \in S$ حيث كان $yay = y$.

لتكن S شبه زمرة بها على الأقل ثلاث عناصر وكانت $x \in S$ بحيث كان $S - \{x\}$ تشكل زمرة . برهن أن S هي زمرة منتظمة إذا كان وفقط إذا كان $x^2 = x$.

الحل

إذا كانت $x^2 = x$ فإن : $x^3 = x^2 = x$ أي أن $xxx = x$ والآن $G = S - \{x\}$ زمرة ، ليكن $y \in S - \{x\}$. فإن $yy^{-1} = ey = y$ حيث e هو المحايد للزمرة G .

وحيث أن $S[= G \cup \{x\}$ فإن S تكون منتظمة .

وبالعكس لتكن S منتظمة فإننا نهدف إلى إثبات أنه لأي $y \in G$ $xy = x = yx$.
نفرض أن $xy \neq x$ فإن $xy \in G$ ، وبالتالي : $(xy)y^{-1} = x \in G$ وذلك غير معقول ، وبالتالي فإن $xy = x$ بنفس الطريقة $yx = x$. حيث S منتظمة فإنه يوجد عنصر $a \in S$ بحيث كان $xax = x$.

إذا كان $a \in G$ فإن :

$$ax = x \Rightarrow xx = x \Rightarrow x^2 = x$$

إذا كان $a = x, a \notin G$ فإن :

$$xax = x \Rightarrow x^3 = x$$

لتكن $x^2 \neq x$ فإن $u = x^2 \in G$. وحيث أن S بها على الأقل ثلاث عناصر فإنه يوجد $v\,(\neq u)$ في G .

الآن : $zu = v$ لها حل في G . لكون $z \in G$ ،

$$zu = zu^2 = (zx)\,x = xx = x^2 = u$$

أي أن : $u = v$. وهذا يعتبر غير معقول ، وبالتالي $x^2 = x$.

ملاحظة

إذا كان في شبه زمرة S يوجد عنصر $t \in S$ بحيث كان

$$xt = tx = t$$

لكل $x \in S$ فإن t تسمى "صفر" S ، وبالتالي في تمرين 6 السابق لاحظنا أنه إذا كانت S شبه زمرة منتظمة بها على الأقل ثلاث عناصر ، وكانت $x \in S$ بحيث كان $S - \{x\}$ زمرة ، فإن x "صفر" لـ S .

تمارين

-1 تعريف : في شبه زمرة G ، عنصر a يسمى متساوي القوة (إديمبوتنت) إذا كان $a^2 = a$. أثبت أنه إذا كانت G زمرة فإن $a \in G$ هو أيدمبوتنت إذا وفقط إذا كان $a = e$ ، المحايد للزمرة G .

-2 إعط مثالاً لشبه زمرة تحتوي أكثر من أيدمبتونت واحد ولكن لا تحتوي محايد .

-3 (a) من المعروف ومن خلال نظرية 3.2 أن شبه الزمرة المنتهية التي تحقق قانونا الحذف هي زمرة . اعط مثالاً لمجموعة منتهية غير خالية G مع عملية ثنائية بحيث كانت G تحقق قانوني الحذف ولكن G ليست زمرة .

[**إرشاد** اعتبر المجموعة $G = \{1, \alpha, \beta, \gamma, \delta\}$ مع العملية الثنائية المعرفة من خلال جدول الضرب التالي . حيث أنه لا وجود عمود أو صف يحتوي نفس العناصر في مكانين أو أكثر ، وبالتالي قانونا الحذف تحققاً] .

	1	α	β	γ	δ
1	1	α	β	γ	δ
α	α	1	γ	δ	β
β	β	δ	α	1	γ
γ	γ	β	δ	α	1
δ	δ	γ	1	β	α

(b) وضح أن أي مجموعة بها العناصر 1 و 2 و 3 و 4 تكون زمرة تحت أي عملية ثنائية يتحقق معها قانون الحذف والمحايد .

-4 برهن أن شبه زمرة منتهية G مع محايد هي زمرة إذا وفقط إذا G تحتوي أيدمبوتنت واحد .

أعط مثالاً يوضح أنه إذا أسقطنا المحايد من السؤال السابق ، فإن النتيجة لا تكون صحيحة .

إرشاد

اعتبر $G = \{0, 2\}$ تحت عملية الضرب بمقياس 4 .

5- لتكن G شبه زمرة لها محايد e مع الخاصية التي تقول : لأي $a \in G$ يوجد $a' \in G$ بحيث كان إما $aa' = e$ أو $a'a = e$. برهن أن G هي زمرة .

6- لتكن G شبه زمرة مع أيديمبوتنت e بحيث كان :

(i) كل عنصر في G له على الأقل معكوس أيسر واحد بالنسبة إلى e .

(ii) كل عنصر في G له على الأكثر معكوس أيمن واحد بالنسبة إلى e .

وضح أن G تكون زمرة .

7- إذا كانت G زمرة بحيث كان : $(ab)^2 = a^2b^2$ لكل $a, b \in G$ وضح أن G يجب أن تكون (إبدالية) .

أعط مثالاً لتوضيح أن هذه النتيجة لا تتحقق بالنسبة لشبه زمرة .

8- إذا كانت G زمرة بحيث كان $(ab)^i = a^ib^i$ لثلاثة أعداد صحيحة متتالية i ولكل $a, b \in G$. وضح أن G تكون (إبدالية) .

أعط مثالاً لتوضح أن هذه النتيجة لا تحدث بالنسبة لشبه الزمرة .

إرشاد

[اعتبر مثال 14]

9- وضح أن نتيجة المسألة رقم (8) لا تتحقق إذا افترضنا العلاقة $(ab)^n = a^nb^n$ لعددين صحيحين متتاليين فقط .

[إرشـــــاد اعتـــبر $T = \{\pm 1, \pm i, \pm j, \pm k\}$ وعـــرف $i^2 = j^2 = k^2 = -1$ و $ij = -ji = k, kj = -jk = i$ و $ki = -ik = j$ فـإن T تكـون زمـرة T يطلـق عليها الزمرة الكواتيرينية ، خذ $n = 4, 5$ **]** .

1- وضح أنه إذا كان في زمرة ما $a^2 = e \quad \forall a \in G$ فإن G تكون (إبدالية) .

[إرشاد $(ab)^2 = e \Rightarrow ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ **]** .

2- أثبت أنه إذا كانت G شبه زمرة منتهية مع قوانين الحذف المتقاطعة ، أي أن $xy = yz \Rightarrow x = z$ فإن G تكون زمرة (إبدالية) .

[إرشاد اعتبر $(xy)x = x(yx)$ **]** .

3- إذا لم يكـــن في زمـــرة G عنصـــر c يختلـــف عـــن محايـــد e بحيـــث كـــان $(ab)^2 = (ba)^2, c^2 = e$ تتحقق لكل a, b بالتالي بين أن G تكون إبدالية .

4- لأي a في زمرة G وأي عدد صحيح n تعرف a^n على النحو التالي : $a^0 = e$ إذا كان n موجب فإن $a^n = a^{n-1}.a$ وإذا كان n سالباً أي أن $n = -m$ حيث m عدد صحيح موجب فإن $a^n = (a^{-1})$ برهن القوانين التالية :

(i) $(a^n)^{-1} = (a^{-1})^n = a^{-n}$.

(ii) $a^n . a^m = a^{n+m}$.

(iii) $a^{nm} = (a^n)^m$.

(iv) لكل $x \in G$: $(x^{-1}ax)^n = x^{-1}a^n x$.

(v) إذا كان $ab = ba$ فإن $(ab)^n = a^n b^n$.

5- إذا كان في زمرة G : $xy^n = y^{n+1}x$ و $yx^n = x^{n+1}y$ لبعض $n \in N$. أثبت أن $x = y = e$ حيث e هو محايد الزمرة G .

6- (هايز) G شبه زمرة ولكل $x \in G$ يوجد عنصر وحيد y في G بحيث كان $xyx = x$. برهن أن G هي زمرة .

7- لتكن S شبه زمرة والتي فيها لعدد صحيح ثابت $k \geq 1$ و $x^{k+1} = x$ و $xy^k x = yx^k y$ لكل x, y في S . وضح أن S إبدالية .

8- لتكن S شبه زمرة بحيث أنه يوجد $e \in S$ يحقق : $xe = x$ لكل $x \in S$. افترض لكل زوج مرتب $(x, y) \in S$, $x \neq y$ يوجد عنصر وحيد $w \in S$ بحيث كان $xw = y$. وضح أن S تكون زمرة .

9- لتكن $J = \left\{ \begin{pmatrix} x & y \\ x & y \end{pmatrix} \ : \ x, y \in R \ \text{ مع } \ x + y \neq 0 \right\}$. وضح أن J تكون شبه زمرة تحت عملية ضرب المصفوفات ، وأن J لها محايد أيسر وكل عنصر من J له معكوس أيمن . هل J زمرة (الجواب : لا) .

10- لتكن S شبه زمرة إذا كان لكل $x, y \in S$ ، $x^2 y = yx^2$. أثبت أن S زمرة إبدالية .

11- أعط مثالاً لتوضيح أن نتيجة التمرين (19) السابق ربما لا تكون صحيحة إذا كان لدينا فقط $yx = y$ لكل $x, y \in S$ في حالة $x^2 y = y = yx^2$ لكل $x, y \in S$.
[إرشاد خذ $S = \{a, b\}$ وعرف $a^2 = a, ab = a, ba = b, b^2 = b$ **]** .

3– الزمرة الجزئية Subgroups

لتكن H مجموعة غير خالية و $*$ عملية ثنائية في H ، ولتكن A مجموعة جزئية غير خالية من H . من المعروف أن A يقال لها مجموعة جزئية مغلقة من H بالنسبة إلى العملية الثنائية $*$ ، إذا كان لكل $a, b \in A$ يكون $a * b \in A$. في هذه الحالة الراسم

$f : A \times A \to A$ والذي فيه $f(a, b) = a * b$ يطلق عليه عملية ثنائية في A ويشار لها بالزمر $*$.

لتكن G زمرة ولتكن A مجموعة جزئية غير خالية من G ربما يحدث أن تكون A مغلقة بالنسبة إلى العملية الثنائية في G وأن A نفسها زمرة تحت نفس العملية . مثل هذه الحالة تحدث أحيانا ، وهذا يوصلنا إلى المفهوم التالي :

تعريف 14.2

إذا كانت G زمرة تحت عملية ثنائية $*$ وكانت H مجموعة جزئية غير خالية من G . فإن H يطلق عليها زمرة جزئية من G إذا حققت ما يلي :

(1) H مغلقة بالنسبة للعملية $*$ (خاصة الانغلاق) .

(2) H تكون زمرة تحت العملية الثنائية في H الحادثة من $*$.

ليكن e المحايد للزمرة G فإنه ببساطة G و $\{e\}$ يكونان زمراً جزئية من G . هذه الزمر الجزئية تسمى زمراً جزئية بالمعنى الواسع حتماً من G . الزمرة الجزئية H من زمرة G تسمى زمرة جزئية فعلية إذا كانت تختلف عن كل من G ، $\{e\}$.

إذا كانت G زمرة و H زمرة جزئية من G ، فبهدف التمييز نشير دائماً للعملية الثنائية المقدمة في H بنفس الزمر الذي نشير به للعملية الثنائية في G .

3– أمثلة على الزمر الجزئية

مثال 16

المجموعة E مجموعة كل الأعداد الصحيحة الزوجية هي زمرة جزئية من زمرة الأعداد الصحيحة الجمعية Z .

مثال 17

المجموعة Z هي زمرة جزئية من زمرة الأعداد النسبية الجمعية Q .

مثال 18

لتكن : $H = \{1, -1\}, G = \{1, -1, i, -i\}$

حيث $i^2 = -1$ فإن G هي زمرة تحت عملية الضرب العادية للأعداد المركبة وتعتبر H زمرة جزئية من G .

مثال 19

لتكن G زمرة الضرب لكل المصفوفات غير المنفردة من السعة 2×2 على الأعداد المركبة ، ولتكن H مجموعة المصفوفات التالية :

$$\pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ \pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},\ \pm\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix},\ \pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

من الواضح أن $H \subseteq G$. كما طلب في مثال 10 ، H هي زمرة تحت عملية ضرب المصفوفات . إذن H تعتبر زمرة جزئية من G .

مثال 20

المجموعة Q^+ مجموعة الأعداد النسبية الموجبة غير الصفر هي زمرة جزئية من زمرة الضرب Q^* لكل الأعداد النسبية غير الصفر .

من خلال الحقيقة القائلة أن الزمرة لها فقط أيدمبوتنت idempotent واحد (المسألة رقم (1) ، (2)) وأن معكوس أي عنصر من G وحيد يأتي مباشرة ما يلي :

قضية 2-15

إذا كانت G زمرة وكانت H زمرة جزئية من G فإن :

(1) e المحايد في G هو أيضاً محايد H .

(2) لكل $a \in H$ فإن $a^{-1} \in H$

الآن نبرهن النظرية التي بها يمكننا تحديد ما إذا كانت المجموعة الجزئية المعطاة من الزمرة هي زمرة جزئية أم لا .

نظرية 2-16

المجموعة الجزئية غير الخالية H من زمرة G تعتبر زمرة جزئية من G إذا وفقط إذا كان :

$$a, b \in H \Rightarrow ab^{-1} \in H$$

البرهان

لتكن H زمرة جزئية من G وليكن $a, b \in H$ من خلال القضية 2-15 (2) فإن $b^{-1} \in H$. فباستخدام خاصية الانفلاق في H نستنتج أن $ab^{-1} \in H$.

وبالعكس ، لتكن H مجموعة غير خالية وجزئية من G بحيث كان $ab^{-1} \in H$ لكل $a, b \in H$ فيكون :

i- حيث أن H غير خالية فإنه يوجد على الأقل $a \in H$ ، وبالتالي فإن $aa^{-1} \in H$ أي أن $e \in H$ ، وعليه فإن H يحتوي المحايد e .

ii- لتكن $b \in H$. حيث $e \in H$ ، كذلك eb^{-1} أي أن $b^{-1} \in H$ إذن $b \in H \Leftarrow b^{-1} \in H$.

iii- $ab \in H \Leftarrow a \in H$ و $b^{-1} \in H$ (حسب (ii))

$$\Leftarrow a(b^{-1})^{-1} \in H$$

أي أن $ab \in H$ لأن $b = (b^{-1})^{-1}$ بالتالي H مجموعة جزئية مغلقة في G .

من الواضح أن العملية الثنائية على H تنسيقية لأنها تنسيقية على G ، أي أن H زمرة جزئية .

نظرية 2-17

لتكن G زمرة و H مجموعة جزئية منتهية غير خالية من G فإن H تكون زمرة جزئية من G إذا وفقط إذا كان $ab \in H$ لكل : $a, b \in H$.

البرهان

إذا كانت H زمرة جزئية من G فإنه من خلال التعريف :

$$a, b \in H \Rightarrow ab \in H$$

وبالعكس لتكن H مجموعة جزئية منتهية وغير خالية من G .

بحث :

$$a, b \in H \Rightarrow ab \in H$$

أي أن H شبه زمرة منتهية ، وبالإضافة إلى ذلك قانوناً الحذف يتحققان في H لأنهما متحققان في G . بالتالي فإن H زمرة جزئية (نظرية 2-6) .

نحن نعلم أنه لأي عددين صحيحين a, b يكون $a \equiv b \pmod{m}$ إذا وفقط إذا كان $m \mid a - b$ أو ما يكافئ أن $a - b$ مضاعف صحيح للعدد m . بالتالي $a \equiv b \pmod{m}$ إذا وفقط إذا كان $a - b \in (m)$ أعد الزمرة الجزئية في Z التي تتكون من مضاعفات m .

لذا فإن التطابق بين عددين صحيحين b, a قريب الارتباط بالزمرة الجزئية (m) .

تعريف 2-18 (التطابق الأيمن معيار زمرة جزئية)

لتكن G زمرة و H زمرة جزئية في G . إذا أعطينا $a, b \in G$ ، فإن a يقال له المطابق الأيمن إلى b معيار H { رمزيا $a \equiv_r b \pmod{m}$} إذا وفقط إذا كان $ab^{-1} \in H$.

نظرية 2-19

إذا كانت G زمرة وكانت H زمرة جزئية في G فإن العلامة $\equiv_r$ الخاصة بالتطابق الأيمن معيار H هي علاقة تكافؤ في G . علاوة على ذلك لأي $a \in G$ فإن المجموعة $\{ha : h \in H\}$ تمثل فصل التكافؤ الذي ينتمي إليه a .

البرهان

لتكن $a, b \in G$ و e المحايد H .

(1) الانعكاس

حيث أن $aa^{-1} = e \in H$ $\left(\bmod H\right)$ $a \equiv_r a$.

(2) التماثل أو التناظر

$$a \equiv_r b(\bmod H) \Rightarrow ab^{-1} \in H$$
$$\Rightarrow (ab^{-1})^{-1} \in H$$

وبالتالي فإن :
$$ba^{-1} \in H$$
$$\Rightarrow b \equiv_r a(\bmod H)$$

(3) التعدي

$$a \equiv_r b(\bmod H), b \equiv {}_r c(\bmod H)$$
$$\Rightarrow ab^{-1} \in H, bc^{-1} \in H$$
$$\Rightarrow ac^{-1} = (ab^{-1})(bc^{-1}) \in H$$
$$\Rightarrow a \equiv_r c(\bmod H)$$

وبالتالي فإن علاقة التطابق الأيمن بمعيار H هي علاقة تكافؤ في G . اجعل $Cl(a)$ ترمز إلى فصل التكافؤ الذي ينتمي إليه العنصر a . أي أن :

$$Cl(a) = \{b \in G : b \equiv {}_r a(\bmod H)\}$$

واجعل Ha تشير إلى المجموعة $\{ha : h \in H\}$

الآن $b \in Cl(a) \Rightarrow b \equiv {}_r a(\bmod H)$

$$\Rightarrow ba^{-1} \in H \Rightarrow b = (ba^{-1})a \in Ha$$

إذن $Cl(a) \subseteq Ha$

مرة أخرى إذا كان $c \in Ha$ فإن $c = ha$ لبعض العناصر $h \in H$ $\Rightarrow ca^{-1} = h \in H$.

$$\Rightarrow c \equiv_r a(\text{mod } H) \Rightarrow c \in Cl(a)$$

إذن $Ha \subseteq Cl(a)$

وبالتالي فإن $Cl(a) = Ha$

تعريف 2-20

مجموعة مصاحبة يمنى .

لتكن G زمرة و H زمرة جزئية من G . لأي $a \in G$.

المجموعة : $Ha = \{ha : h \in H\}$ تسمى مجموعة مصاحبة يمنى للزمرة الجزئية H المحددة بواسطة a .

لقد وجدنا أن المجموعة المصاحبة اليمنى Ha ليست سوى فصل تكافؤ محدد بواسطة العلاقة المتمثلة في التطابق الأيمن معيار (mod) H ، والذي ينتمي إليه a .

من التشابه بين نظرية 2-19 وتعريف 2-18 وتعريف 2-20 لدينا :

تعريف 2-21

التطابق الأيسر معيار (mod) زمرة جزئية : لتكن G زمرة و H زمرة جزئية من G. للعناصر المعطاة $a, b \in G$ ، a يسمى مطابقاً أيسر للعنصر b معيار H (رمزياً $a \equiv_l b(\text{mod } H)$) إذا وفقط إذا كان $a^{-1}b \in H$.

نظرية 2-22

إذا كانت G زمرة وكانت H زمرة جزئية من G فإن العلاقة $\equiv_l$ للتطابق الأيسر معيار H هي علاقة تكافؤ في G . وزيادة على ذلك لأي $a \in G$ المجموعة : $\{ah : h \in H\}$ هي فصل التكافؤ الذي ينتمي إليه a .

تعريف 2-23 المجموعة المصاحبة اليسرى

لتكن G زمرة و H زمرة جزئية من G . لأي $a \in G$ المجموعة : $aH = \{ah : h \in H\}$ تسمى مجموعة مصاحبة يسرى للزمرة الجزئية H والتي تتحدد بالعنصر a .

والآن نبرهن نظرية مفيدة للغاية في المجموعات المصاحبة بدون استخدام مفهوم التطابق مقياس (mod) زمرة جزئية ، ومن ناحية أخرى فإن هذه النظرية ضمنياً محتواة في نظرية 2-19 .

نظرية 2-24

إذا كانت G زمرة ، و H زمرة جزئية من G وكان $a, b \in G$ فإن :

(1) $Ha = H \Leftrightarrow a \in H$

(2) $Ha = Hb \Leftrightarrow ab^{-1} \in H$

(3) $aH = bH \Leftrightarrow a^{-1}b \in H$

البرهان

(1) الآن (لأن $e \in H$) $Ha = H \Rightarrow ea \in Ha = H$

أي أن $a \in H \Leftarrow Ha = H$

ليكن $a \in H$ ، فإن لكل $h \in H$ يكون $ha \in H$ لأن H زمرة جزئية ، وبالتالي ومن التعريف $Ha \subseteq H$.

الآن : لأي $h \in H$ ، $h = (ha^{-1})a \in Ha$ وهكذا ينتج $H \subseteq Ha$.

إذن $Ha = H$

وبالتالي $Ha = H \Leftrightarrow a \in H$

(2) $Ha = Hb \Rightarrow a \in Hb$

حيث $a = ea \in Ha$

$\Rightarrow a = hb$ (لبعض $h \in H$)

$\Rightarrow ab^{-1} = h \in H$

مرة أخرى (لبعض $h \in H$) $ab^{-1} \in H \Rightarrow ab^{-1} = h$

$\Rightarrow a = hb$

$\Rightarrow Ha = H(hb) = (Hh)b$

$= Hb$ (لأن $Hh = H$ حسب (1))

إذن $Ha = Hb \Leftrightarrow ab^{-1} \in H$

برهن الجزء (3) شبيه لبرهان الجزء (2) إذا كانت G زمرة إبدالية وكانت H زمرة جزئية من G .

فإن لأي $h \in H$ ، $a \in G$ ، $ah = ha$ وعليه $Ha = aH$.

ولكن إذا كانت G زمرة غير إبدالية من لا يمكننا القول أن لأي $a \in G$ ولأي زمرة جزئية H من G يكون $aH = Ha$.

من هذا المنطلق الزمرة G يمكن أن تحوي زمرة جزئية H بحيث يتحقق $Ha = aH$ لكل $a \in G$ كما هو واضح في المثال التالي :

مثال 21

لتكن G زمرة من المصفوفات :

$$\pm\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \pm\begin{bmatrix}i & 0\\0 & -i\end{bmatrix}, \pm\begin{bmatrix}0 & i\\i & 0\end{bmatrix}, \pm\begin{bmatrix}0 & 1\\-1 & 0\end{bmatrix}$$

(انظر مثال 10) وليكن H زمرة جزئية تتكون من : $\pm\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \pm\begin{bmatrix}i & 0\\0 & -i\end{bmatrix}$

إذن H زمرة جزئية من G (وضح ذلك) . نترك للقارئ كيفية إثبات أن $aH = Ha$ لكل $a \in G$.

تعريف 2-25

زمرة جزئية H من زمرة G يقال أنها زمرة جزئية عادية من G إذا كان : $Ha = aH$ لكل $a \in G$ بالنسبة للزمرة G ، فإن G و $\{e\}$ دائماً زمرتان جزئيتان عاديتان من G وهاتان الزمرتان الجزئيتان تسميان زمراً جزئية تافهة .

الزمرة $G \neq \{e\}$ التي ليس لها أي زمرة جزئية عادية غير تافهة يطلق عليها زمرة بسيطة . في مثال (21) السابق H زمرة جزئية عادية غير تافهة من G .

الزمرة الجزئية العادية تعرف أيضاً بالزمرة الجزئية اللامتغيرة أو زمرة جزئية مترافقة ذاتياً .

من الواضح أن كل زمرة جزئية لزمرة إبدالية هي زمرة جزئية عادية .

النظرية التالية تعطينا الخاصية المميزة والمفيدة للزمرة الجزئية العادية .

نظرية 2-26

زمرة جزئية H من زمرة G هي عادية إذا وفقط إذا كان : $g^{-1}hg \in G$ لكل $h \in H, g \in G$.

الرهان

لتكن H زمرة جزئية عادية من G . وليكن $h \in H, g \in G$

فإن $Hg = gH$ (تعريف الزمرة الجزئية العادية)

والآن $hg \in Hg = gH$

وبالتالي فإن $hg = gh_1$ (لبعض العناصر $h_1 \in H$)

أي أن $g^{-1}hg = h_1 \in H$

وبالعكس ليكن H زمرة جزئية بحيث كان :

$$g^{-1}hg \in H \ , \quad \forall h \in H, g \in G$$

اعتبر $a \in G$ لأي $h \in H$, $a^{-1}ha \in H$

إذن $ha = a(a^{-1}ha) \in aH$

ونستنتج أن $Ha \subseteq aH$

ليكن $b = a^{-1}$

فإن $b^{-1}hb \in H$

ولكن $b^{-1}hb = (a^{-1})^{-1}ha^{-1} = aha^{-1}$

وهذا يعطي $aha^{-1} \in H$

بالتالي فإن $ah = (aha^{-1})a \in Ha$

وهذا يبرهن أن $aH \subseteq Ha$

وبالتالي فإن $aH = Ha$

هذه النظرية توضح بصورة مكافئة أن الزمرة الجزئية H من الزمرة G يمكن تعريفها لتكون زمرة جزئية عادية إذا كان $g^{-1}hg \in HH, \forall h \in H, g \in G$.

تعريف 2-27 رتبة الزمرة

عدد عناصر الزمرة يسمى رتبة الزمرة .

رتبة الزمرة السيشار إليها بالرمز $\circ(G)$. الزمرة التي لها رتبة منتهية تسمى زمر منتهية . باستخدام مفهوم المجموعات المصاحبة سنبرهن نظرية تعود إلى لاجرانج والتي تعبر عن العلاقة بين رتبة الزمرة المنتهية ورتبة الزمرة الجزئية منها . وقد لعبت هذه النظرية دوراً أساسيا في تطور نظرية الزمر المنتهية .

نظرية 2-28 (لاجرانج)

رتبة أي زمرة جزئية في زمرة منتهية يقسم رتبة الزمرة .

البرهان

لتكن G زمرة منتهية و H زمرة جزئية في G . نفرض أن $\circ(H) = n$. لأي $a \in G$ نعرف $f : H \to Ha$ بحيث يكون $f(h) = ha$. هذا الراسم فوقي إذ أن كل عنصر في Ha هو من النمط $h \in H, ha$. إضافة إلى ذلك فإنه لأي عنصرين $h_1, h_2 \in H$ فإن $f(h_1) = f(h_2) \Rightarrow h_1 a = h_2 a \Rightarrow h_1 = h_2$ (قانون الحذف في اليمين) . أي أن f راسم أحادي في H فوقي على Ha وهذا يعني أن $\circ(H) = \circ(Ha)$.

ليكن $Ha_1, Ha_2, \ldots, Ha_t$ المجموع الكلي للمجموعات المصاحبة المختلفة للزمرة الجزئية H في الزمرة G .

إذن هذا العدد (t) في المجموعات المصاحبة اليمنى التي تؤلف المجموع الكلي لفصول التكافؤ المختلفة في G حددت بعلاقة التطابق الأيمن معيار H (mod) (نظرية 2-19) .

وبالتالي فإن $Ha_1, Ha_2, \ldots, Ha_n$ هي مجموعات جزئية منفصلة في G وأن $G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_t$.

كما رأينا سابقاً فإن $\circ(Ha_i) = \circ(H) = n, \ \forall\, i = 1, 2, \ldots, t$.

إذن : $\circ(G) = nt$ وبالتالي فإن $\circ(G) \mid \circ(H)$.

يتضح من برهان النظرية السابقة أن $\dfrac{\circ(G)}{\circ\,(H)}$ يساوي عدد المجموعات المصاحبة اليمنى للزمرة الجزئية H من G .

تعريف 2-29 دليل الزمرة الجزئية

لتكن G زمرة و H زمرة جزئية G . فإن عدد المجموعات المصاحبة اليمنى (اليسرى) للزمرة الجزئية H في G يسمى دليل H في G .

دليل H في G يرمز له بالرمز $[G : H]$. أي أن نظرية لاجرانج يمكن إعادة صياغتها على النحو التالي :

نظرية 2-30

لأي زمرة جزئية H من زمرة منتهية G $\circ(G) = \circ(H)[G : H]$.

لأي زمرة منتهية G إذا كان k عدداً صحيحاً موجباً بحيث كان $k \mid \circ(G)$. فليس من الضروري أن تحتوي G زمرة جزئية من الرتبة k [أنظر نظرية 2-30] وبذلك إذا كانت G إبدالية وكان العدد k قاسماً لرتبة G أي $\circ(G)$ فإن G يجب أن تحوي زمرة جزئية من الرتبة k ، وسوف نذكر البرهان فيما بعد .

تعريف 2-31 رتبة عنصر

لتكن G زمرة وليكن $a \in G$ ، فإنه يقال أن a له رتبة منتهية n إذا كان n أصغر عدد صحيح موجب بحيث يكون $a^n = e$ ، e المحايد للزمرة G .

فإذا لم يوجد عدد صحيح موجب k يحقق $a^k = e$ ، فإن a يعتبر ذو رتبة غير منتهية .

الرمز $\circ(a)$ سوف يشير إلى رتبة a .

تعريف 2-32 الزمرة الدورية

تسمى الزمرة G زمرة دورية إذا وجد عنصر $b \in G$ بحيث كان كل عنصر من G هو قوة للعنصر b . يطلق على b مولد G ، ويشار للزمرة G بالرمز $< b >$.

إذا كانت العملية في G تشير إلى الجمع فيمكننا القول أن G زمرة دورية إذا وجد عنصر a من G بحيث كان كل عنصر من G على الصورة na حيث n عدد صحيح .

مثال 22

لتكن $G_n = \left\{ e^{\frac{2\pi ri}{n}} \; : \; r = 0, 1, 2, \ldots, n-1 \right\}$ زمرة الجذور النونية للواحد الصحيح.

وليكن $a = e^{\frac{2\pi i}{n}}$ ، فإن $a \in G_n$ (أي عدد صحيح r ، $\left(e^{\frac{2\pi ri}{n}} = \left(e^{\frac{2\pi i}{n}} \right)^r = a^r \right)$. كل عنصر من G_n هو أس أو قوة للعنصر a .

أي أن G_n زمرة دورية مولدة بواسطة a .

مثال 23

زمرة الجمع Z زمرة دورية مولدة بواسطة 1 حيث $1 \in Z$ وكل عنصر n من عناصر Z يمكن كتابته على النحو : $n = n.1$.

نظرية 2-33

زمرة من رتبة n هي دورية إذا وفقط إذا وجد فيها عنصر رتبته n .

البرهان

لتكن G زمرة دورية من رتبة n وليكن a مولد G نضع $H = \{a^i \mid i \in Z\}$ من الواضح أن H زمرة جزئية من G . وحيث أن G منتهية فلا يمكن أن تكون من رتبة غير منتهية .

ليكن $\circ(a) = m$. والمطلوب إثبات أن H تحوي m عنصراً . الآن : $a, a^1, a^2, \ldots, a^{m-1}, a^m = e$ كلها تنتمي إلى H وليس من بينها اثنان متساويان ، بناء على أن $\circ(a) = m$. إذن H فيه على الأقل m عنصر . لتكن $x \in H$ إذن $x = a^j$ ، $j \in Z$.

الآن : $0 \le r < m$ ، $j = mk + r$ ، k و r عددان صحيحان .

إذن : $x = a^j = (a^m)^k a^r = a^r$. وبالتالي فإن أي عنصر من H هو أحد العناصر : $a, a^2, a^3, \ldots, a^m$. لذلك فإن : $H = \{a, a^2, a^3, \ldots, a^m\}$ وهذا يبرهن المطلوب .

حيث أن $G =< a >, G \subseteq H$ بمعنى آخر فإن $G = H$ وأيضاً $n = \circ(G) = \circ(H) = m = \circ(a)$.

وبالعكس لتكن G زمرة من الرتبة n و $b \in G$ يكون من الرتبة n .

كما سبق $K = \{b^r : r \in Z\}$ هي زمرة جزئية من G بها n عنصر لأن $\circ(b) = n$.

حيث أن $K \subseteq G$ و $\circ(K) = n = \circ(b)$ فإن $K = G$ ، وينتج أن G زمرة دورية متولدة بواسطة b .

والآن لتكن G أي زمرة وكان $a \in G$. فإذا كان $H = \{a^n \mid$ صحيح n أيعدد$\}$.

اعتبر أي عنصرين $x = a^n, y = a^m$ في H . فنجد أن $xy^{-1} = a^n . a^{-m} = a^{n-m} \in H$ وهذا يؤدي إلى أن H زمرة جزئية من G .

من الواضح أن H زمرة دورية مولدة بواسطة a . هذه الزمرة الجزئية تسمى زمرة جزئية دورية من G مولدة بواسطة a ونكتب ذلك $H =< a >$.

نظرية 2-34

إذا كان G زمرة منتهية فإن رتبة أي عنصر في G تقسم رتبة G .

البرهان

لتكن G زمرة منتهية و $a \in G$ ، ولتكن $H =< a >$ زمرة جزئية دورية من G مولدة بواسطة a .

أي أن $\circ(H) = \circ(a)$ (نظرية 2-33) .

ومن نظرية لاجرانج $\circ(H) \mid \circ(G)$. إذن $\circ(a) \mid \circ(G)$. □

نتيجة 2-35

إذا كانت G زمرة منتهية فإن لأي $a \in G$ يكون $a^{\circ(G)} = e$.

البرهان

لتكن $\circ(G) = N, \circ(a) = n$. في نظرية 2-34 يكون $N = nm$ لعدد صحيح موجب m . إذن $a^N = (a^n)^m = e^m = e$ ، بالتالي تحققت النتيجة . □

نظرية 2-36

في أي زمرة G يتحقق التالي :

(1) لأي عنصرين $a, x \in G$ فإن $\circ(a) = \circ(x^{-1}ax)$.

(2) إذا كان لأي عنصر $a \in G$ ، $\circ(a)$ منتهية فإنه لأي عدد صحيح m إذا كان $a^m = e$ فإنه يؤدي إلى أن $\circ(a) \mid m$.

(3) لأي عنصرين $a, b \in G$ فإن $\circ(ab) = \circ(ba)$.

(4) إذا كان $\circ(a) = n$ والعدد الصحيح الموجب k يقسم n $(k \mid n)$ فإن $\circ(a^k) = \dfrac{n}{k}$.

البرهان

(1) ليكن n أي عدد صحيح موجب ، أي :

$$a^n = e \Leftrightarrow x^{-1}a^n x = x^{-1}ex = e \Leftrightarrow (x^{-1}ax)^n = e$$

لأن $(x^{-1}ax)^n = x^{-1}a^n x$. بالتالي $\circ(a) = \circ(x^{-1}ax)$.

(2) ليكن $\circ(a) = n$ و m أي عدد صحيح حيث $a^m = e$.

الآن حسب خوارزمية إقليدس فإن $m = nq + r$ لعددين صحيحين q و r حيث $0 \le r < n$. فإن $e = a^m = (a^n)^q a^r = ea^r = a^r$.

بما أن n هو أصغر عدد صحيح موجب بحيث $a^n = e$ ، عليه فإن $r < n$ و $r > 0$ وهذا مرفوض .

إذن $r = 0$ ويكون $m = nq$ أي أن $\circ(a) = n \mid m$ وهذا يبرهن (2) .

(3) بما أن $ab = b^{-1}(ba)b$ ، فإن $\circ(ab) = \circ(ba)$ حسب الجزء (1) .

(4) ينتج من (2) . □

مثال 24

اعتبر الزمرة $G = \{1, -1, i, -i\}$ حيث $i = \sqrt{-1}$. الآن $\circ(G) = 4$.

(i) $i^4 = 1$ ولكن لا يوجد عدد صحيح موجب $m < 4$ بحيث $i^m = 1$ هذا يعني أن $\circ(i) = 4$ وبوضوح يكون $4 \mid \circ(G)$.

(ii) الآن $(-1)^2 = 1$ و $(-1)^3 \neq 1$ وهذا يؤدي إلى أن $\circ(-1) = 2$ ومن الواضح $\circ(-1) \mid \circ(G)$.

(iii) بما أن $1 = i^4$ ، $-1 = i^2$ ، $-i = i^3$ ، $i = i$ نجد أن G زمرة دورية مولدة بالعنصر i . لاحظ أن G مولدة بالعنصر $-i$ أيضاً ولكن 1- أو 1 لا يولدان G .

نظرية 2-37

لأي زمرتين جزئين H و K في زمرة G يكون ما يلي :

(1) $H \cap K$ أيضاً زمرة جزئية من G .

(2) إذا كانت H عادية في G فإن $H \cap K$ تكون عادية في K .

(3) إذا كانتا H و K كلتاهما عادية في G ، فإن $H \cap K$ تكون عادية في G .

البرهان

(1) لما كان : $e \in H \cap K$ فإن $H \cap K$ غير خالية .

الآن : $a, b \in H \cap K \Rightarrow a, b \in H, a, b \in K$

$$\Rightarrow ab^{-1} \in H, ab^{-1} \in K$$

$$\Rightarrow ab^{-1} \in H \cap K$$

وبالتالي فإن : $H \cap K$ هي زمرة جزئية من G .

(2) لتكن H عادية في G ، وليكن $x \in K$ و $a \in H \cap K$ ، فإن $x^{-1}ax \in K$ حيث $x, a \in K$ ، زيادة على ذلك $x^{-1}ax \in H$ لأن H عادية و $a \in H$.

ونستنتج أن :

$$x^{-1}ax \in H \cap K \quad \forall x \in K, a \in H \cap K$$

أي أن $H \cap K$ زمرة جزئية عادية من K .

(3) لتكن K, H زمرتان جزئيتان عاديتان من G .

الآن : $x \in G, a \in H \cap K \Rightarrow x \in G, a \in H, a \in K$

$$\Rightarrow x^{-1}ax \in H, x^{-1}ax \in K$$

لأن H, K كلتاهما زمرة جزئية عادية من G .

هذا يؤدي إلى أن $x^{-1}ax \in H \cap K$

إذن $H \cap K$ زمرة جزئية عادية من G . □

تعريف 2-38

إذا كان A و B مجموعتين غير خاليتين من زمرة $< G, * >$ فإننا نقصد من $A * B$ المجموعة : $\{a * b : a \in A, b \in B\}$. إذا كانت العملية في G هي الضرب فإن $A * B$ يشار إليها بالرمز AB ، ويطلق عليها ضرب A في B . إذا كانت العملية في G

هي الجمع فإن $A * B$ يشار إليها بالرمز $A + B$ ويطلق عليها مجموع فإن $A * B$ يشار إليها $A + B$ ويطلق عليها مجموع A و B .

نظرية 2-39

لتكن H و K زمرتين جزئيتين من زمرة G . فإن HK تكون زمرة جزئية من G إذا وفقط إذا كان $HK = KH$.

البرهان

لتكن HK زمرة جزئية من G . اعتبر $h \in H, k \in K$ فإن $(kh)^{-1} = h^{-1}k^{-1} \in HK$ ، وبالتالي $kh \in HK$ طالما كانت HK زمرة جزئية من G . وينتج أن $KH \subseteq HK$.

مرة ثانية $hk \in HK \Rightarrow (hk)^{-1} \in HK \Rightarrow (hk)^{-1} = h_1k_1$ لبعض العناصر $k_1 \in K, h_1 \in H$

$$\Rightarrow hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$$

وبالتالي : $HK \subseteq KH$

أي أن : $HK = KH$

وبالعكس لتكن $HK = KH$. من الواضح أن $e \in HK$ وبالتالي فإن HK غير خالية .

الآن لتكن $x, y \in HK$ فإن $x = h_1k_1$ و $y = h_2k_2$ لبعض $h_1, h_2 \in H$ و $k_1, k_2 \in K$.

بأن $xy^{-1} = h_1k_1(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1}$

الآن $(k_1k_2^{-1})h_2^{-1} \in KH$ ، ومن الفرض $KH = HK$ ، وبناء عليه $(k_1k_2^{-1}) = h_3k_3$ لبعض العناصر $h_3 \in H, k_3 \in K$ فإننا نحصل على $xy^{-1} = h_1(h_3k_3) = (h_1h_3)k_3 \in HK$ وهذا يعني أن : $x, y \in HK \Rightarrow xy^{-1} \in HK$

إذن HK تكون زمرة جزئية من G .

نتيجة 2-40

إذا كانت H, K زمرتين جزئيتين من G إما H أو K عادية في G فإن HK تكون زمرة جزئية من G .

البرهان

لتكن H زمرة جزئية عادية من G . إذن لكل $k \in K$ ، $Hk = kH$ وهذا يعطي $HK = KH$.

إذن KH تكون زمرة جزئية من G . بنفس الطريقة إذا كانت K عادية فإن لكل $h \in H$ ، $hK = Kh$ والذي يؤدي إلى $HK = KH$. إذن النتيجة نحصل عليها من النظرية السابقة . □

نتيجة 2-41

إذا كان H و K زمرتين جزئيتين من الزمرة الإبدالية G . فإن HK تكون زمرة جزئية من G .

ملاحظة (1)

في الفصل الثالث [البند 3 ، المسألة 8] فإننا نعطي مثالاً لزمرتين جزئيتين K, H من زمرة G والتي فيها $HK \neq KH$ ، وبالتالي HK ليست بصورة عامة زمرة جزئية .

ملاحظة (2)

في الفل الثالث [بند 3 ، المسألة 7 ، iii] قد نعطي مثالاً لزمرتين جزئيتين K, H من زمرة G بحيث كان $HK = KH$ ولكن أياً من H و K ليست عادية في G وننصح

القراء بأن لا يحاولوا فهم أو حل المسائل التي أشير إليها سابقاً قبل التمكن من موضوع زمر التباديل .

نظرية 2-42

إذا كانت H و K زمرتين جزئيتين منتهيتين من زمرة G ، فإن :

$$\circ(HK) = \frac{\circ(H) . \circ(K)}{\circ(H \cap K)}$$

البرهان

ليكن $D = H \cap K$ وليكن $K = \bigcup_{i=1}^{t} Dk_i$ تحليل K إلى المجموعات المصاحبة اليمنى المنفصلة للزمرة الجزئية D في K فإن $t = \frac{\circ(K)}{\circ(D)}$ وعلاوة على ذلك $HK = H\left(\bigcup_{i=1}^{t} Dk_i\right) = \bigcup_{i=1}^{t} Hk_i$ لأن $HD = H$ ينتج من $D \subseteq H$.

الآن نريد إثبات أن المجموعات المصاحبة اليمنى $Hk_1, Hk_2, \ldots, Hk_i$ مختلفة زوجا زوجاً وإلا فبفرض $Hk_i = Hk_j$ لبعض j, i . هذا يعطينا $k_i.k_j^{-1} \in H$ ولكن عندها $k_ik_j^{-1} \in K$ ، إذن $h_ih_j^{-1} \in H \cap K = D$.

وينتج أن $Dk_i = Dk_j$ و $i = j$.

إذن $Hk_1, Hk_2, \ldots, Hk_i$ مختلفة ، وعليه فهي مجموعات مصاحبة يمنى منفصلة في H . كل واحدة ذات عناصر عددها $\circ(H)$ ونحصل على :

$$\circ(HK) = \circ(H)t = \frac{\circ(H). \circ(K)}{\circ(D)} = \frac{\circ(H). \circ(K)}{\circ(H \cap K)}$$

تمارين محلولة

تمرين (1)

إذا كانتا H, K زمرتين جزئيتين من زمرة G فإنه لأي $a, b \in G$ ، إما $Ha \cap Kb = \phi$ أو $Ha \cap Kb = (H \cap K)\, c$ لبعض $c \in G$.

الحل

نفرض أن $Ha \cap Kb$ غير خالية . لتكن $c \in Ha \cap Kb$ ولكن $c \in Hc$ و $c \in Kc$. وبالتالي فإن $c \in Ha \cap Hc$ كذلك فإن $c \in Kb \cap Kc$ وهذا يؤدي إلى أن $Ha = Hc$ ، $Kb = Kc$. أي $Ha \cap Kb = Hc \cap Kc$.

الآن : $H \cap K \subseteq H \Rightarrow (H \cap K)\, c \subseteq Hc$

وكذلك : $H \cap K \subseteq K \Rightarrow (H \cap K)\, c \subseteq Kc$

وبالتالي فإننا نحصل على : $(H \cap K)\, c \subseteq Hc \cap Kc$

مرة ثانية : $t \in Hc \cap Kc \Rightarrow t = hc = kc$

لبعض : $h \in H, k \in K$

كنتيجة : $h = tc^{-1} = k \in H \cap K$

وبالتالي : $t \in (H \cap K)\, c$

وهذا يعطي : $Hc \cap Kc \subseteq (H \cap K)\, c$

إذن : $Ha \cap Kb = Hc \cap Kc = (H \cap K)\, c$

تمرين (2) (بوانكاريه)

إذا كان K, H زمرتين جزئيتين من أدلة منتهية في G . أثبت أن $H \cap K$ هي أيضاً ذات دليل منته .

الحل

لـتكن : $[G:H]=m$ و $[G:K]=n$ ، ولـتكن $Ha_1, Ha_2, \dots, Ha_m$ كـذلك $Kb_1, Kb_2, \dots, Kb_n$ مجموعات مصاحبة يمنى مختلفة لكل من K, H على الترتيب .

الآن ومـن تمـرين (1) لأي $1 \le i \le m$ و $1 \le j \le n$ ، أمـا $Ha_i \cap Kb_j$ خاليـة أو $Ha_i \cap Kb_j = (H \cap K)\, c_{ij}$ لـــبعض $c_{ij} \in G$ ، وأيضــــاً $(H \cap K)z_{ij} = Hz_{ij} \cap Kz_{ij}$ ، وبالتالي فإن كل مجموعة مصاحبة يمنى للزمرة الجزئية $H \cap K$ تتحدد بواسطة تقاطع مجموعة مصـاحبة يمـنى للزمـرة الجزئيـة H ومجموعـة مصـاحبة يمـنى للزمـرة الجزئيـة K . أي أن عـدد المجموعــات المصــاحبة اليمـــنى المختلفــة للزمـــرة الجزئيـــة $H \cap K$ علـــى الأكثـــر يســـاوي mn .

تمرين (3)

لتكن G زمرة وليكن $a \in G$ من الرتبة m ، فإن $\circ(a^k) = \dfrac{m}{(m,k)}$.

الحل

لــــيكن $(m,k)=d$. إذن $m = cd$ ، $k = bd$ لــــبعض $b, c \in N$ بحيـــث $(b,c)=1$.

الآن $(a^k)^c = (a^{bd})^c = a^{bcd} = a^{bm} = e$ ، حيث e هو المحايد للزمرة G .

علاوة على ذلك إذا كان $(a^k)^e = e$ فإن :

$$m \mid kl \Rightarrow cd \mid bdl \Rightarrow c \mid bl$$

ولكن $(c,b)=1$ وبالتالي $c \mid l$. إذن $\circ(a^k) = c = \dfrac{m}{d}$.

تمرين (4)*

إذا كـان p هـو أصغر عامـل أولي لرتبـة زمـرة منتهيـة G . بـرهن أن أي زمـرة جزئيـة ذات دليل p تكون عادية .

الحل

لتكن H زمرة جزئية من G ذات دليل p .

أولاً – نحن نريد إثبات أنه إذا كانت $x \notin H$ فإنه لكل $x^i \notin H; i = 1, 2, \ldots, p-1$.

فإذا كان ما نريد غير صحيح فإننا نستطيع أن نجد $1 \le k \le p-1$ بحيث يكون $x^k \in H$. ليكن j هو أصغر عدد صحيح موجب بحيث كان $x^j \in H$ بتعبير آخر $x^t \notin H$ لقيم : $t = 1, 2, \ldots, j-1$.

لتكن : $m = \circ(x)$ و $n = \circ(G)$ وحيث أن $m \mid n$ و $1 < j < p$ وكان p أصغر عامل أولي للعدد n ، فإننا نحصل على أن j لا يمكن أن تقسم m ، وبالتالي يمكننا أن نجد $q, r \in Z$ بحيث كان $m = qj + r$ ، مع $0 < r < j$.

وحيث أن رتبة x هي m فإن $x^m = e$ حيث e هو محايد G ، وهذا يؤدي إلى أن $(x^j)^q x^r = e \Rightarrow x^r \in H$ لأن $x^j \in H$ هذا يتعدى اختيارنا j . وبالتالي فإن ما نريد قد تحقق .

لإثبات النتيجة الرئيسية ، نفترض أن H ليست زمرة جزئية عادية من G . وبالتالي يوجد بعض $x \in G$ و $h \in H$ بحيث كان $x^{-1}hx \notin H$. من الواضح أن $x \notin H$.

مما برهنا يكون $x^i \notin H$ لكل $i = 1, 2, \ldots, p-1$ ، كذلك عندما يكون $1 \le i < j \le p-1$ ، $Hx^i = Hx^j \Rightarrow x^i = h_1 x^j$ لبعض $h_1 \in H$ ويؤدي إلى أن $x^{j-i} = h_1^{-1} \in H$ ويعد ذلك غير معقول . وفي هذه الحالة فقط حصلنا على أن $H, Hx, Hx^2, \ldots, Hx^{p-1}$ كلها مجموعات مصاحبة يمنى مختلفة لـ H .

لتكن $y = x^{-1}hx$ فإنه عندما $y \notin H$ ، بأسلوب مماثل فإننا نحصل على كون $H, Hy, Hy^2, \ldots, Hy^{p-1}$ كلها مجموعات مصاحبة يمنى مختلفة للزمرة الجزئية H .

وبالتالي فإن المجموعتين :

$$\{H, Hy, Hy^2, \dots, Hy^{p-1}\}, \{H, Hx, Hx^2, \dots, Hx^{p-1}\}$$

متساويتان . إذن $Hx = Hy^r$ لبعض $h' \in H$. وكنتيجة :

$$x = h'x^{-1}h^r x \Rightarrow h'x^{-1} = h^{-r} \Rightarrow h^r h' = x$$

ولكننا عندئذ سنحصل على كون $x \in H$ وهذا غير معقول . أي أن H هي زمرة جزئية عادية من G .

ملاحظة

كحالة خاصة من هذا التمرين فإننا نحصل على أن كل زمرة ذات دليل يساوي 2 هي زمرة جزئية عادية .

تمرين (5)

برهن أن الزمرة المنتهية ذات الرتبة الزوجية بها على الأقل عنصر من الرتبة 2 .

الحل

لتكن G زمرة من رتبة $2n$.

ضع : $T = \{x \in G : x^2 = e\}$

و : $S = \{x \in G : x^2 \neq e\}$

من الواضح أن : $T \cap S = \phi$ وأن $G = T \cup S$ ، وبالتالي فإن :

$$\circ(G) = \circ(T) + \circ(S)$$

الآن : نفترض أن S غير خالية ، إذن : $x \in S$ يؤدي إلى أن $x^{-1} \in S$ و $x \neq x^{-1}$ هذا يعني $\circ(S)$ هو عدد زوجي ≥ 2 أي أن $\circ(S) = 2m$ ، m عدد صحيح ≥ 1 .

ونستنتج أن $\circ(S) = 2k$ ، k هو عدد صحيح > 0 . وهذا يؤدي إلى أن : $\circ(T) = 2n - 2k = 2(n-k)$ عدد زوجي .

ولما كان $e \in T$ ، $\circ(T) \geq 1$ وعليه $\circ(T) \geq 2$ وبالتالي فإنه يوجد على الأقل عنصر واحد وليكن $a \in T$ ، $a \neq e$.

ولما كان $a \in T \Rightarrow a^2 = e$ فإن $\circ(a) = 2$.

تمرين (6)

إذا كانت H زمرة جزئية من G بحيث كان $x^2 \in H$ لجميع العناصر $x \in G$ ، برهن أن H هي زمرة جزئية عادية من G .

الحل

لأي $g \in G$ ، $h \in H$ فإن $(gh)^2 \in H$ كذلك $g^{-2} \in H$ حيث أن H زمرة جزئية ، $h^{-1}g^{-2} \in H$ كذلك $(gh)^2h^{-1}g^{-2} \in H$ ، هذا يعطينا أن $ghghh^{-1}g^{-2} \in H$ أي أن $ghg^{-1} \in H$ إذن H تكون زمرة جزئية عادية من G .

تمرين (7)

إذا كانت H زمرة جزئية من زمرة G بحيث كان دليل H في G هو 2 فإن H زمرة جزئية عادية من G .

(لاحظ أنه إذا كان G زمرة لها رتبة منتهية فإن النتيجة تأتي مباشرة من تمرين (4) . نحن نقدم حلين للحالة العامة :

حل (I)

ليكن $a \in G$. إذا كان : $a \in H$ فإن : $aH = H = Ha$ وإذا كان : $a \notin H$ فإن $H \neq aH \Rightarrow G = H \cup aH$ حيث : $H \cap aH = \{e\}$.

بنفس الطريقة $G = H \cup Ha$ و $H \cap Ha = \{e\}$.

من تمرين (5) . بند (1) الفصل (1) حصلنا على $aH = Ha$ إذن H هي زمرة جزئية عادية من G .

حل (II)

ليكن $a \in G$ فإذا كان $a \in H$ فإن $a^2 \in H$ لأن H زمرة جزئية من G .

نفرض أن $a \notin H$. اعتبر a^2H ، G ذوات مجموعتين مصاحبتين يساريتين للزمرة الجزئية H هما H و aH إذا كانت $a^2H = aH$ فإن $aH = H$ وهذا يؤدي إلى أن $a \in H$ ، وهذا يتعارض مع الفرض .

وبالتالي فإن $a^2H = H$ أي أن $a^2 \in H$ ، إذن لكل $a \in G$ يكون $a^2 \in H$ من تمرين (6) السابق H زمرة جزئية عادية من G .

تمارين

1- بين أنه إذا كانت H مجموعة جزئية منتهية غير خالية من زمرة G . فإن H تكون زمرة جزئية من G إذا وفقط إذا كان $HH \subseteq H$.

2- إعط مثالاً يوضح أن الزمرة G يمكن أن يكون لها مجموعة جزئية غير خالية H بحيث يكون $HH \subseteq H$ رغم أن H لا تكون زمرة جزئية من G .

3- وضح أنه إذا كانت H و K زمرتين جزئيتين عاديتين في الزمرة G فإن HK تكون زمرة جزئية عادية من G . وزيادة على ذلك وضح أن تلك النتيجة ليست بالضرورة محققة إذا كانت إحداها فقط عادية .

4- اعتبر الزمرة G والزمرة الجزئية H من G ، لتكن : $G = Ha_1 \cup ... \cup Ha_t$ تحليل G إلى مجموعات مصاحبة يمنى منفصلة لـ H . وضح أن : $G = a_1^{-1}H \cup ... \cup a_t^{-1}H$ هي تحليل G إلى مجموعات مصاحبة يسرى من H .

5- إعط مثالاً لزمرة G لها زمرة جزئية H وعنصرين a, b بحيث يكون $Ha = Hb$ لكن $aH \neq bH$.

6- إذا كانت $H \subseteq K$ زمرتين جزئيتين من زمرة منتهية وضح أن : $[G : H] = [G : K][K : H]$.

[**إرشاد** من نظرية لاجرانج : $\circ(G) = \circ(K)[G : K]$ ، $\circ(K) = \circ(H)[K : H]$ و $\circ(G) = \circ(H)[G : H]$] .

7- لتكن Z زمرة الجمع للأعداد الصحيحة وأنه لأي عدد صحيح موجب n كان H_n تعبر عن مجموعة كل مضاعفات n . وضح ما يلي :

(i) H_n هي زمرة جزئية من Z .

(ii) دليل H_n في Z هو n .

(iii) لأي عددين صحيحين موجبين m, n إذا كان k, j هما عامل مشترك أكبر ومضاعف مشترك أصغر لهما على الترتيب . فإن $H_k = H_m \cap H_n$ و $H_j = H_n + H_m$.

8- لتكن H زمرة جزئية من زمرة G . أثبت ما يلي :

(i) لأي $x \in G$ ، $x^{-1}Hx = \{x^{-1}hx \mid h \in H\}$ هي زمرة جزئية من G .

[**إرشاد** استخدم نظرية 2-16] .

(ii) $\circ(H) = \circ(x^{-1}Hx)$

[**إرشاد** وضح أن $h \leftrightarrow x^{-1}hx$ تمثل تناظراً أحادياً بين عناصر H وتلك التي في $x^{-1}Hx$] .

(iii) إذا كانت G منتهية وكانت $n = \circ(H)$ بحيث كانت G لا تحوي أي زمرة جزئية غير H من رتبة n . أثبت أن H عادية في G .

9- إذا كانت $a \in G$ تعرف $N(a) = \{x \in G : ax = xa\}$ أثبت ما يلي :

(i) $N(a)$ زمرة جزئية من G .

(ii) لأي عنصرين $x, y \in G$ فإن $N(a)x = N(a)y \Leftrightarrow x^{-1}ax = y^{-1}ay$

[**إرشاد** استخدم الحقيقة لأي زمرة جزئية H ، $Hx = Hy \Leftrightarrow xy^{-1} \in H$]

تعريف

$N(a)$ تسمى : المركز أو المنظم للصفر a .

10- إذا كانت G زمرة ، فإن المركز $Z(G)$ للزمرة G تعرف على النحو : $\{z \in G : zx = xz \; \forall \, x \in G\}$. برهن أن $Z(G)$ هي زمرة جزئية عادية من G .

11- * وضح بمثال أنه إذا كانت H زمرة جزئية عادية من G وأن K هي زمرة جزئية عادية من H فإن K ربما لا تكون زمرة جزئية عادية من G .

12- * إعط مثالاً لزمرة G وزمرة جزئية H من G بحيث يكون $aHa^{-1} \subset G$ لبعض $a \in G$.

13- لتكن H و K زمرتين جزئيتين عاديتين من H بحيث كان $H \cap K = (e)$.
وضح أن : $hk = kh \, \forall \, h \in H, k \in K$.
[**إرشاد** وضح أن $hkh^{-1}k^{-1} \in H \cap K$] .

14- H هي مجموعة جزئية غير خالية من زمرة G بحيث كان : $Hx = HxH$ لجميع : $x \in G$ ، وضح أن $Hx = xH$.

15- ليكن a, b عنصرين من زمرة G بحيث كان $ab = ba$ ، أثبت أنه إذا كان لكل من $\circ(a)$ و $\circ(b)$ عددان صحيحان أوليان نسبياً للآخر فإن $\circ(ab) = \circ(a)\circ(b)$. وضح بالأمثلة أن النتيجة ليست صحيحة عندما :
(i) $ab \neq ba$ (ii) $ab = ba$ ولكن $\circ(a)$ و $\circ(b)$ ليسا أوليين بالنسبة لبعضهما البعض .

16- إذا كانت T زمرة جزئية دورية عادية في الزمرة G ، وضح أن كل زمرة جزئية من T تكون عادية في G .

17- وضح أنه إذا كانت كل زمرة جزئية دائرية من G عادية فإن كل زمرة جزئية من G تكون عادية .

18- إذا كان a عنصراً من الزمرة G ذات الرتبة المنتهية وكان k أي عدد صحيح غير الصفر . أثبت أن : $\circ(a) = \circ(a^k)$ إذا وفقط إذا كانت k و $\circ(a)$ أوليان بالنسبة إلى بعضهما البعض .

19- بين أن كل زمرة رتبتها عدد أولي تكون دائرية .

20- بين أن زمرة جزئية H من زمرة G تكون عادية في G إذا وفقط إذا كان حاصل ضرب أي مجموعتين مصاحبتين يمينيتين من H في G تكون أيضاً مجموعة مصاحبة يمنى من HG .

21- إذا كان G له فقط عنصر واحد a من رتبة n ، برهن أن : $a \in Z(G)$.

22- لتكن H و K زمرتين جزئيتين عاديتين من زمرة منتهية بحيث $\circ(H)$ و $\circ(K)$ أوليان نسبياً ، وضح أنه لأي $h \in H$ ، $k \in K$ يكون $hk = kh$.

[**إرشاد** استخدم نظرية لاجرانج] .

23- (إتش . بي . مان .) إذا كانت G زمرة منتهية وكانت A, B مجموعتين جزئيتين غير خاليتين من G . برهن أنه إما : $G = AB$ أو $\circ(G) \geq \circ(A) + \circ(B)$.

24- بين أنه إذا كانت G زمرة ذات عدد منته من الزمرة الجزئية فإن G تكون منتهية .

25- ** لتكن A و B زمرتين جزئيتين من زمرة G . إذا كان $[G : A]$ منته فأثبت أن : $[A : A \cap B] \leq [G : B]$ ويتحقق التساوي إذا وفقط إذا كان $G = AB$.

26- في المسألة (25) السابقة أثبت أنه إذا كان $[G : A]$ أيضاً منته فإن : $[G : A \cap B] \leq [G : A][G : B]$ ويتحقق التساوي إذا وفقط إذا كان $G = AB$.

27- إذا كان في الزمرة G وإذا كان $a^5 = e$ و $aba^{-1} = b^2$ للعنصرين $a, b \in G$. أثبت أنه إذا كانت $b \neq e$ فإن $\circ(b) = 31$.

28- إذا كان H و K زمرتين جزئيتين من زمرة منتهية G وكان $\circ(H) > \sqrt{\circ(G)}$ و $\circ(K) > \sqrt{\circ(G)}$. بين أن : $\circ(H \cap K) > 1$.

29- * (أويلر) إذا كان n عدداً صحيحاً موجباً وكان a أولياً نسبة إلى n . أثبت أن : $a^{\phi(n)} \equiv 1 \pmod{n}$ حيث $\phi(n)$ هو عدد الأعداد الصحيحة الموجبة الأصغر من n وهو أولي نسبة للعدد n .

30- (فيرمات) إذا كان p عدداً أولياً صحيحاً وكان a أي عدد صحيح فأثبت أن $a^P \equiv a$ (مقياس p) .

31- لتكن Q مجموعة كل الأعداد النسبية وكانت :

$$G = \{(a, b) : a, b \in Q, a \neq 0\}$$

عرفت $*$ على G على النحو التالي $(a, b) \neq (c, d) = (ac, ad + b)$

وضح أن : $< G, * >$ زمرة غير إبدالية ، اعتبر $H = \{(1, b) : b \in Q\}$. أثبت أن H زمرة جزئية عادية من G .

32- إذا كانت الزمرة G هي اتحاد عائلة من الزمر الفعلية العادية كل اثنتين منهما ليس بنهما مشترك سوى المحايد . وضح أن G زمرة إبدالية .

33- إذا كانت B, A زمرتين جزئيتين لكل منهما دليل منته في زمرة G وكان $[G : A]$ و $[G : B]$ أوليان نسبة إلى بعضهما البعض ، وضح عندئذ أن $G = AB$.

[إرشاد استخدم المسألة 26 السابقة] .

34- ** لمجموعة جزئية غير خالية S من زمرة G عرفت $S^k = \left\{\prod_{i=1}^{k} S_i : S_i \in S\right\}$ لأي عدد صحيح موجب k . برهن أن إذا كانت G فيها n عنصراً فإن S^n هي زمرة جزئية من G .

35- ** بين أنه إذا كانت الزمرة G ذات رتبة زوجية فإن عدد العناصر ذوات الرتبة 2 يكون فردياً .

36- G زمرة إبدالية ذات n من العناصر :

$g_1, g_2, \dots, g_n$. وضح أن $(g_1 . g_2 . \dots g_n)^n = e$.

-37 أعط مثالاً لزمرة G وعنصرين $a, b \in G$ بحيث يكون كل من $\circ(a)$ و $\circ(b)$ منته ولكن (ab) ليس له رتبة منتهية .

[**إرشاد** اعتبر الزمرة $S(R)$ ، مجموعة كل الدوال الأحادية الفوقية من R إلى R] .

عرفت $a(x) = -x$ و $b(x) = 1 - x$ لكل $x \in R$. من الواضح أن $\circ(a) = \circ(b) = 2$ ولكن رتبة ab غير منتهية .

3

زمر القسمة – والهومورفزمات – والتباديل

Quotient Groups – Homomorphisms and Permutations

مقدمة

رأينا في الفصل الأخير أن هناك عدداً كبيراً من أمثلة مجموعات ذات أنواع مختلفة . في هذا الفصل نحاول متابعة عمل ما يأتي :

1- تقديم فكرة الهومومورفزم وقد نقيم علاقة بين مختلف المجموعات .

2- إعطاء بعض طرق بناء المجموعة الجديدة من المجموعات المعروفة .

3- دراسة زمر التباديل .

4- أخيراً نقدم الترافق بين عناصر المجموعة ، وعليه نفجر (نوسع) البناء الداخلي للمجموعة .

1- مجموعات خارج القسمة

لتكن G زمرة و N زمرة جزئية عادية من G ، نحن نعلم أن $Nx = xN \ \forall \ x \in G$ ، أي أن المرفقات اليسارية واليمينية للزمرة الجزئية متساوية لكل $x \in G$.

لذلك ليست هنالك حاجة للتمييز بين المرافقات اليسايرية واليمينية للمجموعة الجزئية العادية N . لذلك سنقول بأن Nx مجموعة مرافقة للمجموعة N .

لتكن G / N رمزاً لمجموعة جميع مرافقات المجموعة N في G .

نظرية 3-1

لتكن G زمرة ولتكن N زمرة جزئية فعلية من G ، المجموعة G / N مجموعة كل مرافقات N في G ، تمثل زمرة تحت العملية الثنائية التركيبية وتعرف كالآتي :

لكل $aN, bN \in G / N$ $\qquad (Na)(Nb) = Nab$

البرهان

قبل أن نبدأ بتفاصيل البرهان ، سنذكر ملاحظة حول تعريف التركيب أعلاه . على ما يبدو فإن عملية الضرب $(Na)(Nb) = N(ab)$ تعتمد على اختيار عناصر التمثيل لـ b, a Nb ، Na على التوالي .

على كل حال إذا أردنا تعريف عملية الضرب لأي مرافقين ، لابد أن تنتبه إلى أن عملية الضرب لا تعتمد على العنصرين b, a لكنها تعتمد على المرافقات Nb, Na نفسهم .

ويمكن أن نجد أربعة عناصر b_1, b, a_1, a بحيث يكون $Nb = Nb_1, Na = Na_1$ ومن صيغة الضرب

$$(Na_1)(Nb_1) = N(a_1b_1), N(a)(Nb) = N(ab)$$

وكما أن $(Na_1) = (Na), Nb = Nb_1$ فمن الطبيعي أن نتوقع أن يكون :

$$(Na)(Nb) = (Na_1)(Nb_1)$$

أي أنه

$$Nab = Na_1b_1$$

بغير ذلك سيكون تعريف التركيب الذي عرف سابقاً بلا معنى ، والآن سنأتي إلى البرهان الحقيقي .

لتكن $\qquad Na = Na_1, Nb = Nb_1$

مثال 5

لتكن E زمرة الجمع للأعداد الزوجية ، فتكون الدالة $f : Z \to E1$ المعرفة بـ $f(n) = 2n \quad \forall n \in Z$ تمثل هومومورفزم لأن أي عنصر في E هو على شكل $2n$ حيث

$n \in Z$ لذلك حصلنا على أن f شاملة ، لذلك فإن E تمثل الهومومورفزم الصوري للمجموعة Z . وكذلك f سوف تكون واحد لواحد (1-1) (؟) .

وبعد الاتفاق على أن عملية الضرب هي دلالة للتركيب الثنائي . نستطيع أن نقول بأن الدالة f من الزمرة G إلى الزمرة G' سوف تكون تشاكل إذا كانت . $f(ab) = f(a)f(b) \quad \forall\, a, b \in G$

تعريف 4.3 نواة الهومومورفزم

لتكن f تشاكل من الزمرة G إلى الزمرة G' فإن نواة الدالة f هي المجموعة $\{x \in G \mid f(n) = e'\}$ حيث e' يمثل المحايد في الزمرة G' ، وسنرمز لنواة الدالة f بالرمز . $\ker f$

نظرية 3-5

لتكن G', G أي زمرتين e', e هما المحايدان بالتالي . إذا كانت f تمثل هومومورفزم من G إلى G' فإن :

1- $f(e) = e'$.

2- $f(x^{-1}) = f(x)^{-1}$ جزئية

3- نواة الدالة f $\ker f$ تمثل زمرة طبيعية من G .

البرهان

1- بما أن $e \,.\, e = e$ فإن $f(e)f(e) = f(e)$ ، وبما أن $f(e) \in G'$ فإن $f(e)f(e) = e'f(e)$ ، فهذا يؤدي إلى $f(e) = e'$ بواسطة الحذف من اليمين .

2- لكل $x \in G$ ، بسبب $xx^{-1} = e$ سوف نحصل على :

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$$

وبنفس الطريقة $x^{-1} = e$ هذا يعطي $f(x^{-1})f(x) = e'$ ، لذلك . $f(x^{-1}) = f(x)^{-1}$

3- بما أن $f(e) = e'$ $e \in \ker f$ فإن هذا يعني أن $\ker f \neq \phi$ ، لتكن b, a تنتمي إلى $\ker f$, $x \in G$:

$$a \in \ker f, b \in \ker f \ \to \ f(a) = e', f(b) = e'$$
$$\to \ f(a) = e', f(b^{-1}) = f(b)^{-1} = e'$$
$$\to \ f(ab^{-1}) = f(a)f(b)^{-1} = e'e' = e'$$
$$\to \ ab^{-1} \in \ker f$$

وهذا يبرهن أن $\ker f$ يمثل زمرة جزئية من G ، بقي أن نبين بأنها عادية كذلك .

والآن :

$$f(x^{-1}ax) = f(x^{-1}), f(a)f(x) =$$
$$f(x)^{-1}f(a)f(x) =$$
$$f(x)^{-1}e'f(x) =$$
$$f(x)^{-1}f(x) = e'$$

وهذا يؤدي إلى أن $x^{-1}ax \in \ker f$

لذلك فإن $\ker f$ تمثل زمرة جزئية طبيعية من G .

تعريف 3-6 الأيزومورفزم

دالة الهومومورفزم f من الزمرة G إلى الزمرة G' تسمى دالة أيزومورفزم إذا كانت الدالة f 1-1 . من الواضح الآن أن الأيزومورفزم و الهومورفزم يمثلان معاً إيبيمورفزم ومونومورفزم ، وبالإضافة إلى ذلك فإن الأيزومورفزم من الزمرة G إلى نفسها يسمى أيزومورفزم ذاتي للزمرة G (Outomorphism) .

مثال 6

لأي زمرة G فإن دالة المحايد $i : G \to G$ تمثل هومومورفزم ذاتي لأن $i(x) = x \quad \forall x \in G$ ، وواضح جداً أنها 1-1 وشاملة .

بالإضافة إلى ذلك لأي $x, y \in G$ $\quad i(xy) = xy = i(x)i(y)$

ولذلك فإنها تمثل هومومورفزم ذاتي للزمرة G .

مثال 7

لتكن R^+ هي زمرة الضرب للأعداد الصحيحة الموجبة ، سوف نعرف :

$f : R^+ \to R^+$

بواسطة $\forall \quad x \in R^+$ $\quad f(x) = x^2$. الآن لأي $x, y \in R^+ \leftarrow$ فإن :

$f(xy) = (xy)^2 = x^2y^2 = f(x)f(y$

وبالإضافة إلى ذلك ، إذا كان $\quad f(x) = f(y) \to x^2 = y^2 \to x = y$

لأن $x > 0, y > 0$ ، لذلك فإن الدالة f هي 1-1 .

والآن خـذ $x \in R^+$ $\quad \sqrt{x} \in R^+$ لـذلك $f\left(\sqrt{x}\right) = \left(\sqrt{x}\right)^2 = x$ ، وهـذا يـبرهن أن f شاملة . لذلك فإن f تمثل هومومورفزم ذاتي للزمرة R^+ .

مثال 8

لأي عنصر $a \in G$ عرف $f_a : G \to G$ بواسطة :

$$f_a(x) = axa^{-1} \quad \forall \quad x \in G$$

لأي $x, y \in G$ فإن

$$f_a(xy) = axya^{-1}$$
$$= (axa^{-1})(aya^{-1}) = f_a(x)f_a(y)$$
$$f_a(x) = f_a(y) \to axa^{-1} = aya^{-1} \to x = y$$

وبما أن $f_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x$ فإن f شاملة .

لذلك فإن f تمثل هومومورفزم ذاتي للمجموعة G ، بالإضافة إلى ذلك فإن هومومورفزم في مثالي 2 ، 5 فلا يمثلان هومومورفزم ذاتي .

نظرية 3-7

دالـة الهومومـورفزم f مـن الزمـرة G إلى الزمـرة G' تمثـل مونومـورفزم إذا وفقـط إذا $\ker f = \{e\}$.

البرهان

لتكن f دالة هومومورفزم من الزمرة G إلى الزمرة G' . ولنفرض أن f هي 1-1 .

لتكن $x \in \ker f$ فإن $f(x) = e'$ حيث e' هو المحايد للمجموعة G' .

وكذلك $f(e) = e'$ (نظرية 3-5) .

هذا يؤدي إلى $f(x) = f(e) \to x = e$ ، وهذا يبرهن أن $\ker f = \{e\}$ ، وبالعكس لتكن

$\ker f = \{e\}$

ولتكن $x, y \in G$ بحيث أن $f(x) = f(y)$

Then $$\begin{aligned} & f(x)f(y)^{-1} = e' \to f(xy^{-1}) = e' \\ & f(x) = f(y^{-1}) \to f(x)f(y^{-1}) = e' \\ & \to xy^{-1} \in \ker f = \{e\} \\ & \to xy^{-1} = e \to x = y \end{aligned}$$

لذلك فإن f أحادية 1-1 .

تعريف 3-8

يقال للزمرة G بأنها أيزومورفزم الزمرة G' إذا وجد دالة هومومورفزم من G إلى G' ويرمز لها بالرمز $G \cong G'$.

نظرية 3-9

لتكن G_3, G_2, G_1 أية ثلاثة زمر فإن :

(1) $G_1 \cong G_2$ (معاكس) .

(2) $G_1 \cong G_2 \leftarrow G_2 \cong G_1$ (تناظر) .

(3) $G_1 \cong G_3 \leftarrow G_2 \cong G_3, G_1 \cong G_2$ (تعدي) .

البرهان

(1) عـرف الدالـة $i : G_1 \to G_1$ بحيـث أن $\forall \quad x \in G$ $\quad i(x) = x$ وهـي دالـة المحايـد للمجموعـة G_1 وهـي دالـة أيزومـورفزم ذاتي علـى G_1 ، كمـا في (مثـال 6) ، ولذلك $G_1 \cong G_1$.

(2) $G_1 \cong G_1$ هـذا يعني أنه توجد دالة أيزومـورفزم f مـن G_1 إلى G_2 . ولأن f هـي أحاديــة (1-1) وشــاملة فــإن الدالــة : $f^{-1} : G_2 \to G_1$ المعرفــة كمــا يلــي : $f^{-1}(y) = x$. إذا كانــت $f(x) = y$ لأي $y \in G_2$. ســوف تكــون أحاديــة (1-1) وشاملة .

لتكن $y_1, y_2 \in G_2$ ، بما أن f شاملة يمكن إيجاد $x_1, x_2 \in G$ بحيث أن :

$$f(x_2) = y_2, \quad f(x_1) = y_1$$

وهذا يؤدي إلى $f^{-1}(y_2) = x_2, f^{-1}(y_1) = x_1$ ، على كل حال :

$$f(x_1x_2) = f(x_1)f(x_2) = y_1y_2$$

تعطي $$f^{-1}(y_1y_2) = x_1x_2 = f^{-1}(y_1)f^{-1}(y_2)$$

هذا يبرهن أن f^{-1} هومومـورفزم ، ولذلك ستكون f^{-1} دالة أيزومورفزم من G_2 إلى G_1 . وهذا يعني أن $G_2 \cong G_1$.

(3) لتكن $G_2 \cong G_3, G_1 \cong G_2$ هـذا يعني وجـود دالـة أيزومـورفزم f مـن G_1 إلى G_2 . ودالة أيزومورفزم g من G_2 إلى G_3 .

$g \circ f : G_1 \to G_3$ هي أحادية وشاملة أيضاً . ولأن لأن $x, y \in G_1$

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y))$$

لأن $f(x), f(y) \in G_2$

$$= [(g \circ f)(x)][(g \circ f)(y)]$$

وهـذا يـبرهن أن $g \circ f$ هـي دالـة هومومـورفزم ، وهـذا يعـني أن $g \circ f$ هـي دالـة أيزومـورفزم فوقية من G_1 إلى G_3 .

وهذا يعني أن $G_1 \cong G_3$ ، وهذا يبرهن النظرية .

ملاحظات

1- في برهان الجزء الثالث (3) في النظرية أعلاه عندما برهنا أن $g \circ f$ دالة هومومورفزم فلن نحتاج لنبرهن أن g ، f دوال أحادية وشاملة ، وهذا يؤدي إلى أن دالة التركيب (طالما عرفت) لأي دالتين هومومورفزميتين تكون هومومورفزمية .

2- النظرية أعلاه تقرر أننا إذا أخذنا عائلة من المجموعات ، فإن علاقة الأيزومورفزم سوف تكون علاقة تكافؤية بين هذه العائلة ، لذلك إذا كانت المجموعة G_1 أيزومورفزم المجموعة G_2 فمن السهل أن نقول أن G_2, G_1 أيزومورفزميتان عندما تكون مجموعتان أيزومورفزميتان فإن عالم الجبل يمكن أن يقول أنهما متساويان جوهرياً والسبب يعود للأسباب الآتية :

عالم الجبل يهتم بدراسة التركيبات الثنائية على المجموعة وليس على الجوهر الطبيعي لعناصر تلك المجموعة .

ولذلك إذا كانت $G_1 \cong G_2$ وكانت f واقعة تحت الأيزومورفزم من G_1 إلى G_2 فهذا يؤدي إلى أن لأي : $x, y \in G \to xy = z$ ، $f(x)f(y) = f(z) \to$

وهذا يعني أن f معرفة على معرفة على x وعلى y .

ولذلك فإن $f(x)f(y)$ سوف تكون مساوية لـ $f(xy)$ المعرفة على G_2 كما أن xy معرفة على G_1 .

وبناء عليه فإن التركيب الثنائي من G_2 معرفة بشكل كامل إذا كان التركيب الثنائي في G_1 والدالة f دالة معرفة . وبنفس الطريقة يمكن تعريف التركيب الثنائي على G_2 ودالة g من G_2 إلى G_1 وتكون أيزومورفزم ، وعندئذ يكون التركيب الثنائي على G_1 معرف تعريفاً

كاملاً ، ومن هذا فإن جميع الخصائص من واحدة من الزمر G_2, G_1 سوف يعتمد فقط على التركيب الثنائي المعرف . لذلك فجميع الخصائص من الأخريات تعتمد على ذلك التركيب الثنائي أيضاً .

لهذه الأسباب فإن عالم الجبر يعتبر أي مجموعتين أيزومورفزميتين متطابقتان .

نظرية 3-10 (نظرية الهومومورفزم)

لتكن G أي زمرة إذا كانت N زمرة جزئية عادية من G فإن G/N سوف تكون هومومورفزم صوري إلى G ، وبالعكس إذا كانت أي زمرة G' تمثل هومومورفزم لـ G فإن G' سوف تكون أيزومورفيك لزمرة قسمة من G . في الحقيقة إذا كانت f دالة هومومورفزم من G إلى G' فإن $G' \cong G/\ker f$

البرهان

نعرف الدالة $f : G \to G/N$ بواسطة $\forall \ a \in G$ $f(a) = Na$ ، ويسبب

$$f(ab) = Nab = (Na)(Nb)$$
$$= f(a)f(b) \qquad \forall \ a, b \in G$$
$$f(c) = Nc, \quad Nc \in G/N$$

سنرى أن f هي دالة هومومورفزمية من G إلى G/N ، وبالعكس لتكن G' تمثل هومومورفزم صوري للمجموعة G ، فهذا يعني وجود دالة هومومورفزم g من G إلى G' .

لتكن $N = \ker g$ نحن نعلم أن N هي زمرة جزئية عادية من G . (نظرية 3-5) واعتبر أن زمرة القسمة G/N .

نعرف $f : G/N \to G'$ بواسطة $\forall \ a \in G$ $f(Na) = g(a)$ أولاً سوف نبين أن f معرفة تعريفاً جيداً .

لتكن $a_1, a_2 \in G$ أنه $Na_1 = Na_2$

$$\rightarrow \quad a_1 a_2^{-1} \in N \rightarrow g(a_1 a_2^{-1}) = e'$$

حيث e' هو العنصر المحايد للمجموعة G' .

$$\rightarrow \quad g(a_1)g(a_2)^{-1} = e' \rightarrow g(a_1) = g(a_2)$$
$$\rightarrow \quad f(Na_1) = f(Na_2)$$

وهذا يبين أن f معرف تعريفاً جيداً .

والآن لأي $Na, Nb \in G / N$

$$f[[Na](Nb)] = f(Nab) = g(ab)$$
$$= g(a)g(b) = f(Na)f(Nb)$$

وهذا يبين أن f دالة شاملة .

بالإضافة إلى ذلك

$$f(Na) = f(Nb) \rightarrow g(a) = g(b)$$
$$\rightarrow \quad g(a)g(b)^{-1} = e' \rightarrow g(ab^{-1}) = e'$$
$$\rightarrow \quad ab^{-1} \in \ker g = N \rightarrow Na = Nb$$

وهذا يبين أن f هي دالة أحادية (1-1) .

وأخيراً لتكن $x \in G'$ ، بما أن g دالة شاملة إذن يوجد $a \in G$ بحيث أن $g(a) = x$ ← $f(Na) = g(a) = x$ ، وهذا يبرهن أن f هي دالة شاملة أيضاً .

إذن f سوف تكون دالة أيزومورفزم من G / N إلى G' وهذا يعني $G / N \cong G'$.

وهذا يبرهن النظرية .

تعريف 3-11 (الهومومورفزم الطبيعي)

لتكن N زمرة جزئية عادية من الزمرة G ، فإن الدالة :

$f : G \rightarrow G / N$ معرفة بواسطة $\forall \ x \in G \quad f(x) = Nx$ تدعى الهومومورفزم الطبيعي (أو القانوني) من G إلى G / N .

نظرية 3-12 (النظرية الأولى للأيزومورفزم)

لتكن f دالة هومومورفزم من الدالة G إلى الزمرة G' و $H = \ker f$ ، K' أي زمرة جزئية عادية من G' .

و
$$K = \{x \in G \mid f(x) \in K'\} = f^{-1}(K')$$

فإن K هي زمرة جزئية عادية من G و $G / K \cong G' / K'$.

البرهان

عرف الدالة $g : G \to G' / K'$ بواسطة $g(x) = K'f(x) \quad \forall\ x \in G$

لتكن $a, b \in G$ فإن $g(ab) = K'f(ab) = K'f(a)f(b)$

(لأن f هي دالة هومومورفزم) .

ولذلك $g(ab) = [K'f(a)][K'f(b)] = g(a) . g(b)$

وهذا يبين أن g دالة هومومورفزم .

بالإضافة إلى ذلك لتكن $K'a' \in G' / K', a' \in G'$ بما أن f هي دالة شاملة إذن يوجد $a \in G$ بحيث أن $f(a) = a'$ فإن $g(a) = K'f(a) = K'a'$.

لذلك g تكون هومومورفزم من G إلى G' / K' ، وبواسطة النظرية الأساسية للهومومورفزم .

$$G / \ker g \cong G' / K'$$

إذا بينا أن $\ker g = K$ فإن ذلك سيتبعه أن K هي زمرة جزئية طبيعية من G . $G / K \cong G' / K'$.

والآن لو كانت K' هي المحايد للمجموعة G' / K'

$$x \in \ker g \leftrightarrow g(x) = K'$$
$$\Leftrightarrow K'f(x) = K' \Leftrightarrow f(x) \in K'$$
$$\Leftrightarrow x \in K$$

(بواسطة تعريف K) و

وهذا يعني أن : $x \in \ker g \Leftrightarrow x \in K$

يعني أن $\ker g = K$

وهذا يبرهن النظرية .

نظرية 3-13 (نظرية فريثمان)

لتكن H و K زمر جزئية طبيعية من G بحيث أن $H \subseteq K$ فإن K / H زمرة جزئية عادية من G / H و $\dfrac{G / H}{K / H} \cong G / K$.

البرهان

سوف نأخذ القارئي للتأكد من أن K / H زمرة جزئية طبيعية من G / H .
بالإضافة إلى ذلك $f : G \to G / H$ تعرف بواسطة $f(x) = Hx$ والتي تمثل هومومورفزم طبيعي من G إلى G / H بحيث أن :

$$K = f^{-1}(K / H) = \{x \in G \mid Hx \in K / H\}$$

(بواسطة النظرية أعلاه) $$G / K \cong \frac{G / H}{K / H}$$

نظرية 3-14 (النظرية الثانية للأيزومورفزم)

لتكن K, H هي زمر جزئية عادية من G بحيث أن H هي جزئية طبيعية من G ، فإن $H \cap K$ تمثل زمرة جزئية طبيعية من g, k $K /(H \cap K) \cong HK / H$.

البرهان

بسبب أن H هي زمرة جزئية عادية من G و $HK = KH$ ، حيث HK هي زمرة جزئية من G .

بالإضافة إلى ذلك $H = He \subseteq HK$

وهذا يعطي أن H هي زمرة جزئية عادية من HK .

وهذا يؤدي إلى أن HK / H معرفة .

ولنعرف الآن الدالة f حيث $f : K \to HK / H$ بواسطة $f(K) = HK$.

f دالـة هومومـورفزم ، ولتعتبر أن أي $Ha \in HK / H, a \in HK$ والآن $a \in HK$ تعطـي أن $a = hk$ لبعض $h \in H$ ، $k \in K$ أي أنه :

$$Ha = (Hh)k = Hk = f(k)$$

هـذا يبـني أن f دالـة شـاملة ، وبواسـطة النظريـة الأساسـية للهومومـورفزم نحصـل علـى $k / \ker f \cong Hk / H$ ، وإذا استطعنا تكوين أن $\ker f = H \cap K$ فإننا سنحصل على أن $H \cap K$ زمرة جزئية عادية من K و $K /(H \cap K) \cong HK / H$.

والآن H تمثل المحايد إلى HK . لذلك فإن أي عنصر $k \in K$:

$$k \in \ker f \leftrightarrow f(k) = H$$

لأن $k \in K$ $\quad \Leftrightarrow Hk = H \Leftrightarrow k \in H \Leftrightarrow k \in H \cap K$

أي أنـه $k \in \ker f \Leftrightarrow k \in H \cap K$ وهـذا يؤدي إلى أن $\ker f = H \cap K$. لـذلك يتبـع ما يلي :

نظرية 3-14 (a) (نظرية التقابل)

لتكن N زمرة جزئية من الزمرة G . يوجد تقابل أحادي 1-1 بين الزمر الجزئية من G التي تحتوي N والزمرة الجزئية لـ G / N .

وهذا التقابل يعطي كذلك 1-1 بين الزمرة الجزئية العادية من G التي تحتوي N والزمر الجزئية في G / N .

البرهان

ليكن f هومومورفزم فوقي G إلى G / N لتكن H زمرة جزئية من G تحتوي N .

فإن $$f(H) = \{f(h) / h \in H\} = \{hN / h \in H\} = H / N$$

تمثل زمرة جزئية من G / N (لماذا ؟) .

ولنعتبر أن أي زمرتين جزئيتين (K, H) من G تحتوي على N بحيث أن $f(H) = f(K)$ وهذا يعني $H / N = K / N$. وهذا يؤدي إلى أن :

$$k^{-1}h \in N \subseteq k \to h = k(k^{-1}h) \in K$$

ولذلك $H \subseteq K$.

وبنفس الطريقة يمكننا إثبات أن $K \subseteq H$ ، وهذا يعني أن $H = K$ ، ولذلك يمكننا ملاحظة أن الدالة من H إلى $f(H)$ سوف تكون أحادية 1-1 .

لتكن X أي زمرة جزئية من G / N .

ضع $$Y = \{x \in G / f(x) \in X\}$$

بما أنه لأي $f(n) = N \in X, h \in N$ (N هو المحايد للمجموعة G / N) لذلك $n \in Y$. $N \subseteq Y$.

وكذلك إذا كانت $$t \in X \subseteq G / N$$

$t = gN = f(g)$ لذلك $g \in y$.

وبهذه الطريقة نرى أن أي عنصر من X سوف يكون من النوع $f(y)$ مع $y \in Y$.

والآن سوف نبين أن Y هي زمرة جزئية من G .

من الواضح أن Y مجموعة غير خالية (لأن $N \subseteq Y$) .

إذا كانت $y_1, y_2 \in Y$ فهذا يؤدي إلى أن $f(y_1) \in X$.

$$\begin{aligned}
&f(y_2) \in X \to f(y_1)[f(y_2)]^{-1} \in X \\
&\to f(y_1)f(y_2^{-1}) \in X \to f(y_1y_2^{-1}) \in X \\
&\to y_1y_2^{-1} \in Y
\end{aligned}$$

لذلك فإن Y تمثل زمرة جزئية من G وتحتوي على N . وبما أن $f(Y) = X$ فإننا سنحصل على أن الدالة من $H \to f(H)$ هي دالة أحادية .

وأخيراً لتكن H زمرة جزئية عادية من G وتحتوي على N ولنعتبر $f(H)$.

لتكن $gN \in G/N, hN \in f(H)$ فإن :

$$gNhN(gN)^{-1} = (ghg^{-1})N \in f(H), gHg^{-1} \in H$$

من هذا الطريق $f(H)$ هي زمرة جزئية عادية من G .

لتكن K زمرة جزئية عادية من G/N ، ضع $L = \{x \in G \mid f(x) \in K\}$ ، وبهذا نستطيع أن نرى مما سبق أن $N \subseteq L, k = f(L)$ و L هي زمرة جزئية من G .

لتكن $g \in G$ و $x \in L$ فإن $f(xgx^{-1}) = f(g)f(x)f(g)^{-1} \in K$

حيث $f(g) \in G/N$ ، $f(x) \in N$ و K زمرة جزئية عادية من G/N . وهذا يؤدي إلى أن $g \times g^{-1} \in L$ وهذا يبرهن أن L زمرة جزئية عادية من G/N وتحتوي على N .

تمارين عملية

تمرين 1

لأي $a, b \in R$ و $a \neq 0$ عـــرف $f : R \to R$ بواســـطة $f_{ab}(x) = ax + b$ ، ولتكن :

$$N = \{f_{1b} \in G\}, G = \{f_{ab} \mid a, b \in R, a \neq 0\}$$

برهن أن N تمثل زمرة جزئية عادية من G ولأن $G/N \cong$ للزمرة غير الصفرية من الأعداد الحقيقية تحت عملية الضرب .

الحل

$f_{10}(x) = x$ هذا يبين أن الدالة المحايدة $i_R \in G$ لذلك فإن G ليست خالية .

لتكن $a, b, c, d \in R$ مع $c \neq 0, a \neq 0$ وهذا يؤدي :

$$f_{ab}[f_{cd}(x)] = f_{ab}(cx + d) = a(cx + d) + b = acx + ad + b$$

$ac \neq 0 \to a \neq 0, c \neq 0$ حين $f_{ac}, ad + b \to$ وهذا يؤدي إلى أن :

$$f_{ab}f_{cd} = f_{ac,ad+b} \qquad (1)$$

c مع المساعدة من (1) يمكننا برهنة أن G هي زمرة مع وهي تعمل على المحايد و :

$$f(ab)^{-1} = f_{a^{-1},-a^{-1}b}$$

من الواضح أن $f_{10} \in N$ ، لذلك N غير خالية .

بالإضافة إلى ذلك $f_{1b}, f_{1d} \in N$ وهذا يؤدي إلى :

$$f_{1b}(f_{1d})^{-1} = f_{1b}f_{1d} = f_1,-d + b \in N$$

لذلك فإن N زمرة جزئية من G ، ومرة أخرى إذا كانت $f_{1c} \in N, f_{ab} \in G$ لذلك :

$$f_{ab}f_{1c}(f_{ab})^{-1} = f_{a,ac+b}f_{a^{-1},-a^{-1}b} = f_1, ac \in N$$

لذلك N تمثل زمرة جزئية عادية من G .

وأخيراً لتكن K زمرة غير صفرية من الأعداد الحقيقية تحت عملية الضرب عرف $\theta : G \to K$ بواسطة $\theta(f_{ab}) = a$ لكل $f_{ab} \in G$ من الواضح أن θ هي شاملة . والآن :

$$\theta(f_{ab}f_{cd}) = \theta(f_{ac,ad+b}) = ac = \theta(f_{ab})\theta(f_{cd})$$

وهذا يؤدي إلى أن θ هي هومومورفزم .

المحايد للمجموعة $K =$

$$\begin{aligned} f_{ab} \in \ker\theta &\leftrightarrow \theta(f_{ab}) \\ &\leftrightarrow a = 1 \\ &\leftrightarrow f_{ab} = f_{1b} \leftrightarrow f_{ab} \in N \end{aligned}$$

لذلك $\ker\theta = N$.

وبواسطة النظرية الأساسية للهومومورفزم $H\ G/N \cong K$.

تمرين 2

إذا كانت G زمرة بحيث أن $G/Z(G)$ دوارة عندما تمثل $Z(G)$ مركز G بين أن G تبديلية .

الحل

ضع $N = Z(G)$ و $G / N < gN >$ لبعض $g \in G$.

لتكن $a, b \in G$ فإن $aN = (gN)^K = g^K N$ و $bN = (gN)^{-1} = g^{-1}N$ لبعض $K, L \in Z$ وهذا يؤدي إلى $n_1, n_2 \in N$ و $a = g^K n_1, b = g^1 n_2$ وهذا يؤدي إلى $ba = g^{L+K} n_1 n_2, ab = g^{K+L} n_1 n_2$ حيث $n_1, n_2 \in N$ $= ZG$

لذلك $ab = ba$.

تمرين 3

إذا كانت R^* زمرة غير صفرية من الأعداد الحقيقية تحت عملية الضرب . وهذا يبين أن $(R^*, .)$ ليس أيزومورفزم مع $(R, +)$.

الحل

$R^* \in 1-$ هي من الرتبة 2 فإذا كان دائماً $(R, +) \cong (R^*, .)$ مثلاً تحت الأيزومورفيزم f عندئذ $f(-1)$ يجب أن تكون من الرتبة 2 (لماذا ؟) .

ولكن $a \in R, na = 0$ ← $n = 0$ أو $a = 0$ ، لذلك لا توجد عناصر من الرتبة 2 في $(R, +)$ لذلك $(R^*, .)$ ليس أيزومورفزم مع $(R, +)$.

تمرين 4

N زمرة جزئية عادية من G . بين أن G / N إبدالية إذا وفقط إذا كانت لكل $x, y \in G$ ، $xyx^{-1}y^{-1} \in N$.

الحل

في حالة $xyx^{-1}y^{-1} \in N$ لكل $x, y \in G$:

$$xyx^{-1}y^{-1}N = N \rightarrow xNy \;\; N(xN)^{-1}(yN)^{-1} = N$$

$xNyN = yNxN \rightarrow G/N$ إبدالية

وبالعكس لتكن G/N إبدالية ، لذلك لأي $x, y \in G$:

$$xNyN(xN)^{-1}(yN)^{-1} = (xN)\,(xN)^{-1}(yN)\,(yN)^{-1} = NN = N$$

والآن :

$$xyx^{-1}y^{-1}N = xNyNx^{-1}Ny^{-1}N = xNyN(xN)^{-1}(yN)^{-1} = N$$

$$\rightarrow \quad xyx^{-1}y^{-1} \in N$$

تمرين 5

إذا كانت H زمرة جزئية من G بين أن W = تقاطع كل gHg^{-1} ، تمثل زمرة جزئية من G .

الحل

بواسطة الفرض $W = \bigcap_{g \in G} gHg^{-1}$

وبسبب أن كل gHg^{-1} زمرة جزئية من G و W زمرة جزئية من G .

$$w \in W \rightarrow w \in gHg^{-1} \quad \forall\, g \in G \rightarrow g^{-1}Wg \in H \quad \forall\, g \in G$$

لتكن $x \in G$ فإن :

$$xwx^{-1} = xg\,(g^{-1}wg)g^{-1}x^{-1} \in xgH(xg)^{-1} \quad \forall\, g \in G$$

والآن لأي عنصر t في G نستطيع أن نكتبه $xx^{-1}t = xg$ ، عندما $g = -x^{-1}t \in G$ ولذلك :

$$xwx^{-1} \in tHt^{-1} \quad \forall\, t \in G \rightarrow xwx^{-1} \in W$$

لذلك W زمرة جزئية عادية من G .

مسائل

1- إذا كانت f هومومورفزم من الزمرة G إلى G' ، برهن أن $G / \ker(f) \cong f(G)$.

2- لأي دالة هومومورفزمية $f : G \to H$ برهن أنه ، إذا كانت $x \in G$ لها رتبة منتهية فإن $\circ(f(x)) / \circ(x)$ تتضمن أن f (مونومورفزم) (أحادية التشاكل) (1-1) ، إذا وفقط إذا :

$$\circ(x) = [\circ(f(x))] \quad \forall x \in G$$

3- و4- صنف الدوال المعطية الآتية إلى فئات :

(i) ليست شاملية الهومورفزم (أندو) .

(ii) شاملة الهومورفزم لكنها ليست ذاتية الهومومورفزم (أتومور) .

(iii) أيزومورفززم ولكنها ليست أوتومورفزم .

(iv) أوتومورفزم .

(v) مونومورفزم لكنها ليست أيزومورفزم .

لتكن Z زمرة الجمع للأعداد الصحيحة :

(a) $f_1(x) = -x \quad \forall x \in Z, f_1 : Z \to Z$

(b) $f_2(x) = | x | \quad \forall x \in Z, f_2 : Z \to Z$

I $f_3(x) = x + 2 \quad \forall x \in Z, f_3 : Z \to Z$

(d) $f_4(x) = -3x \quad \forall x \in Z, f_4 : Z \to Z$

لتكن C^* زمرة الضرب لأي عدد مركب غير صفري :

(e) $g_1(x) = x^4 \quad \forall x \in C^*; g_1 : C^* \to C^*$

(f) $g_2(x) = \overline{x} \quad \forall x \in C^*; g_2 : C^* \to C^*$

(g) $g_3(x) = | x | \quad \forall x \in C^*; g_3 : C^* \to C^*$

(h) $g_4(x) = -x \quad \forall x \in C^*; g_4 : C^* \to C^*$

لتكن G أي زمرة إبدالية من الرتبة 8 :

(i) $h_1 : G \to G$; $h_1(x) = x^4 \quad \forall x \in G$

(j) $h_2 : G \to G$; $h_2(x) = x^3 \quad \forall x \in G$

(k) $h_3 : G \to G$; $h_3(x) = x^{-1} \quad \forall x \in G$

5- برهن أن الزمرة G إبدالية إذا وفقط إذا كانت الدالة $f : G \to G$ التي تعطى بما يلي $f(x) = x^{-1}$ تمثل أوتومورفزم في G .

6- لتكن G تمثل زمرة إبدالية و n عدد صحيح موجب ، نعرف $f : G \to G$ بواسطة $f(x) = x^n \quad \forall x \in G$ ، بين أن f هي (إندومورفزم) من G . إذا كانت G منتهية بحيث أن n و $\circ(G)$ هما أوليان نسبياً ، بين أن f هي أوتومورفزم في G .

7- لتكن $f : G \to G$ هي دالة هوموموفزمية ، برهن ما يلي :

(i) لأي زمرة جزئية H من G ، $f(H)$ هي زمرة جزئية من G' .

(ii) لأي زمرة جزئية K' من G' ، $f^{-1}(K')$ هي زمرة جزئية من G ، وتحوي $\ker f$ و $f^{-1}(K')$ هي زمرة جزئية عادية من G عندما K' هي زمرة جزئية عادية في G' .

(iii) إذا كانت f دالة شاملة فإن لأي زمرة جزئية عادية K من G ، $f(K)$ زمرة جزئية عادية من G' .

(iv) إذا كانت f شاملة و K زمرة جزئية من G تحتوي على $\ker f$ (نواة f) فإن $f^{-1}[f(K)] = K$ ويتضمن ذلك أنه توجد رابطة واحد لواحد بين الزمر الجزئية من G التي تحتوي على $\ker f = H$ وزمرة جزئية من G . هذه الرابطة (المراسلة) تعطي أيضاً واحد لواحد (1-1) من الروابط

بين الزمر الجزئية العادية من G والتي تحتوي على $\ker f$ والزمر الجزئية العادية من G' .

8- برهن بأن صور الهومومورفزم من الزمر الدائرية الإبدالية تكون إبدالية . أعط مثالاً وبين بأن صور الهومومورفزم للزمر الإبدالية الدائرية سوف لا يضمن أن تكون زمرة بنفسها .

9- برهن بأنه إذا كانت للزمرة G دالة بحيث أن $f : G \to G$ والتي تعطى بما يلي $f(x) = x^3 \quad \forall x \in G$ دالة أيزومورفزم فإن G زمرة إبدالية .

10- نستعرض الزمر غير الإبدالية G حيث أن الدالة $f : G \to G$ المعرفة بما يلي $f(x) = x^4$ تمثل أوتومورفزم .

11- N زمرة جزئية عادية ذات دليل منتهي في الزمرة G و H زمرة جزئية ذات رتبه منتهية . إذا كانت $[G : N]$ إذا كانت أولية نسبياً إلى $\circ(H)$ فبين أنه $H \subseteq N$.

12- N هي زمرة جزئية منتهية من الزمرة H, G زمرة جزئية ذات دليل منته في G . إذا كانت $[G : H]$ أولية نسبياً إلى $\circ(N)$ فبين أن $H \subseteq N$.

13- إذا كانت H تمثل زمرة جزئية من الزمرة G ، بحيث أن $x^2 \in H$ لأي $x \in G$ ، برهن بأن G / H إبدالية .

14- لتكن f, H, G زمرة ، العلاقة $G \times H$ بحيث أن $\operatorname{dom} f = G$ ، بالإضافة إلى أن f تحقق الشروط الآتية :

(i) $(x, a) \in f, (y, b) \in f \to (xy^{-1}, ab^{-1}) \in f$

(ii) إذا كانت e', e يمثلان المحايدان إلى H, G بالتتالي ، فإن :

$$(e, a) \in f \to a = e'$$

برهن بأن f تمثل هومومورفزم من G إلى H .

[ملاحظة : برهن أن $(x, a) \in f, (x, c) \in f \to a = c$] .

15- لتكن G_i تمثل زمرة لكل $i = 1, 2, \ldots, n$

عرف $\pi G_i = G_1 \times G_2 x \ldots x\, Gn$

بين أن πG_i تمثل زمرة تحت التركيب

$$(a_1, a_2, \ldots, a_n)\,(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

إذا كانت H_i تمثل زمرة جزئية عادية من G_i لكل $i = 1, 2, \ldots, n$ برهن بأن :

$$\frac{\pi G_i}{\pi H_i} \cong \pi \frac{(G_i)}{H_i}$$

2- زمر التباديل

لتكن S مجموعة ولتكن $A(S)$ إلى مجموعة كل التباديل إلى S ، يجب أن نبرهن مبكراً أن $A(S)$ زمرة .

إذا كانت H أي مجموعة غير فارغة من $A(S)$ بحيث أن H مغلقة تحت التركيب في $A(S)$ ولأي عنصر في H ، فإن المعكوس لهذا العنصر موجود في H أيضاً . لذلك فإن H تمثل زمرة جزئية من $A(S)$.

ومن ناحية أخرى نستطيع أن نقول أنه إذا كانت H تمثل مجموعة التباديل من المجموعة S بحيث أن H مغلقة تحت نتائج التركيب ومعكوس جميع عناصر H هو أعضاء في H . فإن H تمثل زمرة مع عملية نتائج التركيب .

أي زمرة من هذه الزمر تسمى زمرة التحويل أو زمر التباديل ، هذه الزمر ذات أهمية عظيمة لأننا سنبين أن نظرية كايلي (التي ذكرت) لأي زمرة ممكن وصفها بواسطة زمرة التباديل وبالإضافة إلى ذلك فإن هذه الزمر ذات مصادر غنية للأنواع المختلفة من الأمثلة وكذلك الأمثلة المعاكسة للزمر ذات الخصائص المتنوعة .

وبشكل رئيسي ومحدود حالياً سنتعامل مع الزمر الإبدالية على المجموعات المنتهية لتكن S مجموعة منتهية تحتوي على n من العناصر ولتكن $f \in A(S)$ سنرمز إلى f بواسطة الرمز الآتي :

$$\begin{pmatrix} a_1 a_2, \ldots, a_n \\ b_1 b_2, \ldots, b_n \end{pmatrix}$$

في الصف الأول $a_1, a_2, \ldots a_n$ هي n من العناصر في S .

في الصف الثاني $b_1, b_2, \ldots b_n$ تمثل صور a_i تحت الدالة f .

وبصورة رئيسية فإن رتبة عناصر S وضعت في الصف الأول ، هذا الرمز يعرف برمز الصفين لـ f .

مثال 9

لتكن $S = \{a_1, a_2, a_3, a_4\}$ ، عرف $f : S \to S$ بواسطة التعريف الآتي :

$$f(a_1) = a_2, f(a_2) = a_3, f(a_3) = a_1, f(a_4) = a_4$$

والآن نستطيع كتابة الدالة كما يلي :

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_1 & a_4 \end{pmatrix} = \begin{pmatrix} a_1 & a_3 & a_4 & a_2 \\ a_2 & a_1 & a_4 & a_3 \end{pmatrix} =$$

$$\begin{pmatrix} a_2 & a_3 & a_1 & a_4 \\ a_3 & a_1 & a_2 & a_4 \end{pmatrix}$$

هنا نلاحظ أننا كتبنا الدالة f بثلاثة طرق فقط ، ونستطيع كتابة الدالة f بعدة طرق وهي $4! = 24$ طريقة . ولنعود إلى المناقشة العامة .

لتكن عناصر S وضعت لبعض الرتب المعرفة ولنقل $a_1, a_2, \ldots, a_n$ ، الآن $b_i = f(a_i)$ ولأن b_i هي واحدة من $a_1, a_2, \ldots, a_n$ فإن $b_i = a_{ki}$ لبعض الأعداد الصحيحة k_i المحصورة بين 1 و n ولأن $b_1, \ldots b_n$ جميعها أعداد مختلفة $k_n, \ldots, k_1$ هي كل الأعداد من 1 إلى n لبعض الرتب ، لذلك :

$$\begin{pmatrix} 1 & 2 & 3\ldots & n \\ k_1 & k_2 & k_3\ldots & k_n \end{pmatrix}$$

هي تبديل إلى $\{1, 2, 3, \ldots, n\}$ ، هذا التبديل يحسب بصورة طبيعية بواسطة f وبالعكس تعطي التبديل كما يلي

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}$$

إلى $\{1, 2, 3, \ldots, n\}$ ، وسنحصل على التبديل

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_{k_1} & a_{k_2} & \ldots & a_{k_n} \end{pmatrix}$$

في S ، تقريباً يكون هذا التبديل f في S وحيداً ويحسب بواسطة التبديل في $\{1, 2, 3, \ldots, n\}$ والرمز a لا يلعب أي دور في حساب f .

ولذلك يمكن كتابة

$$f = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_{k_1} & a_{k_2} & \ldots & a_{k_n} \end{pmatrix}$$

وللسهولة نكتبها كما يلي

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}$$

بالإضافة إلى ذلك سوف نأخذ $S = \{1, 2, \ldots, n\}$.

مثال 10

لتكن f, S هي نفسها في المثال 9 ، فإن

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

قضية 15.3

لتكن f هي تبديل للمجوعة S نعرف العلاقة $\sim$ على S كما يلي :

لأي $a, b \in S$ ، $a \sim b$ إذا وفقط إذا $f^n(a) = b$ لبعض الأعداد الصحيحة n . هذه العلاقة هي علاقة تكافؤ .

البرهان

ليكن $a, b, c \in S$

1- الانعكاس ، بما أن $f^0(a) = I(a) = a$ إذن $a \sim a$ هنا I هي التبديل المحايد للمجموعة S .

2- التناظر $a \sim b \leftarrow f^n(a) = b$ لبعض العدد الصحيح $n \leftarrow f^{-n}(a) = b$ $\leftarrow b \sim a$.

3- التعدي $b \sim c, a \sim b \leftarrow f^n(a) = b$ لبعض n عدد صحيح $f^m(b) = c$ لبعض m عدد صحيح

$$\begin{aligned} \rightarrow f^{n+m}(a) &= (f^m \circ f^n)(a) = f^m(f^n(a)) \\ &= f^m(b) = c \rightarrow a \sim c \end{aligned}$$

هذا يبرهن أن العلاقة $\sim$ هي علاقة تكافؤ على S .

والعلاقة $\sim$ تقسم S إلى صفوف تكافؤ منفصلة وكل صف تكافؤ يحسب بواسطة العلاقة $\sim$ يسمى المدار إلى f .

قضية 16.3

إذا كانت S مجموعة منتهية ، $f \in A(S)$ و $s \in S$ فإنه يوجد عدد صحيح موجب k بحيث أن مدار f إلى S ينتمي إلى $\{s, f(s), f^2(s), \ldots, f^{k-1}(s)\}$.

البرهان

بما أن S منتهية ، $A(S)$ لها رتبة منتهية ، لذلك $\circ(f)$ منتهية . ولتكن $\circ(f) = m$ فإنه $f^m = I \leftarrow f^m(s) = I(s) = s$.

ليكن k هو أصغر عدد صحيح موجب بحيث أن $f^k(s) = s$ فإننا ندعي بأن $s = f^0(s), f(s), f^2(s), \ldots, f^{k-1}(s)$ جميعها مختلفة ، وتحققان :

$$0 \leq l_1 \leq l_2 \leq k-1$$

بحيث أن $f^{L_1}(s) = f^{L_2}(s)$ إذن :

$$f^{l_2 - l_1}(s) = s, 0 < l_2 - l_1 < k$$

وهذا يناقض كون k هي أصغر ما يمكن . لذلك فإن جميع مزاعمنا صحيحة .

والآن إذا كان أي عنصر s' يمثل مدار بالنسبة إلى s فإن $s' = f^l(s)$ لبعض الأعداد الصحيحة l . ولكن $l = kq + r$ لبعض الأعداد الصحيحة r, q بحيث أن :

$$0 \le r \le k - 1$$

فإن $f^r(s) = f^r\left|(f^k)^q(s)\right| = s' = f^l(s)$ وبما أن $f^k(s) = s$ فهذا يؤدي إلى : $f^{kq}(s) = s$ (لماذا؟) .

بالإضافة إلى ذلك وحيث أن $0 \le r \le k - 1$ و $f^r(s)$ هي عناصر المجموعة $s, f(s), f^2(s), \ldots, f^{k-1}(s)$ ، لذلك $s, f(s), \ldots, f^{k-1}(s)$ هي العناصر الوحيدة المختلفة في المدار المنتهي إلى s . وهذا يبرهن القضية .

تعريف 3-17 (التباديل الدائرية)

لتكن S مجموعة منتهية . التبديل f في S يسمى تبديل دوارة إذا وجدت عناصر $i_1, i_2, \ldots, i_i$ في S . بحيث أن :

$$f(i_1) = i_2, f(i_2) = i_3, \ldots, f(i_i) = i_1$$

ولأي $j \in S$ ويختلف عن $i_1, i_2, \ldots, i_i$ فإن $f(j) = j$ ، وسنرمز إلى التبديل f بالرمز $(i_1, i_2, \ldots, i_i)$. هذا الاصطلاح f يسمى اصطلاح الصف الواحد ، بالإضافة إلى ذلك t تسمى طول الزمرة f .

الدورة ذات الطول t تدعى أيضاً الدورة $- t$.

ملاحظة

يمكننا أن نقول أن التبديلة f للمجموعة S (تقريبياً) تكون دائرية إذا كانت f تمتلك على الأقل مداراً واحداً يحتوي على أكثر من عنصر (برهن) .

مثال 11

لتكن $S = \{1, 2, 3, 4\}$ فإن $(1\,3\,2)$ يرمز للتديل f على S بحيث أن $f(1) = 3$ ، $f(3) = 2$ ، $f(2) = 1$ ، $f(4) = 4$ وفي الترقيم ذو الصفين فإن :

$$(1\,3\,2) = f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

f تبديلاً دورارة ذاتطول 3 ، وملاحظة أخرى أنه $(1\,3\,2) = (2\,1\,3) = (3\,2\,1)$

وبنفس الطريقة $(2\ 1)$ يمثل تديلاً دواراً من المجموعة $\{1, 2, 3, 4\}$ ذات طول 2 .

$$(1\,2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

مثال 12

لتكن $S = \{1, 2, 3, 4\}$ ولتكن $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$

سنحسب مدار f ، نلاحظ أن $f(1) = 2$ ، $f(2) = 1$ بواسطة البديهية (3-16) فإننا نرى أن $\{1, 2\}$ هي مدار f ومرة أخرى . $f(3) = 4$ ، $f(4) = 3$ لذلك $\{3, 4\}$ هي مدار إلى f أيضاً . وبما أن $f(5) = 5$ إذن $\{5\}$ تمثل مدار لنفسها .

1- المدار للتبديل الآتي :

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 5 \end{pmatrix}$ هو $\{4, 4\}, \{1, 2, 3\}$

2- إن المدار الوحيد للتبديل :

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$ هو المجموعة S نفسها

تعريف 3-18 (تبديل المواضع)

الدورة ذات الطول 2 تدعى بإبدال الموضع .

تعريف 3-19 (التباديل المنفصلة)

التبديلين g, f للمجموعة S يقال عنهما منفصلين إذا تحققت ما يلي :

-1 لأي $j \in S \quad f(j) \neq j \leftarrow g(j) = j$

-2 لأي $j \in S \quad g(j) \neq j \leftarrow f(j) = j$

وهذا يعني أنه إذا أي عنصر في S تحرك بواسطة f فإنه سيكون ثابتاً بواسطة g وإذا أي عنصر في S تحرك بواسطة g فإنه سيكون ثابتاً بواسطة f .

ملاحظة

أي تبديلين منفصلين f ، g يكونان إبداليان ومن أجل ذلك .

ليكن $x \in S$ ، ولنفرض أن $f(x) \neq x$ فهذا يؤدي أن $g(x) = x$ والآن إذا كانت $y = f(x)$ فإننا سنرى أن $f(y) = f\{f(x)\} \neq y$

ومن ناحية أخرى $x = f(x)$ لذلك $g(y) = y$

لذلك $(g \circ f)(x) = g\{f(x)\} = g(y) = y$

وكذلك $(f \circ g)(x) = f\{g(x)\} = f(x) = y$

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

والآن ليكن $f(x) = x$ فإنه سيكون هنالك حالتين :

$g(x) \neq x$ أو $g(x) = x$

وفي حالة المشكل ، $g\{g(x)\} \neq g(x)$ لذلك $f[g(x)] = g(x)$ بالإضافة إلى ذلك $g[f(x)] = g(x)$ لذلك $fg(x) = gf(x)$.

وفي الحالة الأخرى $f\{g(x)\} = f(x) = x$ ، $g(f(x)) = g(x) = x$

وفي هذه الحالة أيضاً $(f \circ g)(x) = (g \circ f)(x)$

وهذا يبين أن f ، g إبداليين .

مثال 13

لتكن $S = \{1, 2, 4, 5\}$ ، الدورة $(2\ \ 1)$ هي إبدال وضع . وبنفس الطريقة $(3\ \ 2)$ ، $(1\ 4)$. هما أيضاً تباديل وضع في S .

أوجد جميع التباديل الموضحة الممكنة إلى S (سوف تكون 10 في العدد) .

مثال 14

لتكن $S = \{1, 2, 3, 4, 5\}$ $f = (1\,3\,2)$ ، $f = (4\,5)$ بواسطة تعريف $f(1) = 3$ ، $f(3) = 2$ ، $f(2) = 1$ ولـيكن $g(1) = 1$ ، $g(3) = 3$ ، $g(2) = 2$ ومـرة أخـرى $g(4) = 5$ ، $g(5) = 4$ ولكـن $f(4) = 4$ ، $f(5) = 5$ هـذا يبـين أن f ، g تباديـل منفصلة .

ملاحظة

من اليسير التأكد من أن أي تبديلين غير محايدين دائريين هما منفصلين أم لا . ولرؤية إذا كانت هذه التباديل تملك أي عناصر مشتركة في ترقيم الصف الواحد أم لا . إذا كانت تملك أي عناصر مشتلكة في ترقيم الصف الواحد فإنها ليست منفصلة وبعكس ذلك تكون منفصلة .

وكمثال على ذلك $(3\ \ 2\ \ 1)$ ، $(5\ \ 4\ \ 3)$ ليست منفصلة لأن 3 عنصر متشرك . ولكن $(2\ \ 1)$ ، $(7\ \ 3)$ منفصلة لأنها لا تحوي على عناصر مشتركة ، ومع الاحتفاظ بميزة القاعدة سنحاول أن أي من الثنائيات الدوارة منفصلة .

(i) $(1\ 2)$ ، $(3\ 2)$ (ii) $(4\ 5\ 2)$ ، $(1\ 3)$ (iii) $(1\ 3\ 5)$ ، $(2\ 4\ 3)$.

وللتحقق من الملاحظة سنتركها للقارئ .

تعريف 3-20 (التباديل الدوارة)

لتكن S أي مجموعة منتهية غير فارغة ولتكن f أي تبديل على S . لو أخذنا $s \in S$ بواسطة برهان البديهية (3-16) يوجد عدد صحيح موجب k بحيث :
$s, f(s), f^2(s) \dots f^{k-1}(s)$ مختلفة جميعها و $\{s, f^1(s), f^2(s) \dots f^{k-1}(s)\}$ هي المدار في S .
التبديل الدوار $(s\ f(s) \dots f^{k-1}(s))$ تدعى بالدوارة على f .

مثال 15

لتكن $S = \{1, 2, 3, 4, 5\}$, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ فإن :
$(1 f(1) f^2(1)) = (1\,2\,3)$ دوارة في f ومرة أخرى حيث $s = f(4)$ ، $4 = f(5) = f(f(4)) = f^2(4)$ ، $\{4, 5\}$ دورة أيضاً في f ، وفي الحقيقة أن (3 2 1) و (5 4) هما الدائرتين الوحيدتين في f ، ونلاحظ أن هنالك دائرتين منفصلتين .

نظرية 3-21

أي تبديلين دائريين من مجموعة منتهية تكونان منفصلتين .

البرهان

لتكن $(s, f(s_1) \dots f^{k-1}(s_1))$ و $(s_2\ f(s_2) \dots f^{k-1}(s_2))$ أي دوارتين مختلفتين في f .

بواسطة تعريف الدوارة نعلم بأنه المجموعة $(s_1 f(s_1), \dots, f^{k-1}(s_1))$ و $(s_2 f(s_2), \dots, f^{k-1}(s_2))$ ذات مدار مختلف في f .

والآن لأي مدارين مختلفين في f ليس هنالك أي عنصر مشترك بينهما (بديهية 3-15) ولذلك $(s_1 f(s_1), \dots, f^{k-1}(s_1))$ و $(s_2 f(s_2), \dots, f^{k-1}(s_2))$ لا تحتوي على عنصر مشترك ، وهذا يؤدي إلى أن الدوارتين منفصلتين .

نظرية 3-21

أي تبديل لا يساوي المحايد من مجموعة منتهية يمكن التعبير عنه عن طريق دوارات منفصلة وكلها ذات طول أكبر من 1 .

البرهان

لـتكن S أي مجموعـة منتهيـة غـير فارغـة أو خاليـة و $f \in A(S)$ ، لـتكن $\sigma_1, \sigma_2, \dots, \sigma_t$ هـي كـل الـدوارات في f هـذه الـدورات سـوف تكـون منفصـلة (بديهيـة 3-21). سوف نبين أن

$$f = \sigma_1, \sigma_2, \dots, \sigma_i$$
$$\sigma_1 = (a_1, a_2, \dots, a_r)$$
$$\sigma_2 = (b_1, b_2, \dots, b_s)$$
$$\sigma_t = (l_1, l_2, \dots, l_u)$$

اعتبر
$$\sigma_1, \sigma_2, \dots, \sigma_t = (a_1, a_2, \dots, a_r)\,(b_1, b_2, \dots, b_s), \dots, (l_1, l_2, \dots l_u)$$

لتكن $x \in S$ ، بما أن مدار f يحسب دوارات وحيدة في f وأي عنصر في S سوف يقع في أحد المدارات في f ، فإنه يوجد دوارة σ_i بحيث أن x سوف تكون أحد عناصرها .

لتكن $\sigma_i = (k_1, k_2, \dots, k_m)$ و $x = k_j$ لبعض $1 \le j \le m$ فإنه وبواسطة التعريف $f(x) = k_j + 1$ إذا كانــت $j < m$ و $f(x) = k_1$ إذا كانــت $j = m$ وهـــذا يعـــني أن $f(x) = \sigma_i(x)$ وبمـــا أنـــه لا يوجـــد أي عنصـــر في σ_i يقـــع في الـــدوارات $\sigma_1, \sigma_2, \dots, \sigma_{i-1}, \sigma_{i+1}, \dots, \sigma_t$ هذه الدوارات تذهب إلى العناصر الثابتة $k_1, k_2, \dots, k_m$ لذلك $(x) = \sigma_i(x) = f(x)$ أي أنـه $f = \sigma_1, \sigma_2, \dots, \sigma_t$ ولحـد الآن لم نسـتخدم حقيقـة كـون f ليست المحايد في S وأيضاً لم نبين أن طول الدوارة σ_i هو أكبر من 1 .

وكحالة الاحتواء في أي تركيب لـ f كضرب دائري طول الدورة I القوس يختص .

ليكن :

$$f = \sigma_1, \sigma_2, \sigma_3, \dots, \sigma_r \qquad (1)$$

$$= n_1, n_2, \dots, n_w \qquad (2)$$

تمثيلان لـ f كضرب دوائر غير متقاطعة طول كل منها > 1 .

افـرض أي $n_l(l = 1, 2, \dots, w)$ وأن n_l هـي دارة . لـدينا $l = (c_1, c_2, \dots, m)$ لـبعض قـيم $c_1, c_2, \dots, c_m$ في $\{1, 2, \dots, n\}$ ، نأخـذ $c_k ck = 1, 2, \dots, m)$ ليسـت في أي n_i مـع $i \neq l$ لذلك $n_i(c_k) = c_l$ لكل $i \neq l$ ولدينا $f(c_k) = n_l(l_k) = c_{k+1}$ لكل $k = 1, 2, \dots, m - 1$ و :

$$f(c_m) = n_l(c_m) = c_1 \qquad (3)$$

كما أن

$$f(c_1) = n_l(c_1) = c_2; f(c_1) = f(c_2) = n_1(c_2) = c_3$$

$$f^3(c_1) = f(c_3) = c_l(c_3) = c_4, \dots, f^{m-1}(c_1) = c_m$$

وأن

$$f^m(c_1) = c_1$$

$$\{c_1, c_2, \dots, c_m\}$$

ليست في مدار f .

والآن إذا كـان c_1 لـيس عنصـراً في أية σ_j فإنهـا سـوف تعطـي $\sigma_j(c_1) = c_1$ لكـل $j = 1, 2, \dots, v$ ولـذلك $f(c_1) = c_1$ وهـذا غير ممكـن لأن $f(c_1) = c_2 \neq c_1$ وإذاً يوجـد σ_i بحيث أن c_1 عنصراً فيها كما لآ n_l .

مـن الممكـن البرهـان أن العناصـر لـ σ_i محتـواة في مـدار f . لأن c_1 عنصـراً في σ_i تلاحـظ أن المـدار $\{c_1, c_2, \dots, c_m\}$ يحتـوي علـى كـل العناصـر σ_i ، لـذلك كمـا في n_l ، لـذلك لـدينا $\sigma_r(c_k) = c_k$ وأن $f(c_k) = \sigma_i(c_k)$ لكـل $k = 1, 2, \dots, m$ و $r \neq i$.

وهكذا بالاستمرارية يمكن وباستخدام (3) أن نحصل على :

$$c_2 = f(c_1) = \sigma_i(c_1), c_3 = f(c_2) = \sigma_i(c_2), \dots,$$
$$c_m = f(c_{m-1}) = \sigma_i(c_{m-1})$$

وأن $c = f(c_m) = \sigma_i(c_m)$ لذلك فإن $\sigma_i(c_1, c_2, \ldots, c_m)$ لذلك فإن كل n_l هي مساوية لبعض σ_i ، وكذلك كل σ_r مع $r \neq i$ هي غير مرتبطة من σ_i ، ولذلك تساوي σ_i نحصل على n_l تساوي σ_i لـ i وحيد . وبطريقة مشابهة كل σ_k مساوي لبعض n_j الوحيدة. ولذلك يوجد (1-1) تمثيل بين σ_i و n_l بحيث أن هذا التمثيل الدائري متساوي ، وهذا يحقق البرهان . □

استنتاج 3-23

أي تباديل كمجموعة منتهية S يحتوي على أكثر من عنصرين ، هو قرب تبديل الموقع .

البرهان

افرض أي دارة $(a_1a_2 \ldots a_m)$ طولها m ، إذا كان $m > 1$ ، تواضح أن $(a_1a_2 \ldots a_m) = (a_1a_m)(a_1g_{m-1})\ldots(a_1a_3)(a_1a_2)$. وإذا كان $m = 1$ فإن (وكما في S تحتوي على أكثر من عنصر واحد) فإنه يوجد $b \in S$ يجب أن $b \neq a_1$ ونحصل على $(a_1) = (a_1b)\,(ba_1)$ ومن النظرية السابقة كل تبديل هو ضرب دارة . لذلك نستطيع أن نمثل كل تبديل على شكل ضرب تبديل الموقع .

نظرية 3-24

ليكن f تبديل لمجموعة منتهية S ، فإن في كل التمثيلات لـ f كضرب لتبديل الموقع وإلا فإن عدد تباديل الموقع هي عادةً ما تكون إما زوجية أو أن تكون فردية .

البرهان

ليكن $f = \sigma_1\sigma_2 \ldots \sigma_t$ تمثيل لـ f كضرب لدوائر منفصلة ، طول كل منها > 1 ، إذا كان بعض العناصر ، ولتكن x من S ليست في أية دائرة σ_i فإننا تضيف (x) أو بعض آخر الدائرة التي طولها 1 في التمثيل أعلاه لـ f ، وبهذه الطريقة كل عنصر في S هو في بعض الدارة لـ f .

ليكن $N(f) = \sum_{i=1}^{k} [l(\sigma_i') - 1]$ حيث أن (σ) يمثل طول الدارة σ' . كما أن كل دارة σ^1 طولها 1 ، $l(\sigma') - 1 = 0$ ، $N(f) = \sum_{i=1}^{t} [l(\sigma_i) - 1]$ ، $N(f)$ هي وحيدة التعريف وغير سالبة وصحيحة ، سوف تبين أن أي معاملة لـ f لضرب دارات غير مرتبطة يحتوي على عدد زوجي أو فردي من تباديل الموقع واعتماداً على $N(f)$ هل هي زوجي أو فردي . هذا سوف يساعدنا على برهان الاستنتاج ، ولهذه التحضيرات تحتاج إلى الصيغ التالية

$$(ab)\,(ac_1c_2 \ldots c_nbd_1d_2 \ldots d_k) = (bd, N, \ldots d_k)\,(ac_1c_2 \ldots c_n)$$

وأن

$$(ab)\,(bd_1 \ldots d_k)\,(ac_1c_2 \ldots c_n) = (ac_1c_2 \ldots c_nbd_1d_2 \ldots d_k)$$

واعتماداً على هذه الصيغ إذا كان b, a موجدان في نفس الدارة لـ f فإن $N[(ab)f] = N(f) - 1$ وإذا كان a و b موجودان في دارات مختلفة لـ f فإن $N[(ab)f] = N(f) + 1$ إذا كان في أية حالة .

$$N[(ab)f] = N(f) \pm 1 \qquad (1)$$

الآن نفرض أن f هي ضرب لتباديل الموقع . وليكن :

$$f = (a_1b_1)\,(a_2b_2) \ldots (a_mb_m)$$

سوف نبرهن الناتج استخدام الاستقراء على m ، إذا كانت $m = 1$ فإن $N(f) = 1$ وبالتالي يتحقق الناتج بشكل مبسط .

افرض أن $m > 1$ والناتج متحقق لكل تمثيل لتباديل كضرب لـ $m - 1$ لتباديل المواقع . والآن : $(a_1b_1)f = (a_2b_2)\ldots(a_mb_m)$ ، وبطريقة الاستقراء $m - 1, N[(a_1b_1)f]$ كلاهما زوجي أو فردي . وعلى أية حال بواسطة (1) ، $N[(a_1b_1)f] = N(f) \pm 1$ وهذا يبين $N(f)$ و m هما إما كلاهما فردي أو كلاهما زوجي ، وهذا يتمم البرهان .

ملاحظة

برهان آخر لهذه النظرية معطى في التمارين الخارجية بعد النظرية 3-34 .

تعريف 3-25 (التباديل الفردية أو الزوجية)

التبديل f لمجموعة منتهية غير خالية S يسمى زوجي أو فردي اعتماداً على كون f ممثلة على شكل ضرب عدد زوجي أو فردي من عدد التباديل للموقع .

نظرية 3-26

لأي $n > 1$ ، المجموعة الجزئية A_n من S_n تحتوي على كل التباديل الزوجية هي مجموعة جزئية طبيعية من S_n ومن الدليل 2 .

البرهان

ليكن $x = \{1, 2, \ldots, n\}$ وكذلك S_n زمرة كل التباديل لـ x ، بما أن $I = (1\,2)\,(1\,2)$ و $I \in A_n$ هذا يعني أن A_n ليست خالية ، والآن ليكن $f, g \in A_n$ وأن

$$f = (a_1b_1)\,(a_2b_2)\ldots(a_tb_t)$$

وأن

$$g = (c_1d_1)\,(c_2d_2)\ldots(c_ud_u)$$

التمثيلين g, f كضرب لعدد زوجي من التباديل للمواقع i ، بحيث أن كلا u, t هما زوجي ، وبالاستمرارية $t + u$ هو زوجي ، على أية حال :

$$f \circ g^{-1} = (a_1b_1)\ldots(a_tb_t)\,(c_ud_u)\,(c_{u-1}d_{u-1})\ldots(c_1d_1)$$

هو ضرب لتباديل $t+u$ ، نستنتج أن $f \circ g^{-1}$ هي تباديل زوجية أيضاً . ولذلك $f \in A_n$ و $g \in A_n$ يؤدي إلى $f \circ g^{-1} \in A_n$ ، ولذلك A_n هي زمرة جزئية .

افرض أن $(1 \quad 2)$. $(1 \quad 2)$ هي تبديل فردي فإن $(1\,9) \notin A_n$ وبشكل مماثل $A(1\,2) \neq A_n$ وبما أن كل تبديل زوجي في S_n هو في A_n وإذا بينا أن كل تبديل فردي في S_n هو في $A_n(1\,2)$ فإننا سوف تنتج أن كل عنصر في S_n هو إما في A_n أو في $A_n(1\,2)$ ، وهذا سوف يعطينا $S_n = A_n \cup A_n(1\,2)$ و A_n هي لديها دليلان في S_n .

بما أن كل زمرة جزئية من الدليل 2 هي طبيعية . سوف نحصل كذلك على أنه A_n هي طبيعية في S_n . لذلك ليكن $f \in S_n$ و f هي فردية ، واضحاً أن $f(1\,2)$ هي زوجية . لذلك $f(1\,2) \in A_n$ فإن $f = [f(1\,2)](1\,2) \in A_n(1\,2)$ وهذا يحقق النتائج . □

تعريف 3-26 (a)

لأي $n \geq 1$ ، S_n تسمى زمرة متماثلة من الدرجة n .

تعريف 3-26 (b)

لأي $n \geq 1$ ، A_n تسمى زمرة متناوبة من الدرجة n .

نظرية 3-27 (كايلي)

كل زمرة هي آيزومورفزم لزمرة تباديل .

البرهان

لتكن G زمرة و $A(G)$ تمثل زمرة كل التباديل للمجموعة G ، لكل $a \in G$ تعرف $f_n : G \to G$ بحيث $f_a(x) = ax$.

ولكل $x \in G$ ، لأي $x, y \in G$ $f_a(x) = f_a(y) \Rightarrow ax = ay$
$\Rightarrow x = y$

لذلك f هو $(1 - 1)$ متباينة ، وأبعد من ذلك $f_a(a^{-1}x) = aa^{-1}x = x$ تبين أن f هي شاملة . لذلك $f_a \in A(G)$ والآن لأي $a, b, x \in G$ ،

$$(f_a \circ f_b)(x) = $$
$$= f_a[f_b(x)] = f'_a(bx) = a(bx) = f_{ab}(x)$$

وهذا يؤدي إلى أن $f_a \circ f_b = f_{ab}$ تعرف $\sigma : G \to A(G)$

بحيث $\sigma(a) = f_a \quad \forall\ a \in G$

فإن لكل $\sigma(ab) = f_{ab} = f_a \circ f_b = \sigma(a) \circ \sigma(b), a, b \in G$

وكذلك $\sigma(a) = \sigma(b) \Rightarrow f_a = f_b \Rightarrow f_a(e) = f_b(e)$

$\Rightarrow ae = be \Rightarrow a = b$

لذلك σ هي هومومورفزم أحادية من G إلى $A(G)$.

لذلك G هي أيزومورفزم إلى $\sigma(G)$ والتي تكون زمرة جزئية من $A(G)$ ، زمرة تباديل ، وهذا يبرهن النظرية . □

الزمرة الإبدالية S_3 في المجموعة $x = \{1, 2, 3\}$ تعطي قاعهدة مهمة في نظرية الزمر ، هي زمرة غير إبدالية الأصغر سوف نبين أنه يوجد فقط اثنين من الأنواع للزرة من الرتبة 6 .

نظرية 3-28

يوجد فقط زمرتين من الرتبة 6 ، واحد دارة والثانية أيزومورفزم إلى S_3 .

البرهان

ليكن G زمرة من الرتبة 6 ، بما أنه يوجد خمسة عناصر غير العنصر المحايد و $x \leftrightarrow x^{-1}$ هي دالة اعتماد تباينية بين العناصر ومعكوساتها ، يوجد عنصر $(a \neq e) \in G$ بحيث أن a هو معكوس نفسه $(\circ(a) = 2)$ لتكن G زمرة إبدالية و H زمرة جزئية $< a >$ ، والآن $\circ(G/H) = 3$ يؤدي إلى أن G/H دائرية .

ليكن bH العنصر المولد لـ G / H ، بما أن $\circ(bH) \mid \circ(b)$ نحصل على أن $\circ(b) = 3$ أو 6 إذا كانت $\circ(b) = 6$ منها وببساطة G هي دائرية . أما إذا كانت $\circ(b) = 3$ فإن $\circ(ab) = 6$ لأن $ab = ba$ و $\circ(a)$ و $\circ(b)$ هما غير أوليان (قضية 4-23) لذلك ومرة أخرى G زمرة دائرية مولدة بالعنصر ab . افرض الآن أن G ليست دائرية ، فإن G لا يمكن أن تكون إبدالية ، لذلك كل العناصر غير المحايدة في G لا يمكن أن تكون من الرتبة 2 (الفصل 2 المقطع 2 المسألة 10) ، لذلك يوجد c في G بحيث أن $\circ(c) = 3$ و $ac \neq ca$. ليكن $H = \{e, c, c^2\}$ كما أن $H, [G : H] = 2$ زمرة جزئية طبيعية ، وهكذا فإن $a^{-1}ca \in H$ ولذلك $a^{-1}ca = c$ أو c^2 ولكن $ac \neq ca$. نحصل على أن $a^{-1}ca = c^2$ أو بمعنى آخر $ca = ac^2$. والآن $a \notin H$ ، إذن نحصل على أن

$$G = H \cup aH = \{e, c, c^2, a, ac, ac^2\}$$

وعلى طريقة الإثبات ، التطبيق $f : G \to S_3$

والمعطى بـ

$$f(e) = I, f(a) = (1\,2), f(c) = (1\,2\,3)$$

$$f(c^2) = (1\,3\,2), f(ac) = (2\,3), f(ac^2) = (1\,3)$$

هي أيزومورفزم ، وهذا يتمم البرهان . □

بالاستعانة بالنظرية 3-28 يمكن أن نبين معكوس نظرية لاكرانج ليس صحيحاً . وهذا ما سنقوم به في النظرية 3-31 ، ولكن أولاً لنبرهن القضية التالية .

قضية 3-29

الزمرة S_4 ليس فيها عنصر من الرتبة 6 .

البرهان

عناصر S_4 هي $\{1, 2, 3, 4\}$ وليكن $\sigma(\neq 1) \in S_4$ فإن $\sigma = \sigma_1\sigma_2 \dots \sigma_t$ حيث أن $\sigma_1, \sigma_2, \dots \sigma_t$ هي أزواج من الدارات المنفصلة طول كل منها أكبر من 1 . بما أن الرموز التي

تظهر في σ_i هي من بين $\{1, 2, 3, 4\}$ ، لا يمكن أن يكون طول σ_i أكبر من 4 ، ولا يملك أي عنصرين σ_i, σ_j $(i \neq j)$ رمز من أصولها .

لدينا $t \leq 2$ ، لذلك يوجد σ دارة أو σ يمكن أن تمثل على شكل ضرب دارتين منفصلتين طول كل منهما 2 . إذا كانت σ ضرب لدارتين منفصلتين ، طول كل منهما 2 ، فإن σ من الرتبة 2 ، لذلك S_4 لا تملك أي عنصر من رتبة تزيد على 4 .

نظرية 3-30

A_4 لا توجد فيها زمرة جزئية من الرتبة 6 .

البرهان

من الاستنتاج السابق A_4 لا تملك أي عنصر من الرتبة 6 ولذلك A_4 لا يمكن أن تملك زمرة جزئية دائرية من الرتبة 6 ، ولذلك إذا كانت كل الزمر الجزئية من A_4 برتبة 6 يجب أن تكون أيزومورفزمية لـ S_3 (نظرية 3-28) . ليكن H هو الزمرة الجزئية من A_4 ، ولذلك $H \cong S_3$ ، H تحتوي على ثلاثة عناصر من الرتبة 2 لكل منها وعنصرين من الرتبة 3 لكل منهما . العناصر من A_4 ومن الرتبة 2 هي $(1\ 2)\ (3\ 4)$ و $(1\ 3)\ (2\ 4)$ و $(1\ 4)\ (2\ 3)$ فقط .

لتكن σ هي أيزومورفزم بين H و S_3 ، والآن :

$$\sigma[(1\ 2)\ (3\ 4)\ (1\ 3)\ (2\ 4)] = \sigma[(1\ 4)\ (2\ 3)]$$

$(1\ 4)\ (2\ 3)$ من الرتبة 2 $\Leftarrow$ رتبة $\sigma[(1\ 4)\ (2\ 3)]$ هي 2 أيضاً ، ولكن S_3 ضرب لعنصرين مختلفة ومن الرتبة 2 ولكن يوجد عنصر من الرتبة 3 ، ولذلك في S_3 رتبة $\sigma[(1\ 4)\ (2\ 3)]$ ، وهذا تناقض . هذا البرهان يبين أن فرضياً كانت خاطئة ، لذلك A_4 لا تحتوي على زمرة جزئية من الرتبة σ . □

ملاحظة

انظر إلى البرهان الأقصى لهذه النظرية في التمارين الخارجية في نهاية النظرية 3-34 .

ملاحظة

لاحظ أن $\circ(A_4) = 12$ وأن $6 \mid 12$. لذلك النظرية 3-29 تبين أن عكس نظرية لاكرانج هو خطأ .

لنستذكر أن الزمرة $G[\neq e]$ تسمى زمرة بسيطة غذ لم تحتوي على أية زمرة جزئية فعلية عادية .

كل زمرة ذات رتبة أولية هي بسيطة وذلك لانه لا يوجد فيها زمرة جزئية والتي تسمى زمرة جزئية طبيعية فعلية ! .

السؤال المنطقي هل توجد هناك زمرة بسيطة ورتبتها مركبة ؟ الجواب على ذلك هو ، نعم ، بالفعل أنه يوجد ما لانهاية منا لزمر البسيطة ذات الرتبة المركبة . لنبيين ذلك من الضروري أن نبرهن أن A_n هي بسيطة لكل $n \geq 5$ ، سوف نبرهن ذلك الاستعانة ببعض الاستنتاجات والتي فيها نأخذ $n \geq 5$.

قضية 3-31

كل عنصر من A_n هو ضرب ثلاث دارات .

البرهان

ليكن $1, \alpha, \beta$ ثلاثة عناصر مختلفة من $\{1, 2, \ldots, n\}$ ولكل $x \in A_n$ التمثيل لضرب عدد زوجي لتباديل المواقع وكل تباديل المواقع $(\alpha\beta)$ حيث أن $\alpha \neq 1$

و $\beta \neq 1$ يمكن أن تمثل بالشكل $(1\alpha)\,(1\beta)\,(1\alpha)$. لذلك x ذاتها يمكن أن تكتب على الشكل $(1\alpha_1)\,(1\alpha_2)\ldots(1\alpha_r)$ حيث أن r زوجي وأن $\alpha_i \in \{1, 2, \ldots, n\}$ وأكثر من ذلك $(1\alpha)\,(1\beta) = (1\beta\alpha)$ وأن r هو زوجي وهذا يؤدي إلى أن كل عدد زوجي من التباديل هو ضرب لـ 3 دارات . □

ملاحظة

من الممكن ملاحظة أن $n \geq 3$ (وليست $n \geq 5$) في البرهان السابق .

قضية 3-32

إذا احتوت الزمرة الجزئية الطبيعية H من A_n دارة طولها 3 ، فإن $H = A_n$.

البرهان

في عرض القضية 3-31 كان من الضروري للبرهان أن كل دارة طولها 3 تنتمي إلى H .

ليكن $(\alpha\beta\gamma)$ أي دارة طولها 3 وليكن $(xyz) \in H$ ، افرض $\theta \in S_n$ بحيث أن

$$\theta(x) = \alpha, \theta(y) = \beta, \theta(z) = \gamma$$

فإن

$$\theta(xyz)\theta^{-1} = (\alpha\beta\gamma)$$

لذلك إذا كانت $\theta \in A_n$ ، فإن $(\alpha\beta\gamma) \in H$ ولأن H هو زمرة جزئية طبيعية من A_n .

ولذلك لنفرض أن $\theta \notin A_n$ ، نأخذ u, v في المجموعة $\{1, 2, \ldots, n\}$ مختلفة عن x, y, z (وهذا ممكن لأن $n \geq 5$) ، ولأن θ هي فردية فإن

$$\theta(uv) \in A_n$$

لذلك

$$\theta(uv)\,(xyz)[\theta(uv)]^{-1} \in H$$

$$\Rightarrow \quad \theta(uv)\,(xyz)\,(uv)\theta^{-1} \in H$$

$$\Rightarrow \quad \theta(xyz)\theta^{-1} \in H$$

لأن (xyz) و (uv) هي منفصلة ولأن

$$(uv)\,(xyz)\,(uv) = (xyz)\,(uv)^2 = (xyz)$$

$$\Rightarrow \quad (\alpha\beta\gamma) \in H$$

وهذا يحقق النتيجة □ .

نتيجة 3-33

إذا احتوت الزمرة الجزئية الطبيعية H من A_n حاصل ضرب التباديل الموقعية لعنصرين منفصلين فإن $H = A_n$.

البرهان

ليكن $H \in (xy)(uv)$ حيث (xy) و (uv) هما منفصلين . نأخذ w في المجموعة $\{1, 2, \dots, n\}$ مختلف عن x, y, u, v وهذا ممكن لأن $n \geq 5$ ، ضع $\theta = (uvw)$ واضح أن $\theta \in A_n$ ، بحيث $\theta(xy)(uv)\theta^{-1} \in H$ بمعنى آخر $(uvw)(xy)(uv)(wvu) \in H$

$$\Rightarrow \quad (vu)(xy) \in H$$

وعلى اية حال فإن H هي زمرة جزئية ، ولذلك $(xy)(uv)(vw)(xy) \in H$ أو بمعنى آخر $(uvw) \in H$ ، لذلك $H = A_n$ (النتيجة 3-32) .

الآن نحن على استعداد لبرهان استنتاجنا الرئيسي .

نظرية 3-34

ليكن $H \neq \{1\}$ هي زمرة جزئية طبيعية من A_n ، سوف نبين أن $H = A_n$ ، لأن $H \neq \{1\}$ يوجد $\alpha = \alpha_1\alpha_1\alpha_3 \dots \alpha_n, \alpha(\neq I) \in H$ هو تركيب α في الدارات المنفصلة طول كل منها أكبر من واحد ، لأنها متصلة نستطيع أن نفرض أن الطول لـ σ_i أكبر من طول σ_{i+1} ، لكل $i = 1, 2, \dots, k-1$ ، تظهر أربعة حالات :

(i) واحدة على الأقل من σ_i طولها أكبر من 3 .

(ii) σ_1 و σ_2 طولهما 3 .

(iii) σ_1 طولها 3 والبقية (σ_i) هي تباديل موقعية .

(iv) كل σ_i هي تباديل موقعية .

الحالة الأولى (i)

لأنه يوجد على الأقل دارة واحدة طولها أكبر من 3 وتبعاً لاختيارنا للطول تنازلياً للمرتبة فإن قيمة σ_1 هي دارة طولها أكبر من 3 .

ليكن $r > 3, \sigma_1 = (a_1 a_2 \ldots a_r)$ افرض أن $\theta = (a_1 a_2 a_3)$ واضح أن $\theta \in A_n$ ولذلك $\theta \alpha \theta^{-1} \in H$ لأن H هي زمرة جزئية طبيعية في A_n أو بمعنى آخر

$$(a_1 a_2 a_3)\ \delta_1 \delta_2 \ldots \delta_k (a_3 a_2 a_1) \in H$$

$$\Rightarrow \quad \sigma_2 \sigma_3 \,.\, \sigma_k (a_1 a_2 a_3)\,(a_1 a_2 \ldots a_r)\,(a_3 a_2 a_1) \in H$$

ولأن σ_i منفصلة فإن :

$$\sigma_2 \sigma_3 \ldots \sigma_k (a_1 a_4 a_5 \ldots a_r a_2 a_3) \in H$$

ولكن H هي زمرة جزئية ، لذلك

$$\sigma^{-1} \sigma_2 \sigma_3 \ldots \sigma_k (a_1 a_4 a_5 \ldots a_r a_2 a_3) \in H$$

$$\Rightarrow \quad \sigma_k^{-1} \sigma_{k-1}^{-1} \ldots \sigma_2^{-1} \sigma_2 \sigma_3 \ldots \sigma_k \sigma_1^{-1} (a_1 a_4 a_5 \ldots a_r a_2 a_3) \in H$$

ولأن σ_i كلها منفصلة فإن

$$(a_r a_{r-1} \ldots a_3 a_2 a_1)\,(a_1 a_4 a_5 \ldots a_r a_2 a_3) \in H$$

$$\Rightarrow \quad (a_1 a_3 a_r) \in H$$

وبالتتابع $H = A_n$ (نتيجة 3-32) .

الحالة الثانية (ii)

ليكن

$$\sigma_2 = (a_4 a_5 a_6), \sigma_1 = (a_1 a_2 a_3)$$

نفرض أن

$$\theta = (a_5 a_6 a_1)$$

لأن $\theta \in A_n$ و H هي زمرة جزئية طبيعية من A_n فإن $\theta \circ \theta^{-1} \in H$ ، أو بمعنى آخر

$$(a_5 a_6 a_1)\ \sigma_1 \sigma_2 \ldots \sigma_k (a_1 a_6 a_5) \in H$$

وهذا يعطي

$$\alpha^{-1} \sigma_3 \sigma_4 \ldots \sigma_k (a_1 a_4 a_6)\,(a_2 a_3 a_5) \in H$$

أو بمعنى آخر

$$\sigma_k^{-1} \sigma_{k-1}^{-1} \ldots \sigma_2^{-1} \sigma_1^{-1} \sigma_3 \sigma_4 \ldots \sigma_k (a_1 a_4 a_6)\,(a_2 a_3 a_5) \in H$$

$$\Rightarrow \quad (\sigma_k^{-1} \sigma_{k-1}^{-1} \ldots \sigma_3^{-1} \sigma_3 \sigma_4 \ldots \sigma_k)\ \sigma_2^{-1} \sigma_1^{-1} (a_1 a_4 a_6)\,(a_2 a_3 a_5) \in H$$

$$\Rightarrow \quad (a_6 a_5 a_4)\,(a_3 a_2 a_1)\,(a_1 a_4 a_6)\,(a_2 a_3 a_5) \in H$$

$\Rightarrow \quad (a_1a_6a_3a_4a_5) \in H$

ووصلنا إلى الحالة الأولى (i) . لذلك ومرة أخرى $H = A_n$.

الحالة الثالثة (iii)

ليكن $\sigma_1 = (a_1a_2a_3)$ ولكل σ_i لكل $i = 2, 3, \ldots, k$ هي تباديل موقعية .

$$\alpha = \sigma_1\sigma_2 \ldots \sigma_k \in H$$

$$\Rightarrow \quad \alpha^2 = \sigma_1^2\sigma_2^2 \ldots \sigma_k^2 \in H$$

$$\Rightarrow \quad \sigma_1^2 \in H$$

لأن $\sigma_i^2 = 1$ لكل قيم $i = 2, 3, \ldots k$

$$\Rightarrow \quad (a_1a_2a_3)^2 \in H$$

$$\Rightarrow \quad (a_3a_2a_1) \in H$$

وبالتتابع $H = A_n$ (النتيجة 3-32) .

الحالة الرابعة (iv)

ليكن $\qquad \sigma_2 = (a_3a_4), \sigma_1 = (a_1a_2)$

نفرض أن $\theta = (a_3a_4a_1)$ لأن $\theta \in A_n$ و H هي زمرة جزئية طبيعية من A_n فإن

$\theta\alpha\theta^{-1} \in H$ أو بمعنى آخر $\qquad (a_3a_4a_1)\sigma_1\sigma_2 \ldots \sigma_k(a_1a_4a_3) \in H$

$$\Rightarrow \quad \sigma_3\sigma_4 \ldots \sigma_k(a_3a_4a_1)(a_1a_2)(a_3a_4)(a_1a_4a_3) \in H$$

$$\Rightarrow \quad (a_4a_3)(a_2a_1)(a_1a_4)(a_2a_3) \in H$$

$$\Rightarrow \quad (a_1a_3)(a_2a_4) \in H$$

وهذا يؤدي إلى $H = A_n$ (النتيجة 3-33) ، ولذلك فإن A_n هي زمرة بينية لكل قم $n \geq 5$.□

التمرين الأول

برهن أن S_n عدد الدارات المختلفة والتي طولها $n \geq r$ هي $\frac{1}{r} \cdot \frac{n!}{(n-r)!}$.

الحل

عدد الترتيبات لـ r من الأشياء والمسحوبة من n من الأشياء هو $^{n}P_r = \dfrac{n!}{(n-r)!}$.

كما أن لكل دارة $(a_2a_3 \dots a_ra_1), (a_1a_2 \dots a_r)\ (a_ra_1a_2 \dots a_{r-1})$

هي متشابهة ، وعدد دارات r هو $\dfrac{1}{r}\dfrac{n!}{(n-r)!}$.

التمرين الثاني

A_n ليس فيها زمرة جزئية ومنتهية 6 .

الحل

لأن الدارات ذات الطول 3 من S_4 هي تباديل زوجية ، كل دارات ثلاثية في S_4 محتواه في A_4 ، بواسطة التمرين الأول السابق ، فإن عدد الدارات الثلاثية المختلفة في A_4 هي $8 = \dfrac{1}{3}.\dfrac{4!}{(4-3)!}$.

لتكن H زمرة جزئية من A_4 ، من الرتبة 6 ، كل الدارات الثالثة في A_4 لا يمكن أن تنمي إلى H ، ليكن x دارة ثلاثة في A_4 ، لذلك $x \notin H$ ، لأن $a(x) = 3$ الزمرة الجزئية $k = \{e, x, x^2\}$ تحتوي على ثلاثة عناصر ، حيث أن e هو العنصر المحايد في A_4 .

والآن $x \notin H, x^2 = x^{-1} \notin H$

$$\Rightarrow \qquad H \cap k = \{e\} \Rightarrow \circ(Hk) = \frac{\circ(H) \circ (k)}{\circ\,(Hak)} = \frac{6-3}{1} = 18$$

وهذا غير ممكن لأن Hk هي مجموعة جزئية من A_4 وأن A_4 لها 12 عنصر . لذلك فإن هذا تناقض ، وبالتتابع فإن A_4 ليس لها زمرة جزئية ذات رتبة 6 .

التمرين الثالث

ليكن f تبديل مجموعة منتهية S ، فإن كل التمثيلات لـ f لضرب لتباديل المواقع أو عدد تباديل المواقع هي عادة ما تكون زوجية أو فردية .

الحل

ليكن الناتج هو خطأ (لنفرض العكس) ونستطيع أن نجد تبديل $f \in ACS$ والذي يمكن أن يمثل كضرب لعدد زوجي من تباديل الموقع وفي نفس الوقت كضرب لعدد فردي من تباديل الموقع . لذلك

$$f = (a_1b_1)(a_2b_2)\dots(a_rb_r)\ a_i, b_i \in S$$
$$= (c_1d_1)(c_2d_2)\dots(c_sd_s)\ c_i, d_i \in S$$

حيث أن r زوجي و s فردي ، لذلك

$$f^{-1} = (c_sd_s)\dots(c_2d_2)(c_1d_1)$$

كما $(xy)^{-1} = (xy)$ لكل قيم $x, y \in S$.

إذا كان I هو التبديل المحايد فإن

$$I = ff^{-1} \Rightarrow I = (a_1b_1)\dots(a_rb_r)(c_sd_s)\dots(c_2d_2)(c_1d_1)$$

كتركيب لـ I مضروب لـ $r+s$ ، أو بمعنى آخر عدد فردي من التباديل ، وبهذه الطريقة تستطيع كتابة

$$I = (\alpha_1\beta_1)(\alpha_2\beta_2)\dots(\alpha_k\beta_k)$$

حيث $k, \alpha_i, \beta_i \in S$ هو عدد فردي . افرض أن $(\alpha_i\beta_i)$ إذا كانت $\alpha_i \neq 1$ و $\beta_i \neq 1$ تستطيع كتابة

$$(\alpha_i\beta_i) = (1\beta_1)(1\alpha_i)(1\beta_i)$$

وكمتتابعة

$$I = (1r_1)(1r_2)\dots(1r_2)$$

حيث أن t هو عدد فردي و

$$r_1r_2\dots r_t \in S - \{1\} \qquad (1)$$

افرض أن تأثير I في r_t و $I(r_t) = r_t$ ، وأبعد من ذلك (Ir_t) نأخذ r_t إلى 1 ، ولذلك لكي نجهزها بالعودة إلى $(Ir_t)r_t$ يجب أن نكرر 1 ومن الاتجاه الأيسر لـ (1) عدد زوجي من المرات ، وبالتشابه للترتيب نستطيع أن نعطي توضيحاً لكل تبديل موضعي

$$(Ir_j) \quad 1 \le j \le t$$

يجب أن يكرر عدد زوجي من المرات وهذا يؤدي إلى أن t يجب أن تكون زوجية ، وهذا تناقض لذلك فرضيتنا هي خاطئة ولذلك العبارة في المسئلة صحيحة .

التمرين الرابع

H زمرة جزئية من S_n لبعض قيم $n \geq 1$ الصحيحة إذا كان H يحتوي على عدد فردي من التباديل ، بين أن مجموعة كل التباديل الزوجية في H من الزمرة الجزئية الطبيعية H هي من الدليل 2 .

الحل

افرض $x, x = \{1,-1\}$ زمرة جزئية من الأعداد الحقيقية تحت عملية الضرب .

نعرف $\theta : H \to x$

بحيث $\theta(f) = 1$

إذا كان f تبديل زوجي في H و $\theta(f) = -1$

إذا كان f تبديل فردي في H وتستطيع أن نبرهن أن θ في هومومورفزم هي شاملة و H يحتوي على تباديل فردية ، وكذلك $\ker\theta$ هي مجموعة كل التباديل الزوجية من H ، لذلك $\ker\theta$ هو زمرة جزئية طبيعية من H ، الجزء الأول من المسألة قد برهن . بواسطة النظرية الأساسية للهومومورفزم $\frac{H}{\ker\theta} \cong x \Rightarrow \frac{\circ(H)}{\circ\,(\ker\theta)} = \circ(x) = 2$

ومنه أن دليل $\ker\theta$ هو 2 .

التمرين الخامس

إذا كانت H زمرة جزئية من الزمرة S, G هي مجموعة كل (Left cosets) من H في G ، فإنه يوجد هومومورفزم θ في G إلى $A(s)$ بحيث $\ker\theta$ هو أكبر زمرة جزئية ضيعية في G والتي تكون محتواة في H .

البرهان

نفرض $\theta : G \to A(s)$

بحيث $\theta(g) = T_g$

حيث أن $T_g(xH) = gxH$ لكل $xH \in S$ ، أولاً تبين أن $T_g \in A(s)$ واضح أنه T_g هو تطبيق من S إلى S ، وكذلك

$$T_g(xH) = T_g(yH) \Rightarrow gxH = gyH$$
$$\Rightarrow (gy)^{-1}gx \in H \Rightarrow y^{-1}x \in H$$
$$\Rightarrow xH = yH$$

إذن T_g هي دالة متباينة . علاوة على ذلك ، أي مجموعة مشاركة يسارية $xH \in S$ يمكن كتابتها بالشكل $g(g^{-1}xH)$ فإذا T_g هي دالة شاملة .

وأبعد من ذلك أي مجموعة مشاركة يسارية $xH \in S$ ممكن أن تكتب على الشكل $g(g^{-1}xH)$ لذلك T_g شاملة ، وبالتتابع $T_g \in A(s)$ ، ومرة أخرى $\theta(gh) = T_{gh}$ حيث أن

$$T_{gh}(xH) = (gh)xH = g(hxH) = T_g(hxH) = T_gT_h(xH)$$
$$\Rightarrow T_{gh} = T_gT_h$$

لذلك $\theta(gh) = T_gT_h = \theta(g)\theta(h)$ ، وهذا يقودنا إلى أن θ هي هومومورفزم من G إلى $A(s)$ ، والآن

$$g \in \ker \theta \Rightarrow T_g = I$$

حيث أن I هو العنصر المحايد في $A(s)$ ، وهذا يعطي

$$T_g(xH) = xH$$

لكل قيم $x \in H$ لكل قيم $x \in H$

$$\Rightarrow gxH = xH$$
$$\Rightarrow geH = eH \Rightarrow gH = H \Rightarrow g \in H$$

لذلك $\ker \theta \subseteq H$ ، وأبعد من ذلك إذا كانت N زمرة جزئية عادية من G ، محتواة في H فإن كل $n \in N$

$$\theta(n) = T_n$$

حيث أن

$$T_n(xH) = nxH = x(x^{-1}nx)H$$

لكل قيم $x \in G$ ولكن N هي زمرة جزئية طبيعية من G ، $x^{-1}nx \in N \subseteq H$ وهذا يؤدي إلى أنه $x^{-1}nx \in H$ ، ولذلك تحصل على أن

$$T_n(xH) = xH$$

ولكل قيم $x \in G$ أو بمعنى آخر $T_n = I$ لذلك $n \in \ker\theta$ ، وبالتتابع $\ker\theta$ هو أكبر زمرة جزئية طبيعية في G محتواة في H .

التمرين السادس

إذا كانت G زمرة منتهية و $H \neq G$ هو زمرة جزئية من G ، بحيث أن $\theta(G)\mathrm{l}i(H)!$ فإن H يجب أن تحتوي على زمرة جزئية طبيعية غير ناضة في G .

الحل

من التمرين الخامس أعلاه ، $\ker\theta \subseteq H$ لذلك $H \neq G$ و $\ker\theta \neq G$ ، وأبعد من ذلك $\ker\theta = \{e\}$ حيث أن e هي العنصر المحايد في G ، لذلك $T \cong \frac{G}{\ker\theta}$ حيث أن T هي زمرة جزئية من $A(s)$ تعطي $\theta(G) = \theta(T)$ يجب أن تكون معامل لـ $\theta[A(s)]$ ولكن $\theta[A(s)] = i(H)!$ وهذا يقودنا إلى أن $\theta(G) \mid i(H)!$ وهذا تناقض للنظرية . لذلك $\ker\theta \neq \{e\}$ وهذا يعني أن H تحتوي على زمرة جزئية طبيعية غير تافهة من G .

التمرين السابع

G زمرة من الرتبة $2n$ ، حيث أن n فردي ، بين أن G تملك زمرة جزئية طبعية من الرتبة n .

الحل

G تحتوي على عنصر واحد على الأقل من الرتبة 2 وألا تستطيع أن تجزء G إلى اتحاد أزواج منفصلة $\{a, a^{-1}\}$ ، $\{b, b^{-1}\}$ ، ... وعنصر فردي $\{e\}$ حيث أن $\{e\}$ هو العنصر المحايد في G ، وهذا يؤديث إلى أن عدد العناصر في G هو عدد فردي ، لذلك ليكن

$a \in G$ من الرتبة 2 . افرض أن T_a حيث أن $T_a(x) = \theta x$ لكل قيم $x \in G$ و T_a هي تبديل في المجموعة G (تحقق ؟) ، لذلك

$$T_a^9(x) = T_a[T_a(x)]$$
$$= T_a(ax) = a^2x = ex = x$$

لكل مدارات T_a التي تحوي عنصرين وعدد مختلف من المدارات في $T_a = 2n / 2 = n$ ولكل مدار معتمداً على دارة ، T_a لها n من الدارات كل منها بطول 2 ، ليكن $\sigma_1, \sigma_2, \ldots, \sigma_n$ كل الدارات الثنائية (التباديل الموقعية) لـ T_a . لذلك $T_a = \sigma_1\sigma_2 \ldots \sigma_n$ ولأن n فردية ، T_a هي تباديل فردية في $A(G)$ ليكن $K = \{T_g \mid g \in G\}$. K هي زمرة جزئية من $A(G)$ وأن $G \cong K$ تحت التطبيقي $f(g) = T_g$ (أثبت) ولأن $K, T_a \in K$ تحتوي على عدد فردي من التباديل ، لذلك G تحتوي على زمرة جزئية طبيعية $H = f^{-1}(N)$ من الدليل 2 ، ولكن

$$\theta(H) = \frac{\theta(G)}{i(H)} = \frac{2n}{2} = n$$

لذلك G تملك زمرة جزئية طبيعية من الرتبة 2 .

مسائل

1- أوجد مدارات الدارات للتباديل التالية وتمثيل كل منها على شكل ضرب داراتها :

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 1 & 6 \end{pmatrix}$

(iii) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ (iv) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

2- مثل التباديل التالية على شكل دارات متصلة :

(i) $(1\ 2\ 3)\ (4\ 5)\ (1\ 3\ 4\ \ 5)$

(ii) $(1\ 2)\ (5\ 4)\ (3\ 2)\ (1\ 7)\ (2\ 8)$

(iii) $(4\ 5)\ (1\ 2\ 3)\ (3\ 2\ 1)\ (5\ 4)\ (2\ 6)\ (1\ 4)$

3- ليكن f تبديل على مجموعة منتهية و $f = \sigma_1\sigma_2 \ldots \sigma_l$ تمثل f على شكل ضرب دارات منفصلة إذا كانت $\circ(\sigma_i) = m_i$ لكل i بين أن $\circ(f) = \text{lcm}$ لـ $m_1, m_2, \ldots m_l$.

4- لتكن $f = (a_1a_2 \ldots a_n)$ دارة طولها $n(> 1)$ برهن ما يلي :

(i) $f^{r-1}(a_1) = a_r \qquad 2 \le r \le n$

(ii) استنتج من (i) أنه $\circ(f) \ge n$

(iii) أثبت أن $f^n(a_i) = a_i \qquad 1 \le i \le n$

(iv) برهن أن $\circ(f) = n$

5- بين أن الدارة ذات الطول n هي إما فردية أو زوجية التباديل ، اعتماداً على n زوجية أو فردية .

6- باستخدام حقيقة أي مجموعة جزئية مغلقة منتهية ليست خالية من زمرة ، هي زمرة جزئية ، برهن كل مما يلي :

(i) $H = \{I, (1\,2)\,(3\,4), (1\,3)\,(2\,4), (1\,4)\,(2\,3\,1)\}$ هي زمرة جزئية طبيعية من A_4 .

(ii) $k = \{I, (1\,4)\,(2\,3)\}$ هي زمرة جزئية طبيعية من H .

(iii) k زمرة جزئية من A_4 ولكن k ليست طبيعية في A_4 (ذلك أن $k \subset H \subset A_4$ و k هي طبيعية في H و H طبيعية في A_4 على الرغم من ذلك k ليست طبيعية في A_4) .

7- برهن ما يلي :

(i) كل تبديل f في S_n $(n > 1)$ يمكن تمثيلية على شكل حاصل ضرب تبديل مواقع ، $(1\,2), (1\,3), \ldots, (1\,n)$.

(ii) أي تبديل f في S_n $(n > 1)$ يمثل تمثيلية على شكل حاصل ضرب $(1\,2), (2\,3), (3\,4), \ldots, (n-1, n)$.

إرشاد [استخدم الجزء i] .

(iii) $H = \{I, (1\,2)\}, K = \{I, (1\,2\,3), (1\,3\,2)\}$ هما زمرتان جزئيتان من S_4 بحيث أن كلاهما طبيعية ، ولكن $KH = HK$ (تم البرهان في مثال لزمرتين جزئيتين H, K التين ليستا طبيعيتين ولكن ضربهما HK زمرة جزئية) .

8- افرض أن $H = \{I, (1\,2)\}, K = \{I, (1\,3)\}$ زمرتين جزئيتين من S_3 ، أثبت أن $HK \neq KH$.

9- برهن أن الزمرة ذات الرتبة P^9 ، حيث أن P هو عدد أولي ، يجب أن تملك زمرة جزئية من الرتبة P .

10- G زمرة من الرتبة $2^k m$ حيث أن $k \geq 1$ عدد صحيح وأن m هو عدد فردي ، إذا كان G له زمرة جزئية دائرية من الرتبة 2^k ، برهن أن G لها زمرة جزئية طبيعية من الدليل 2^k .

11- لـ $a \in A_n$ ، تعرض $\pi_a : A_n \to A_n$ بواسطة $\pi_a(x) = axa$ لكل قيم $x \in A_n$ وليكن $C(A_n) = \{\pi_a \mid a \in A_n\}$ أثبت أن $\circ[C(A_n)] = \circ(A_n)$ لكل قيم $n \geq 4$.

12- إذا كان T, S مجموعتان منتهيتان بحيث أن $\circ(T) = \circ(S) = n$ فبرهن أن $S_n \cong T_n$.

13- يبين أن $Z(S_3)$ أو بمعنى آخر مركز S_3 يحتوي على التبديل المحايد فقط ! .

14- بين أن الزمرة $S = \bigcup_{n=1}^{\infty} S_n$ تحتوي بالضبط زمرة جزئية طبيعية واحدة A تختلف عن S و $\{e\}$ حيث أن $\{e\}$ هي العنصر المحايد في S ، وأكثر من ذلك A من الدليل 2 في S .

15- بين أن S_3 صورة هومومورفزم لـ S_4 .

3– أوتومورفزمات الزمر وبناء الزمر الدوارة

ليكن G زمرة $A(G)$ ترمز إلى مجموعة كل التباديل في G ، نحن نعرف أن $A(G)$ هي زمرة تحت ناتج التركيب ، ليكن $\mathrm{Aut}(G)$ ترمز إلى مجموعة كل الأوتومورفزمات في G ، من التعريف ، نعرف أن كل أوتومورفزم في G هو تطبيق متباين في G وشامل مع نفسه ، لذلك $\mathrm{Aut}(G) \subseteq A(G)$ ، نحن كذلك نعرف أن التطبيق المحايد هو أوتومورفزم ، وعلى أية حالة المسئلة هي حساب كل الأوتومورفزمات الممكنة في زمرة ، وبشكل عام صعب نوعاً ما حتى نستطيع أن نبرهن ما يلي :

نظرية 3-35

لأي زمرة G ، المجموعة $\mathrm{Aut}(G)$ لكل الأوتومورفزمات في G هي زمرة نحن نتائج التركيب .

البرهان

لأن التطبيق المحايد I في G هو في $\mathrm{Aut}(G) \neq \phi, \mathrm{Aut}(G)$.

(I) الانغلاق : ليكن $f, g \in \mathrm{Aut}(G)$ ، وأن f, g كلاهما تطبيق متباين من G إلى G ، $f \circ g$ هي كذلك تطبيقا متباين من G إلى G وأبعد من ذلك لأي $a, b \in G$

$$f \circ g(ab) = f[g(ab)] = [f(g(a)g(b)]$$

لذلك g هي أوتومورفزم ، كذلك f هي أوتومورفزم و $g(a), g(b) \in G$ ، لدينا

$$f[g(a)g(b)] = [f\{(g)\}][f\{g(b)\}] = [f \circ g(a)][f \circ g(b)]$$

أو بمعنى آخر

$$(f \circ g)\,(ab) = [f \circ g(a)][(f \circ g)\,(b)]$$

وبالتتابع $f \circ g$ هي أوتومورفزم و $f \circ g \in \mathrm{Aut}(G)$ ، وهذا يبرهن الانغلاق لـ $\mathrm{Aut}(G)$.

(II) **التجميع** : الآن النتائج لتركيب التطبيق هي بشكل عام تجميعية التركيب في $\mathrm{Aut}(G)$ هي كذلك تجميعية .

(III) **وجود العنصر المحايد** : لأن $I \in \mathrm{Aut}(G)$ وأن $f \circ I = f = I \circ f$ لكل $I, f \in \mathrm{Aut}(G)$ هو المحايد في $\mathrm{Aut}(G)$.

(IV) **وجود المعكوس** : ليكن $f \in \mathrm{Aut}(G)$ ، ولأن f هي تطبيق متباين وشامل في G إلى G ، f^{-1} معرف و f^{-1} كذلك تطبيق متباين في G وشامل من G إلى G ، والآن ليكن $a, b \in G$ لأن f شاملة ، يوجد $f(x) = a, f(y) = b$ وهذا يعطي أن $f^{-1}(a) = x, f^{-1}(b) = y$ وبالتتابع $ab = f(x)f(y) = f(xy) = f\left[f(x)f^{-1}(b)\right]$ ، لذلك $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$ ذلك أننا وجدنا f^{-1} هي إندومورفزم متباين من G إلى G ، لذلك f^{-1} هي أوتومورفزم في G ، وبالتتابع $f^{-1} \in \mathrm{Aut}(G)$ وهي لذلك $f \circ f^{-1} = f^{-1} \circ f = I$ لذلك $\mathrm{Aut}(G)$ هي زمرة .

ملاحظة

ويمكن برهان النتائج السابق بالأسلوب التالي :

$$f, g \in \mathrm{Aut}(G) \Rightarrow f \circ g^{-1} \in \mathrm{Aut}(G)$$

(لماذا ؟) . لذلك $\mathrm{Aut}(G)$ هي زمرة جزئية من $A(G)$ وهذا برهان أن $\mathrm{Aut}(G)$ هي زمرة .

قضية 3-36

ليكن G زمرة و $a \in G$ ، فإن التطبيق $f_a : G \to G$ والمعرف $f_a(x) = axa^{-1}$ هي أوتومورفزم في G ، وللبرهان انظر المثال 8 . □

تعريف 3-37 (الأوتومورفزم الداخلي)

ليكن a أي عنصر في الزمرة G ، الأوتومورفزم $f_a : G \to G$ والمعطى $f_a(x) = axa^{-1}$ لكل $x \in G$ لأي $x \in G, a \in G$ ،

$$f_a \circ f_{a^{-1}}(x) = f_a\left[f_{a^{-1}}(x)\right] = f_a\left[a^{-1}x(a^{-1})^{-1}\right]$$
$$= f_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x = I(x)$$

وهذا يؤدي إلى $f_a \circ fa^{-1} = I$ ، وبالمثل $f_{a^{-1}} \circ f_a \mid (x) = I(x)$ لذلك $fa^{-1} \circ f_a = I = f_a \circ fa^{-1}$ ، وبهذه الطريقة يتبين أن $(f_a)^{-1} = fa^{-1} \in In(G)$ كذلك لكل $f_a, f_b \in In(G)$ والحساب البسيط يبين أن $f_a \circ f_b = f_{ab} \in In(G)$ لذلك $In(G)$ هي زمرة جزئية من $\mathrm{Aut}(G)$ ، لكي تبين أن $In(G)$ هي زمرة جزئية طبيعية $\mathrm{Aut}(G)$ وهي فقط المتبقية لبرهان $\sigma \circ f_a \circ \sigma^{-1} in(G)\ \sigma \in Aut(G), f_a \in In(G)$

ليكن $x \in G$ وأن $\sigma \circ f_a \circ \sigma^{-1}(x) = (\sigma \circ f_a)\left[\sigma^{-1}(x)\right] = \sigma\left[a\sigma^{-1}(x)\, a^{-1}\right]$

$$= \sigma(a)\sigma\left[\sigma^{-1}(x)\right]\sigma(a^{-1}) = \sigma(a)\, x\left[\sigma(a)\right]^{-1}$$
$$= f_{\sigma(a)}(x)$$

لذلك $\sigma a f_a \circ \sigma^{-1} = f_{\sigma(a)} \in In(G)$.

والآن نفرض أن الجزء الأخير من النظرية ، لذلك نحضر التعريف $g : G \to In(G)$ بواسطة $g(a) = f_a$ لكل $a \in G$ ، لذلك

$$g(ab) = f_{ab} = f_a \circ f_b = g(a) \circ g(b)$$

لكل $a, b \in G$ تعطي g هي هومومورفزم ، g هي شاملة ، لذلك كل عنصر في $In(G)$ هو من الصيغة f_a وبواسطة التعريف $f_a = g(a)$ ، وبواسطة تطبيق أساسيات النظرية للهومومورفزم نحصل على $In(G) \cong \dfrac{G}{\ker g}$ ، وهذا سوف ينتج إذا برهنا أن $\ker g = Z(G)$.

الآن $a \in \ker g \Leftrightarrow g(a) = I$ والعنصر المحايد $In(G)$

$$\Leftrightarrow f_a = I \Leftrightarrow f_a(x) = I(x) \qquad \forall\ x \in G$$

$\Leftrightarrow axa^{-1} = x$ (تعريف f_a)

$\Leftrightarrow a \in Z(G)$ [تعريف $Z(G)$]

لذلك $\ker g = Z(G)$ وهذا يتمم البرهان □ .

ملاحظة

إذا كانت G زمرة غير إبدالية فإن $Z(G) \neq G$ وبالتتابع $G / Z(G)$ ليست زمرة بينة وأبعد من ذلك بسبب النظرية السابقة $In(G)$ هي كذلك ليست زمرة بينة ، وبالتتابع إذا كانت الزمرة G ليست إبدالية فإن G لا تملك أوتومورفزم غير بينة . إذا كانت الزمرة G إبدالية ، فإن كل أوتومورفزماتها الداخلية هي محايدة ، لذلك النظرية السابقة لا تحتاج لبرهاننا لغير الأوتومورفزمات غير المحايدة في الزمرة الإبدالية .

قضية 3-39

كل زمرة جزئية لزمرة دوارة هي دوارة .

البرهان

ليكن $G =< a >$ زمرة دوارة ، وليكن H زمرة جزئية من G إذا كان $H = (e)$ وببساطة H هي دوارة ، افرض أن $H \neq (e)$ لذلك يوجد $a^n \in H$ بحيث أن $a^n \neq e$ ، وأن $a^{-n} = (a^n)^{-1} \in H$ ، وكما n أو $-n$ هي صحيحة موجبة ، تستطيع أن تقول أن $a^n \in H$ لبعض القيم الموجبة الصحيحة لـ n . ليكن k أصغر عدد صحيح موجب بحيث أن $a^k \in H$ ، إثبتنا أن $H =< a^k >$ فإنه يؤدي إلى أن H هي زمرة دوارة .

لذلك ليكن $b \in H$ ، ولأن $b = a^m, b \in G$ لبعض القيم الصحيحة لـ m ، خوارزمية القسمة تعطي $m = kq + r$ لبعض القيم الصحيحة لـ q و r مع $\circ \leq r < k$ والآن $a^r = a^m(a^k)^{-q} \in H$ بأصغرية k يعطي $r = 0$ ، لذلك $m = kq$ و $b = (a^k)^q$ لذلك $H =< a^k >$ ، وهذا يبرهن القضية .

نتيجة 3-40

أي زمرة جزئية لزمرة الجمع للأعداد الصحيحة هي من الصيغة $< n >$ حيث أن n هي بعض الأعداد الصحيحة غير السالبة .

البرهان

لأن الزمـرة الجمعيـة للأعـداد الصـحيحة دوارة إذن النـاتج يتبـع مـن القضـية السابقة .

4- العناصر المترافقة

تعريف 3-48

لتكن G زمرة و $a, b \in G$ فإن a يسمى مرافق لـ b في G إذا وجد $c \in G$ بحيث أن $a = c^{-1}bc$ الرمز $a \sim b$ سوف برمز لكون a مرافق لـ b .

قضية 3-49

علاقة التكافؤ على الزمرة G هي علاقة تكافؤ .

البرهان

1- **الانعكاس** : لأن $a = a^{-1}aa$ ، $a \sim a$.

2- **التناظر** : $a \sim b \Rightarrow x^{-1}bx$ لبعض $x \in G$.

$$\Rightarrow b = xax^{-1} = y^{-1}ay$$

حيث $y = x^{-1}$ $\quad \Rightarrow b \sim a$

3- **التعدي** : $a \sim b, b \sim c$

$$\Rightarrow a = x^{-1}bx, b = y^{-1}cy$$

لبعض $x, y \in G$

$$\Rightarrow a = x^{-1}(y^{-1}cy)x = (yx)^{-1}c(yx)$$
$$\Rightarrow a \sim c$$

وهذا تمام البرهان .

القضية أعلاه تبين أنه يمكن تجزئة الزمرة G إلى صفوف تكافؤ تحت علاقة الترافق كل صف تكافؤ يسمى صف ترافق . لأي $a \in G$ ، $c(a)$ يرمز لصف الترافق والذي a تنتمي إليه ، أي أن $c(a) = \{b \in G = a \sim b\}$ بمعنى $c(a)$ يتضمن جميع العناصر من النوع $x^{-1}ax$ لذلك $a \in Z(G)$ إذا وفقط إذا كانت $C(a) = \{a\}$ وكحالة خاصة $C(e) = \{e\}$.

لتكن G زمرة منتهية ولتكن $C(a_1), C(a_2), \dots, C(a_t)$ مجموعة كل صفوف الترافق من G ولتكن $Ca_1, Ca_2, \dots, Ca_t$ هي رتبها حسب الترتيب لأنها تكون منفصلة مثنى مثنى ولأن اتحادها يعطي G نحصل على أن $\circ(G) = \sum_{i=1}^{t} Ca_i$ أو أكثر اختصاراً $\circ(G) = \sum_{a} C_a$ حيث أن المجموع يتحرك على جميع العناصر a يأخذ صفوف الترافق واحدة تلو الأخرى ، لذلك سيكون الهدف هو تحديد طبيعة C_a وعلاقتها بصف تكافؤها .

تعريف 3-50 (مركز أو منظم العنصر)

لأي عنصر في الزمر G المجموعة $N(a) = \{x \in G \mid ax = xa\}$ تسمى مركز أو منظم a في G .

قضية 3-51

لأي $a \in G$ ، $N(a)$ هي زمرة جزئية من G .

البرهان

إذا كان e هو محايد G فإن $ea = ae$ يعطي أن $e \in N(a)$ فإذاً $N(a) \neq \phi$.

لتكن $y \in N(a), x \in N(a)$ فإن :

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$$

فإذاً $xy \in N(a)$

مرة أخرى $$ax = xa \Rightarrow x^{-1}a = ax^{-1} \Rightarrow x^{-1} \in N(a)$$

إذاً $N(a)$ هي زمرة جزئية من G .

نظرية 3-52

إذا كانت G زمرة منتهية و $a \in G$ فإن $C_a = \dfrac{\circ(G)}{\circ [N(a)]}$.

البرهان

ليكن $\circ(G) = n$ إذا كان $tdN(a)$ من المجموعات المشاركة المختلفة $N(a)x_1, N(a)x_2, \ldots, N(a)x_t$ فإننا نعلم $t = \dfrac{\circ(G)}{\circ (N(a))}$.

الآن

$$\begin{aligned}
& 1 \leq i, j \leq t, x_i^{-1}ax_i = x_j^{-1}ax_j \\
\Rightarrow \quad & x_i x_j^{-1} a x_j x_i^{-1} = a \Rightarrow x_i x_j^{-1} a (x_i x_j^{-1})^{-1} = a \\
\Rightarrow \quad & (x_i x_j^{-1})a = a(x_i x_j^{-1}) \Rightarrow x_i x_j^{-1} \in N(a) \\
\Rightarrow \quad & N(a)x_i = N(a)x_j \Rightarrow i = j
\end{aligned}$$

ولأن $N(a)x_i$ جميعهم مختلفون فإذاً $x_i^{-1}ax_i = x_j^{-1}ax_j \Rightarrow i = j$ ، إذاً

$x_1^{-1}ax_1, x_2^{-1}ax_2, \ldots, x_t^{-1}ax_t$

جميعها مرافقات a مختلفة إذا بينا أن هذه هي المترافقات الوحيدة لـ a ينتج أن $C(a)$ تحوي t عنصر فقط ، أي أن $C(a) = t = \frac{\circ(G)}{\circ[N(a)]}$ افرض لبعض $x \in G$ $b = x^{-1}ax$. لأن $G = \bigcup_{i=1}^{t} N(a)x_i, x = cx_i$ لبعض $c \in N(a)$ ولبعض الأعداد الموجبة i لذلك $x^{-1}ax = (cx_i)^{-1}a(cx_i) = x_t^{-1}(c^{-1}ac)x_i = x_i^{-1}ax_i$ لأن $c^{-1}ac = a$. إذاً أي مترافق b لـ a يساوي $x_i^{-1}ax$ وهذا يثبت أن a لها فقط t من المترافقات $x_i^{-1}ax_i, i = 1, 2, \ldots, t$ وهذا هو برهان النظرية . □

نتيجة 3-53

لأي زمرة منتهية $\circ(G) = \sum_a \frac{\circ(G)}{\circ(N(a))}$ حيث أن المجموع يجري على عناصر a مأخوذاً كل واحد على أنه صف ترافق .

البرهان

لتكن $C(a_1), C(a_2), \ldots, C(a_k)$ جميع صفوف التكافؤ المختلفة على G فإن حقيقة كون هذه الصفوف منفصلة مثنى مثنى واتحادها يعطي G تعطي أن $\circ(G) = \sum_{i=1}^{k} Ca_i$ حيث $Ca_i = \circ[C(a_i)]$ والنظرية السابقة تعطي $Ca_i = \frac{\circ(G)}{\circ(N(a_i))}$ إذاً $\circ(G) = \sum_{i=1}^{k} \frac{\circ(G)}{\circ(N(a_i))}$ وهذا برهنان النتيجة . □

نتيجة 3-54

لتكن G زمرة منتهية و $Z(G)$ هو مركزها فإن $\circ(G) = \circ(Z(G)) + \sum_a \frac{\circ(G)}{\circ(N(a))}$ حيث أن المجموع مأخوذ على العناصر a بأخذ واحد من كل صف ترافق يحتوي على أكثر

من عنصر يسمى معادلة الصف على الزمرة G ، نرغب تمرير ملاحظة هي أن معادلة الصف تلعب دوراً مهماً في تطوير بناء الزمر المنتهية الغير إبدالية ، القاريء المهتم يمكن أن يجد أنها ستستخدم في الفصل اللاحق ، وقبل أن ينتهي البند ، نبرهن نتيجتين على الزمر بواسطة معادلة الصف .

نظرية 3-56

إذا كان $\circ(G) = p^n$ حيث p عدداً أولياً فإن $Z(G) \neq (e)$.

البرهان

لتكن $z = \circ(Z(G))$ بواسطة معادلة الصف

$$p^n = Z + \sum_a \frac{\circ(G)}{\circ\left[N(a)\right]} \qquad (1)$$

حيث أن المجموع يأخذ على عناصر a بأخذ واحد من كل صف ترافق $C(a)$ لها أكثر من عنصر واحد (أي أن $a \notin Z(G)$) الآن لأي $a \notin Z(G)$ ، $\circ(N(a)) < \circ(G) = p^n$ و $\circ(N(a)) \mid \circ(G)$ تعطي أن $\circ(N(a)) = p^{na}$ لبعض $1 \leq n_a < n \Rightarrow p \mid \frac{\circ(G)}{\circ(N(a))}$ ، وأيضاً $p \mid p^n$ فإذاً بواسطة (1) نحصل على $p \mid z$ وهذا يبرهن أن :

$$p \mid \circ(Z(G)) \Rightarrow \circ(Z(G)) > 1 \Rightarrow Z(G) \neq (e)$$

نتيجة 3-57

إذا كان $\circ(G) = p^2$ حيث p عدداً أولياً ، فإن G إبدالية .

البرهان

لأن G زمرة إبدالية إذا وفقط إذا كان $Z(G) = G$ يكفي أن نبين أن $\circ(G) = p^2 \Rightarrow Z(G) = G$. لتكن $\circ(G) = p^2$ بواسطة نظرية لاكرانج $\circ(Z(G)) \mid p^2$ ،

لذلك $\circ(Z(G)) = 1$ أو p أو p^2 ، وبواسطة النظرية 3-56 ، $\circ(Z(G)) \neq 1$ ، إذاً $\circ(Z(G))$ تساوي p أو p^2 . افرض أن $\circ(Z(G)) = p$ وافرض أن $a \in G$ بحيث أن $a \notin Z(G)$ ، لأنه لأي $b \in N(a), ba = ab, b \in Z(G)$ وهكذا $Z(G) \subseteq N(a)$ وأيضاً $a \in N(a)$ ولكن $a \notin Z(G)$ ، إذاً $N(a) \neq Z(G)$ ينتج أن $\circ(N(a)) > \circ(Z(G)) = p$ ولكن $\circ(N(a)) \mid p^2$ وهكذا $\circ(N(a)) = p^2$ و $N(a) = G$ ، هذا يؤدي إلى أن $a \in Z(G)$ وهذا يناقض الفرض $a \notin Z(G)$ لذلك $\circ(Z(G)) = p^2$ ، ولذلك $G = Z(G)$ وهذا تمام البرهان □ .

تمارين محلولة

تمرين 1

تبديلان σ و η لمجموعة منتهية S يسميان متماثلان إذا وجد دالة متباينة من الدورة σ إلى η بحيث أن الدورة لها نفس الطول . بين أن تبديلان من مجموعة منتهية S متماثلان ، إذا وفقط إذا كانا مترافقان .

الحل

ليكن σ و η مترافقان فيوجد $g \in S_n$ بحيث أن $\eta = g^{-1}\sigma g$ ، لتكن $\sigma = (a_1a_2 \dots a_t)(b_1b_2 \dots b_n) \dots (c_1c_2 \dots c_s)$ حيث $a_i, b_j, \dots, c_k \in S$ لكل $1 \leq i \leq t, 1 \leq j \leq n, \dots, 1 \leq k \leq s$ وكل الدوارات على اليمين تكون منفصلة مثنى مثنى وكل عنصر في S هو من نفس الدورة لأن g هو راسم شامل فيمكن نجد $e_1, e_2, \dots, e_t, \dots, f_1 f_2, \dots, f_n, \dots, l_1, l_2, \dots, l_s$ بحيث أن

$$g(e_i) = a_i \ \forall 1 \leq i \leq t, g(f_i) = b_i$$
$$\forall 1 \leq j \leq n, \dots, g(l_k) = c_k \quad \forall 1 \leq k \leq s$$

فإن $\eta = g^{-1}\sigma g = (e_1e_2 \dots e_t)(f_1f_2 \dots f_n)\dots(l_1l_2 \dots l_s)$

بما أن g هي متباينة فإن طول كل دورة [تحت التابع

$(a_1a_2 \dots a_t) \leftrightarrow (e_1, e_2, \dots e_t), (b_1b_2 \dots b_n) \leftrightarrow (f_1, f_2, \dots, f_n) \dots$
$(c_1c_2 \dots c_s) \leftrightarrow (l_1l_2 \dots l_s)$]

تكون متساويات ، إذاً σ و η هما متماثلان .

ينتج أن σ و η تبادلان متماثلان في S_m ونستطيع كتابة

$$\sigma = (a_1a_2 \dots a_t)(b_1b_2 \dots b_n)\dots(c_1c_2 \dots c_s)$$
$$\eta = (x_1x_2 \dots x_t)(y_1y_2 \dots y_n)\dots(z_1z_2 \dots z_s)$$

حيث $t, n \dots s$ هي أعداد صحيحة أكبر أو تساوي 1 ، بحيث أن $t + n + \dots + s = m$

ضع

$$h = \begin{pmatrix} a_1, a_2, \dots, a_t, & b_1, b_2, \dots, b_n & , \dots, & c_1, c_2, \dots, c_s \\ x_1, x_2, \dots, x_t, & y_1, y_2, \dots, y_n & , \dots, & z_1, z_2, \dots, z_s \end{pmatrix}$$

ويمكن التحقق بأن h هو تبديل في S_m لأن

$$(h^{-1}nh)(a_1) = h^{-1}\eta(x_1) = h^{-1}(x_2) = a_2, \dots, (h^{-1}\eta h)(a_t) =$$
$$h^{-1}\eta(x_t) = h^{-1}(x_1) = a_1, h^{-1}\eta h(b_1) = h^{-1}\eta(y_1) = h^{-1}(y_2) = b_2$$
$$\dots h^{-1}\eta h(b_n) = h^{-1}\eta(y_n) = h^{-1}(y_1) = b_1 \dots h^{-1}\eta h(c_1) =$$
$$h^{-1}\eta(z_1) = h^{-1}(z_2) = c_2, \dots, h^{-1}\eta h(c_s) = h^{-1}\eta(z_s) =$$
$$h^{-1}(z_1) = c_1$$

نحصل على $h^{-1}\eta h = \sigma$ فإذاً σ و η مترافقات .

تمرين 2

خذ أي عدد صحيح موجب ، متتابعة الأعداد الموجبة $n_1, n_2, \dots, n_r$ بحيث أن $n_1 \geq n_2 \geq \dots \geq n_r$ و $n = n_1 + n_2 + \dots + n_r$ تسمى تجزئة n ولتكن $p(n)$ يمثل عدد التتجزئات لـ n بين أن عدد صفوف الترافق في s_n هو $p(n)$.

لاحظ ، لأن $1 = 1$ هو التجزئة الوحيدة لـ 1 $p(= 1) = 1$ ، $2 = 2$ و $2 = 1 + 1$ هما التجزئتان لـ 2 إذاً $p(2) = 2$ ، $3 = 3$ ، $3 = 2 + 1$ ، $3 = 1 + 1 + 1$ هي التجزئات الثلاثة لـ 3 إذاً $p(3) = 3$ ، ونترك للقارئ التحقق من أن $p(4) = 5, p(5) = 7, p(6) = 11$.

الحل

لتكن $\sigma \in S_n$ يمكننا كتابة σ على شكل حاصل ضرب من دوريات منفصلة $(a_1a_2 \dots a_{r_1})(b_1b_2 \dots b_{r_2}) \dots (c_1c_2 \dots c_{r_k})$ بحيث أن $r_1 \geq r_2 \geq \dots \geq r_k$ و $r_1 + r_2 + \dots + r_k = n$ وهذا يساوي التجزئة بواسطة التمرين السابق فإن تبديلان مترافقان إذا وفقط إذا كانا متماثلان ، أي بمعنى آخر يعطيان نفس التجزئة بالنسبة لصفوف الترافق ، نحصل على تجزئة وحيدة لـ n وبالعكس نأخذ التجزئة $n_1 \geq n_2 \geq \dots \geq n_s, n_1 + n_2 + \dots + n_3 = n$ هناك تبديل f يكون له الدورة من النوع

$$(\alpha_1\alpha_2 \dots \alpha_{n_1})(\beta_1\beta_2 \dots \beta_{n_2}) \dots (\delta_1\delta_2 \dots \delta_{n_s})$$

كل $g \in S_n$ تماثل f هي مترافقة مع f وكل تبديل في S_n مترافق مع f هو متماثل مع f في هذا الاعتبار نأخذ أي تبديل يمكن تحديد صف مرافق وحيد لـ f إذاً يوجد تمثيل متباين بين صفوف الترافق في S_n وتجزئة لـ n ، لأنه يتبع عدد صفوف الترافق في S_n يساوي $p(n)$.

تمرين 3

لتكن G زمرة منتهية ، افرض أن أوتومورفزم f في G ترسل أكثر من ثلاثة أرباع عناصر G إلى معكوساتها . أثبت أن G هي زمرة إبدالية وأن

$$f(x) = x^{-1} \quad \forall \quad x \in G$$

الحل

افرض أن G زمرة غير إبدالية فإذن $Z = Z(G) \neq G$ هذا يعطي

$$\circ(Z) \leq \tfrac{1}{2} \circ (G) \Rightarrow \circ (G - Z) \geq \frac{\circ(G)}{2}$$

لذلك بسبب الفرضية يوجد $x \in G - Z$ بحيث أن $f(x) = x^{-1}$ مرة أخرى

$$x \in G - Z \Rightarrow N(x) \neq G \Rightarrow \circ\left[N(x)\right] \leq \frac{\circ(G)}{2}$$

$$\Rightarrow \circ\left[G - N(x)\right] \geq \frac{\circ(G)}{2}$$

ولأن f ترسل أكثر من ثلاثة أرباع عناصر الزمرة G إلى معكوساتها ، يوجد $y \in G - N(x)$ بحيث أن $f(y) = y^{-1}$ لكن

$$S = \left\{y \in G - N(x) \mid f(y) = y^{-1}\right\}$$

الشرط المعطى على f يعطي $\circ(S) > \frac{\circ(G)}{4}$ ، المجموعة $xS = \{xs \mid s \in S\}$ كل عناصرها مختلفة ، ولذلك $\circ(xS) = \circ(S) > \frac{\circ(G)}{4}$.

ندعي أن لأي من $z \in xS$ ، $f(z) \neq z^{-1}$ ، وما عدا ذلك لتكن $z \in xS$. بحيث أن $f(z) = z^{-1} \Rightarrow f(xs) = (xs)^{-1}$ لبعض

$$s \in S \Rightarrow f(x)f(s) = s^{-1}x^{-1} \Rightarrow x^{-1}s^{-1} = s^{-1}x^{-1} \Rightarrow xs = sx \Rightarrow s \in N(x)$$

وهذا يخالف لتعريف S . لذلك ادعاؤنا قد تحقق .

لهذا يوجد أكثر من $\frac{\circ(G)}{4}$ عناصر (أي ، عناصر xs) التي لا يمكن أن ترتبط تطبيقياً بمعكوساتها . وهذا يخالف الشرط المفروض على f ، لذلك $G = Z$.

أخيراً لتكن H . $H = \left\{x \in G \mid f(x) = x^{-1}\right\}$ و H زمرة جزئية من G لأن G هي إبدالية . لذلك إذا $H \neq G$ ، سنحصل على $\circ(H) \leq \frac{\circ(G)}{2}$ ،

أي أن عـدد العناصر مـن G الـذي يـرتبط تطبيقيـاً بمعكوسـاتها يكـون أقـل مـن أو مسـاوٍ لـ $\frac{\circ(G)}{2}$. وهذا خلاف الفرض . لأن $H = G$. وبكلمات أخرى

$$f(x) = x^{-1} \quad \forall \quad x \in G$$

مسائل

1- بين أن أزواج التباديل التالية متماثلة :

(i) $(1\ 2)$ ، $(1\ 3)$.

(ii) $(1\ 2)$ $(3\ 4)$ ، $(1\ 4)$ $(2\ 3)$

(iii) $(1\ 2\ 3)$ $(4\ 5)$ ، $(1\ 4\ 5)$ $(2\ 3)$

(iv) $(1\ 3\ 4)$ $(2\ 5\ 6)$ ، $(1\ 5\ 6)$ $(3\ 4\ 2)$

2- العنصر في مركز الزمرة يسمى عنصر مترافق ذاتياً . بين أن فقط العنصر المترافق ذاتياً في أي S_n لـ $n \geq 3$ هو المحايد . بمعنى أن $Z(S_n) = I$ لجميع $n \geq 3$ أثبت أن زمرة 4 كليف هي زمرة جزئية نامية من A_4 .

3- أثبت أن زمرة منتهية غير تافهة كل عنصر فيها غير المحايد يتبادل مع نصف عناصر الزمرة بالضبط .

4- لتكن G زمرة $a \in G$ بحيث أن a له فقط مترافقان استخدم حقيقة كون أن أي زمرة جزئية من G من الدليل 2 هي ناظمية واستنتج أن $N(a)$ هي زمرة جزئية ناظمية في G .

5-

(a) لتكن H زمرة إبدالية من الرتبة p^n ، حيث p عدداً أولياً بين بواسطة الاستنتاج على n أنه توجد زمر جزئية

$$H = H_0 > H_1 > H_2 > \ldots > H_n = (e)$$

من الرتب $p^n, p^{n-1}, \ldots, p, p^0 = 1$ بحسب الترتيب .

(b) استخدم (a) لتبين أنه إذا كانت $\circ(G) = p^n$ (G قد لا تكون إبدالية) فإنه يوجد زمر جزئية $N_i (i = 0, 1, 2, \dots, n)$ من الرتب $p^i (i = 0, 1, 2, \dots, n)$ بحيث أن $N_0 > N_1 > \dots > N_n = (e)$ وكل N_{i+1} هي ناظمية في N_i لأي $i = 0, 1, 2, \dots, n-1$.

[إرشاد $Z(G) \neq (e)$ **]** .

6- إذا كانت G زمرة غير إبدالية من الرتبة p^3 حيث p عدداً أولياً بين أن $\circ[Z(G)] = p$.

[إرشاد : استخدم الحقيقة ، إذا كانت $\frac{G}{Z(G)}$ دوارة فإن G إبدالية**]** .

7- إذا كانت G زمرة من الرتبة p^n و p عدد أولي و $H \neq G$ هي زمرة جزئية من G ، بين أنه يوجد $a \in G, a \notin H$ بحيث أن $aHa^{-1} = H$.

8- إذا كانت G زمرة من الرتبة p^n و p عدد أولي وإذا كان $N \neq \{e\}$ هي زمرة جزئية ناظمية من G برهن أن $N \cap Z(G) \neq \{e\}$ حيث أن $Z(G)$ هي مركز G .

9- أعطي مثالاً لزمرة G من الرتبة p^n و p عدد أولي وزمرة جزئية $H \neq \{e\}$ من G برهن أن $H \cap Z(G) = \{e\}$ حيث $Z(G)$ هو مركز G .

10- أعطي مثالاً لأوتومورفزم لزمرة غير إبدالية منتهية G والتي ترسل ثلاثة أرباع عناصر G بالضبط إلى معكوساتها .

11- لتكن θ هومومورفزم من الزمرة G إلى نفسها بحيث أن $\theta f = f\theta$ لكل $f \in \text{Aut}(G)$. ولتكن K مجموعة كل العناصر $x \in G$ بحيث أن $\theta^2(x) = \theta(x)$. بين أن K هي ناظمية من G و G/K هي إبدالية .

12- في أي زمرة G المجموعة الجزئية f المتكونة من جميع العناصر التي لها عدد منتهي من المترافقات في G هو مميز الزمرة الجزئية ، برهن ذلك .

13- الزمرة G تسمى زمرة FC (زمرة مرافق منتهي) إذا وفقط إذا كل $x \in G$ لها فقط عدد منتهي من المترافقات . برهن الآتي :

(i) الزمرة المنتهية هي زمرة FC .

(ii) الزمرة الإبدالية هي زمرة FC .

(iii) إذا كان $[G : Z(G)]$ منتهية فإن G هي زمرة FC .

(iv) الزمرة الجزئية أو زمرة القسمة لزمر FC هي زمرة FC .

14- بين أن $Z(G) = \cap\{C(x) \mid x \in G\}$ حيث $C(x) = \{y \in G \mid yx = xy\}$

15- لتكن y, x عنصران في زمرة G برهن أن :

(i) $C(x) \subseteq C(y)$ إذا وفقط إذا كانت $y \in Z[C(x)]$.

(ii) $C(x) \subseteq C(y)$ إذا وفقط إذا كانت $Z[C(x)] \supseteq Z[C(y)]$.

16- حدد جميع صفوف الترافق في S_4 .

4

نظرية التركيب في الزمرة

Structure Theory of Groups

في هذا الفصل سوف نناقش بعض المسائل والمفاهيم المنتقاه في نظرية الزمر ، وفهم برهان كل منها لأهميتها البالغة ، وفهم التركيب الداخلي للزمر .

1. الضرب المباشر

لتكن G زمرة ، لقد ناقشنا سلفاً الزمر الجزئية وزمر القسمة للزمرة G (في الفصل الثاني والثالث) والحقيقة كانت هذه زمراً جديدة منشأة من G ، هناك عدة طرق أخرى لبناء زمر جديدة من واحدة أو أكثر من زمرة معطاة ، تلك الزمر تختلف عن فصول الزمر الجزئية وزمر القسمة ، أحدى الطرق بالغة الأهمية هي طريقة تكوين الضرب المباشر للزمر . وفي هذا الفصل نناقش مفهوم الضرب المباشر ونعطي بعضاً من تطبيقاته .

نظرية 1.4

ليكن $G_1, G_2, ..., G_n$ هي n من الزمر ، وأن $G = G_1 \times G_2 \times G_3 ... \times G_n$ هو الضرب الكارتيزي لها ، فإذا كان $a = (a, a_2, ..., a_n), b = (b_1, b_2, ..., b_n)$ تنتمي إلى G فإن ab يعرف على إنه

$$ab = (a_1 b_1 , a_2 b_2 ... , a_n b_n)$$

وتكون G زمرة تحت هذا التركيب .

البرهان

ليكن $a = (a_1, a_2 ..., a_n)$ و $b = (b_1, b_2, ..., b_n)$ و $c = (c_1, c_2, ..., c_n)$ تنتمي إلى G لكل $e_i, i = 1, 2, ..., n$ هو العنصر المحايد لـ G_i وكذلك $e = (e_1, e_2, ..., e_n)$.

(1) الانغلاق

مــن التعريــف $ab = (a_1b_1, a_2b_2, \dots, a_nb_n)$ فــإن a_ib_i ينتمــي إلى G_i ,$1 \le i \le n$ لذلك نحصل على $ab \in G$ وهذا يبرهن أن G مغلقة تحت عملية التركيب .

(2) التنسيق

الآن $a(bc) = (a_1, a_2 \dots, a_n)(b_1c_1, b_2c_2, \dots, b_nc_n)$

$$= [a_1(b_1c_1), a_2(b_2c_2), \dots, a_n(b_nc_n)]$$

وبالمثل $(ab)c = [(a_1b_1)c_1, (a_2b_2)c_2, \dots, (a_nb_n)c_n]$

لذلك فإن $a_i(b_ic_i) = (a_ib_i)c_i$ لكل قيم i ومنها نحصل على $(ab)c = a(bc)$.

(3) وجود العنصر المحايد

بما أن $ae = (a_1e_1, a_2e_2, \dots, a_ne_n)$

$$(a_1, a_2, \dots, a_n) = (e_1a_1, e_2a_2, \dots, e_na_n) = ea$$

لكل a ينتمي إلى G .

إذاً العنصر e المحايد ، موجود في G .

(4) وجود النظائر

لكـــــل $a = (a_1, a_2, \dots, a_n)$ معطـــــاة تعنتمـــــي إلى G وإذا كـــــان $a' = (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$

فإن $aa' = (a_1a_1^{-1}, a_na_2^1, \dots, a_na_n^{-1})$

$$= (e_1, e_2, \dots, e_n)$$

وبالمثــل $a'a = e$ ولــذلك فــإن $a^{-1} = a'$ وهــي تنتمــي إلى G . وهــذا يــبرهن أن G هــي زمرة .

طالما برهنا النظرية السابقة فإننا الآن نعرف الضرب الخارجي المباشر للزمر .

تعريف 4.2 الضرب الخارجي المباشر

ليكن $G_1, G_2, ..., G_n$ عدداً منتهياً من الزمر $G = G_1 \times G_2 \times ... \times G_n$ فإن G هي زمرة تحت التركيب الثنائي المعرف على أنه $ab = (a_1b_1, a_2b_2, ..., a_nb_n)$ لكل العناصر $a = (a_1, a_2, ..., a_n)$ و $b = (b_1, b_2, ..., b_n)$ في G هذه الزمر تسمى الضرب الخارجي المباشر للزمر G_i .

إذا كانت كل الزمر آبيلية وعمليات التركيب كلها جمعية ، فإننا عادة نشير لهذه التركيبات الجمعية في G كجمع مباشر لـ $G_1, G_2, ..., G_n$ ، لذلك نكتبها بالصورة $G = G_1 \oplus G_2 \oplus G_3 \oplus ... \oplus G_n$.

مثال 1

ليكن $G = Z \times Z$ حيث أن Z هي زمرة جمعية للأعداد الصحيحة .

فعندما يكون $x = (n_1, m)\ y = (n_2, m_2) \in G, \chi + y = (n_1 + n_2, m_1 + m_2)$ فإن G تكون زمرة تحت هذا التركيب الجمعي .

هنا $(0,0)$ هو العنصر المحايد ، ولكل $(n,m) \in G$ يكون $(-n, -m)$ هو النظير .

مثال 2

ليكن Z هي زمرة الجمع للأعداد الصحيحة ، و C^* هي زمرة الضرب للأعداد المركبة غير الصفرية . افرض أن $G = Z \times C^*$ لكل $x = (x_1, Z_1), y = (x_2, Z_2) \in G$ نعرف $xy = (x_1 + x_2, z_1 z_2)$ فتكون G زمرة تحت هذا التركيب الثنائي $(0,1)$ هو العنصر المحايد ولكل $(n, x) \in G$ فإن نظيره هو $(-n, x^{-1})$.

مثال 3

لتكن $G_1 =< a >$ و $G_2 =< b >$ زمرتين دائريتين من الرتبة 2 و 3 على الترتيب إذا e_2, e_i العنصرين المحايدين لـ G_1 و G_2 على الترتيب فإن $G_1 = \{e_1, a\}$ و $G_2 = \{e_2, b, b^2\}$ ومنها $G = G_1 \times G_2$.

$$G = G_1 \times G_2 = \{(e_1, e_2), (e_1, b), (e_1, b^2), (a, e_2), (a, b), (a, b^2)\}$$

لكل $X = (a_1, a_2),\ y = (b_1, b_2) \in G$

تعرف $xy = (a_1, b_1, a_2, b_2)$

تحت هذا التركيب G تصبح زمرة بأخذ $u = (a, b)$ نرى أن :

$$u^2 = (a^2, b^2) = (e_1, b^2), u^3 = (a^3, b^3) = (a, e_2),$$
$$u^4 = (a^4, b^4) = (e_1, b), u^5 = (a^5, b^5) = (a, b^2),$$
$$u^6 = (a^6, b^6) = (e_1, e_2)$$

لذلك $G =< u >$ هو زمرة دائرية من الرتبة 6 .

نظرية 4.3

(1) ليكن $G_1, G_2, \ldots G_n$ عدداً منتهياً من الزمر و $G = G_1 \times G_2 \times \ldots \times G_n$ هو ضربها المباشر لكل $(1 \le i \le n)$ افرض أن e_i هو العنصر المحايد لـ G_i عندئذ يكون :

1- لكل i $G_i' = \{(e_1, e_2, \ldots e_{i-1}, a_i, e_{i+1}, \ldots, e_n) | a_i \in G\}$ هي زمرة جزئية طبيعية للزمرة G إيزومورفيك مع G_i .

2- لكل $a_{j'} \in G_j', a_i' \in G_i', i \neq j$ و $a_i' a_j' = a_j' a_i'$.

3- لكل $a \in G$ يمكن تمثيلها وشكل وحيد بالصورة $a_1' a_2' a_3' \ldots a_n'$ حيث يكون $a_i' \in G_i'$ بمعنى أنه إذا كان $a_i', b_i' \in G$ $a_1' a_2' \ldots a_n' = b_1' b_2' \ldots b_n'$ فإن $\forall_i$ $a_i' = b_i'$

البرهـان : لكـل i تعـرف $f:G_i \to G$ بالصـورة $f_i(a_i)=(e_1,e_2...e_{i-1},a_i,e_{i+1},...e_n)$ لكـل $a_i \in G_i$.

لأي $a_i,b_i \in G_i$ يكون

$$\begin{aligned} f_i(a_ib_i) &= (e_1, e_2, e_3...e_{i-1}, a_ib_i, e_{i+1}, ...e_n) \\ &= (e_1, e_2, e_3,...e_{i-1}, a_i, e_{i+1}, ..., e_n)(e_1, e_2, e_2b_i, e_{i+1}, e_n) \\ &= f_i(a_i)f_i(b_i) \end{aligned}$$

لذلك فإن f_i هي هومومورفيزم كما أن :

$$\begin{aligned} & f_i(a_i)=e=(e_1,e_2,e_i,...e_n) \Leftrightarrow a_i \in \ker f_i \\ & (e_1,e_2...e_{i-1},a_i,e_{i+1},...e_n) \Leftrightarrow \\ & =(e_1,e_2...e_{i-1},e_i,e_{i+1},...,e_n) \Leftrightarrow e_i=a_i \end{aligned}$$

لذلك فإن $\ker f_i=(e_i)$ وأن f_i مونوموفيزم لـ G_i إلى G لذلك فإن $f_i(G_i)\cong G_i$.

من تعريف G_i نلاحظ أن $f_i(G_i)=G_i'$ وبناء عليه فإن $G_i' \cong G_i$.

اعتبر أن $x=(x_1,x_2,...,x_n)\in G$ وأن $a_i' \in G_i'$ عندئذ يكون :

$$\begin{aligned} x^{-1}a_i'x &= (x_1^{-1}, x_2^{-1}, ..., x_n^{-1})(e_1, e_2,...e_i, e_{i+1}, ...e_n)(x_1, x_2, ...x_n) \\ &=(e_1,e_2,...e_{i-1},x_i^{-1}a_ix_i,e_{i+1},...e_n)\in G_i' \end{aligned}$$

لذلك فإن G_i' هي زمرة جزئية عادية في G .

(2) افرض أن

$$a_i'=(e_1,e_2...,e_{i-1},a_i,e_{i+1},...,e_n)\in G_i'$$

$$a_j'=(e_1,e_2...,e_{j-1},a_j,e_{j+1},...,e_n)\in G_j'$$

حيث $i \neq j$ فيكون

$$\begin{aligned} a_i'a_j' &=(e_1^2,e_2^2,...,a_ie_i,e_{i+1}^2,...,e_{j-1}^2,e_ja_j,e_{j+1}^2,...e_n^2) \\ &=(e_1,e_2...,a_i,e_{i+1},...,e_{j-1},a_j,e_{j+1},...,e_n) \end{aligned}$$

وكذلك

$$a_j'a_i'=(e_1,e_2...,e_{i-1},a_i,e_{i+1},...,e_{j-1},a_j,e_{j+1},...,e_n)$$

أي أن $a_i'a_j'=a_j'a_i'$.

(3) افرض أن $a=(a_1,a_2...,a_n)\in G$

واضح أن
$$a=(a_1e_2,e_3,\dots,e_n)(e_1,a_2,e_3,\dots e_n)\dots(e_1,e_2,\dots a_n)$$
$$=a_1{'}a_2{'}a_3{'}\dots a_n{'}$$

حيث أن
$$a_1{'}=(a_1,e_2,e_3,\dots e_n)\in G_1{'},\dots a_n{'}=(e_1,e_2,\dots,a_n)\in G_n{'}$$

سوف نبين الآن أن المتتابعة $a_1{'},a_2{'},\dots,a_n{'}$ وحيدة .

افرض كذلك أن $b_i{'}\in G_i{'}$ حيث $a=b_1{'}b_2{'}b_3{'}\dots b_n{'}$.

من التعريف
$$b_1{'}=(b_1,e_2,e_3,\dots,e_n),b_2{'}=(e_1,b_2,e_3,\dots,e_n)$$
$$\dots=b_n{'}=(e_1,e_2,\dots,e_{n-1},b_n)$$

لبعض العناصر $b_1\in G_1{'},b_2{'}\in G_2{'},\dots,b_n{'}\in G_n{'}$ هذا يعطي :
$$a=(b_1,b_2,b_3,\dots,b_n)$$

كما أعطى
$$a=(a_1,a_2,\dots,a_n)$$

فبناءاً عليه
$$(a_1,a_2,a_3,\dots,a_n)=(b_1,b_2,b_3,..b_n)$$
$$\Rightarrow a_i=b_i\forall_i\Rightarrow a_i{'}=b_i{'}$$

وهذا يتمم البرهان .

دعنا الآن نحاول النظر في النظرية السابقة من زاوية مختلفة ، ولنبدأ بالزمر $G_1,G_2,\dots,G_n$ ونكوّن الزمرة G بالخصائص التالية :

(i) G لها زمر جزئية $G_n{'}\dots G_1{'},G_2{'},G_3{'}$.

(ii) لكل $i\neq j$ إذا كان $a_j{'}\in G_j{'},a_i{'}\in G_i{'}$ فإن $a_i{'}a_j{'}=a_j{'}a_i{'}$

(iii) كل عنصر $a\in G$ يمكن التعبير عنه بصورة وحيدة بالشكل $a=a_1{'}a_2{'}\dots a_n{'}$ حيث $a_i{'}\in G_i{'}$ لكل $1\leq i\leq n$.

والآن لتكن G أية زمرة (لا تخلط G مع الضرب المباشر في الأعلى) .

يمكن لـ G أن تحوي زمراً جزئية $H_1,H_2,\dots,H_n$ بالخصائص التالية :

(i) عندما $i\neq j$, $h_j\in H_j,h_i\in H_i$ يكون $h_ih_j=h_jh_i$.

(ii) كل عنصر a من G يمكن التعبير عنه بصورة وحيدة على شكل حاصل الضرب $h_1h_2h_3...h_a, h_i \in H_i 1 \le i \le n$.

وفيما يلي سوف نبرهن تحت هذا الموقف أن G هي أيزومورفيك لحاصل الضرب الخارجي المباشر $H_1, H_2, ..., H_n$ بمعنى أننا سوف نثبت أن G تساوي أيزوموفيا لـ $H_1 \times H_2 \times ... \times H_n$ وقبل إثبات هذه النتيجة نعرف مفهوم الضرب الداخلي المباشر .

تعريف 4.4 (الضرب الداخلي المباشر)

تُدعى الزمرة G ضرباً اتجاهياً داخلياً لزمرها الجزئية $H_1, H_2, ..., H_n$ إذا تحققت الشروط التالية :

(i) لكل $a_i a_j = a_j a_i \Leftarrow a_i \in H_i, a_j \in H_j, i \ne j$.

(ii) لكل $x \in G$ قابل للتمثيل بصورة وحيدة $x = x_1x_2x_3..x_n$ بمعنى أنه إذا كان كذلك $x = y_1y_2...y_n, y_i \in H$

$, x_i \in H_i$ $1 \le i \le n$ فإن $x_i = y_i \forall_i$ إذا كانت عملية التركيب الزوجية في G هي الجمع فإننا نقول أن G هو الجمع الداخلي المباشر لـ $H_1, H_2, ..., H_n$ وتكتب :

$$G = H_1 \oplus H_2 \oplus ... \oplus H_n$$

نظرية 4.5

إذا كان G هو الضرب الداخلي المباشر للزمر الجزئية $H_1, H_2, ..., H_n$ فإن $G \cong H_1 \times H_2 \times ... \times H_n$.

البرهان

نعرف $f : H_1 \times H_2 \times ... \times H_n \to G$ بحيث :

$$f(x) = x_1x_2x_3..x_n \qquad \forall x = (x_1, x_2x_3, ...x_n) \in H_1 \times H_2 \times ... \times H_n$$

نفرض أن $x=(x_1,x_2,x_3,...,x_n),\ y=(y_1,y_2,y_3,...,y_n)\in H_1\times H_2\times H_3\times...\times H_n$

فيكون $f(xy)=x_1x_2x_3,...,x_ny_1y_2...y_n=x_1y_1x_2y_2x_3y_3...x_ny_n$

ومن تعريف الضرب الداخلي المباشر فإن $x_iy_j=y_jx_i$ لكل $i\neq j$ ولذلك فإن :

$$f(xy)=x_1x_2..x_ny_1y_2...y_n=f(x)f(y)$$

أي أن f هي هومومورفيزم .

زد على ذلك أن $f(x)=f(y)$ يؤدي إلى أن :

$$x_1x_2..x_n=y_1y_2...y_n\Rightarrow x_i=y_i\quad\forall\quad i=1,2,\dots,n$$

(التعريف ii-4.4) $\Leftarrow x=y$ عليه فإن f هي تطبيق أحادي ، وأكثر من ذلك إذا كانت $a\in G$

$a=a_1a_2..a_n\qquad a_i\in H_i$

فإن $f(a_1a_2..a_n)=a_1a_2a_3..a_n$

وهذا يؤدي إلى أن f تطبيق شامل ، ولذلك فإن f هي أيزومورفيزم وأن $G\cong H_1\times H_2\times...\times H_n$.

النظرية التالية تعطي معياراً ممتازاً لتحديد متى تكون الزمرة G ضرباً داخلياً مباشراً لزمرها الجزئية $H_1,H_2,...,H_n$.

نظرية 4.6

ليكن G زمرة و $H_1,H_2,H_3,...,H_n$ زمراً جزئية من G ، فتكون G هي ضرباً داخلياً مباشراً لـ $H_1,H_2,H_3,...,H_n$ إذا وفقط إذا تحققت الشروط التالية :

(1) لكل i, H_i هي زمرة جزئية عادية من G .

(2) $H_i\cap\left(\prod_{j\neq i}H_j\right)=(e)$.

(3) $G=\pi_{i=1}^{n}H_i$.

البرهان

لتكن G ضرباً داخلياً مباشراً لزمرها الجزئية $H_1,H_2,H_3,...,H_n$ و ليكن $a_k \in H_k$ وأن $x = x_1x_2...x_n, x_i \in H_i, 1 \le i \le n$
أي عنصر من G حيث أن $\forall_i \neq K$ $x_ia_k = a_kx_i$ فإننا نحصل على $x^{-1}a_kx = x_k^{-1}a_kx_k \in H_k$ هذا يؤدي إلى أن H_k هي زمرة جزئية عادية من G وهذا يبرهن (1) .

الآن $d \in H_i \cap \underset{j\neq i}{\pi} H_j \Leftarrow d \in H_i$ و $d = d_i \Leftarrow d \in \pi H_j$ ، $d = d_1d_2...d_n$ لبعض العناصر $d_k \in H_K$ لكل قيم $k = 1,2,...,n \Leftarrow d_1d_2...d_{i-1}d_{i+1}...d_n = ee..ed_ie..e$ $\Leftarrow d_i = e$ من وحدانية التمثيل على شكل ضرب $\Leftarrow d = e$ أي أن $H_i \cap \prod_{j\neq i} H_j = (e)$ وهذا يبرهن (2) .

(4) نستنتج مباشرة من تعريف الضرب الداخلي المباشر وبالعكس ليكن $H_1,H_2,...,H_n$ هي زمر جزئية من G تحقق الشروط (1) و (2) و (3) .

خذ أي عددين صحيحين متمايزين $k \neq l$ بين n,l .

من (2) يكون $H_k \cap \prod_{j\neq k} H_j = (e)$ وحيث أن $H_L \subseteq \underset{j\neq k}{\pi} H_s, L \neq K$ فإن $H_k \cap H_l = (e)$.

ليكن $x_l \in H_l, x_k \in H_k$ عندئذ يكون $x_k^{-1}x_L^{-1}x_Kx_L = (x_K^{-1}x_L^{-1}x_K)x_L \in H_L$
لأن H_L هي زمرة جزئية عادية في G وبالمثل

$$x_K^{-1}x_L^{-1}x_Kx_L = x_K^{-1}(x_L^{-1}x_Kx_L) \in H_K$$

لذا فإن $x_K^{-1}x_L^{-1}x_Kx_L \in H_K \cap H_L = (e)$ وهذا يعطي أن $x_K^{-1}x_L^{-1}x_Kx_L = (e)$ $\Leftarrow x_Kx_L = x_Lx_K$.

الآن من (3) $G = H_1H_2...H_n$ فبأخذ $x \in G$ يكون :

$$x = x_1x_2...x_n, x_i \in H_i, \forall_i$$

لإثبات صحة العكس نحتاج فقط لنبين وحدانية التمثيل السابق ، ولإجراء ذلك نفرض أن

$$x_1x_2x_3...x_n = y_1y_2...y_n$$

لبعض العناصر $x_i, y_i \in H_i$ ولكل قيم i .

افرض أن L قيمة ثابتة ، حيث أنه $\forall \quad K \neq L$ فإن كل عنصر في H_K هو إبدالي مع كل عنصر في H_i (ثبت ذلك قبلاً) فإننا نحصل على :

$$x_K^{-1}Y_K = (x_1y_1^{-1})(x_2y_2^{-1})...(y_Ky_{K-1}^{-1})(x_{K+1}y_{K+1}^{-1})...(x_ny_n^{-1}) \in H_K \cap \Pi H_j = (e)$$

$$x_K^{-1}y_K = e \Rightarrow x_K = y_K \forall_K = 1, 2, ..., n$$

وهذا يتمم البرهان .

نتيجة 4.7

إذا كان G هو الضرب الداخلي المباشر للزمر الجزئية $H_1, H_2, ..., H_n \,(n>1)$ وكان $K = \prod_{j=2}^{n} H_i$ فإن G أيضاً هي ضرب داخلي مباشر لـ K, H_1 .

البرهان

من (2) $H_1 \cap \underset{j=2}{\overset{n}{\pi}} H_j = (e) \Rightarrow H_1 \cap K = (e)$ وحيث أن K هو ضرب الزمر الجزئية العادية K هي نفسها عادية أيضاً ، فإن $H_1K = H_1H_2..H_n = G$ ولذلك فإن G هو ضرب داخلي مباشر لـ H_1 و K .

ملاحظة : كما رأينا سابقاً إذا كان الزمرة G هي ضرب داخلي مباشر لزمر جزئية $H_1, H_2, ..., H_n$ فإن $G \cong H_1 \times H_2 \times ... \times H_n$ ومرة أخرى إذا كانت الزمرة G هي ضرب خارجي مباشر للزمر $G_1, G_2, ..., G_n$ فإن G تحوي زمراً جزئية $G_1', G_2', ..., G_n'$ بحيث يكون

$G_i' \cong G_i$ لكل قيم G,i هو الضرب الداخلي المباشر للزمر $G_1,G_2,...,G_n$ وكما هو مألوف لدينا أن نعتبر أن زمرتين إيزومورفيتين هما بالضرورة متساويتان ، فيمكننا مراعاة أن الضرب الداخلي المباشر مثل الضرب الخارجي المباشر وندعوه ببساطة الضرب المباشر .

ومن ثم فإذا قلنا أن G هو ضرب مباشر على الزمر $G_1,G_2,...,G_n$ فإن كل G_i تكون زمرة جزئية عادية من G ويكون $G=\underset{i=1}{\overset{n}{\pi}} G_i$ و $G_i \cap \underset{j\neq i}{\pi} G_i=(e)$ لكل $i=1,2,...,n$.

والآن نفرض أن G هي ضرب مباشر للزمر $G_1,G_2,...,G_n$ لكل $i=1,2,...,n$ G_i تدعى معامل مباشر للزمرة G ، وفي حالة ما تكون G جمعاً مباشراً للزمر $G_1G_2..G_n$ عندئذ لكل $i=1,2,...,n$ تسمى G_i حداً جمعياً للزمرة G ، الآن نعطي بعض الأمثلة على الضرب المباشر والجمع المباشر .

مثال 4

ليكن $G=<a>$ زمرة دائرية من الرتبة 6 ، وليكن $H=\{e,a^2,a^4\}$ و $K=\{e,a^3\}$ باستخدام حقيقة $o(a)=e$ فعلى الفور نستنتج أن K,H هما زمرتين جزئيتين من G رتبتهما 2 و 3 على الترتيب ، كما يمكن ملاحظة أن :

(i) أن $H\cap K=\{e\}$.

(ii) وكما أن G زمرة آبيلية ، فإن كلاً من K,H زمرة جزئية عادية .

(iii)
$$\begin{aligned} HK &= \{ee, ea^3, a^2e, a^2a^3, a^4a^3\} \\ &= \{e, a^3, a^2, a^5, a^4, a\} = G \end{aligned}$$

لأن $a^6=e$ ولذا فإن G هي ضرب داخلي مباشر للزمرتين K,H (في النظرية 4.6 نأخذ $H_2=K, H_1=H, n=2$) .

مثال 5

في الفصل (2.1) المسألة (iv) 6 عرفنا زمرة كلاً من رباعية V كانت تحتوي على أربعة عناصر $1, a, b, c = ab$ هذه الزمرة آبيلية $a^2 = b^2 = (ab)^2 = 1$ بحيث كان $H = \{1, a\}$ و $K = \{1, b\}$ هما زمرتان جزئيتان من V .

يوجد زمرة جزئية عادية $H \cap K = \{1\}, G = HK$ لذا فإن G هي ضرب مباشر للزمرتين الجزئيتين .

نفرض أن G هي زمرة آبيلية جمعية منتهية ، وأن $o(G) = n = P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_t^{\alpha_t}$ هو تحليل الرتبة n للزمرة G إلى قوى متمايزة لأعداد أولية ، لكل عدد أولي $P|o(G)$ نفرض أن $S(P) = \{X \in G \,|\, P^K X = a\}$ ولبعض قيم K الأكبر من الصفر ، وكما يبدو لاحقاً في القضية المساعدة 4.7 فإن $S(P)_\lambda$ هي زمرة جزئية من G وهذه الزمرة الجزئية $S(P)$ تسمى زمرة سايلو الجزئية من الرتبة P من G ، وسوف نبين أن G هي جمع داخلي مباشر لزمر سايلو الجزئية لها ، وبناء عليه فإن بناء G سيعُرف بالكامل إذا عرفنا بناء كل زمر سايلو الجزئية للزمرة G ، ومسألة تحديد بناء زمر سايلو الجزئية مكانها الصحيح هو الفصل التالي .

قضية مساعدة 4.7

لكل عدد أولي $P | o(G)$ حيث أن G هي زمرة جزئية آبيلية جمعية ، فإن المجموعة $S(P)$ هي زمرة جزئية من G .

البرهان

نفرض أن O هو المحايد الجمعي للزمرة G ، فكما أن $PO = o$ فإن $o \in S(P)$ وبناء عليه فإن $S(p) \neq \phi$.

الآن $x, y \in S(p) \Rightarrow P^K x = O, P^L y = O$

لـــبعض الأعـــداد الموجبـــة L, K ، لـــيكن $n = ma_x(K, L)$ عندئـــذ يكـــون $P^n x = P^n P^{n-k} P^K x = o$ بالمثل يكون $P^n y = P^{n-L} P^L y = o$.

$$\Rightarrow P^n(x - y) = P^n x - P^n y = o - o = 0$$
$$\Rightarrow x - y \in S(P)$$

ولذلك فإن $S(P)$ هي زمرة جزئية من G .

قضية مساعدة 4.8

لـيكن x أي عنصر مـن الرتبـة mn في الزمـرة G بحيـث أن $(m,n)=1$ فإنـه يوجـد $y, Z \in G$ بحيث يكون

$$x = yz = zy$$
$$o(y) = m$$
$$o(z) = n$$

البرهان : لأن $(m,n)=1$ فإنه يوجد عددين صحيحين t, s بحيث يكون $1 = tm + sn$ وليكن $z = x^{tm}, y = x^{sn}$ وحيـث أن z, y همـا قـوتان لـنفس العنصـر x فـإن $x^{tm} = x^{sn+tm} = s = x$ والآن $yz = zy = x^{sm}$ لأن $(y)^m = (x^{sn})^m = (x^{nm})^s = e$ وهـــذا يعطـــي أن $o(x) = mn$ وبالمثل $o(y) = m_1, / m$ وأن $z^n = e$ وعندئذ $oz = n_1 / n$:

$$(yz)^{m_1 n_1} = y^{m_1 n_1} z^{n_1 m_1} = ee = e \Rightarrow o(x) | m_1 n_1 \Rightarrow mn | m_1 n_1$$

وعلـى أيـة حـال $m_1 | m_1, n_1 | n_1$ فيجـب أن يكـون $n - n_1, m = m_1$ وهـذا يـبرهن أن $o(y) = m, o(z) = n$.

قضية مساعدة 4.9

لـيكن x أي عنصـر في G بحيـث $o(x) = n = n_1 n_2 n_3 .. n_r$ حيـث أن $n_1, n_2, .. n_r$ هي أعداد أولية مثنى مثنى* فإن $x = x_1 x_2 .. x_r$ لبعض العناصر $(1 \le i \le r), x_i \in G$ بحيث أن $o(x_i) = n_i, \forall_i$ وكل x_i هو قوة للعنصر x .

البرهان

* متزاوجية أولياً تعني أن $i \neq j = 1, 2, 3, ..., r \forall (n_i, n_j) = 1$

عند $r=1$ يمكننا أخذ $x_1=x$ وينتج الناتج بتطبيق الاستنتاج نفرض أن $r>1$ والنتيجة متحققة لـ $r-1$ ونفرض $n'=n_1n_2..n_{r-1}$ وكذلك $n_r=m$ واضح نظرياً أن $(n_i,n_r)=1$ ولكل قيم $i\neq r$ $\Rightarrow (n',n_r)=1 \Rightarrow (n',m)=1$

من القضية المساعدة (4.8) يكون $x=yz=zy$ لبعض العناصر $x,y\in G$ ويكون $o(y)=n', o(z)=m=n_r$ وكما لاحظنا في القضية المساعدة السابقة فإن كلاً من z,y يمكن أن يكونا قوة للعنصر x .

الآن $o(y) = n_1n_2..n_{r-1}$ ومن الاستنتاج يكون $y=y_1y_2...y_{r-1}$ لبعض العناصر $y_i\in G$ بحيث يكون $o(y_i)=n_i$ وأن y_i هي قوى للعنصر y $(i=1,2,...,r-1)$ وحيث أن y نفسها هي قوة للعنصر x فنحصل على أن كل y_i هو قوة للعنصر x ، بأخذ $x_i=y_i$ ولكل قيم i من $r-1..2,1$ $x_r=z$ نحصل على $x=x_1x_2x_3..x_r$ بحيث أن $o(x_i)-n_i$ ولكل x_i هي قوة لـ x وهذا يبرهن القضية .

ملاحظة

إذا كانت العملية الثنائية للزمرة G هي الجمع ، ففي القضية السابقة يجب أن يكتب $x=x_1+x_2+x_3+...+x_r$.

نظرية 4.10

أي زمرة آبيلية جمعية منتهية هي جمع مباشر داخلي لزمرة سايلو الجزئية .

البرهان

ليكن G زمرة آبيلية منتهية (جمعياً) $o(G)=n=P_1^{\alpha_1}P_2^{\alpha_2}...P_t^{\alpha_t}$

بحيث أن P_i هي أعداد أولية متمايزة و d_i هي أعداد جمعية $(1 \le i \le t)$ فإن $S(p_1),...,S(P_t)$ هي فقط زمر سايلو الجزئية للزمرة G لأن $P_1,...,P_2$ هي فقط أعداد أولية تقسم رتبة G .

(I) الآن ليكن $x \in G$ فإن $o(x) \big| o(G) = P_1^{\alpha_1}...P_t^{\alpha_t}$ ليعطي $o(x) = P_1^{\beta_1} P_2^{\beta_2}...P_t^{\beta_t}$ لبعض القيم β_i بحيث أن $o \le \beta_i \le \alpha_i$.

والآن $P_1^{\beta_1}, P_2^{\beta_2},...,P_t^{\beta_t}$ هي متزاوجة التوافق الأولي ، لذلك فإن $x = x_1 + x_2 + x_3 + ... + x_t$ (الاستنتاج 4.9) بحيث كل x_i هو من رتبة $P_i^{\beta_i}$ لذا فإن $P_i^{\beta_i} x_i = o$ تعطي $x_i \in S(P_i) \forall_i$ وهذا يوضح أن $x \in G$ أي أن $x = x_1 + x_2 + ... + x_t$ لبعض قيم $x_i \in S(P_i')$ وأن $1 \le i \le t$

وبناء عليه $G = S(P_1) + S(P_2) + ... + S(P_t)$

(II) اعتبر $S(P_i) \cap \sum_{j \ne i} S(P_i)$ و

$$x \in S(P_i) \cap \sum_{j \ne i} S(P) \Rightarrow x \in S(P_i)$$

$$x = x_1 + x_2 + ... + x_{i-1} + x_{i+1} + ... + x_n$$

لبعض قيم $(j \ne i) x_j \in S_j$.

والآن من التعريف $x \in s(p_i)$ لبعض قيم $k_i > o$

$$\Rightarrow \quad p_i^{ki} x = o$$

$$\Rightarrow \quad o(x) \big| p_i^{ki}$$

ومرة أخرى كل $j \ne i$ $\quad x_j \in s(p_j)$

$$\Rightarrow \quad p_j^{kj} x_j = o$$

وافرض أن $m = P_1^{k1} P_2^{k2} ... P_{i-1}^{ki-1} P_{i+1}^{ki+1} ... P_n^{kn}$

عندئذ يكون $mx_j = o$ لكل قيم $j \ne i$

$$\begin{aligned} mx &= m(x_1 + x_2 + ... + x_{i-1} + x_{i+1} + ... + x_n) \\ &= mx_1 + mx_2 + ... + mx_{i-1} + mx_{i+1} + ... + mx_n \\ &= 0 \end{aligned}$$

وتـؤدي إلى $m|o(x)$ يـؤدي إلى أن $o(x)|m$ ، $o(x)\left|p_i^{R_i}\right.$ ومنهـا m, p_i^{ki} همـا مترافقـان أوليـان وبالتالي $o(x)=1$ بمعنى أن $x=o$ لذا فإن $s(p_i)\cap\sum_{j=i}s(p_j)=(o)$ وإضافة إلى ذلك بشكل مبسط كل $s(p_i)$ هـو زمـرة جزئيـة عاديـة مـن G ولـذلك G هـي جمـع داخلـي مباشـر للزمـر الجزئية $s(p_i)(i=1,2,...,n)$ وهذا يتمم البرهان .

تمارين

1. إذا كانت G زمرة و K,H زمرتين جزئيتين من G بحيث كان $G=H\times K$ برهن أن $H\cong G/K$ وكذلك $K\cong G/H$.

إشـــاد : لكـــل $k\in K, h\in H, x=hk, x\in G$ عـــرف $f:G\to H$ $g:G\to K$ بواســـطة $g(x)=K, f(x)=h$ وبـين أن g,f هما هومومورفيتـان علـى K,H بالترتيـب مـع H,K نواتهما على التقابل .

2. ليكن $G=<a>$ أي زمرة دائرية من الرتبة mn حيث $(m,n)=1$ افرض أن K,H هما زمرتان جزئيتان فيها من الرتبة n,m على الترتيب ، بين أن $G=H\times K$.

3. افرض $G_1=<a>$ و $G_2=<b>$ زمرتين دائريتين من الرتبة n,m على الترتيب ، بحيث $(m,n)=1$ بين أن $G=G_1\times G_2$ هي زمرة آبيلية من الرتبة mn وهي غير دائرية.

4. ليكن G_1,G_2,G_3 أي ثلاث زمر ، بين كل مما يأتي :

(i) $o(G_1\times G_2)=o(G_1)o(G_o)$

حيث كل G_i هي زمرة منتهية .

(ii) $G_1\times G_2\cong G_2\times G_1$

(iii) $$\begin{aligned} G_1\times(G_2\times G_3) &= G_1\times G_2\times G_3 \\ &= (G_1\times G_2)\times G_3 \end{aligned}$$

5. باستخدام نظرية لاجرانج أو بغيرها بين أن أي زمرة G من الرتبة 4 تكون آبيلية وزيادة على ذلك بين أنه إذا كانت G دائرية أو G هي أيزومورفيك للضرب المباشر لزمرتين دائريتين من الرتبة 2 .

6. ليكن G زمرة منتهية فيها $a^2=e$ لكل $a\in G$ بين أن G هي ضرب مباشر داخلي لعدد منته من الزمر الجزئية كل منها من الرتبة 2 .

$o(G)=2^n$ لبعض قيم $n\geq o$.

7. ليكن لبعض قيم $n \geq o$ زمرة آبيلية منتهية ، اثبت أن كل زمرة جزئية لسايلو هي زمرة جزئية مميزة للزمرة G .

8. ليكن G زمرة آبيلية منتهية وأن $H_1, H_2 .. H_t$ هو عدد منته من الزمر الجزئية من G بحيث كان $G = H_1 H_2 .. H_t$ و $o(G) = \prod_{i=1}^{t} o(H_i)$ اثبت أن $G = H_1 \times H_2 \times ... \times H_t$.

9. $G_1, G_2, .. G_n$ هي n من الزمر ، بين أن :

$$Z(G_1 \times G_2 \times ... G_n) = Z(G_1) \times Z(G_2) \times ... \times Z(G_n)$$

10. برهن أن زمرة الأعداد النسبية Q مع الجمع لا يمكن أن تكتب على شكل جمع مباشر لزمرتين جزئيتين غير تافهتين .

11. لتكن N زمرة جزئية عادية من G ، إذا كانت $G = H \times K$ حيث H, K زمرتان جزئيتان من G . برهن ان إما أن تكون N آبيلية أو أن N تقاطع H أو K تقاطعاً غير تافه .

12. إذا كانت M, N زمرتان جزيئتان عاديتان من G فاثبت أن $G / M \cap N$ هي أيزومورفيك للزمرة الجزئية للضرب المباشر الخارجي لـ $G / M \times G / N$.

إرشاد : عرف $Q : G \to G / N \times G / N$ بحيث $[\theta(x) = (Mx, Nx)$.

13. الزمرة G تسمى قابلة للتحليل إلى عوامل إذا وفقط إذا كان $G = H \times K$ حيث الزمرتين الجزئيتين H, K تحققان $H \neq \{e\}, k \neq \{e\}$ ، و e هو العنصر المحايد في G ، بين أن الزمرة الدائرية من الرتبة 6 هي قابلة للتحليل بينما S_3 هي ليست كذلك .

14. برهن أن زمرة الضرب R للأعداد الحقيقية غير الصفرية قابلة للتحليل .

إرشاد : $[R = R^{+} x \{1, -1\}$.

15. الزمرة تسمى دورية إذا كان كل عنصر من عناصر G ذو رتبة منتهية . بين إذا كان $G_1, G_2, ..., G_n$ زمراً دورية فإن $G_1 \times G_2 \times ... \times G_n$ تكون زمرة دورية أيضاً .

16. برهن أنه إذا كان H عاملاً مباشراً للزمرة G فإن كل زمرة جزئية عادية لكل من H, K تكون زمرة عادية للزمرة G أيضاً .

2- نظرية سايلو

من المؤكد أن القارئ قد لاحظ استخدامنا لنظرية لاجرانج للزمر المنتهية وتوابعها ، ولسوء الحظ فإن عكس نظرية لاجرانج لا يتحقق على وجه العموم ، وكما نعلم فإن الزمر المتتابعة A_4 هي من الرتبة 12 ولكن A_4 لا تحوي أي زمرة جزئية من الرتبة 6 وأحد الأهداف الرئيسية لهذا الفصل هو فحص بعض النظريات التي تعطي الشروط الكافية لقاسم K لرتبة لزمرة منتهية G بحيث تحتوي G على زمرة جزئية من الرتبة K ، والنظرية 4.12 تثبت ان عكس نظرية لانجرانج متحققاً للزمرة الآبيلية المنتهية .

وأيضاً سوف تتحقق بعض النظريات التي تعطي علاقات بين بعض الزمر ذات النوعية الخاصة للزمر المنتهية .

النظرية الأم في هذا السياق ابتدعها الرياضي النرويجي سايلو ، وابتداءً سوف نبرهن نظرية كوشي .

نظرية 11.4 (نظرية كوشي للزمر الآبيلية)

إذا كانت G زمرة آبيلية منتهية ، و $P|o(G)$ حيث P عدد أولي ، فإنه يوجد $a(\neq e)\in G$ بحيث أن $a^P=e$.

البرهان

طالما أن $P/o(G)=n,P$ لبعض قيم $n_1\geq 1$ فإننا نتقدم بالاستنتاج على n_1 ، ليكن $n_1=1$ فإن $o(G)=P$ و حيث أن كل زمرة ذات رتبة أولية تكون دائرية فإن G هي زمرة دائرية ، أي أنه يوجد $a\in G$ بحيث $G=<a>$ وعندئذ يكون $o(a)=o(G)=P$ (النظرية 2.33) وبناء عليه فإن $a^P=e, a\neq e$ تتحقق لـ $n_1=1$ ولكي نطبق الاستقراء ، نفرض أن $n_1>1$ ونفرض كذلك أن النتيجة محققة لكل زمرة آبيلية G التي لها $o(G')=mP$

ولهـا $m<n_1$ أي أنـه نعـرف أن النتيجـة صـحيحة لكـل الزمـر الآبيليـة مثـل G' بحيـث أن $P/o(G')$ و $o(G')<o(G)$ فيما أن $o(G)=n_1P$ ليست عدداً أولياً فإن G يجب أن تحتوي زمرة جزئية فعلية (نظرية (3.47(a)) .

نفـرض أن G فيهـا زمـرة جزئيـة فعليـة N بحيـث أن $P/o(N)$ فكـان $o(N)<o(G)$ فمن الاستقراء يوجد $a\in N$ بحيث يكون $a^P=e,a\neq e$ هذا العنصر هو أيضاً موجود في G إذاً النتيجة تحقق إذا كان للزمرة G زمرة جزئية فعلية N مع $P/o(N)$.

نفـرض الآن أن P لا تقسـم رتبـة أي زمـرة جزئيـة فعليـة في G ونفـرض أن H هـي أي زمرة جزئية فعلية من G فيكون $o(G)=o(G/H).o(H)$ وهـذا يعطـي $P/o(G/H)$ لآن $P \nmid o(H)$ زد على ذلك أن $o(G/H)=o(G)/o(H)<o(G)$ ومن فروض الاستنتاج G/H تحتـوي عنصـراً bH مـن الرتبـة p لـذا فـإن $bH\neq H$ و $H=(bH)^p=b^PH$ وهـذا يعطـي $b^p\in H$ ومنه ينتج أن $(bp)^{o(H)}=e$ (النتيجة 35.2) .

ليكن $a=b^{o(H)}$ فإن $a^p=e$ فإذا كان $a=e$ فإننا نحصل على $o(bH)/o(H)$

$$\Rightarrow \qquad p/o(H)$$

وهذا تناقض ، والصواب هو $a(\neq e)\in G$ بحيث أن $a^P=e$.

نظرية 12.4

إذا كانـت G زمـرة آبيليـة منتهيـة و K عـدداً صـحيحاً موجبـاً يقسـم $o(G)$ فـإن G ... زمرة جزئية من الرتبة K .

البرهان

سـوف نـبرهن هـذه النظريـة بواسـطة الاسـتنتاج على $o(G)$ إذا كـان $o(G)=1$ فـإن $K/o(G)\Rightarrow K=1$ في هذه الحالة ستكون G هي نفسها زمرة جزئية من الرتبة K ، لتطبيق الاستنتاج نفرض أن $o(G)>1$ والنتيجة متحققة لكل الزمر الآبيلية المنتهية من رتبة $< o(G)$

بالإمكان نفرض أن $K>1$ حيث أنه عندما $K=1$ فإن (e) هي الزمرة الجزئية من G ذات الرتبة 1 ليكن P عدداً أولياً بحيث يكون P/K عندئذ يكون $P/o(G)$ ، وباستخدام نظرية كوشي المعطاة سابقاً يوجد $a\in G$ بحيث يكون $o(a)=P$ لتكن $H=<a>$ هي الزمرة الدائرية الجزئية والمتولدة بالعنصر a فإن $o(H)=P$.

الآن G/H هي زمرة آبيلية بحيث أن $o\left(\frac{G}{H}\right)=\frac{o(G)}{o(H)}=\frac{o(G)}{P}<o(G)$

طالما P/K فإن $K=K_1P$ و $K_1/o(G/H)$ ولذلك وبواسطة فروض الاستنتاج G/H لها زمرة جزئية ولتكن T من الرتبة K_1 لذلك كل زمرة جزئية من G/H هي من الصيغة K/H حيث K هي زمرة جزئية من G تحتوي H عندئذ :

$$o(K)=o(K/H)o(H)=K_1P=K$$

وهذا يتمم البرهان .

نظرية 13.4 (نظرية سايلو الأولى)

لتكن G زمرة منتهية من الرتبة $n=P^Kq(K\geq 1)$ حيث P عدد أولي و q عدد صحيح موجب ، بحيث $(p,q)=1$ فإنه لكل $G(1\leq i\leq k)i$ لها على الأقل زمرة جزئية واحدة من الرتبة P^i .

البرهان

ليكن $o(G)=p^kq$ إذا كان $o(G)=P$ فإن G هو زمرة دائرية من الرتبة P والنظرية متحققة ببساطة .

الآن نستكمل البرهان بواسطة الاستنتاج على $o(G)$ افرض أن النتيجة متحققة لكل الزمر T ذات الرتبة $<o(G)$ بحيث $p/o(T)$ ليكن $Z(G)$ هو مركز G فيكون لدينا الحالات الآتية :

الحالة الأولى $\mathbf{p/o(Z(G))}$: في هذه الحالة وبواسطة نظرية كوشي للزمر الآبيلية يوجد $a\in Z(G)$ لأن a تتبادل مع كل عناصر G $H=<a>$ هي زمرة جزئية عادية من G من

الرتبة p إذا كان $k=1$ من الرتبة p فإن H هي الزمرة الجزئية المطلوبة من G نفرض أن $o(G/H)=P^{k-1}q, k>1$ وبواسطة فروض الاستنتاج . G' تحتوي على الزمرة الجزئية $\overline{H}_i$ من الرتبة p^i والآن لكل i و $\overline{H}_i = H_i / H$ لبعض الزمر الجزئية H_i من G التي تحوي H فإن

$$\circ (H_i) = \circ(\overline{H}_i) \circ (H) = P^{i+1}$$
$$i = 1, 2, \ldots, k-1$$

تكتب $K_1, K_2, K_3, \ldots K_k$ للزمر $H, H_1, H_2, \ldots, H_{k-1}$ نلاحظ أن :

$$\circ (K_i) = P^i \quad \forall_i = 1, 2, \ldots, k$$

الحالة الثانية $P \nmid \circ (z(G))$: لدينا $o(G) = o[Z(G)] + \sum_{N(a)\neq G} \frac{o(G)}{o[N(a)]}$ حيث المجموع يجري على العنصر a مأخوذاً من واحداً من كل فصل مرافق يحتوي على أكثر من عنصر واحد حيث أن $p/o(G)$ فإن $p/\frac{o(G)}{o[N(a)]}$ لكل a والتي فيها $N(a)\neq G$ فسوف نحصل من المساواة السابقة $p/o[Z(G)]$ والتي هي ضد فرضية هذه الحالة ، ولذلك يوجد $a\in G$ بحيث $N(a)\neq G$ و $P \nmid \frac{o(G)}{o[N(a)]}$.

والآن $o(G)=\frac{o(G)}{o[N(a)]}\bullet o[N(a)]$ و $P \nmid \frac{o(G)}{o[N(a)]}$ فإن $P^K/o(G)$ تؤدي إلى $P^k \nmid o[N(a)]$ ولكن $o[N(a)]<o(G)$ ولذلك بواسطة فروض الاستنتاج فإن $N(a)$ تحتوي على زمر جزئية H_i من الرتبة $(1\le i\le k)P^i$ والتي هي أيضاً زمر جزئية من G وهذا يحقق البرهان .

نتيجة 14.4 (نظرية كوشي للزمر المنتهية)

إذا كان العدد الأولي P يقسم رتبة الزمر المنتهية G فإن G تحتوي على الأقل عنصراً واحداً من الرتبة P .

البرهان : بواسطة نظرية سايلو الأولى G يحتوي على زمرة جزئية H من الرتبة P لذا فإن H هي دائرية ، لذلك يوجد عنصر $a \in H$ بحيث $H = < a >$ ومنها $P = o(H) = o(a)$.

نتيجة 15.4

إذا كان $P^k / o(G)$ و $P^{k+1} \nmid o(G)$ فإن G لها زمرة جزئية من الرتبة P^k .

البرهان : البرهان مباشرة من النظرية 13.4 .

تعريف 16.4 (*P-subgroup*)

إذا كان P عدداً أولياً ، فإن الزمرة الجزئية H للزمرة G تسمى ***P-subgroup*** إذا كانت رتبة كل عنصر في H هي قوة للعدد P ، وعلى وجه الخصوص إذا كان العنصر في G من رتبة هي أحدى قوى عدد أولي ثابت P فإن G تسمى ***P-group*** .

ليكن G زمرة منتهية إذا كان $o(G) = P^K$ فإن (وكما في نظرية لانجرانج) لكل $a \in G$, $o(a)/P^K$, $o(a)$ هي قوى ، وبناء عليه فإن G هي ***P-group*** .

بالاتجاه المعاكس إذا كان G ***P-group*** فلا يوجد عدداً أولياً $q \neq p$ يمكن أن يقسم $o(G)$ لأنه خلافاً لذلك فإن G تحوي عنصراً من رتبة q وهو عدداً أولياً مختلف عن p (نظرية كوشي) نستنتج أنه إذا كانت G زمرة ***P-group*** فإنه $o(G) = P^K$ هو قوى للعدد P وهكذا G هي ***P-group*** إذا وفقط إذا $o(G)$ هو قوى P .

تعريف 17.4 (زمرة جزئية P سايلو من زمرة منتهية)

ليكن G زمرة منتهية و P عدد أولي بحيث أن $P^K / o(G)$ و $P^{K+1} \nmid o(G)$ فإن أي زمرة جزئية من G من الرتبة P^K تسمى زمرة جزئية P سايلو من G التعريف أعلاه يؤدي إلى أن كل الزمر الجزئية P سايلو من G من نفس الرتبة وبالتحديد P^K لأن أي زمرة

جزئية $P-$ هي من رتبة قوة العدد P نرى أنه لا توجد زمرة جزئية $HP-$ من G يمكن أن تكون تحتوي فعلياً زمرة جزئية $P-$ سايلو من G .

مثال 6

ليكن $G=<a>$ أي زمرة دائرية من الرتبة 8 وبما أن $8=2$ وقوى لعدد أولي فإن G هي زمرة من النوع *P-group* .

مثال 7

افرض S_3. $o(S)=6=3.2$ لذلك $3/o(S_3)$ ولكن $3^2\dagger\ o(S_3)$ لذلك فإن أي زمرة سايلو جزئية ثلاثية للزمرة S_3 هي من الرتبة 3 والآن :

$A_3=\{I,(123),(132)\}$

هي فقط الزمرة الجزئية من S_3 من الرتبة 3 لذلك فإن A_3 هي زمرة سايلو الجزئية الثلاثية الوحيدة من S_3 ومرة أخرى القوة الأكبر للعدد 2 والتي تقسم $o(S_3)$ هي 2 وبهذه الطريقة أي زمرة جزئية لسايلو ثنائية للزمرة (S_3) هي من الرتبة 2 والزمرة الجزئية الوحيدة من S_3 ومن الرتبة 2 هي $H_1=\{I,(1,2)\},H_2=\{I,(13)\},H_3=\{I,(23)\}$ فإن هذه الزمر الجزئية الثلاث كلها من نوع زمر سايلو الثنائية للزمرة S_3 .

مثال 8

اعتبر A_4 $o(A_4)=12=2^2.3i$ لذلك فإن λ أي زمرة جزئية لسايلو ثنائية من A_4 هي من الرتبة 4 وأي زمرة جزئية لسايلو ثلاثية من A_4 هي من الرتبة 3 .

والآن $V_4=\{I,(12)(34),(13)(24),(14)(23)\}$

هي زمرة جزئية من A_4 من الرتبة 4 و V_4 هي الزمرة الجزئية الوحيدة الثنائية لسايلو (انظر نظرية سايلو الثالثة) كما أن $H_1 = \{I, (123), (132)\}$ هي الزمرة الجزئية الثلاثية لسايلو من A_4 ، في الحقيقة A_4 لها أربعة زمر جزئية ثلاثية لسايلو (احسبها ؟؟) .

مثال 4

الزمرة $G = \{\pm 1, \pm i, \pm j, \pm k\}$ من *Quaternions* ليست إبدالية من الرتبة 8 وحيث أن $8 = 2^3$ فإن G زمرة ثنائية لسايلو *2-group* .

تعريف 15.4

ليكن S أي مجموعة جزئية غير خالية من الزمرة G و $x \in G$ فإن $x^{-1}Sx$ تمثل المجموعة $\{x^{-1}Sx : s \in S\}$ و $x^{-1}Sx$ يسمى مرافق S محدد بالعناصر x .

تعريف 19.4

ليكن S أي مجموعة جزئية غير خالية من G و K زمرة جزئية من G فإن منظم S في K هو المجموعة $N_k(S)$

$$N_K(S) = \{x \in K : x^{-1}Sx = S\}$$

وللسهولة تكتب $N(S)$ للزمرة $N_G(S)$ وتسمى $N(S)$ منظم S وفكرة الترافق لعنصرين من الزمرة G وفكرة المنظم $N(a)$ لعنصر $a \in G$ هي كما ذُكر في الفصل الثالث نستطيع إثبات أن العلاقة الترافقية على عائلة كل المجموعات الجزئية غير الخالية G هي علاقة تكافؤ و $N(S)$ هي زمرة جزئية من G والبراهين تسير في نفس الخطوط كما في العلاقة الترافقية للعناصر والمنظم $N(a)$ لعنصر $a \in G$ ، وببساطة فإنه لأي زمرة جزئية K من G يكون $N_K(S) = N(S) \cap K$ ولذلك فإن $N_K(S)$ هي أيضاً زمرة جزئية من G ونريد أن نعطي كلمة تحذير أنه للمجموعة الجزئية S من G و $x^{-1}Sx = S$ ليس بالضرورة تتطلب أن

$xS=Sx$ لكل $s\in S$ وهذا يمكن رؤيته في أن الزمرة G ليست آبيلية ، يوجد $g\in G$ بحيث أن $xg\neq gx$ لبعض قيم $x\in G$ ، بمعنى أن $x^{-1}gx\neq g$ وعلى أية حالة نحن نعلم أن $g^{-1}Gg=G$ ومرة أخرى للزمرة $N\,a$ يوجد عدد من المرافقات لأي مجموعة جزئية S يساوي دليل $N(S)$ في G وأكثر من ذلك إذا كانت S زمرة جزئية من G فإنه لكل $s\in S$ $s^{-1}Ss=S$ تعطي $S\subseteq N(S)$ ومن التعريف $x^{-1}Sx=s$ لكل $x\in N(S)$ لذا فإن S هي زمرة جزئية عادية في $N(S)$ ، وإذا كانت S هي عادية في أي زمرة جزئية H من G فإن $x^{-1}Sx=s$ ولكل قيم $x\in H$ ولذلك $H\subseteq N(S)$ وهذا يبين أن $N(S)$ هي أكبر زمرة جزئية في G التي فيها S هي زمرة عادية .

افرض زمرة جزئية K من G وإذا كان $x,y\in K$ فإن :

$$x^{-1}Sx=y^{-1}Sy\Leftrightarrow yx^{-1}Sxy^{-1}=S\Leftrightarrow xy^{-1}\in K\Leftrightarrow xy^{-1}\in N_K(S)\Leftrightarrow N_K(S)x=N_K(S)y$$

لذلك فإن عدد المرافقات للزمرة S يحسب من عناصر K التي تساوي دليل الزمرة $N_K(S)$ في K .

قضية مساعدة

لتكن P زمرة جزئية $P-$ سايلو للزمرة المنتهية G عندئذ فإن P تحتوي على كل عناصر $N(P)$ التي رتبتها قوة من قوى P .

البرهان

ليكن $x\in N(P)$ وليكن $x^{P^K}=e$ لبعض قيم $K\geq o$ حيث أن P هي عادية في $N(P)$ وأن $N(P)/P$ هي زمرة وأن $xP\in N(P)/P$ عندئذ $(xP)^{P^K}=x^{P^K}P=p$ تعطي

$$o(xP)/P^{-K} \qquad \Rightarrow \qquad o(xp)=P^t$$

لبعض قيم $t\geq o$ وليكن $\overline{K}$ زمرة جزئية من $N(p)/P$ والمولدة بواسطة $\bar{x}=xp$ فإن $o(\bar{x})=o(\overline{K})=P^t$.

والآن $\overline{K}=K/P$ لبعض الزمر الجزئية k من $N(p)$ محتواة في P .

ليكن $o(p)=p^{\alpha}$ فإن $o(K)=o(\overline{K})o(P)=P^{t+\alpha}$ لذلك K زمرة جزئية من نوع P من G محتواة في P حيث أنه لا يوجد زمرة جزئية من نوع P من G يمكن أن تحوي زمرة جزئية p سايلو من G ، فإننا نحصل على أن $K=p$ لذلك فإن $xp=P$ ، و $x\in P$ وهذا يتمم البرهان .

نظرية 21.4

لتكن G زمرة منتهية و P عدد أولي بحيث $P/o(G)$ فإن :

أ- كل زمرة جزئية من G فإنها ترافق واحدة للأخرى (النظرية الثانية لسايلو) .

ب- عدد الزمرة الجزئية p- سايلو يكون على الصورة $1+mp$ حيث m عدد صحيح غير سالب بحيث يكون $(1+mp)/o(G)$ (النظرية الثالثة لسايلو) .

البرهان

(أ) ليكن $o(G)=P^{K}q$ حيث $(P,q)=1$ و $K\geq 1$ ونفرض أن S زمرة جزئية p- سايلو من G وأن مجموعة كل المرافقات في S ونريد أن نبين أن كل زمرة جزئية p- سايلو P في G تكون مرافقة للزمرة S أو بمعنى آخر $P\in M$.

افرض عكس ذلك أنه يوجد زمرة جزئية p سايلو من G والتي لا ترافق S نفرض أن P' أي زمرة جزئية p سايلو من G مختلفة عن P فيكون $\circ(P)=P^{K}$ فنحصل على $p\not\subset P'$ وهذا يؤدي إلى وجود $x\in p$ بحيث أن $x\notin P'$ ومن ثم $x^{-1}P'x\neq P'$ وإلا فإن $x^{-1}P'x=P'$ يؤدي إلى $x\in N(P')$ والآن x هو عنصر من P ورتبته أحدى قوى p ولذلك فمن القضية المساعدة 20.4 فإن $x\in P$ وهذا تناقض ، لذلك فإن عدد مرافقات P' المحددة بعناصر من p هو أكبر من واحد للعدد ،

وحيث أن هذا العدد يساوي $[P:N_p(P')], N_p(P)\neq P$ كما أن $o(P)=P^K$ وأن $P:N_P(P')]/P^K$ فنحصل من ذلك على أن عدد المرافقات P^t لبعض $L\geq 1$ ولذلك فإنه مضاعف للعدد P .

(ب) في M تعرف العلاقة $(\sim)$ كما يلي $S_1 \sim S_2 \Leftrightarrow S_1 = x^{-1}S_2x$ لبعض قيم $x\in P$ وهذه علاقة تكافؤ وتقسم M إلى فصول تكافؤ لذلك لأي $S'\in M$ $S'\neq P$ وعدد المرافقات في S' يحسب بواسطة عناصر P مضروبة في p (انظر المقطع السابق) ولذلك فإن فصل التكافؤ يحتوي على عدداً من العناصر مساوي مضاعفات للعدد الذي تنتمي إليه P لأن ذلك محقق لكل فصل تكافؤ فإننا نحصل على أن عدد العناصر t في M هو مضاعف للعدد P على أية حال $t=[G:N(S)]$ وحيث أن $N(S)\supseteq S$ و $[G:S]=q$ فإن $[G:N(S)]/q$ وهذا يعطينا p/t لما p/q وهذا تناقض لحقيقته المثبتة سابقاً ، وهي أن t هي من مضاعفات p فإن p يجب أن ترافق s .

ج- ليكن M مجموعة كل الزمر الجزئية p- سايلو من G لنأخذ $P\in M$ كما في (أ) تعرف علاقة تكافؤ $(\sim)$ في M كما يلي :

$$S_1 \sim S_2 \Leftrightarrow S_1 = x^{-1}S_2x$$

لبعض قيم $x\in p$ والآن إذا كان S أية زمرة جزئية P سايلو من G تختلف عن p كما في (أ) فإن عدد مرافقات S يتحدد بعناصر P كمضاعفات p ، وهذا يبين أن عدد العناصر في أي فصل تكافؤ التي لا ينتمي إليه P هو مضاعفات للعدد p وبما أن $x^{-1}px=P$ لكل $x\in P$.

العنصر الوحيد في فصل التكافؤ الذي ينتمي إليه P لذا فإن عدد عناصر M هو على صورة $mp+1$ حيث m هو عدد صحيح غير سالب لأن عدد الزمر الجزئية المترافقة يقسم رتبة الزمرة فإن $1+mp$ يقسم رتبة الزمرة G وهذا هو تمام البرهان .

ملاحظة : $(1+mp)P^K q$ و $(1+mp, p^K) \Leftarrow q |(1+mp)$.

نظرية 22.4

لتكن G زمرة منتهية و P عدداً أولياً يقسم رتبة G عندئذ كل زمرة جزئية B من G ستكون محتواة في زمرة ما جزئية من نوع p سايلو من G .

البرهان

لتكن M مجموعة كل الزمر p سايلو الجزئية من G بواسطة نظرية سايلو الثالثة يكون عدد عناصر M مساوياً $(1+mp)$ لبعض الأعداد الصحيحة غير السالبة m على M عرّف العلاقة $(\sim)$ كالآتي لأي $P_1, P_2 \in M$ $P_1 \sim P_2$ إذا وفقط إذا $P_1 = x'P_2x$ لبعض $x \in B$ هذه علاقة تكافؤ ولأي $P \in M$ عدد عناصر M في صف الترافق P هو نفس عدد مترافقات P محدداً بعناصر B إذا كان لبعض $P \in M$ $B \not\subset p$ فإنه يوجد $x \in B$ بحيث أن $x \notin p$ إذا كان $x^{-1}Px = p$ فكما أن رتبة x هي قوة للزمرة P و B هي زمرة جزئية من نوع p و $x \in N(P)$ فإننا نحصل على $x \in p$ (القضية المساعدة 20.4) وهذا تناقض ، ومن ثم فإن العدد t لمترافقات P يكون أكبر من 1 ، على أية حال $t = [B : N_B(P)]$ و $o(B) = P^t$ لبعض الأعداد الصحية غير السالبة ℓ فنحصل على أنه $t = P^S$ لبعض $S \geq 1$ وهكذا فإن t هي مضاعف للعدد P بناء على ذلك إذا كان لا يوجد p في M محتواة في B فإن عدد العناصر في كل فصل تكافؤ سيكون مضاعفاً للعدد p وهذا سوف يخالف حقيقة أن عدد عناصر M هو $1+mp$ وعليه نوجد زمرة جزئية P سايلو من G بحيث يكون $B \subseteq P$ وهذا هو برهان النظرية .

تمارين محلولة

تمرين (1)

إذا كانت G زمرة منتهية و P عدداً أولياً يقسم $o(G)$ برهن أن زمرة سايلو P الجزئية P من G هي زمرة جزئية عادية من G إذا وفقط إذا كانت P هي زمرة سايلو P الجزئية الوحيدة من G .

الحل

افرض $o(G)=p^k q$ بحيث أن $(p,q)=1$ فإذاً $o(p)=p^K$ لتكن $g\in G$ gPg^{-1} هي زمرة جزئية من G لأن $gPg^{-1} = gP'g^{-1} \Rightarrow P = P', P, P^{-1} \in P$ نحصل على أن $o\left(gPg^{-1}\right) = o\left(P\right) = P^K$ ولكن بواسطة الفرض هذا يعني $gPg^{-1} = P$ فإذاً P هي زمرة جزئية عادية من G .

بالاتجاه الآخر لتكن P هي زمرة سايلو p العادية الجزئية من G ولتكن Q هي أي زمرة سايلو P جزئية من G بواسطة نظرية سايلو الثانية فإن P,Q يجب أن يكونا مترافقين أي أن $Q=xPx^{-1}$ لبعض قيم $x\in G$ ولكن P هي زمرة جزئية عادية في G فإذاً $xPx^{-1} = P$ فإذاً $Q=P$.

تمرين 2

إذا كانت G هي زمرة الرتبة $P^K S$ حيث P عدد أولي بحيث أن $(p,s)=1$ فبين أن كل زمرة جزئية من الرتبة P هي زمرة جزئية عادية من واحدة على الأقل من الزمر الجزئية من الرتبة P^{i+1} حيث $i=1,2,...,K-1$.

(لاحظ أن هذا الافتراض يعتبر جزء من نظرية السايلو الأولى في كثير من المؤلفات) .

الحل

نطبق الاستنتاج على $o(G)$ إذا كان $o(G)=P$ فإن تحقق المطلوب يكون بشكل بين .

افرض أن النتيجة متحققة لكل الزمر T من الرتبة أصغر من $o(G)$ بحيث أن $P/o(G)$ لتكن $Z=Z(G)$ هي مركز الزمرة G يكون لدينا حالتان حالة I $P/o(Z)$ بواسطة نظرية كوجي للزمر التبديلية فإنه يوجد $a\in Z$ بحيث أن $o(a)=p$ فإذاً $H=<a>$ هي زمرة جزئية عادية في G من الرتبة p إذا كان $K=1$ P^{i+1},P^{i}, نأخذ الأعداد $P,1$ على الترتيب فإذاً نتيجتنا تكون متحققة إذا كان $K>1$ فإن $o(G/H)=P^{K-1}S<o(G)$ وبواسطة استنتاج الفروض أي زمرة جزئية من G/H من الرتبة P^{i} هي عادية في زمرة جزئية واحدة على الأقل من G/H من الرتبة P^{i+1} لكل $i=1,2,...,K-2$ لتكن K هي زمرة جزئية من G ومن الرتبة $i=1,2,...,K-1,P^{2}$ في حالة $K/H,K\leq H$ هي زمرة جزئية من G/H من الرتبة P^{i-1} وبواسطة استنتاج الفروض فإنه يوجد زمر جزئية L/H من G/H من الرتبة P^{i} بحيث أن K/H هي عادية في L/H فإذاً K هي زمرة جزئية عادية في $o(L)=o(L/H)o(H)=p^{i},L$ $P=P^{i+1}$ فإذاً النتيجة تكون متحققة لجميع الزمر الجزئية من G من الرتبة $i=1,2,...,K-1,P^{i}$ في حالة كون $H\not\subset K$.

افترض الآن $H.K$ الآن $o(H\cap K)|o(H)\Rightarrow o(H\cap K)=1$ أو P بما أن $o(H\cap K)=P\Rightarrow H\cap K=HH\subseteq K$ نحصل على $o(H\cap K)=1$ ينتج أن $o(HK)=o(H)o(K)=P^{i+1}$ لأن $H\subseteq Z$ ، K زمرة جزئية عادية من HK (برهن !) فإذاً مرة أخرى النتيجة متحققة لكل الزمر الجزئية من G من الرتبة P^{i} ، $i=1,2,...,K-1$.

حالة II $P \nmid o(Z)$: لتكن K زمرة جزئية من G من الرتبة P^i $(1 \le i \le K-1)$ الآن $o(K \cap Z) = 1 , P \nmid o(Z)$ هذا يعطي :

$$o(KZ) = o(K)o(Z) = p^i o(Z) \le P^K S = o(G)$$

باستنتاج الفروض فإنه يوجد زمرة جزئية N من KZ بحيث أن K زمرة جزئية عادية من الزمرة G فإذاً النتيجة متحققة في الحالة II أيضاً .

تمرين 3

إذا كانت G زمرة من الرتبة P^n حيث P عدداً أولياً و n عدداً صحيحاً ≥ 1 لها بالضبط زمرة جزئية واحدة من الرتبة P^{n-1} فبرهن أن G زمرة دوارة .

الحل

ليكن $o(G) = P^n$ حيث P عدداً أولياً و n عدد صحيحاً موجباً ، افرض أن H هي زمرة جزئية من G من الرتبة P^{n-1} لأن $G \ne H$ يوجد عدد من $a \notin H , a \in G$ الآن $o(a) \big| p^n \Rightarrow o(a) = p^m , o \le m \le n$.

إذا كانت $m \ne n$ الزمرة الجزئية الدوارة T من G المتولدة من a تكون من الرتبة P^m $o \le m \le n-1$ بواسطة التمرين 2 يوجد زمرة جزئية K من الرتبة P^{n-1} بحيث أن $T \subseteq K$ وبواسطة الفرض $K = H$ فإذاً $< a > = T \subseteq H$ ولكن هذا يعطي أن $a \in H$ وهذا تناقض فإذاً $m = n$ و $o(a) = P^n$ نستنتج أن G زمرة دوارة .

تمرين 4

بين أنه لا توجد زمرة من الرتبة 30 تكون بسيطة .

الحل

لتكن G زمرة من الرتبة 30 . لاحظ أن $30 = 2.3.5$ فإذاً G لها على الأقل زمرتين جزئيتين سايلو 5 (عدد الزمر الجزئية السايلو 5) هو $1+5K$ فإذاً $(1+5K)/6$ فإذاً $K = 0$ أو

$K=1$ إذا كانت $K=0$ فإن زمرة السايلو الجزئية 5 هي زمرة جزئية عادية ، إذا كانت $K=1$ فإن عدد الزمر الجزئية السايلو 5 هو 6 ولتكن $H_6, H_5, H_4, H_3, H_2, H_1$ هم زمر السايلو الجزئية لأن $o(H_i \cap H_j)=1$ لأي $i \neq j$ فهذه الزمر السايلو الجزئية تحوي 24 عنصر من الرتبة 5 وهناك عنصر واحد من الرتبة 1 ، وهكذا فإن فقط 5 عناصر زمر G السايلو 3 الجزئية من G هو $1+3m$ بحيث أن $1+3m \mid 10$.

فإذاً $m=0$ أو 3 إذا كانت $m=0$ فيكون لدينا فقط زمرة 3 سايلو الجزئية واحدة والتي يجب أن تكون عادية ، إذا كانت $m=3$ يكون لدينا 10 زمر سايلو 3 جزئية ، لكن هذه ستكون تحوي 20 عنصر من الرتبة 3 وهذا منافٍ للفرضية أعلاه ، فإذاً G إما أن يكون لها زمر جزئية عادية من الرتبة 5 أو زمر جزئية عادية من الرتبة 3 وهكذا G ليست بسيطة .

تمرين 5

G زمرة من الرتبة P^n حيث P هو عدد أولي و n عدد صحيحاً أكبر من أو يساوي 1 . برهن أن أي زمرة من الرتبة P^{n-1} هي زمرة جزئية عادية من G .

الحل

لتكن H هي زمرة جزئية من G بحيث أن $o(H)=P^{n-1}$ ، بواسطة التمرين 2 فإنه يوجد زمرة جزئية K من G بحيث أن H زمرة جزئية عادية في K و $o(K)=P^n$ ولكن هذا يؤدي إلى أن $K=G$ وهكذا فإن H زمرة جزئية عادية من G .

ملاحظة : من الآن سوف نعطي حلاً لهذا التمرين والذي لا يعتمد على نتيجة تمرين 2 .

سوف نطبق الاستنتاج على n لـ $n=1$ ، G زمرة دوارة من رتبة أولية والزمرة الجزئية الوحيدة من الرتبة P^{n-1} هي $\{e\}$ حيث أن e هو محايد الزمرة G وهذه الزمرة الجزئية العادية البينة .

افرض الآن $n>1$ ولتكن النتيجة صحيحة لكل الزمر الجزئية T من الرتبة P^m ، $1\le m<n$ ولتكن H زمرة جزئية من G من الرتبة P^{n-1} ، H زمرة جزئية عادية من $N(H)$ ، إذا كان $N(H)=H$ فإن $o[N(H)]=P^n$ فإذاً $N(H)=G$ فإذاً ينتج أن H زمرة جزئية عادية من G .

افرض الحالة $N(H)=H$ بما أن $Z=Z(G)$ هو مركز الزمرة G ، $Z \subseteq N(H) \Rightarrow Z \subseteq H$ لأن $P/o(Z)$ فيوجد عنصر $a\in Z$ بحيث أن $o(a)=P$ الزمرة الجزئية $K=<a>$ هي زمرة جزئية من G من الرتبة p الآن $o(H/K)=o\,H\big|o(K)=p^{n-1}/p=P^{n-2}$ بواسطة فرض الاستنتاج H/K هي زمرة جزئية عادية من G/K لأن $o(G/K)=P^{n-1}$ فإذاً H هي زمرة جزئية عادية من G فإذاً النتيجة متحققة .

تمرين 6

بين أنه لا توجد زمرة من الرتبة 108 تكون بسيطة .

الحل

لتكن G زمرة من الرتبة 108 بما أن $108=2^2 3^3$ فإن عدد زمر سايلو 3 الجزئية هي $1+3K$ بحيث أن $1+3k/4$ أما $k=0$ أو $k=1$ في حالة $k=0$ فإنه توجد زمرة سايلو 3 الجزئية واحدة فقط (والتي تكون من الرتبة 27) وهي يجب أن تكون عادية ، فإذاً في هذه الحالة G لها زمرة جزئية عادية من الرتبة 27 نستنتج أن G بسيطة في حالة $k=1$ فإنه هناك أربع زمر سايلو 3 جزئية من G لتكن H_4, H_3, H_2, H_1 بما أن

$$o(H_1\cap H_2)\,|\,o(H_1)\Rightarrow o(H_1\cap H_2)=1,3,9$$

لأن 3 أو $o(H_1 \cap H_2)=1$ يؤدي إلى $o(H_1H_2)=\frac{o(H_1)o(H_2)}{o(H_1 \cap H_2)}>108$ فيكون من الواضح أن $H_1H_2 \le G$ نحصل على $o(H_1 \cap H_2)=9=3^2$ بواسطة تمرين 5 $H_1 \cap H_2$ هي زمرة جزئية عادية من H_1 وبنفس الوقت من H_2 فإذاً :

$$H_2 \subseteq N(H_1 \cap H_2)H_1 \subseteq N(H_1 \cap H_2) \Rightarrow H_1H_2 \subseteq N(H_1 \cap H_2)$$

$$\Rightarrow \qquad o[N(H_1 \cap H_2)] \ge o(H_1H_2)=\frac{o(H_1)o(H_2)}{o(H_1 \cap H_2)}=\frac{27.27}{9}=81$$

لأن $N(H_1 \cap H_2)$ هي زمرة جزئية من G و $o[N(H_1 \cap H_2)]|108$ هذا يؤدي إلى أن :

$$o[N(H_1 \cap H_2)]=108 \Rightarrow N(H_1 \cap H_2)=G$$

الآن $H_1 \cap H_2$ هي زمرة جزئية عادية من $N(H_1 \cap H_2)$ فإذاً $H_1 \cap H_2$ هي زمرة جزئية عادية من من الرتبة 9 فينتج أن G هي ليست زمرة بسيطة .

مسائل

1. لتكن G زمرة منتهية و P عدد أولياً يقسم $o(G)$:

(أ) لأي زمرة سايلو P جزئية P بين أن P هي زمرة سايلو p الجزئية الوحيدة من $N(P)$.

(ب) لتكن P هي زمرة سايلو p الجزئية من G و H هي أي زمرة جزئية من G تحوي $N(P)$ بين أن $N(H)=H$ استنتج ضمنياً أن $N(N(P))=N(p)$.

إرشاد : طبق نظرية سايلو الثانية .

2. برهن أن التعاريف الآتية لزمرة سايلو p الجزئية تكافئ لما معطى قريباً .

تعريف : لتكن G زمرة منتهية و p عدد أولياً فإن الزمرة الجزئية P من G تسمى زمرة سايلو p الجزئية من G إذا حققت الشروط الآتية :

(1) P هي زمرة p الجزئية .

(2) لا توجد زمرة p جزئية من G تحوي P بشكل فعلي .

إرشاد : استخدم النظرية 22.4 .

3. بين أنه إذا كانت H زمرة جزئية عادية من الزمرة المنتهية G و p قاسم أولي لـ $o(G)$ بحيث أنه $[G:H]$ هو مصاحب أولي لـ p فإن H تحوي جميع زمر سايلو p الجزئية من G .

اعط مثال توضح فيه أن النتيجة لا تبقى صحيحة في حالة كون H ليست عادية .

إرشاد : إذا كان p^k هو أعلى قوى لـ P تقسم $o(G)$ فإن $P^K/o(H)$ الآن استخدم نظرية سايلو الثانية .

4. بين أن زمرة p العادية الجزئية K من الزمرة المنتهية G هي محتواة في كل زمر سايلو p الجزئية من G .

إرشاد : استخدم النظرية 22.4 ونظرية السايلو الأولى .

5. برهن أن الزمر من الرتبة 15 و 35 تكون دوارة .

6. اعط مثال لزمرة من الرتبة p^3 ، p عدد أولياً وتكون غير إبدالية .

7. إذا كان $o(G)=36$ برهن أن G لها 1 أو 4 زمر سايلو 3 جزئية .

8. إذا كان $o(G)=56$ برهن أن G لها 1 أو 8 زمر سايلو 7 جزئية ، وبرهن أن G لها زمرة سايلو 2 جزئية عادية .

9. لتكن G زمرة إبدالية و K,H زمرتين جزئيتين منتهيتين من الرتبة n,m برهن أن G لها زمرة جزئية من الرتبة $L\subset M$ من n,m .

إشاد : لأن $m/o(HK)$ و $n|o(HK)$ إذا كان $K=LCM$ من n,m فإن $K|o(HK)$ الآن استخدم النظرية 12.4 .

10. برهن أن زمرة من الرتبة 48 يجب أن تحوي زمرة جزئية عادية من الرتبة 8 أو 16 .

11. برهن أن زمرة من الرتبة p^2q حيث q,p أعداد أولية مختلفة لها على الأقل زمرة سايلو عادية جزئية .

إرشاد : استخدم نظرية السايلو الثالثة .

12. لتكن G زمرة منتهية و p عدد أولياً يقسم $o(G)$ برهن ما يلي :

(أ) إذا كانت K زمرة جزئية عادية من G فإن أي زمرة سايلو p جزئية p من G ، $P\cap K$ هي زمرة سايلو p جزئية من K ينتج أن أي زمرة سايلو P جزئية B من $B=p\cap k,k$ لبعض زمر سايلو p جزئية p من G .

(ب) إذا كان H زمرة جزئية من G فإن لأي زمرة سايلو p جزئية P من G PH/H هي زمرة سايلو p جزئية من G/H ، ينتج أن أي زمرة p سايلو جزئية من G/H هي من الشكل pH/H حيث P هي زمرة سايلو جزئية من G .

13. بين أن الزمرة G هي زمرة $p-$ إذا وفقط إذا وجدت زمرة جزئية عادية N من G حيث أن N و $G \quad N$ كلاهما زمرة p .

14. برهن أنه إذا كانت G زمرة من الرتبة 28 لها زمرة جزئية عادية من الرتبة 4 فإن G يجب أن تكون إبدالية .

15. اعط برهان لنظرية كوجي للزمر المنتهية (ليس بالضرورة إبدالية) ولكن دون الاعتماد على نظرية السايلو الأولى .

16. إذا كان أي زمرة سايلو جزئية من G هي عادية فبين أن G هي حاصل الضرب المباشر من زمر سايلو الجزئية .

17. H هي زمرة جزئية من زمرة منتهية G و p عدداً أولياً يتتم رتبة H إذا كان Q,P هما زمرتا سايلو P جزئية من H وإذا كان T,S هما زمرتا سايلو p جزئية من G بحيث أن $P \leq S$ و $Q \subseteq T$ بين أن $S \neq T$.

18. إذا كانت H زمرة جزئية من زمرة منتهية G و p عدداً أولياً يتمم $o(H)$ بين أن عدد زمر السايلو p الجزئية من H هو أقل من أو يساوي عدد زمر سايلو الجزئية من G .

19. G زمرة جزئية ، P عدد أولياً يقسم رتبة الزمرة G إذا كانت A زمرة جزئية نظامية من G و H هي زمرة سايلو p جزئية من G فبرهن أن $A \cap H$ هي زمرة سايلو p جزئية من A .

إرشاد : رفض النتيجة ، يوجد زمرة سايلو p جزئية P من A وزمرة سايلو p جزئية Q من G بحيث أن $A\cap H\subseteq P=Q$ ، وبواسطة نظرية السايلو الثانية $H=xQx^{-1}$ لبعض عناصر $x\in G$ فإن $xPx^{-1}\subseteq x(A\cap Q)x^{-1}$ لأن $P\subseteq A$ هذا سوف يعطي :

$$xPx^{-1}\subseteq\left(xAx^{-1}\right)\cap\left(xQx^{-1}\right)\Rightarrow xPx^{-1}\subseteq\left(xAx^{-1}\right)\cap H\Rightarrow xPx^{-1}\subseteq A\cap H$$

لأن A هي زمرة جزئية ناظمية من G فيكون $xpx^{-1}\subset P$ ولكن xpx^{-1} هي زمرة سايلو جزئية من G فإذاً سنحصل على الشرط .

20. اعط مثال لزمرة منتهية G وزمرة جزئية A من G حيث أنه عندما P عدداً أولياً يقسم $o(G)$ و H هي زمرة سايلو p جزئية من G فإن $A\cap H$ هي ليست زمرة سايلو P جزئية من A .

إرشاد : خذ $H=\{I,(124),(142)\}A=\{I,(123),(132)\},G=A_4$.

3. الزمر المنتهية الإبدالية

لتكن G زمرة منتهية إبدالية ، بينت النظرية 10.4 أن G يعبر عنها كجمع مباشر (ضرب) من زمرها السايلو الجزئية .

وبصورة ضمنية إذا كانت G دوارة نعلم أن أي زمرة جزئية من G تكون دوارة ، ولأن G يعبر عنها كحاصل جمع مباشر (ضرب) من زمر سايلو الجزئية كل واحدة منها هي دوارة ، ففي هذا البند سوف نرى أن أي زمرة منتهية إبدالية G يمكن التعبير عنها كحاصل جمع مباشر (ضرب) من عدد منتهٍ من زمر جزئية دوارة ، بالبحث عن المكافئات سوف نرمز للعملية الثنائية بالضرب .

مفترضة 23.4

لتكن b,a عنصران من رتب منتهية للزمرة G بحيث أن $o(a)$ و $o(b)$ هما مكملتان أوليتان و $ab=ba$ فإن $o(ab)=o(a).o(b)$.

البرهان

ليكن $o(a)=m$ و $o(b)=n$ ولتكن $H=<ab>$ هي الزمرة الجزئية من G المتولدة بـ ab لأن $(ab)^{mn}=a^{mn}b^{nm}=e$ نحصل على أن $o(H)=o(ab)|mn$ الآن $(ab)^{m}=a^{m}b^{m}=b^{m}\in H$ لأن $a^{m}=e$ ، بما أن $(m,n)=1$ و $o(b)=n$ يكون لدينا $o(b^{m})=o(b)=n$ الآن $b^{m}\in H\Rightarrow o(b^{m})|o(H)\Rightarrow n|o(H)$ وبنفس الطريقة $m|o(H)$ وهكذا يكون $mn|o(H)$ فإذاً $o(H)=mn=o(ab)$ وهذا هو برهان المفترضة .

تعريف 24.4 (الأس للزمرة)

لتكن G زمرة منتهية إذا كان K هو أعلى قوة لجميع عناصر G فإن K الأس للزمرة G أي أن إذا وجد $a\in G$ بحيث أن $o(a)=k$ ولا يوجد عنصر آخر في G له رتبة أعلى من K فإن K يسمى أُس G .

مفترضة 25.4 : الرتبة لأي عنصر في زمرة منتهية إبدالية G يقسم أُس الزمرة G .

البرهان : لتكن K أُس الزمرة G أي أنه يوجد $a \in G$ بحيث أن $o(a)=k$ ولكل عنصر $o(b) \leq o(a) = K , b \in G$ افرض للجدل وجود عنصر $b \in G$ بحيث أن K $o \nmid (b)$ هذا يؤدي إلى وجود عدداً أولياً P بحيث أن لبعض الأعداد الصحيحة الموجبة $p^t / o(b) t$ ولتكن $o(a)$ p^t هذا يعني أننا يمكننا أن نكتب $o(a) = p^\alpha S , o(b) = p^\alpha q$ بحيث أن $(p,q)=1,(p,s)=1$ و $o(a_o)=s$ مفترضة 23.4 تعطي $o(a_o b_o) = p^\alpha s > p^\beta s = o(a)$ وهذا خلاف الفرض أن $k = p^\beta s$ هو أس الزمرة G فإذاً المفترض برهن .

مثال 10

S_3 ليست إبدالية ، أعلى رتبة لأن عنصر في S_3 هو 3 أي أن أُس S_3 هو 3 ، على أية حال (12) عنصر من S_3 من الرتبة 2 وأن $o(12) \nmid 3$.

هذا يبين أن المفترضة أعلاه لا تصح في حالة الزمر غير الإبدالية .

نظرية 26.4 (النظرية الأساسية للزمر الإبدالية المنتهية)

كل زمرة إبدالية منتهية G من الرتبة n هي عبارة عن ضرب مباشر $G = G_1 \times G_2 \times \ldots \times G_t$ حيث G_i زمرة جزئية دوارة من الرتبة n_i بحيث أن n_{i+1} / n_i والعدد الصحيح n_i يحدد بشكل وحيد وأيضاً $n = n_1 n_2 .. n_t$ (لاحظ عندما $o(G)>1$ فإن كل G_i يكون لها $o(G_i)>1$) .

البرهان

نبرهن النتيجة بواسطة الاستنتاج على $o(G)$ إذا كان $o(G)=1$ فإن النتيجة متحققة بشكل واضح .

نفرض أن $o(G)=n>1$ وأن النتيجة متحققة لكل الزمر التبديلية والتي تكون رتبتها أقل من $o(G)$.

لتكن n_1 هو أُس الزمرة G و g_1 هو عنصر في G من الرتبة n_1 ولتكن $G_1 = < g_1 >$ إذا كان $G=G_1$ فإن G نفسها هي دوراة ، لتكن $G \neq G_1$ فإن $1<o(G/G_1)<n$ بواسطة استنتاج الفروض $G/G_1 = \overline{H}_2 \times \overline{H}_3 \times ... \times \overline{H}_t$

حيث كل من $\overline{H}_i$ هي زمرة جزئية دوارة من $\overline{G}=G/G_1$ من الرتبة $n_i>1$ بحيث أن :

$n_{i+1}/n_i \quad \forall_i = 2,3,...,t-1$

وأن :

$$\frac{n}{n_i} = o(\overline{G}) = n_2 n_3 ..n \qquad (1)$$

الآن كل $\overline{H}_i = H_i / G_1$ لبعض الزمر الجزئية H_i في G تحوي G_1 اختر $h_i \in H_i$ بحيث أن $\overline{h}_i = h_i G_1$ هو مولد $\overline{H}_i$ فإن $\overline{h}_i^{ni} = \overline{e} = \overline{G}_1 \Rightarrow h_i^{ni} \in G_1 = < g_1 > \Rightarrow h_i^{ni} = g_1^{mi}$

لبعض القيم m_i بحيث أن $1 \le m_i \le n_1$ لتكن $\alpha_i = (m_2 n_1)$ فإن $m_i = \alpha_i \beta_i$ لبعض $n_1 = \alpha_i \delta_i \,, \beta_i \ge 1$ لبعض $\delta_i \ge 1$ و $(\beta_i, \delta_i)=1$.

الآن $o(g_1)=n_1=\alpha_i \delta_i \Rightarrow o(g_1^{\alpha_i}) = \delta_i$ وبما أن $(\delta_i, \beta_i)=1$ ، $o(g_1^{\alpha_i \beta_i}) = o(g_1^{\alpha_i})$ على أي حال $h_i^{n_i} = g_1^{\alpha i \beta i}$ فإذاً $o(h_i^{ni}) = \delta_i$ من ناحية أخرى :

$$o(\overline{h}_i) \Big| o(h_i) \Rightarrow n_i \Big| o(h_i) \to o(h_i^{ni}) = \frac{o(h_i)}{n_i} \Rightarrow o(h_i) = o(h_i^{ni}) n_i = \delta_i n_i \quad (2)$$

لأن $o(h_i)|n_1$ الأس للزمرة G و $n_1 = \alpha_i \delta_i$ نحصل على $\delta_i n_i | \alpha_i \gamma_i$ أو $n_i|\alpha_i \Rightarrow n_i \delta_i$ لبعض $\delta_i \ge 1$ فإن $h_i^{ni} = g_1^{ni\delta i \beta i}$.

اجعل $g_i = h_i(g_1)$ لكل $i=2,3,...,t-1$ نرى أن :

$$\overline{g}_i = gG = \overline{h}_i \,, g_i^{ni} = h_i^{ni} (g_1)^{-ni\delta i \beta i} = e$$

هذا يجعل $o(g_i)=n_i$.

عرف $H=<g_2><g_3>...<g_t>$ ، H هي زمرة جزئية من G بحيث أن $o(H)|n_2n_3..n_t$

لتكن س $f=G\to G/G_1$ هو هومومورفيزم الطبيعي ، لأن

$$f(H)=<\overline{g}_2>\times<\overline{g}_3>\times..\times<\overline{g}_t>=\overline{H}_2\times\overline{H}_3\times...\times\overline{H}_t=G/G_1$$

وأيضاً $f(H)=(HG_1)/G_1$ نحصل على

$$G=HG_1=G_1H=<g_1><g_2>...<g_t>$$

الحقيقة أن $o(G)=n=n_1n_2...n_t=o(g_1)o(g_2)...o(g_t)$

تعطي $G=<g_1>\times<g_1>\times..\times<g_t>$

وأيضاً $o(<g_i>)=o(g_i)=n_i$ بحيث أن n_{i+1}/n_i افرض أن :

$$G=H_1\times H_2\times...\times H_t \qquad (3)$$

$$=K_1\times K_2\times...\times K_4 \qquad (4)$$

هما تعبيران عن G بشكل حاصل ضرب مباشر لزمر جزئية دورية بحيث أن $o(H_i)=n_i,\ o(K_j)=m_j, i=1,2,...,t, j=1,2,...,4$ ول :

$$i\le t-1,\ n_{i+1}/n_i,\ j\le u-1,\ m_{j+1}/m_j$$

افرض أن $g\in G$ فإن (3) تعطي $g=h_1h_2..h_t\ ,h_i\in H_i$ لأن $o(h_i)|o(H_i)=n_i$ و n_i/n_1 نحصل على $h_i^{n1}=e$ نستنتج أن $g^{n_1}=h_1^{n1}h_2^{n2}..h_t^{nt}=e$ وهكذا $o(g)\le n_1$ لكل $g\in G$ وأيضاً H_1 هي زمرة دوارة من الرتبة n_1 ، H_1 تحوي عنصر من الرتبة n_1 فإذاً n_1 هو أُس للزمرة G وبنفس الطريقة m_2 هو أُس لـ G فإذاً $n_1=m_1$ افترض أننا برهنّا أن $n_1=m_1, n_2=m_2,...,n_{i-1}=m_{i-1}$ لبعض i سوف نبرهن أن $n_i=m_i$ افرض أن جدلاً $n_i\neq m_i$ ولتكن معرفة لتكن $n_i>m_i$ عرف $K=\{x^{mi}\,|\,x\in G\}$ لأن أي $x,y\in G, x^{mi}y^{-mi}=(xy^{-1})^{mi}\in G$ نحصل على أن K هي زمرة جزئية من G ، افرض أن

لأي $K=1,2,...,t$ $H_K=<a_K>$ ولكـــــــــــــل $K_j=<b_i>, j=1,2,...,4$ لأن لأي $b_j^{mi}=e, o(K_j)=m_j|m_i, j\geq i$ فيكون $K=<b_1^{mi}>\times<b_2^{mi}>\times..\times<b_{i-1}^{mi}>$ وهكذا :

$$o(K)=\frac{m_1}{m_i}\frac{m_2}{m_i}...\frac{m_{i-1}}{m_i}, o(b_j)=m_j\forall_j \qquad (5)$$

وأيضاً $G=<a_1>\times..\times<a_t>$ (من 3) لدينا :

$$K=<a_1^{mi}>\times<a_2^{mi}>\times..\times<a_t^{mi}>$$

الآن $$o\left(a_k^{mi}\right)=\frac{n_k}{(m_i, n_k)} \qquad \forall_K = 1,2,...,t$$

نستنتج أن :

$$o(k)=\frac{n_1}{(m_i,n_1)}\frac{n_2}{(m_i,n_2)}\cdots\frac{n_i}{(m_i,n_i)}\frac{n_{i+1}}{(m_i,n_{i+1})}\cdots\frac{n_t}{(m_i,n_t)} \qquad (6)$$

الآن $m_i|m_j$ و $m_j=n_j$ لكل $j<i$ بواسطة فرضنا وهكذا :

$$\frac{n_i}{(m_i,n_j)}=\frac{m_j}{(m_i,m_j)}=\frac{m_j}{m_i} \qquad \forall_j<i$$

فإذاً من (5) و (6) نحصل على :

$$1=\frac{n_i}{(m_i,n_i)}\cdots\frac{n_t}{(m_i,n_t)} \qquad (7)$$

على أي حال $m_i<n_i$ تعطي $\frac{n_i}{(m_i,n_i)}>1$ بما أن ينتج من (7) لا يمكن أن تتحقق هذه تعطي $m_i=n_i$ وهكذا بواسطة الاستنتاج $m_i=n_i\forall_i$ فإذاً $n=n_1n_2..n_t=m_1m_2..m_u$ وهكذا يجب أن نحصل أيضاً على أن $t=u$ وهذا هو تمام البرهان .

نتيجة 27.4

كل زمرة p إبدالية G يمكن التعبير عنها كحاصل ضرب داخلي مباشر من زمر دوارة $G = G_1 \times G_2 \times ... \times G_r$ بحيث أن $o(G_i) = p^{mi}$ $\forall_i = 1, 2, ..., r$ و $\forall_j = 1, 2, ..., r-1, m_i \geq m_{j+1}$ وأيضاً P^{mi} تحدد بشكل وحيد .

البرهان

بواسطة النظرية السابقة يمكن التعبير :

$$G = G_1 \times G_2 \times .. G_r \qquad (1)$$

بحيث أن G_i هي زمرة جزئية دوارة من الرتبة n_i وأن $n_{j+1} | n_j \forall_j \leq r-1$ لأن G هي زمرة p فإن أي G_i هي زمرة p يكون لدينا $o(G) = p^m$ لبعض $n_i = o(G_i) = p^{mi} \forall_i$ لأن $n_{i+1} | n_j$ نحصل على $m_{j+1} \leq m_i$ لكل $j \leq r-1$ إذا كانت :

$$G = H_1 \times H_2 \times ... \times H_S \qquad (2)$$

هو تركيب آخر لـ G لزمر جزئية دوارة بحيث أن $\forall i = 1, 2, ..., S$ $o(H) = p^{ui}$ وأن $\forall j \leq s-1$ $u_j \geq u_{j+1}$ نرى أن $\forall i \leq s-1$ $o(H_{j+1}) | o(H_j)$ ويكون بواسطة النظرية السابقة $r-S$ وأن $\forall i = 1, 2, ..., r$ $o(H_i) = o(G_i)$ وهذا تحقيق للنتيجة .

ملاحظة 1 : لتكن G زمرة p إبدالية منتهية كما رأينا في النتيجة السابقة يمكن التعبير $G = G_1 \times G_2 \times ... \times Gr$ كحاصل ضرب داخلي مباشر من زمر p جزئية دوارة G_i من الرتبة p^{ni} الأعداد p^{n1}, p^{n2}, p^{nr} متحدة بشكل وحيد بواسطة G وتسمى ثوابت G لتكن G' هي زمرة منتهية إبدالية أخرى ، من الواضح أن $G \cong G'$ فإذاً G', G يجب أن يكون لها نفس عدد الثوابت ، وبالعكس إذا كانت G' لها نفس عدد الثوابت مثل G فإنه بواسطة

تعريف الثوابت نحصل على $G' = G'_1 \times G'_2 \times ... \times G'_r$ بحيث أن G'_i هي زمرة دوارة من الرتبة p^{ni} لأن أي زمرتين دوارتين من نف الرتبة هما أيزومورفيتان نحصل على $G_i \approx G'_i$ هذا إذاً يعطي أن $G \cong G'$ فإذاً زمرتان إبداليتان منتهيتان هما إيزومورفيتان إذا وفقط إذا كان لهما نفس مجموعة الثوابت ، وهكذا على سبيل المثال إذا كانت G من الرتبة p^3 فإن المجموعة الممكنة من الثوابت لـ G هي $\{p,p,p^2\},\{p^2,p\},\{p^3\}$ ينتج أنه يوجد مع التشاكل فقط ثلاث زمر تبديلية من الرتبة p^3 . مرة ثانية إذا كانت رتبة G هي p^3 فإن المجموعة الممكنة من الثوابت لـ G هي $\{p,p^2\},\{p^2\}$ فإذاً عدد الزمر الغير إيزومورفية من الرتبة p^2 هما اثنان .

ملاحظة 2 : افرض أي زمرة إبدالية منتهية نحن نعلم أن : $G = S(p_1) \times S(p_2) \times ... \times S(p_t)$ (نظرية 10.4) لأن كل $S(p_i)$ هي زمرة $S(p_i), p_i$ يمكن التعبير عنها كحاصل ضرب مباشر منتهي في زمر p_i دوارة ينتج أن G نفسها يمكن التعبير عنها كحاصل ضرب منتهي من زمر دوارة من قوى فردية . كما في النتيجة السابقة يمكن ملاحظة أن رتبة هذه الزمر الدوارة تحدد بشكل وحيدة بواسطة G نفسها ومجموعة هذه القوى يمكن تحديدها مرة أخرى كمجموعة من ثوابت G ، مرة أخرى فإن زمرتان إبداليتان منتهيتان هما أيزومورفيتان إذا وفقط إذا كان لهما نفس مجموعة الثوابت .

تمارين محلولة

تمرين 1

لتكن G زمرة إبدالية وليكن $a,b\in G$ عنصران من الرتبة n,m بحسب الترتيب ، بين أنه يوجد عنصر c ينتمي إلي G بحيث أن $o(c)=k$ هو LCM بالنسبة لـ n,m .

الحل

أولاً افرض أن $(m,n)=1$ فإن $k=mn$ ضع $c=ab$ من الواضح أن $c^{mn}=(a^m)^n(b^n)^m=e=o(c)$ هو منتهي وهو أصغر من أو يساوي mn لتكن $o(c)=t$ فإن

$$e=c^k=a^tb^t \Rightarrow a^t=b^{-t} \Rightarrow e=a^{mt}=b^{-mt} \to b^{mt}=e \Rightarrow n|mt \Rightarrow n/t$$

لأن $(m, n) = 1$ وبنفس الطريقة يمكن إثبات أن m/t وأيضاً لأن $(m, n) = 1$ نحصل على mn/t أي أن $mn\le t$ فإذاً $o(c)=mn$.

الآن افرض أن $(m, n) > 1$ يمكن أن نجعل $m=p_1^{\alpha 1}p_2^{\alpha 2}...p_u^{\alpha u}$ و $n=p_1^{\beta 1}p_2^{\beta 2}...p_u^{\beta u}$ حيث أن p_i هي أعداد أولية مختلفة و α_i,β_i هي أعداد صحيحة غير سالبة بحيث أن $\alpha_i\ge\beta_i\forall 1\le i\le t$ و $\forall t+1\le j\le u \quad \alpha_j<\beta_j$ خذ $k=p_1^{\alpha 1}p_2^{\alpha 2}...p_t^{\alpha t}p_{t+1}^{\beta_{t+1}}...p_u^{\beta_u}$ ضع $g=a^{p_{i+1}{}^{\alpha i+1}...p_k{}^{\alpha_k}}$ و $h=b^{p_1{}^{\beta_1}p_2{}^{\beta_2}...p_t^{\beta_t}}$ فلذلك $o(g)=p_1^{\alpha_1}p_2^{\alpha_2}...p_t^{\alpha_t}$ و $o(h)=p_{t+1}^{\beta_{t+1}}...p_u^{\beta u}$ من الواضح أن $o(g)$ و $o(h)$ هي متممات أولية فإذاً وبواسطة الحالة الأولى $c=gh$ لها رتبة تساوي $p_1^{\alpha_1}p_2^{\alpha_2}...p_t^{\alpha_t}p_{t+1}^{\beta_{t+1}}...p_u^{\beta u}$ أي أن $o(c)=k$.

تمرين 2

إذا كان n هو أُس للزمرة الإبدالية G فإذاً لكل $a\in G$ فإن $o(a)$ يقسم n .

الحل

ليكن $o(a)=m$ إذا كان m لا يقسم n فإن $LCM=[m_1n]$ لكل من n,m هو بالضبط أكبر من n بواسطة التمرين أعلاه فإنه يوجد عنصر $c\in G$ بحيث أن $o(c)=[m_1n]>n$ وهذا خلاف تعريف الأُس .

ملاحظة : هذا يعطي برهان آخر للمفترضة 25.4 .

تمرين 3

لتكن G زمرة إبدالية ومنتهية والتي فيها عدد حلول المعادلة $x^n=e$ على الأكثر n لكل عدد صحيح موجب ، برهن أن G زمرة دائرية .

الحل

لتكن رتبة الزمرة G هي m وليكن n_1 هو أُس الزمرة G لأن لكل $o(a)|n_1, a^{n1}=e, a\in G$ لكل $a\in G$ فإذاً $x^{n-1}=e$ لها m من الحلول فإذاً $m\le n_1$ لأن $x^{n1}=e$ لها n_1 من الحلول ، بما أن أُس الزمرة G هو n_1 فإنه يوجد عنصر $b\in G$ بحيث أن $o(b)=n_1$ ولكن $o(b)|o(G)\Rightarrow n_1|m\Rightarrow n\le m$ فإذاً $m=n1$ أي أن $o(b)=m=o(G)$ نستنتج أن G زمرة دوارة متولدة بـ b .

مسائل

1. أوجد ثوابت زمرة دائرية من الرتبة n .

إرشاد : إذا كان $n = p_1^{\alpha 1} p_2^{\alpha 2} ... p_t^{\alpha t}$ و G زمرة دائرية من الرتبة n فإن $G = G_1 \times G_2 \times ... \times G_i$ حيث G_i هي زمرة جزئية دائرية من G من الرتبة $p_i^{\alpha i}$.

2. استخدم النظرية الأساسية للزمر الإبدالية المنتهية ببرهان ما يلي إذا كانت G زمرة إبدالية منتهية من الأُس n فلا يوجد لها زمر جزئية فعلية قوى جميع العناصر من الرتبة n
3. اعط تفاصيل البرهان لحقيقة أن زمرتين إبداليتين منتهيتين هما إيزومورفيتان إذا وفقط إذا لهما نفس مجموعة الثوابت .
4. زمرة إبدالية لها الثوابت p, p حيث p عدد أولياً . ما عدد الزمر الجزئية من الرتبة p تحوي (جواب $p+1$) .
5. للعدد $n = 20$ ما عدد الزمر الإبدالية الغير إيزومورفية من الرتبة n موجودة (جواب : اثنان) .
6. الزمرة الإبدالية G من الرتبة p, p^3 عدد أولياً لها الثوابت p, p^2 حدد جميع زمرها الجزئية من الرتبة p .
7. لأي عدد صحيح موجب n ولأي عدد أولي p برهن أن عدد الزمر p الإبدالية الغير إيزومورفية من الرتبة p^2 يساوي عدد التجزئة للعدد n .

5

الزمر القابلة للحل ونظرية جوردان هولدر

Solvable Groups and Jordan-Holder Theorem

1- مولدات زمر جزئية والزمر الجزئية المشتقة

سابقاً ناقشنا مفهوم مولد الزمر الدائرية ، نحاول هنا أن نضم نفس المفهوم لزمر اختيارية .

تعريف 5-1

لتكن S مجموعة جزئية من الزمر G ، يقال للزمر الجزئية H في G أنها مولد بالمجموعة S ، إذا كانت تحقق الشروط الآتية :

1- $S \subseteq H$

2- إذا كانت K أية زمرة جزئية من G بحيث $S \subseteq K$ فإن $H \subseteq K$.

نرمز للزمرة الجزئية المولدة بالمجموعة S بالرمز $<S>$.

ملاحظة

افرض F هي عائلة جميع الزمر الجزئية في G والتي تحوي S ، هذه العائلة غير خالية ، لأن $S \subseteq G$ ، عليه فإن $G \in F$ ، لتكن H_1 تقاطع جميع عناصر F ، من الواضح أنه إذا كانت K أية زمرة جزئية من G تحوي S فإن $H_1 \subseteq K$ ، إضافة إلى ذلك $S \subseteq H_1$ لأن $S \subseteq K$ لكل $K \in F$ ، إذن H_1 زمرة جزئية في G مولدة بالمجموعة S ، عليه بصورة بديلة يمكننا القول أن الزمرة الجزئية H في G مولدة بالمجموعة S إذا كانت H تقاطع جميع الزمر الجزئية في G والتي تحوي S .

الآن إذا كانت S مجموعة جزئية في الزمرة G ، فإنه من المحتمل أن تكون G نفسها هي الزمرة الجزئية الواردة في S ، عندئذ S تسمى مجموعة مولدات الزمرة G . على سبيل المثال إذا كانت $G=<a>$ زمرة دائرية ، فإن $S=\{a\}$ هي مجوعة مولدات G وهنا S مجموعة أحادية .

نظرية 5-2

إذا كانت S أية مجموعة جزئية غير خالية في الزمرة G ، فإن الزمرة الجزئية $<S>$ المولدة بالمجموعة S في G هي مجموعة جميع حواصل الضرب المنتهية بالصيغة $a_1\, a_2 \ldots a_n$ حيث يكون إما $a_n \in S$ أو $a^{-1} \in S$.

البرهان

لتكن H مجموعة جميع حواصل الضرب المنتهية بالصيغة $a_1\, a_2 .. a_n$ بحيث a_{n1} أو a_n^{-1} ينتمي إلى S حيث n أي عدد صحيح موجب . اعتبر $x=a_1a_2..a_n$ ، $y=b_1b_2..b_m$ عنصران في H ، فإن $xy=a_1a_2..a_nb_1b_2..b_m$ عبارة عن حاصل ضرب عدد منته في العناصر a,b بحيث إما العامل أو معكوسه ينتمي إلى S ، بالتالي $xy \in H$ ، إضافة إلى ذلك $x^{-1}=a_n^{-1}a_{n-1}^{-1}..a_2^{-1}a_1^{-1}$. اعتبر أي a_i^{-1} .

بما أن a_i أو a_i^{-1} ينتميان إلى S و $a_n = \left(a_n^{-1}\right)$ نجد أنه إما a_n^{-1} أو $\left(a_n^{-1}\right)^{-1}$ تقع في S إذن $x^{-1} \in H$ ، هذا يثبت أن H زمرة جزئية من G ، من الواضح أن $S \subseteq H$ اعتبر أن زمرة جزئية K من G تحوي S فإن كل $a \in S$ يكون أيضاً $a \in K$ ، وبالتالي $a^{-1} \in K$ ، عليه إذا كان $x=a_1a_2...a_n$ عنصراً في H ، حيث $a_n \in S$ أو $a^{-1} \in S$ ، فإن $x \in K$ لأن $a_i \in k$ لكل K ، إذن $H \subseteq K$ وهذا يبرهن أن H زمرة جزئية من G مولدة بالمجموعة S .

مثال 1

لتكن A مجموعة جميع المناقلات في زمرة التناظرات S_r ، بما أن كل $f \in S_n$ هي حاصل ضرب مناقلات وبالتالي عناصر في A نحصل على أن A تولد S_n .

مثال 2

$S=\{1\}$ هي مولدة للزمرة الجميعة للأعداد الصحيحة S .

مثال 3

اعتبر $S_3=\{I,(12),(13),(23),(123),(132)\}$

افرض $a=(12)$ ، $b=(123)$ ، فإن $b^2=(132)$ ، $b^3=I$ ، $ba=(13)$ ، $ab=(23)$ ، إذن نجد أن كل عنصر في S_3 يمكن التعبير عنه كضرب لعناصر المجموعة $A=\{a,b\}$ بالتالي A تولد S_3 .

مثال 4

لتكن $G=\{\pm 1,\pm n,\pm j,\pm K\}$ الزمرة الكواترينية ، و $A=\{i,j\}$. افرض H هي الزمرة الجزئية من G المولدة بالمجموعة A فإن $i\in H$ ، $j\in H$ ، $ij=K\in H$ كذلك $-i=i^3\in H$ ، $-j=j^3\in H$ ، $-K=K^3\in H$ ، $-1=i^2\in H$ ، $1=i^4\in H$ ، هذا يبرهن أن H_1 تحوي جميع عناصر G بالتالي $H=G$ وأن A تولد G .

تعريف 3-5

ليكن b,a أي عنصرين في الزمرة G المبادل للعنصرين b,a هو العنصر $a^{-1}b^{-1}ab$ زمرة المبادلات للزمرة G يرمز لها بالرمز G' وهي الزمرة الجزئية من G المولدة من مجموعة جميع مبادلات الزمرة G .

زمرة المبادلات تسمى أيضاً الزمرة الجزئية المشتقة الأولى ، أو ببساطة الزمرة الجزئية المشتقة .

نظرية 5-4

لتكن G زمرة و G' الزمرة الجزئية لمبادلاتها ، فإن :

1− G' زمرة جزئية عادية من G .

2− لأي زمرة جزئية عادية H من G فإن G/H زمرة أبيلية إذن وفقط إذن كانت H تحوي G' .

البرهان

1− ليكن $a,b \in G$ ، بما أن $\left(a^{-1}b^{-1}ab\right)^{-1} = b^{-1}a^{-1}ba$ هو أيضاً مبادل ، نجد أن كل عنصر في G' هو حاصل ضرب عدد منته من المبادلات .

نظرية 5-3

اعتبر $x \in G$ فإن $x - g_1 g_2 .. g_t$ حيث g_i مبادل لكل $i=1,2,...,t$ ، عليه فإن $g_i = a_i^{-1}b_i^{-1}a_i b_i$ لبعض $a_i , b_i \in G$ ، الآن لأي $a \in G$.

$$a^{-1}x\,a = \left(a^{-1}g_1 a\right)\left(a^{-1}g_2 a\right)...\left(a^{-1}g_t a\right)$$

إضافة إلى ذلك

$$\begin{aligned} a^{-1}g_i a &= a^{-1}a_i^{-1}b_i^{-1}a_n b_i a \\ &= \left(a^{-1}a_i a\right)^{-1}\left(a^{-1}b_i a\right)^{-1}\left(a^{-1}a_i a\right)\left(a^{-1}b_i a\right) \\ &= c^{-1}d^{-1}cd \end{aligned}$$

حيث

$$d = a^{-1}b_i a , c = a^{-1}a_i a$$

هذا يبين لنا أن $a^{-1}g_i a$ هو أيضاً مبادل ، إذاً $a^{-1}xa$ هو حاصل ضرب مبادلات و حسب التعريف $a^{-1}xa \in G'$ ، هذا يثبت النتيجة .

2− اعتبر أن $a,b \in G$ ، افرض G/H أبيلية هذا يؤدي إلى أن :

$$\begin{aligned} &(aH)(bH) = (bH)(aH) \\ &= abH = baH \Rightarrow a^{-1}b^{-1}ab = (ba)^{-1}(ab) \in H \end{aligned}$$

عليه فإن H تحوي كل المبادلات $a^{-1}b^{-1}ab$ بالتالي وبما أن G' يتولد من جميع المبادلات، فإن $G' \subseteq H$.

بالعكس افرض $G' \subseteq H$ فإن $a^{-1}b^{-1}ab \in G'$ هذا يعطينا :

$$\begin{aligned} a^{-1}b^{-1}ab \in H &\Rightarrow abH = baH \\ &\Rightarrow (aH)(bH) = (bH)(aH) \end{aligned}$$

والذي يحقق أن G/H زمرة أبيلية ، بأخذ $H = (e)$ نحصل على نتيجة 5-5 الزمرة G إبدالية إذا وفقط إذا كان $G' = (e)$.

مسائل

1- برهن أن في $S_n(3\le n)$ مجموعة كل 3- دورات تولد A_n .

إرشاد : كل عنصر في A هو حاصل ضرب عدد زوجي من المناقلات لأي مناقلتين (ij) و (kl) في S_n لدينا $(ij)(kl)=(ijl)$ عندما $k=j$

وعندما $l\ne i,j,k\ne i,j$

فإن $(ij)(kl)=(ij)(jk)(jk)(kl)=(ijk)(klj)]$

2- في السؤال السابق استنتج أن مجموعة جميع الـ 3- دورات بالصيغة (ij) تولد A_n .

إرشاد : بين أن أي دورة 3- هو حاصل ضرب دورات 3- بالصيغة $(lij)]$.

3- لأي اندومورفرم ~ للزمرة G برهن أن صورة مبادل ما $a^{-1}b^{-1}ab$ تحت 6 هو أيضاً مبادل ، استنتج أن G هي زمرة جزئية مميزة للزمرة G .

4- لأي زمرة G أثبت أن :

$$G'=\{a_1a_2..a_na_1^{-1}a_2^{-1}a_3^{-1}..a_n^{-1}|a_i\in G,n\ge 2\}$$

5- للزمرة $G=S_3$ أثبت أن :

$$G'=A_3$$

6- لأي زمرة بسيطة غير أبدالية ، برهن أن : $G'=G=1$

[إرشاد : A_n زمرة بسيطة غير إبدالية و $S_n'\subseteq A_n$ **]** .

7- إذا كانت H و K زمرتان جزئيتان من الزمرة G برهن أن :

$$H\subseteq K\Rightarrow H'\subseteq K'$$

8- إذا كانت الزمرة الجزئية للمبادلات من الزمرة G رتبتها m ، بين أن كل عنصر في G له على الأكثر m في المرافقات .

9- لتكن G زمرة مركزها Z لها دليل يساوي n في G ، برهن أن G تحوي على الأكثر n^2 من المبادلات المختلفة .

10- N زمرة جزئية عادية من الزمرة G و $N\cap' = \{e\}$ برهن أن $N\subseteq Z(G)$

2- السلسلة العادية ، الزمر القابلة للحل ونظرية جوردان هولدر

تعريف4.5 السلسلة العادية الجزئية

يقال لمتتابعة من زمر جزئية $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_1 = (e)$

في الزمرة G إنها سلسلة عادية جزئية في G إذا كانت G_{i+1} زمرة جزئية عادية من G ، فكل $i = 1, 2, .. \lambda - 1$. زمر القسمة G_n / G_{i+1} تسمى زمر العامل للسلسلة الجزئية العادية ، إضافة إلى ذلك إذا كانت كل G_i زمرة جزئية عادية من G نفسها ، عندئذ يقال عن السلسلة إنها سلسلة عادية من G .

ملاحظة

العبارة $N = \{G_0, G_1, ..., G_\lambda\}$ هي سلسلة عادية جزئية من الزمرة G يعني بها المتتابعة (1) من زمر جزئية G_i بحيث أن G_{i+1} زمرة جزئية عادية في G_i لجميع $i = 0, 1, ..., \lambda - 1$.

تعريف5.5 (a) (تحسين أو تنعيم)

ليكن $N = \{G_0, G_1, ..., G_\lambda\}$ سلسلة عادية جزئية ، فإن أي سلسلة عادية جزئية $M = \{H_0, H_1, ..., H_\mu\}$ يقال أنها تحسين لسلسلة N إذا كانت $N \subseteq M$.

تعريف (b) 6.5 (تحسين فعلي)

يقال للسلسلة M أنها تحسين فعلي للسلسلة N ، إذا كانت $N \subseteq M$ ولكن $N \neq M$.

ملاحظة : أغلب المؤلفين يستخدمون مصطلح سلسلة عادية بدلاً من سلسلة عادية جزئية .

من المحتمل أن لبعض i, $G_i = G_{i+1}$ في (1) ، عدد العناصر في (1) التي تختلف عن G يسمى طول السلسلة العادية الجزئية ، السلسلة العادية الجزئية يقال عنها أنها فائضة إذا كان $G_i = G_{i+1}$ لبعض $i = 0,1,2,..\lambda-1$ وغير ذلك يقال أنها غير فائضة ، يمكننا أن نكون سلسلة عادية جزئية غير فائضة من واحدة فائضة بحذف G_{i+1} حينما $G_{i+1} = G_i$ لبعض i ، عليه عندما تكون السلسلة العادية الجزئية (1) غير فائضة ، فإن جميع G_i تكون مختلفة ، بالتالي يكون طولها يساوي λ نفسه .

تعريف 7.5

يقال عن الزمرة G أنها قابلة للحل إذا كان لها سلسلة عادية جزئية :

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_5 = (e)$$

بحيث كل زمرة عامل فيها G_i / G_{i+1} هي زمرة إبيلية وعندئذ يتبين لنا أن السلسلة السابقة هي سلسلة قابلة للحل في G .

مثال 5

أي زمرة أبيلية تكون قابلة للحل .

$G \supset (e)$ هي سلسلة عادية في G وزمرة العامل الوحيدة $G/(e)$ الأيزويورفية مع G هي زمرة إبدالية .

مثال 6

اعتبر السلسلة $S_3 \supset A_3 \supset (I)$ زمر العامل لها هما $A_3 , S_3 / A_3$ رتبتاهما $3,2$ على الترتيب .

بما أن أي زمرة رتبتها عدد أولي تكون إبدالية ، فإن زمرتي العامل إبداليتان ، إذاً S_3 قابلة للحل .

مثال 7

اعتبر $S_4 \supset A_4 \supset V_4 \supset \{I\}$ سلسلة عادية جزئية من S_4 ، حيث :
$V_4 = \{I, (12), (34), (13), (14), (23)\}$

زمر العامل هي $V_4, A_4/V_4, S_4/A_4$

رتبتها هي $4,3,2$ على الترتيب ، بما أن كل زمرة رتبتها 4 آبيلية ، فإن جميع زمر العامل أبيلية ، إذاً S_4 قابلة للحل .

نظرية 8.5

أية زمرة جزئية H من زمرة قابلة للحل تكون قابلة للحل .

البرهان

لتكن $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = (e)$

سلسلة قابلة للحل في G ندعي أن :

$$H = H_0 \supseteq (H \cap G_1) \supseteq H_0 \cap G_2 \supseteq \ldots \supseteq H \cap G_n = (e) \ldots(1)$$

هي سلسلة في H قابلة للحل ، بما أن G_{i+1} عادية في G_i مثل :
$i = 0, 1, 2, \ldots, n-1$

نحصل على أن $H_{i+1} = H_n \cap G_{i+1}$ عادية في $H_i = H \cap G_i$.

عرف الراسم $f = H_i \to G_i / G_{i+1}$

بحيث $Vx \in H_i \qquad f(x) = xG_{i+1}$

الراسم f هومومورمزم إضافة إلى ذلك

$$x \in \ker f \Leftrightarrow xG_{i+1} = G_{i+1}$$
$$\Leftrightarrow x \in G_{i+1}$$
$$\Leftrightarrow x \in H \cap G_{i+1} \quad (xcH_i \subseteq H)$$

هذا يؤدي إلى أن $\ker f = H \cap G_{i+1} = H_{i+1}$

النظرية الأساسية للهومورمزم $H_i / H_{i+1} \equiv f(H_i)$

وحيث أن $f(H_i)$

زمرة جزئية من G_i / G_{i+1} و G_i / G_{i+1}

زمرة أبيلية ، فإن $f(H_i)$ آبيلية أيضاً ، بالتالي H_i / H_{i+1} آبيلية .

هذا يثبت أن (1) سلسلة قابلة للحل للزمرة H إذا H زمرة قابلة للحل .

نظرية 9.5

إذا كانت H زمرة جزئية عادية في زمرة قابلة للحل G ، فإن G/H قابلة للحل أيضاً .

البرهان

لتكن $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = (e)$

سلسلة قابلة للحل للزمرة G اعتبر السلسلة :

$$\frac{G}{H} = G_0 / H \supseteq G_1 H / H \supseteq H_2 / H \supseteq \ldots \supseteq G_n H / H = (e) \qquad (1)$$

G_{i+1} عادية في G_i لكل $i = 0, 1, 2, \ldots, n-1$ اعتبر أي $6x \in G_i H$

فإن $x = gh$ لبعض $g \in G_i$ $h \in H$ عليه $xG_{i+1}H = ghG_{i+1}H$

$= gG_{i+1}H$ (لأن لأي زمرة جزئية k من G فإن $Hk = kH$)

$= gG_{i+1}H$ (لأن $hH = H$)

$= G_{i+1}gH = G_{i+1}ghH$ (لأن G_{i+1} عادية في G_i , G_i , $g \in G_i$)

$G_{i+1}Hgh = G_{i+1}Hx$

هذا يثبت أن $G_{i+1}H$ زمرة جزئية عادية في $G_i H$.

إذاً $G_i H / G_{i+1} H = \dfrac{G_i H / H}{G_{i+1} H / H}$

الآن عرف $f = G_i \to G_i H / G_{i+1} H$

بحيث يكون $f(x) = G_{i+1}Hx \quad \forall x \in G_i$

فيكون f هو مومورمزم ، بما أن $G_iH = HG_i$ ، إذا كان $y \in G_iH$ يمكننا كتابة $y = hg$ لبعض $h \in H$ ، $g \in G_i$ فإن $G_{i+1}Gy = G_{i+1}Hhg = G_{i+1}Hg = f(g)$

هذا يبين أن f ... ومن الواضح $G_{i+1} \subseteq \ker f$ وهذا يستحدث هومومورزمزم $f' = G_i / G_{iH} \to G_i / G_{i+1}H$ بحيث : $f'(G_{i+1}x) = G_{i+1}Hx \quad \forall x \in G_i$

الراسم f' هذا فوقي أيضاً ، ومن ثم فإن $G_iH / G_{i+1}H$ عبارة عن صورة هومومورفية للزمرة الآبيلية G_i / G_{i+1} فيجب أن تكون نفسها آبيلية ، وبالتالي كل عامل زمرة للسلسلة العادية الجزئية (1) تكون آبيلية ، هذا يثبت أن G / H قابلة للحل .

نظرية 10.5

إذا كانت H زمرة جزئية عادية من الزمرة G إذا كانت كل من H و G / H هي قابلة للحل عليه فإن G قابلة للحل أيضاً .

البرهان

افرض أن :

$$G / H = G_i / H \supseteq G_1 / H \supseteq \ldots \supseteq G_{t=1} / H \supseteq G_t / H = (e') \qquad (1)$$

سلسلة قابلة للحل للزمرة G / H ، هنا كل G_i هي زمرة جزئية من G تحوي H ، بما أن G_{i+1} / H زمرة جزئية عادية في G_i / H ، كل G_{i+1} زمرة عادية من G_i ، إضافة إلى ذلك $G_t / H = (e')$ يؤدي إلى أن $G_t = H$ ، الآن افرض أن :

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_u = (e) \ldots (2)$$

سلسلة قابلة للحل في H ، فإن :

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_{t-1} \supseteq H \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_u = (e)$$

هي سلسلة قابلة للحل للزمرة G ، هذا يبرهن أن G زمرة قابلة للحل .

نتيجة 11.5

إذا كانت الزمرتان K,H قابلتين للحل ، فإن $H \times K$ قابلة للحل .

البرهان : لتكن $G = H \times K$ فإن $G/H \cong K$ ، بما أن K قابلة للحل ، يكون لدينا G/H قابلة للحل ، وحيث أعطينا H قابلة للحل ، فإنه وحسب النظرية السابقة فإن G تكون كذلك قابلة للحل .

نظرية 10.5

إذا كانت H زمرة جزئية عادية من الزمرة G ، وكان كل من $G/H, H$ قابلا للحل، فإن G تكون قابلة للحل .

نتيجة 12.5

أي زمرة $-P$ منتهية تكون قابلة للحل .

البرهان : لتكن G زمرة $-P$ منتهية (P عدد أولي) فإن $o(G)=P^n$ لبعض $n \geq 0$ ، إذا كان $n=1$ ، فإن G آبيلية ، وعليه فهي قابلة للحل ، لذلك افرض $1<n$ ، نستخدم الاستنتاج على n ، افرض أن النتيجة متحققة للزمرة التي رتبتها P^m بحيث $m<n$ ، الآن $Z(G)$ مركز الزمرة G لا يساوي (e) ، بالتالي $0[Z,G)]=P^K$ لبعض $1 \leq K$ هذا يؤدي إلى أن $G/Z(G)$ زمرة رتبتها P^{n-k} حيث $n-k<n$.

إذاً من فروض الاستنتاج $G/Z(G)$ قابلة للحل ، أيضاً لأن $Z(G)$ آبيلية فهي قابلة للحل ، بأخذ $H=Z(G)$ نجد من النظرية السابقة أن G قابلة للحل .

من البند السابق عرضنا مفهوم الزمرة الجزئية المعادلة ، الآن نورد معياراً لقابلية الزمرة للحل اعتماداً على الزمر الجزئية للمبادلات .

تعريف 13.5

لتكن G زمرة لأي عدد صحيح غير سالب n عرف $G^{(n)}$ بالاستنتاج وكالآتي :

$$G^0 = G$$
$$G^{(n+1)} = \left(G^{(n)}\right)'$$

الزمرة الجزئية لمبادلات $G^{(n)}$ ، $G^{(n)}$ تسمى الزمرة الجزئية النونية للمبادلات أو الزمرة الجزئية المشتقة النونية من G .

الآن نثبت صحة النظرية التالية .

نظرية 14.5

الزمرة G قابلة للحل إذا وفقط إذا كانت $G^{(n)} = (e)$ لعدد صحيح غير سالب n

البرهان

لتكن G زمرة قابلة للحل وافرض أن :

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = (e)$$

سلسلة قابلة للحل ، نبرهن بالاستنتاج أن $G^{(K)} \subseteq G_K$

لكل K ، من الواضح أن $G^{(0)} = G = G_0$ افرض لبعض K يكون $G^{(K)} \subseteq G_K$ ، هذا يعطينا

$$G^{(K+1)} = \left[G^{(K)}\right]' \subseteq G'_K$$

بما أن G_K / G_{K+1} آبيلية ، لدينا $G_{K'} \subseteq G_{K+1}$ (نظرية 4.5) ، بالتالي $G^{(K+1)} \subseteq G_{K+1}$ ، إذاً من الاستنتاج يكون $G^{(K)} \subseteq G_K$ لكل $K = 0, 1, 2, \ldots, n$ بصورة خاصة $G^{(n)} \subseteq G_n$ إذاً $G^{(n)} = (e)$ لأن $G_n = (e)$.

بالعكس افرض أن $G^{(n)} = (e)$ لبعض n ، فإن :

$$G = G^0 \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \ldots \supseteq G^{(n)} = (e)$$

هي سلسلة جزئية عادية من G بحيث أن $G^{(i)}/G^{(i+1)}=G^{(i)}/\left[G^{(i)}\right]'$
آبيلية لأنه لأية زمرة $H/H',H$ آبيلية دائماً ، إذاً G قابلة للحل ، وهذا يكمل إثبات النظرية .

نتيجة 15.5

S_n غير قابلة للحل طالما كان $5\le n$.

البرهان : A_n زمرة بسيطة غير إبدالية ، عليه $A'n\ne(I)$ من جهة ثانية An زمرة بسيطة ، فإن الزمرة الجزئية العادية لها هي An و (I) فقط ، بالتالي :

$$A'n=An\Rightarrow An^{(2)}=(A'n)'=A'n=An$$

بصورة عامة $An^{(K)}=A_K$ لكل عدد صحيح موجب k ، عليه $An^{(K)}\ne(e)$ لكل k إذاً An غير قابلة للحل .

ولأن An زمرة جزئية من S_n ، فإن S_n غير قابلة للحل أيضاً عندما $S\le n$ لأن الزمرة الجزئية لزمرة قابلة للحل تكون قابلة للحل .

تعريف 16.5 (الزمرة الجزئية العادية الأعظمية)

يقال لزمرة جزئية عادية من G أنها زمرة جزئية عادية أعظمية إذا كان $H\ne G$ ولا توجد أي زمرة جزئية عادية K في G بحيث $H\subset K\subset G$.

للزمرة الجزئية العادية H في G نعلم أن أية زمرة جزئية للزمرة G/H تكون بالصيغة K/H حيث K زمرة جزئية في G تحوي H ، كذلك K/H عادة في G/H إذا وفقط إذا كانت K عادية في G ، K/H زمرة فعلية في G/H إذا وفقط إذا كانت $H\subset K\subset G$ ، عليه H زمرة جزئية عادية أعظمية في G إذا وفقط إذا كان $H\ne G$ و G/H لا تحوي زمر جزئية عادية فعلية ، أي أن G/H زمرة بسيطة .

مثال 8

لتكن $G =< a >$ زمرة دائرية رتبتها 10 فإن $H =< a^2 >$ هي زمرة جزئية من G بحيث رتبة G / H تساوي 2 ، عليه G / H زمرة بسيطة و H زمرة عادية أعظمية من G .

مثال 9

إذا كانت G زمرة بسيطة ، فإن (e) زمرة جزئية عادية أعظمية من G لأن G لا تحوي أي زمرة جزئية عادية فعلية .

مثال 10

في $An, (2 < n) S_n$ زمرة جزئية عادية أعظمية . نتذكر تعريف التحسين (تعريف 6.5) ونعيد صياغته كالآتي :

تعريف 17.5

لتكن
$$G = G_0 \supseteq G_1 \supseteq ... \supseteq G_\lambda = (e)$$
سلسلة عادية جزئية من G السلسلة العادية الجزئية
$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq ... \supseteq H = (e)$$
تسمى تحسيناً للسلسلة الأولى إذا كان G_i تساوي واحدة من H_j .

تعريف 18.5

السلسلة العادية الجزئية غير الفائضة $G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_t = (e)$ للزمرة G تسمى سلسلة تركيب من G إذا كان كل زمرة عامل لها G_i / G_{i+1} زمرة بسيطة ، أي أن G_{i+1} زمرة جزئية عادية أعظمية من G_i .

مثال 11

لتكن $G=<a>$ زمرة دائرية رتبتها 24 ، فإن $o(a)=24$ اعتبر السلسلتين :

$$G=<a>\supset<a^2>\supset<a^3>\supset<a^{12}>\supset(e)\ldots(1)$$
$$G=<a>\supset<a^3>\supset<a^6>\supset<a^{12}\supset(e)\ldots\ldots(2)$$

وهما سلسلتان عاديتان في G ، زمر العامل في (1) هي :

$$<a^{12}\supset,<a^6/<a^{12}\supset,<a^2/<a^6\supset,<a>/<a^2\supset$$

ورتبتها هي على الترتيب 2 , 3 , 2 , 2 بما أن هذه الرتب أعداد أولية ، فهي جميعاً زمر بسيطة ، وبالمثل زمر العامل في (2) هي :

$$<a^{12}\supset,<a^6><a^{12}>,<a^3/<a^6>,<a\supset/<a^3\supset$$

ورتبتها على الترتيب هي 3 , 2 , 2 , 2 .

هذه مرة أخرى زمر بسيطة ، عليه (1) و (2) كلاهما سلسلة تركيب في G وهما سلسلتان لهما نفس الطول ، أي 4 إضافة إلى ذلك نجد أن أي زمرتين دائريتين لهما نفس الرتبة ، تكونان أيزومورفيتان فإن :

$$<a\supset/<a^2\geq\cong<a^3\supset/<a^6>,<a^2>/<a^6>\cong<a\supset Ka^3>,$$
$$<a^6\supset/<a^{12}\supset\cong<a^6>/<a^{12}>,<a^{12}>\cong<a^{12}>$$

ومن ثم يوجد تناظر أحادي بين زمر العامل في (1) وزمر العامل في (2) بحيث تكون زمر العامل المتماثلة أيزومورفية .

مثال 12

لتكن $G=S_4$ اعتبر سلسلتين عاديتين جزئين .

$S_4\supset A_4\supset V_4\supset(I)$ (انظر مثال9) (1)

$S_4\supset A_4\supset V_4\supset A\supset(I)$ (1)

حيث $A_4\cong V_4/(I)$ زمرة عامل للسلسلة (1) ، بما أن V_4 زمرة رتبتها 64 فهي غير بسيطة (لأن أي زمرة إبدالية بسيطة رتبتها عدد أولي) .

زمر العامل في (2) هي $A, V_4 / A, A_4 / V_4, S_4 / A_4$ رتبها على الترتيب , 3 , 2 , 2
2 إذاً جميعاً بسيطة و (2) سلسلة تركيب في S_4 .

من الآن فصاعداً الهدف الرئيسي هو إثبات صحة نظرية جوردان هولدر ، ولبلوغ هذا المأرب تدخل بعض المفاهيم ونبرهن بعض النتائج .

تعريف 19.5

يقال لسلسلتين عاديتين جزئيتين :

$$G = G_0 \supseteq G_1 \supseteq G_1 \supseteq \ldots \supseteq G_s = (e) \qquad (1)$$

$$G = G_0' \supseteq G_1' \supseteq G_2' \supseteq \ldots \supseteq G_t' = (e) \qquad (2)$$

لزمرة ما G إنهما متكافئتان أو أيزومورفيتان إذا وجد تقابل أحادي بين عوامل (1) وعوامل (2) بحيث تكون زمر العامل المتناظرة أيزومورفية .

بما أن عدد زمر العامل في (1) و (2) هما t, s فإذا كانت السلسلتان متكافئتين في التعريف يجب أن يكون لهما نفس العدد في زمر العامل ، بالتالي $s = t$. عليه في مثال 11 فإن السلسلتين متكافئتين أو أيزومورفيتان .

القضية التالية مشابهة للنظرية الثانية للأيزومورفزم .

قضية 20.5

لتكن K, H زمرتين جزئيتين في G بحيث $kH = Hk$ لكل $k \in K$ فإن HK زمرة جزئية في G و H زمرة جزئية عادية في HK وأن $H_n K$ زمرة جزئية عادية في K و $\dfrac{HK}{H} \cong \dfrac{K}{HnK}$.

البرهان

بما أن $kH = Hk$ لكل $k \in K$ يكون لدينا $HK = KH$ بالتالي HK زمرة جزئية في G (نظرية 39.2) اعتبر $x \in HK$ فإن $x = hk = kh_1$ لبعض $k \in K, h_1 h_1 \in H$ عندئذ :

$$Hx = Hhk = Hk = kH = k(h_1 H) = kh_1 H = xH$$

أي أن

$$Hx = xH \qquad \forall x \in HK$$

هذا يبين أن H زمرة جزئية عادية في HK ، من اليسير التحقق من أن $H \cap K$ زمرة جزئية عادية من K ، من النظرية الثانية للأيزومورفزم $HK / H \cong K / H \cap K$ هذا يثبت النظرية .

نظرية 21.5 (زاساهاوس)

لتكن C, B زمرتين جزئيتين في C_0, B_0, G زمرتين جزئيتين عادتين في C, B على الترتيب ، فإن

$$\frac{B_0(B \cap C)}{B(B \cap C_0)} \cong \frac{C_0(C \cap B)}{C_0(C \cap B_0)}$$

ملاحظة : لاحظ التماثل ، في الواقع الطرف الأيمن للأيزومورفزم يأتي من الطرف الأيسر بتبديل C, B ، هذه النظرية تسمى أيضاً نظرية (بترفلاي) .

البرهان

ضع $k = B \cap C, H = B_0(B \cap C_0)$ بما أن B_0 زمرة جزئية عادية في B فإن $bB_0 = B_0 b$ لكل $b \in B$ بالأخص ولأن $K \subseteq B$ فإن $kB_0 = B_0 k$ مثل $k \in K$ كذلك C_0 عادية في C يؤدي إلى أن $B \cap C_0$ عادية في $B \cap C$ بالتالي فإن $k(B \cap C_0) = (B \cap C_0)k$ لكل $k \in K$ ، إذاً

$$\begin{aligned} HK &= B_0(B \cap C_0)k = [k(B \cap C_0)] \\ &= (B_0 k)[B_0 C_0] = (kB_0)(B \cap C_0) \\ &= k[B_0(CB_n C_0)] = KH \quad \forall k \in K \end{aligned}$$

وهكذا فإن

$$\frac{HK}{H} \cong \frac{K}{H \cap K} \qquad (1)$$

الآن $HK = B_0(B_nC_0)(B \cap C) = B_0(B \cap C)$

لأن $(B \cap C_0)(B \cap C) = B \cap C \, , B_nC_0 \subseteq B \cap C$

(في الواقع لأي زمرة $gG = G, G$ لكل $g \in G$) ، إضافة إلى ذلك :

$y \in H \cap K \Rightarrow y \leftarrow H \, , y \in K \Rightarrow y = b_0 b \, , y = d$

لبعض $d \in B \cap C \, , b \in B_n C_0 \, , b_0 \in B_0$

$\Rightarrow b_0 b = d \Rightarrow b_0 = db^{-1} \in B_0 nC = CnB_0$

لأن $b^{-1} \in B \cap C_0 \subseteq C_0 \subseteq C \, , d \in C$

عليه فإن $y = b_0 b \in (C \cap B_0)(B \cap C_0)$

هذا يؤدي إلى أن $H \cap k \subseteq (C \cap B_0)(B \cap C_0)$

بما أن $B \cap C_0 \subseteq B \cap C \, , C \cap B_0 \subseteq B \cap C$

فإن $(C \cap B_0)(B \cap C_0) \subseteq B_n C = K$

كذلك $C \cap B_0 \subseteq B_0$

يعطينا $(C \cap B_0)(B \cap C_0) \subseteq B_0(B \cap C_0) = H$

عليه حصلنا على $(C \cap B_0)(B \cap C_0) \subseteq H \cap K$

بالتالي $H \cap K = (C \cap B_0)(B \cap C_0)$

بوضع $H \cap K = (C \cap B_0)(B \cap C_0), HK = B_0(B \cap C)$

في (1) نحصل على

$$\frac{B_0(B \cap C)}{B_0(B \cap C_0)} \cong \frac{B \cap C}{(C \cap B_0)(B_n C_0)} \qquad (2)$$

بتبديل مواقع C, B نحصل على :

$$\frac{C_0(C \cap B)}{C_0(C \cap B_0)} \cong \frac{(C \cap B)}{(B_n C_0)(C_n B_0)} \qquad (3)$$

باستخدام حقيقة أن $B \cap C_0$ زمرة جزئية عادية من $B \cap C$ و $C \cap B_0 \subseteq B \cap C$ نحصل على

$(B \cap C_0)(C \cap B_0) = (C \cap B_0)(B \cap C)$

إذاً
$$\frac{B\cap C}{(C\cap B_0)(B\cap C_0)}=\frac{C\cap B}{(B\cap C_0)(C\cap B_0)}$$

من (2) و (3) نستنتج أن
$$\frac{B_0(B\cap C)}{B_0(B\cap C_0)}\cong\frac{C_0(C\cap B)}{C_0(C\cap B_0)}$$

وهذا يثبت النظرية .

نظرية 22.5 (نظرية شراير للتحسين)

أي سلسلتين عاديتين جزئيتين في الزمرة G لهما تحسينان متكافئان .

البرهان

اعتبر السلسلة العادية الجزئية :

$$G=G_0\supseteq G_1\supseteq G_2\supseteq\ldots\supseteq G_s=(e) \qquad (1)$$
$$G=H_0\supseteq H_1\supseteq H_2\supseteq\ldots\supseteq H_t=(e) \qquad (2)$$

للزمرة G بما أن G_{i+1},ℓ,i,j,k لأي زمرة جزئية عادية من G_i , H_{k+1} زمرة جزئية عادية من Hk نحصل على أن :

$$G_{i,j}=G_{i+1}(G_i\cap H_i)(n=0,1,2,\ldots,5-1,\, j=0,1,2,\ldots,t) \qquad (3)$$
$$H_{k,l}=H_{k+1}(H_k\cap G_l),(k=0,1,2,\ldots,t-1,\ell=0,1,2,\ldots,s) \qquad (4)$$

هما زمرتان جزئيتان من G .

الآن H_{j+1} زمرة جزئية طبيعية من H_j يؤدي إلى أن $G_{i,j+1}$ زمرة جزئية عادية من $G_{i,j}$ بالمثل $H_{k,l+1}$ زمرة جزئية عادية في $H_{k,l}$.

بما أن $H_0=G,H_t=(e)$

يكون لدينا $G_{i,t}=G_{i+1}(G_i\cap H_t)=G_{i+1}(e)=G_{i+1}$

كذلك $G_{i,0}=G_{i+1}(G_i\cap H_0)=G_{i+1}(G_i\cap G)=G_{i+1}G_i=G_i$

وهكذا فإن

$$G_{i,t}=G_{i+1}=G_{i+1},0,\ldots \qquad (5)$$

لكل $i=0,1,2,...,s-2$

بالمثل

$H_{k,s}=H_{k+1}=H_{K+1,0,...}$ لكل $k=0,1,2,...,t-2$ (6)

اعتبر السلسلتين

$$G=G_0=G_{0,0}\supseteq G_{0,1}\supseteq G_{0,2}\supseteq...\supseteq G_{0,t}(=G_1=G_{1,0})\supseteq G_{1,1}\supseteq G_{1,2}\supseteq...$$
$$...\supseteq G_{1,t}(G_2=G_{2,0})\supseteq...\supseteq G_{5-1,0}\supseteq G_{s-1,1}\supseteq...\supseteq G_{s-1,t}=G_s=(e) \quad (7)$$
$$G=H_0=H_{0,0}\supseteq H_{0,1}\supseteq H_{0,2}\supseteq...\supseteq H_{0,s}(H_1=H_{1,0})\supseteq H_{1,1}\supseteq H_{1,2}\supseteq$$
$$...\supseteq H_{1,s}(=H_s=H_{2,0})\supseteq...\supseteq H_{t-1,0}\supseteq H_{t-1,1}\supseteq...\supseteq H_{t-1},s=H_6$$
$$=(e) \quad (8)$$

كلاً من (7) و (8) لهما نفس العدد في الحدود ، أي $ts+1$.

من الواضح G_0 تظهر في (7) شكل $m=1,2,...,5$ ولأن في (5) $G_m=G_{m=1,t}$ نجد أن كل G_m يظهر في (7) لجميع m ، عليه فإن (7) تحسين لـ (1) ، بالمثل (8) تحسين لـ (2) .

الآن من نظرية 21.5 يكون :

$$\frac{G_{r,5}}{G_{r,5+1}}=\frac{G_{r+1}(G_r\cap H_5)}{G_{r+1}(G_r\cap H_{s+1})}\cong\frac{H_{s+1}(H_5\cap G_r)}{H_{s+1}(H_s\cap G_{r+1})}=\frac{H_{s,r}}{H_{s,r+1}}$$

لجميع $r=0,1,2,...,5-1$ ولجميع $S=0,1,2,...,t-i$ عليه (7) و (8) متكافئان ، وهذا يكمل برهان النظرية .

دعنا نرجع الآن إلى سلسلة التركيب ، إن زمرة ما يمكن أو لا يمكن أن يكون لها سلسلة تركيب .في الحقيقة القضية التالية تبين إذا كانت الزمرة الإبدالية غير منتهية ، فلن يكون لها سلسلة تركيب ، بصورة خاصة الزمرة الجمعية للأعداد الصحيحة ليس لها سلسلة تركيب .

قضية 23.5

إذا كانت G زمرة إبدالية لها سلسلة تركيب ، فإن G زمرة منتهية .

البرهان

نبين أولاً أن الزمرة البسيطة الآبيلية يجب أن تكون دائرية ورتبتها عدد أولي ، هذا ينتج مباشرة في نظرية 47.3 والحقيقة أن أي زمرة جزئية من زمرة آبيلية تكون عادية .

الآن افرض أن $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_s = (e)$

سلسلة تركيب من G .

بما أن $\frac{G_{s-1}}{G_s} = \frac{G_{s-1}}{(e)} \cong G_{s-1}$

هي زمرة بسيطة آبيلية ، فإن $P_{s-1} = 0\left(G_{s-1}\right)$ حيث P_{s-1} عدد أولي ، إضافة إلى ذلك $\frac{G_{s-2}}{G_{s-1}}$ بسيطة أولية يؤدي إلى أن $P_{s-2} = 0\left(\frac{G_{s-2}}{G_{s-1}}\right)$ لعدد أولي P_{s-2} .

يمكننا كتابة G_{s-2} كاتحاد منفصل من P_{s-2} من المجموعات المصاحبة :

$G_{s-1}\varphi_1 G_{s-1}a_2 \ , \ldots , \ G_{s-1}a_{Ps-2}$

وكل واحدة تحوي P_{s-1} عنصراً عليه G_{s-2} تحوي $P_{s-1}P_{s-2}$ عنصراً .

وبالتقدم في هذه الطريقة ، نحصل على أن G تحوي $P_0P_1P_2 \ldots P_{s-1}$ عنصراً ، حيث :

$$P_i = 0\left(\frac{G_i}{G_{i+1}}\right)$$

عندما $i = 0, 1, 2, \ldots, s-1$

الآن لتكن G زمرة اختيارية لها سلسلة تركيب :

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_s = (e) \qquad (1)$$

افرض أن $G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_t = (e)$

تحسين للسلسلة الأولى ، هذا التحسين يمكن أن يكون فعلياً إذا كان لبعض j , H_j لا يساوي أياً من G_i ، من الواضح أن $G_i \supset H_j \supset G_{i+1} 6i$ لبعض ، زيادة على ذلك يمكننا اختيار j بحيث $G_i \ldots H_{j-1}$ إذا $H_{j-1} \supseteq G_i \supseteq H_j \supset G_{i+1}$

وكما أن H_j عادية في H_{j-1} نحصل على أن H_j هي أيضاً عادية في G_i ، وبناء عليه فإن H_j / G_{i+1} تكون زمرة جزئية عادية فعلية في G_i / G_{i+1} ولأن G_i / G_{i+1} زمرة بسيطة ، فهذا لا يجوز وبذلك نحصل على أن سلسلة التركيب لا يمكن أن يكون لها تحسين فعلي .

افرض أن $G = G_0{}' \supset G_1{}' \supset \ldots \supset G_u{}' = (e)$

هي سلسلة تركيب أخرى في G من نظرية 22.5 ، فإن (1) و (2) لهما تحسينان متكافئان ، ومن ناحية ثانية ، فكما رأينا سابقاً أن أياً من السلسلتين ليس لها تحسين فعلي ، لذا فإن السلسلتين يجب أن تكونان متكافئتين ، وهذا ما تقرره النظرية الآتية .

نظرية 24.5 (نظرية جوردان– هولدر) للزمر المنتهية .

إذا كانت للزمرة G سلسلة تركيب ، فإن جميع سلسلات التركيب لها متكافئة مثنى مثنى .

بالرغم من أننا برهنّا نظرية جوردان هولدر للزمر بصورة عامة ، هناك برهان آخر في حالة الزمر المنتهية وله أهمية خاصة لسهولته وعدم اعتماده عل نظرية (شراير) للتحسين ، وفيما يلي نعطي ذلك البرهان .

نظرية 25.5 (نظرية جوردان هولدر للزمر المنتهية)

1. كل زمرة منتهية تحوي على الأقل عنصرين لها سلسلة تركيب .
2. إذا كان كل من

$$(e) = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_k = G$$
$$(e) = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_l = G$$

سلسلتان تركيبيتان للزمرة المنتهية G ، فإن $k = \ell$ لكل $i = 0,1,2,..k-1$ يكون :

$$\frac{G_{i+1}}{G_i} \cong \frac{H_{\Pi(i)+1}}{H_{\Pi(i)}}$$

لبعض التباديل Π للمجموعة $\{0,1,2,..k-1\}$ أي أن أي سلسلتين تركيبيتين للزمرة G تكونان متكافئتين .

البرهان

(1) سوف نطبق الاستنتاج على $(G)\circ$ ، افرض $n = (G)\circ$ عندما $n=2$ فإن $(e)=G_0 \subset G_1 = G$ هي سلسلة التركيب الوحيدة للزمرة G لأن $G, G_1/G_0 \cong G$ زمرة دورية رتبتها عدد أولي ، فهي زمرة بسيطة ولهذا فالنظرية متحققة عندما $n=2$.

افرض أن كل زمرة رتبتها $< n$ لها سلسلة تركيب ، وأن G زمرة رتبتها $n > 2$.

إذا كانت G زمرة بسيطة فليس لها زمرة جزئية عادية فعلية ، بالتالي تكون $(e)\subset G_1 = G$ هي سلسلة التركيب الوحيدة لها .

إذا كانت G زمرة غير بسيطة وكانت N زمرة جزئية عادية فعلية في G . بما أن G منتهية ، فإنه توجد فقط عدد منته من الزمر الجزئية العادية الفعلية من G تحوي N ، لتكن M واحدة من هذه الزمر الجزئية والتي تحوي أكبر عدد من العناصر ، فإن M زمرة جزئية عادية أعظمية في G ، من الواضح G/M زمرة بسيطة و $M \neq G$ عليه $O(M) < n$ إذاً حسب فروض الاستنتاج M لها سلسلة تركيب ولتكن :

$$(e)=M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_t = M$$

الآن اعتبر السلسلة :

$$(e)=M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_t = M \subset G \qquad (1)$$

من تعريف سلسلة التركيب ، فإن $\frac{M_{i+1}}{M_i}$ هي زمرة بسيطة لجميع $i=0,1,2,\ldots,t-1$ كذلك $\frac{G}{M_t}=\frac{G}{M}$ زمرة بسيطة ، بالتالي (1) سلسلة تركيب للزمرة G .

(2) افرض أن :

$$(e)=G_0\subset G_1\subset G_2\subset\ldots\subset G_{k-1}\subset G_k=G \qquad (2)$$
$$(e)=H_0\subset H_1\subset H_2\subset\ldots\subset H_{\ell-1}\subset H_\ell=G \qquad (3)$$

هما سلسلتان تركيب لزمرة منتهية G مرة ثانية نطبق الاستنتاج على $O(G)$ لتكن $O(G)=n$ إذا كان $n=2$ فكما رأينا سابقاً فإن للزمرة G سلسلة تركيب واحدة فقط ، وعليه فإن الجزء الثاني من النظرية متحققة للزمر التي رتبتها 2 .

دعنا نفرض أن $O(G)=n>2$ وأن النتيجة صحيحة لجميع الزمر التي رتبتها $n>$ اعتبر الحالتين

$$G_{k-1}=H_{\ell-1} \qquad (\mathrm{I})$$
$$G_{k-1}\neq H_{\ell-1} \qquad (\mathrm{II})$$

الحالة I $G_{k-1}=H_{\ell-1}$ من الواضح أن :

$$(e)=G_0\subset G_1\subset G_2\subset\ldots\subset G_{k-1} \qquad (4)$$
$$(e)=H_0\subset H_1\subset H_2\subset\ldots\subset H_{\ell-1}=G_{k-1} \qquad (5)$$

هما سلسلتان تركيب للزمرة G_{k-1} والتي رتبتها أقل من n .

ومن فروض الاستنتاج تكون السلسلتان (4) و (5) متكافئتين ، هذا يعطي أن $k-1=\ell-1$ أي أن $k=\ell$ وأن السلسلتين (2) و (3) متكافئتين لأن :

$$\frac{Gk}{G_{k-1}}=\frac{G}{G_{k-1}}=\frac{G}{H_{\ell-1}}=\frac{H_\ell}{H_{\ell-1}}$$

وبذلك تحققت الحالة (I) .

الحالة (II) $G_{k-1}\neq H_{\ell-1}$

بما أن كلاً من G_{k-1} و $H_{\ell-1}$ زمرة جزئية عادية أعظمية من G ، فإن $Q=G_{k-1}\cap H_{\ell-1}$ هي زمرة جزئية عادية من G_{k-1} ، كذلك في $H_{\ell-1}$ ، ولأن :

$$Q\subset H_{\ell-1}\,,Q\subset G_{k-1}\,,G_{k-1}\neq H_{\ell-1}$$

زيادة على ذلك $G_{k-1} \neq H_{\ell-1}$ هي زمرة جزئية عادية في G ، الآن :

$$H_{\ell-1} \subseteq G_{k-1}H_{\ell-1}\,, G_{k-1} \subseteq G_{k-1}H_{\ell-1}$$

بما أن $H_{\ell-1}, G_{k-1}$ هما زمرتان جزئيتان عاديتان أعظميتان في G ، فإن $G_{k-1}H_{\ell-1} = G$ (لا يمكن أن تساوي $H_{\ell-1}, G_{k-1}$ في آن معاً) .

لتكن
$$(e) = Q_0 \subset Q_1 \subset Q_2 \subset \ldots \subset Q_m = Q$$

سلسلة تركيب في الزمرة G ندعي أن :

$$(e) = Q_0 \subset Q_1 \subset Q_2 \subset \ldots \subset Q_m (= Q) \subset G_{k-1} \subset G_k = G \qquad (6)$$
$$(e) = Q_0 \subset Q_1 \subset Q_2 \subset \ldots \subset Q_m \subset = Q \subset H_{\ell-1} \subset H_\ell = G \qquad (7)$$

كلاهما سلسلة تركيب في G ، لتحقيق ذلك يكفي إثبات أن $\frac{H_{\ell-1}}{Q}, \frac{G_{k-1}}{Q}$ زمرتان بسيطتان.

الآن
$$\frac{G_{k-1}}{Q} = \frac{G_{k-1}}{G_{k-1} \cap H_{\ell-1}} \cong \frac{G_{k-1}H_{\ell-1}}{H_{\ell-1}} = \frac{G}{\ell - 1},$$

ولكن $\frac{G}{H_{\ell-1}}$ زمرة بسيطة ، بالتالي $\frac{G_{k-1}}{Q}$ زمرة بسيطة ، بالمثل $\frac{H_{\ell-1}}{Q} \cong \frac{G}{G_{k-1}}$ زمرة بسيطة ، مرة أخرى (6) و (7) متكافئتين لأن :

$$\frac{G}{G_{k-1}} \cong \frac{H_{\ell-1}}{Q}, \frac{G_{k-1}}{Q} \cong \frac{G}{H_{\ell-1}} \text{ (كما رأينا سابقاً)}$$

وطول كل من (6) و (7) يساوي $m+2$.

الآن في الحالة (I) السلسلتان (2) و (6) متكافئتين ، عليه $k = m+2$ ، مرة أخرى في الحالة (1) السلسلتان (3) و (7) متكافئتين ، إذاً $\ell = m+2$ بالتالي $k = \ell$ كذلك السلسلتان (6) و (7) متكافئتان ، السلسلتان (2) و (3) متكافئتان ، هذا يكمل إثبات الحالة (II) .

مسائل

1- باستخدام الحقيقة أن أي زمرة بسيطة إبدالية تكون رتبتها عدد أولي أثبت ما يلي :

أ- الزمرة المنتهية G قابلة للحل إذا وفقط إذا كانت لها سلسلة تركيب كل زمرة العامل فيها دورية ورتبتها عدد أولي .

ب- أي زمرة قابلة للحل لها سلسلة تركيب هي زمرة منتهية .

2- لتكن G زمرة لها سلسلة تركيب و H زمرة جزئية عادية من G ، برهن أن للزمرة G سلسلة تركيب أحد حدودها H .

إرشاد : لتكن $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_3 = (e)$ سلسلة تركيب ، اعتبر السلسلة العادية $G \supset H \supset (e)$ من نظرية 22.5 فإن للسلسلتين تحسينان متكافئان .

3- لتكن $G \neq (e)$ زمرة منتهية ، برهن أنه إذا كانت G زمرة قابلة للحل فإن G تحوي زمرة جزئية عادية $H \neq (e)$ إذا كانت G غير قابلة للحل فإن G تحوي زمرة جزئية عادية $H \neq (e)$ بحيث $H' = H$.

إرشاد : استخدم حقيقة أن G قابلة للحل إذا وفقط إذا كانت $G' = (e)$ لعدد صحيح موجب n .

4- حدد سلسلة تركيب للزمرة $n \neq 4, A_n$.

5- لتكن G زمرة منتهية قابلة للحل رتبتها mn بحيث $(m,n)=1$ ، برهن أن G تحوي على الأقل زمرة جزئية واحدة رتبتها m وأي زمرتين من هذا النوع تكونان مترافقين.

6- برهن أن زمرة P - المنتهية (P عدد أولي) دورية إذا وفقط إذا كان لها سلسلة تركيب واحدة فقط .

7- لتكن G زمرة آبيلية منتهية رتبتها P بحيث $(P, P, ..., P)$ هي مجموعة لا متغيرات . برهن أن لها $\frac{(P^n - 1)(P^{n-1} - 1)...(P-1)}{(P-1)^n}$ من سلاسل التركيب .

8- يقال عن زمرة G أنها عديمة القوة إذا كان لها سلسلة عادية :

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq ... \supseteq G_s = (e)$$

بحيث

$$\frac{G_i}{G_{i+1}} \subseteq Z\left(\frac{G}{G_{i+1}}\right), V_i = 0, 1, 2, ..., s-1$$

برهن ما يلي :

أ– كل زمرة عديمة القوة هي قابلة للحل بينما العكس غير صحيح .

ب– الزمرة الجزئية وزمرة القسمة لزمرة عديمة القوة تكون عديمة القوة كذلك .

ت– أي زمرة إبدالية هي عديمة القوة .

ث– إذا كانت G زمرة لها زمرة جزئية عادية H حيث كلاً من الزمرتين G/H و H عديمة القوة ، بين بمثال أن G ليس بالضرورة أن تكون عديمة القوة (قارن مع نظرية 10.5) .

9- برهن أن كل زمرة رتبتها q, p, pq أعداد أولية (ليست بالضرورة مختلفة) هي قابلة للحل .

إرشاد : استخدم نظرية 10.5 .

10- يقال عن زمرة G أنها ... إذا كان $G = G'$ إذا كانت G زمرة بحيث كانت جميع زمرها الجزئية $H(\neq G)$ قابلة للحل ، بينما G ليست قابلة للحل ، بين أن G زمرة تامة .

11- برهن أنه إذا كانت N زمرة جزئية عادية في G و G لها سلسلة تركيب ، فإن للزمرة N سلسلة تركيب .

إرشاد : استخدم سؤال في السابق .

12- لتكن الزمرة G الضرب المباشر للزمرتين الجزئيتين K,H . برهن أن G لها سلسلة تركيب إذا وفقط إذا كانت كل من K,H لها سلسلة تركيب .

13- لتكن $G = H \times K$ عندئذ بين أن G قابلة للحل إذا وفقط إذا كانت كل من K,H قابلة للحل .

ملاحظة : جزء من هذا السؤال في نتيجة 11.5 .

14- برهن أن كل زمرة رتبتها Pqr حيث r,q,p أعداد أولية هي قابلة للحل .

6

نظرة شاملة لبعض الزمر المنتهية

Survey of Some Finite Groups

لقد رأينا من قبل أن زمرتين منتهيتين لهما نفس الرتبة ، ليس بالضرورة أن تكونا أيزومورفيتان ، فمثلاً الزمرة S_3 والزمرة الدائرية من الرتبة السادسة هما من نفس الرتبة ولكن ليستا أيزومورفيتان ، ويمكن للفرد أن يسأل السؤال التالي ذو الصلة الوثيقة ، لو أخذنا عدداً صحيحاً موجباً n فكم عدد الزمر من الرتبة n غير الأيزومورفية الموجودة ؟

نظرية (كايلي) تبين أن أي زمرة من الرتبة n تكون أيزومورفية جزئية من زمرة التناظرات S_n من الدرجة n وتكون المسألة السالبة محلولة إذا استطعنا إيجاد جميع الزمر الجزئية من الرتبة n للزمرة S_n ، وننظر أيهما غير أيزومورفية مثنىً لأن S_n هي زمرة منتهية (من الرتبة $n!$) فإن Sn لها عدد منته فقط من الزمر الجزئية ، ربما يوصى للفرد أن المسألة في أبعد الحالات ما هي إلا تعليل ، ومن ثم من العجيب حقاً أن المسألة تبقى مؤجلة الحل ، هنا ستحل المسألة لبعض القيم الخاصة لـ n مثل pq, p^2 ... الخ ، حيث q, p عددان أوليان وفي حالة الزمر المنتهية الإبدالية تكون المسألة محلولة تماماً باستخدام النظرية الأساسية للزمر المنتهية الإبدالية كما سنرى في النظرية 3.6 .

قضية 1.6

أي زمرتين منتهيتين إبداليتين G^1, G يكون أيزومورفيتان إذا وفقط إذا كان زمر سايلو الجزئية منهما أيزومورفيتان .

البرهان

لتكن $O(G)=P_1^{\alpha}P_2^{\alpha 2}...P_k^{\alpha k}$ حيث P_i'S هي أعداد أولية مختلفة $\alpha_i > o$ أعداد صحيحة ، فيكون :

$$G = S_1 \oplus S_2 \oplus ... \oplus S_k \qquad (1)$$

حيث كل من S_i هي زمرة جزئية P_i – سايكو من G إذا كانت σ هو أيزومورفيزم من G على G' فإن $G^1 = \sigma(G) = \sigma(S_1) \oplus \sigma(S_2) \oplus ... \oplus \sigma(S_k)$

نستنتج أن $O\left(G^1\right) = o(\sigma, G)\ ] = \underset{i=1}{\overset{k}{\pi}} o[\sigma(S_i)] = \underset{i=1}{\overset{k}{\pi}} P_i^{\alpha i} = o(G)$

وأنه $o(\sigma(S_i)) = o(S_i) = P_i^{\alpha i}$

تعطي أن $\sigma(S_1), \sigma(S_2), ..., \sigma(S_k)$

هي زمر جزئية سايلو من G^1 الآن σ يرسم S_i أثرومورفيا على $\sigma(S_i)$ ولذا فغن $S_i \cong \sigma(S_i) \forall_i = 1,2,3,..k$ وهذا يبرهن ضرورة الشرط .

الاتجاه الآخر لتكن G^1, G لهما زمر سايلو جزئية أيزومورفية ، حيث أن $S_1, S_2, ..., S_k$ هي فقط سايلو الجزئية الوحيدة من G فإن G^1 لها زمر سايلو جزئية مقابلة $S_1', S_2', ..., S_k'$ بحيث أن $S_i \cong S_i'$ لكل i تحت أيزومورفيزم σ_i من S_i إلى S_i'

الآن $G^1 = S_1' \oplus S_2' \oplus ... \oplus S_k'$ نعرف $\sigma : G \to G^1$ كالآتي :

خذ $\chi \in G$ (1) تعطي $x = x_1 + x_2 + ... + x_k$ لبعض العناصر الوحيدة $\chi_i \in S_i$ لكل i ، وبوضع $\sigma(x) = \sigma_1(x_1) + \sigma_2(x_2) + ..\sigma_k(x_k)$ يتضح أن $\sigma(\chi) \in G'$ لأي

$$x = x_1 + x_2 + ... + x_n\ ,\ y = y_1 + y_2 + ... + y_n \in G$$

$x_i\ ,\ y_i \in S_i$ لكل i لدينا $x + y = (x_1 + y_1) + (x_2 + y_2) + ... + (x_k + y_k)$

لذلك :

$$\begin{aligned}\sigma(x + y) &= \sigma_1(x_1 + y_1) + \sigma_2(x_2 + y_2) + ... + \sigma_k(x_k + y_k) \\ &= [\sigma_1(x_1) + \sigma_1(y_1)] + [\sigma_2(x_2) + \sigma_2(y_2)] + ... + [\sigma_k(x_k) + \sigma_k(y_k)]\end{aligned}$$

$$= [\sigma_1(x_1) + \sigma_2(x_2) + \dots + \sigma_k(x_k)] + [\sigma_1(y_1) + \sigma_2(y_2) + \dots + \sigma_k(y_k)]$$
$$= \sigma(x) + \sigma(y)$$

وهذا يثبت أن σ هو هومومورفيزم .

الآن
$$\sigma(x) = \sigma(y) \Rightarrow \sigma_1(x_1) + \sigma_2 + (x_2) + \dots + \sigma_k(x_k) =$$
$$\sigma_1(y_1) + \sigma_1(y_1) + \dots + \sigma_k(y_k)$$
$$\Rightarrow \sigma_i(x_i) = \sigma_i(x_i) \qquad \forall_i = 1, 2, \dots, k$$

ومن العلاقة (2)

$$\Rightarrow x_i = y_i \qquad \forall_i = 1, 2, \dots, k$$

وذلك لأن σ_i أحادي .

$x = y \Rightarrow$ أي أن σ أيضاً أحادي .

والآن افرض أي عنصر $x' \in G^1$ (2) تعطي $x' = x_1' + x_2' + \dots + x_k'$

حيث $x_i' \in S_i{}'$ لكل i لأن $\sigma_i : S_i \to S_i{}'$ هو راسم فوقي ، فإنه يوجد $x_i \in S_i$ بحيث أن $\sigma_i(x_k) = x_i'$ ومن ثم يكون

$$\sigma(x) = \sigma_1(x_1) + \sigma_2(x_2) + \dots + \sigma_k(x_k)$$
$$= x_1' + x_2' + \dots + x_k' = x'$$

إذاً σ فوقي ، فبناء عليه يكون $\sigma : G \to G'$ هو أيزومورمزم وأن $G \cong G^1$ وهذا يحقق القضية.

في المسائل المحلولة المعطاة بعد البند 5 الفصل 4 عرفنا تجزئة عدد طبيعي n ونعيد الآن (باختلاف بسيط) التعريف كالآتي :

تعريف 6-2 (تجزئة عدد طبيعي)

ليكن n عدداً طبيعياً فأي تغيير عن العدد n بمجموع أعداد طبيعية يسمى تجزئة للعدد n وسوف نرمز لعدد التجزيئات لعدد n بالرمز $t(n)$.

ملاحظة : عند التعبير عن العدد التطبيقي كمجموع أعداد طبيعية ، فإننا نكتب الأعداد مرتبة تنازلياً وفق القيمة العددية ، فإذا كان $n = n_1 + n_2 + ... + n_k$

فهذا يعني أن $n_1 \geq n_2 \geq ... \geq n_k$

مثال 1

$$4 = 4, 4 = 3+1, 4 = 2+1+1, 4 = 2+2, 4 = 1+1+1+1$$

هذه خمس تجزئيات مختلفة للعدد 4 فيكون $t(4) = 5$.

مثال 2

$$5 = 5, 5 = 4+1, 5 = 3+1+1, 5 = 3+2$$
$$5 = 2+2+1, 5 = 2+1+1+1, 5 = 1+1+1+1+1$$

هذه سبع تجزيئات مختلفة للعدد 5 ويكون $t(5) = 7$.

نظرية 3.6

لأي عدد صحيح موجب $n = P_1^{\alpha 1} P_2^{\alpha 2} ... P_k^{\alpha k}$ حيث الأعداد P_i هي أعداد أولية مختلفة $\alpha_i > 0$ هي أعداد صحيحة ، عدد الزمر الإبدالية غير الأيزومورفية من الرتبة n يساوي حاصل الضرب $t(\alpha_1) t(\alpha_2) ... t(\alpha_k)$.

البرهان

لتكن G زمرة إبدالية من الرتبة n فإن

$$G = S_1 \oplus S_2 \oplus ... \oplus S_k \qquad (1)$$

حيث كل S_i هي زمرة سايلو $P-$ زمرة جزئية من G ومن الرتبة $P_i^{\alpha i}$.

من القضية 6-1 نعلم أن أي زمرتين إبداليتين منتهيتين من الرتبة n هما إيزمورفيتان إذا وفقط إذا كانت المقابلة إيزومورفيتين .زمر سايلو P_i- جزئية ، وهكذا فإذا كان λ_i هي

عدد الزمر الإبدالية غير الإيزومورفية من الرتبة $P_i^{\alpha i}$ فإنه يوجد عدد يساوي $\lambda_1\lambda_2..\lambda_k$ من الزمر الإبدالية غير الإيزومورفية من الرتبة n ولذلك إذا استطعنا بيان أن $\lambda_i = t(\alpha_i)$ فإن النتيجة تتحقق .

اعتبر أي عدد أولي P وأي عدد صحيح موجب α فإننا نحتاج لإثبات أن عدد الزمر الإبدالية غير الأيزومورفية من الرتبة P^α هو $t(\alpha)$. اعتبر أي زمرة إبدالية S من الرتبة P^α فيكون

$$S = A_1 \oplus A_2 \oplus ... \oplus A_L \qquad (2)$$

حيث A_i هي P– زمر جزئية دائرية من الرتبة P^{B_i} يكون $B_1 \geq B_2 \geq ... \geq B_L$ ، من (2) نستنتج أن

$$P^\alpha = \circ(S) = \circ(A_1)\circ(A_2)...\circ(A_L) = P^{B_1+B_2+...+B_L}$$

وهكذا يكون $\alpha = \beta_1 + \beta_2 + ... + \beta_L$ هو تجزئة للعدد α هي اللامتغيرات ، نحن نعلم أن $P^{\beta_1} P^{\beta_2} ,...P^{\beta_L}$ وأن أي P– زمرتين إبداليتين منتهيتين تكونان إيزومورفيتين إذا وفقط إذا كان لهما نفس مجموعات اللامتغيرات ، ومن ذلك ينتج زمرتين P– إبداليتين من الرتبة P^α وإيزومورفيتان سيحددان نفس تجزئيات العدد بصورة وحيدة ، اعتبر تجزئة للعدد α بالصورة $\alpha = r_1 + r_2 + ... + r_m$ نستطيع أخذ $r_1 \geq r_2 \geq - \geq r_m$ بإعادة الترقيم إذا كان ضرورياً . انتق الزمر الدائرية B_i من الرتبة P_i^{ri} $(e = 1, 2, ..., m)$ عندئذ يكون $S = B_1 \oplus B_2 \oplus ... \oplus B_m$ ، P – هي زمرة إبدالية من الرتبة P^α حيث تكون $P^{r_1}, P^{r_2}, ..., P^{r_m}$ هي اللامتغيرات لها ، وقد بيَّنَّا أن أي إبداليتين من الرتبة P^α تكونان إيزوزمورفيتين إذا وفقط إذا كانا يحددان نفس التجزئة للعدد α ، زد على ذلك أنه λ لأي تجزئة للعدد α يقابلها زمرة إيدالية من الرتبة P^α تحدد التجزئة المعطاة للعدد α ، هذا يبرهن بأن عدد الزمر الإبدالية غير الإيزومورفية من الرتبة P^α هو مثل العدد $t(\alpha)$ ، ولهذا ثبتت النظرية .

نظرية 4.6

لأي عدد أولي P الزمرة من الرتبة P^2 إما أن تكون دائرية أو المجموع المباشر لزمرتين دائريتين كل منهما من الرتبة P .

البرهان

لتكن G زمرة من الرتبة P^2 من المعلوم أن G إبدالية (نتيجة 57.5) إذا كانت G فيها عنصر من الرتبة P^2 فإنها تكون دائرية ، نفرض أن G ليست دائرية ، فيكون $P \mid \circ(a)$ لكل $a(\neq e)\in G$ وهنا يُعطى أن $\circ(a) = P$ نختار $a(\neq e)\in G$ فيكون $H=<a>$ زمرة جزئية دائرية من G رتبتها P نختار $b\in G$ بحيث أن $b\notin H$ فتكون الزمرة $K=<b>$ هي أيضاً من الرتبة P . الآن $H\cap K=(e)$ نستنتج من ذلك $\circ(G) = P^2 = \circ(H)\circ(k) = \circ(Hk)$ فلذلك $G=Hk$ وهكذا $G=H\times K$ وهو الضرب المباشر لزمرتين دائريتين كل واحدة من الرتبة P .

ملاحظة

النتيجة السابقة تنتج مباشرة من النظرية 6-3 ، لأن $2=2, 2=1+1$ هما التجزئتان الوحيدتان للعدد 2 ويوجد زمرتان إبداليتان غير إيزومورفيتين من الرتبة P^2 حيث $(P^2), (P,P)$ هما اللامتغيرين لهما على الترتيب في الحالة الأولى G هي زمرة دائرية من الرتبة P^2 ، وفي الحالة التالية G هي حاصل ضرب مباشر لزمرتين دائريتين كل واحدة من الرتبة P .

نظرية 5.6

ليكن كل من q, p عددين أوليين متمايزان ، وليكن $p<q$ إذا كانت G زمرة من الرتبة pq فإن واحد مما يأتي يتحقق :

1. G هي زمرة دائرية (إبدالية) .
2. لها مولدان b,a بحيث أن $a^p=e,b^q=e,a^{-1}ba=b^r$ لعدد ما r بحيث يكون $r\neq 1(\bmod q), r^p\equiv 1(\bmod q)$ و p يقسم $q-1$ (غير إبدالية) .

البرهان

لأن $\circ(G) = pq$ أي G لديها على الأقل زمرة q سايلو جزئية من الرتبة q من نظرية سايلو الثالثة ، فإن عدد الزمر q– سايلو الجزئية هو $1+kq$ لبعض $K\geq O$ و $1+kq$ يقسم p ، ولأن $q>p$ فإن لدينا $k = 0$ وهكذا فإن G لها زمرة q سايلو جزئية واحدة والتي هي عادية ولأن رتبتها عدد أولي فإنها دارية ولتكن مثلاً $<b>$. مرة أخرى G لها على الأقل زمرة P سايلو جزئية واحدة من الرتبة P وعدد هذه الزمر P سايلو الجزئية من G هو $1+kp$ لبعض $k\geq o$ و $1+kp$ يقسم q ولأن q عدداً أولياً يكون لدينا $1+kp=1$ أو $1+kp=q$. في الحالة الأولى G لها زمرة p سايلو جزئية واحدة فقط $<a>$ وهي عادية إذاً $<a>\cap<b>=(e)$ تعطي $ab=ba$ (لأنه إذا كانت K,H زمرتان جزئيتان عاديتان من الزمرة G بحيث كان $H\cap K=(e)$ فإن $[hk=kh\forall hcH, k\in K]$ نستنتج أن $G=<ab>$ وهكذا $\circ(ab) = \circ(a)\circ(b) = pq = o(G)$ هي زمرة دائرية من الرتبة pq .

وقد أغفلنا الحالة عندما $1+kp=q$ حيث ذلك يستدعي أن p تقسم $q-1$ ، ولأن G لها على الأقل زمرة جزئية واحدة ولتكن $<a>$ من الرتبة p كما أن $o(a)=p$ الآن $a^{-1}ba\in<b>$ لأن $<b>$ هي زمرة جزئية عادية من G . نستنتج أن $a^{-1}ba=b^r$ لبعض القيم r حيث $1\leq r\leq q$ فإذا كان $r=1$ فإنه من جديد نحصل على أن $G=<ab>$ زمرة دائرية من الرتبة pq وإذا كانت G غير إبدالية $r\neq 1$ وهكذا فإن $r\neq 1(\bmod q)$.

الآن $a^{-2}ba^2=a^{-1}(a^{-1}b)a=a^{-1}b^ra=(a^{-1}ba)^r=(b^r)^r=b^{r2}$

بالمثل $a^{-3}ba^3=br^3$

وهكـذا . أخـيراً $b=b^{rp}$ فـإذاً $q^{p}=e$ زد علـى ذلـك $r^{-p}ba^{p}=b^{rP}$ هـذا يعطـي أن $r^{P}\equiv 1(\bmod q)$ ونلاحظ أن $<a>\cap<b>=(e)$ ومن ثم فإن :

$$O[<a><b>]=o<a>o<b>=pq=o(G)$$

إذاً $G=<a><b>$ وهكذا فكل عنصر في G هو بالصورة $a^{u}b^{v}$ هذا يبرهن أن G زمرة متولدة بالعنصرين b,a بحيث أن :

$$r^{P}\equiv 1(\bmod q) r\neq 1(\bmod q), a^{-1}ba=b^{r}\ ,b^{q}=e, a^{P}=e$$

و $P/(q-1)$ وفي المقابل نفرض أن q,p,r حيث q,p عددان أوليان بحيث أن $p<q$ يحققان الشروط السابقة . اعتبر زمرتين دائريتين $k=<b>,H=<a>$ من الرتبة q,p على الترتيب .

لتكن G هي المجموعة $H\times K=\{(a^{u}\ ,b^{v})|u,v\in z,1\leq u\leq p,1\leq v\leq q-1\}$

G تحوي pq من العناصر $(a^{n}\ ,b^{y}),(a^{u}\ ,b^{v})$ في G نعرف :

$$(a^{u}\ ,b^{v})(a^{x}\ ,b^{y})=(a^{u+x}\ ,b^{br^{x}+y}) \qquad (1)$$

ولبيان أن هذه العملية معرفة تعريفاً جيداً .

نفرض أن :

$$(a^{u}\ ,b^{v})=(a^{u_1}\ ,b^{v_1}),(a^{x}\ ,b^{y})=(a^{x_1}\ ,b^{y_1})$$

فهذا يستدعي أن :

$$a^{u}=a^{u_1}\ ,b^{v}=b^{v_1}\ ,a^{x}=a^{x}\ \ b^{y}=b^{y_1}$$

$$\ldots\Rightarrow p\,|\,(u-u_1),\,p\,|\,(x-x_1),\,q\,|\,(y-y_1),\,q\,|\,(y-y_1) \qquad (2)$$

$$\ldots\Rightarrow p\,\Big|\,(u+x)-(u_1+x_1)\Rightarrow a^{u+\chi}=a^{u_1+x_1} \qquad (3)$$

لأن $o(a)=p$ مرة أخرى افرض أن :

$$..vr^{x}+y-v_1r^{x_1}-y_1=v\,(r^{x}-r^{x_1})+r^{x_1}(v-v_1)+y-y_1 \qquad (4)$$

بحيث أن $q|(y-y_1),q|(v-v_1)$

فإذا كان $x=x_1$ فمن (4) نستنتج أن

$$q \,\Big|\, \left(vr^{x} + y\right) - \left(v_1 r^{x_1} + y_1\right) \Rightarrow b^{vr^{x}+y} = b^{v_1 r^{x_1}+y_1}$$

أفرض أن $x \neq x_1$ وتحديداً $x < x_1$ فيكون $r^{x} - r^{x^1} = r^{x}\left(1 - r^{x^1 - x}\right)$

ولأن $p \,\Big|\, (x_1 - x), r^{p} \equiv r^{p} \equiv 1 (\operatorname{mod} q)$ فإن :

$$r^{x_1 - x} \equiv 1 \;(\operatorname{mod}\, q) \Rightarrow q \,\Big|\, \left(1 - r^{x_1 - x}\right) \Rightarrow q \,\Big|\, \left(r^{x} - r^{x_1}\right)$$

ومرة أخرى (4) تعطي أن $b^{vr^{x}+y} = b^{vir^{x_1}+y_1}$ فإذاً :

$$\left(a^{u+x}, b^{vr^{x}+y}\right) = \left(a^{u_1+x_1}, b^{v_1 r^{x_1}+y_1}\right)$$

وهذا يبين أن العملية معرفة تعريفاً جيداً .

اعتبر $\left(a^{u}, b^{v}\right), \left(a^{x}, b^{y}\right), \left(a^{s}, b^{t}\right) \in G$

1. التجميع

$$\begin{aligned}
&\left[\left(a^{u}, b^{v}\right)\left(a^{x}, b^{y}\right)\right] \left(a^{S}, b^{t}\right) \\
&= \left(a^{u+x}, b^{vr^{2}+y}\right)\left(a^{s}, b^{t}\right) \\
&= \left(a^{u+x+s}, b^{\left(vr^{x}+y\right)r^{s}+t}\right) \\
&= \left(a^{u+x+s}, b^{vr^{x+s}+yr^{s}+t}\right)
\end{aligned}$$

بالمثل

$$\begin{aligned}
&\left(a^{u}, b^{v}\right)\left[\left(a^{x}, b^{y}\right)\left(a^{s}, b^{t}\right)\right] \\
&= \left(a^{u+x+s}, b^{vr^{x+s}+yt^{s}+t}\right)
\end{aligned}$$

هذا يثبت خاصية (التجميع) .

2. **وجود المحايد** : $e = \left(a^{o}, b^{0}\right)$ بحيث أن :

$$\begin{aligned}
&\left(a^{0}, b^{o}\right)\left(a^{x}, b^{y}\right) = \left(a^{o+x}, b^{or^{x}+y}\right) \\
&= \left(a^{x}, b^{y}\right) = \left(a^{x}, b^{y}\right)\left(a^{o}, b^{o}\right)
\end{aligned}$$

إذاً $\left(a^{o}, b^{o}\right)$ هو المحايد λ في العملية G .

3. **وجود المعكوس اليميني** : أخذ $y, x = p - y$ بحيث يجعل $vr^x + y$ يقبل القسمة على 9 كمثال على ذلك خذ $y = lq - vr^x$ حيث l هو عدد صحيح موجب ، بحيث أن $Lq > Vr^x$.

فإذاً $$\left(a^u , b^v\right)\left(a^x , b^y\right) = \left(a^p , b^{vr^x + y}\right) = \left(a^o , b^o\right)$$

ولذلك فإن G زمرة ، لاحظ إذا كان $b_1 = \left(a^o , b\right), a_1 = \left(a , b^o\right)$ وهكذا فإن b_1 , a_1 يولدان G وأيضاً $a_1^p = \left(a^p , b^o\right) = \left(a^o , b^o\right) = e$ هو المحايد في G بالمثل $b_1^q = e$.

الآن $$a_1 b_1 a_1 = \left(a^{p-1} , b^o\right)\left(a^o , b\right)\left(a , b^o\right) = \left(a^o , b^r\right) = b_1^r$$

فإذاً G زمرة من الرتبة pq متولدة بالعنصرين b_1 , a_1 من الرتبة p q على الترتيب ، $p \mid (q-1), r^p \equiv 1 \pmod q, r \neq 1 \pmod q$

نبين الآن أن أي زمرتين غير إبداليتين G_1 , G' من الرتبة pq تكونان إيزومورفيتين بحيث أن G', G زمرتان متولدتان بالمجموعتين $\{a', b'\}, \{a, b\}$ بحيث أن

$$(b)^q = e \ , \qquad (a)^p = e \qquad , \qquad b^q = e \ , \qquad a^p = e$$

لبعض الأعداد الصحيحة r, r $\quad , a^{-1}ba = b^r \quad (a)^{-1} b^1 a^1 = (b)^{r^1}$

مع أن :

$$r^p \equiv 1 \pmod q \quad , \qquad r' \neq 1 \pmod q \quad , r \neq 1 \pmod q \quad , (r')^p \equiv 1 \pmod q$$

الآن جميع حلول المتطابقة $x^p \equiv 1 \pmod q$ التي لا تطابق 1 معيار q تكون متطابقة مع واحدة من العناصر $r, r^2, r^3, \ldots, r^{p-1}$ معيار q ، وهكذا يكون لدينا $r \equiv r^i \pmod q$ لبعض قيم i الواقعة بين $P-1,1$ فإذاً $b^r = b^{pi} = a^{-1} b a^i$ وإذا وضعنا $b_1 = b, a_1 = a^i$ فإننا نرى b_1 , a_1 أيضاً يولدان G وأن $a_1^{-1} b_1 a_1 = b_1^{r'}$.

نعرف الراسم $\sigma : G \to G$ بالشكل $\sigma\left(a_1^u b_1^v\right) = (a')^u (b')^v$ لكل عددين صحيحين v, u ، وسنترك للقارئ إثبات أن الراسم σ معرف تعريفاً جيداً وهو الإيزومورفيزم .

ملاحظة : النظرية السابقة قدمت أنه لأي عددين أوليين $p<q$ تكون الحالات الآتية متحققة .

(1) إذا كانت p لا تقسم $q-1$ فإن أي زمرة G من الرتبة pq هي زمرة دائرية .

(2) إذا كانت p تقسم $q-1$ فإنه يوجد فقط زمرتان غير إيزوموفيتان من الرتبة pq أحداهما إبدالية (وهي مرة أخرى دائرية لأن q,p عددان أوليان متمايزان) والآخرى غير إبدالية .

مثال 3

اعتبر $p=2$, $q=5$ من الواضح أن $p|(q-1)$ لهذا يوجد زمرتان غير إيزومورفيتين من الرتبة 10 إحدهما دائرية والآخرى متولدة بالعنصرين b,a بحيث أن :

$$a^2=e, b^5=e, a^{-1}ba=b^4$$

لأن $4^2\equiv 1 \pmod 5$.

مثال 4

اعتبر $q=5, p=3$ هنا p لا تقسم $q-1$ ومن ثم فأي زمرة من الرتبة 15 تكون دائرية .

تعريف 6.6

لأي عدد صحيح موجب n الزمرة D_n المتولدة بالعنصرين b,a والتي تحقق العلاقات الآتية $bab^{-1}=a^{-1}$, $b^2=e$, $a^n=e$

الزمرة النونية .

لتكن $H=<a>$, $K=<a>$ زمرتان دائريتان من الرتبة $2,n$ على الترتيب اعتبر المجموعة $G=H\times K=\{(a^u,b^v)|u,v\in Z\}$ لأي $(a^u,b^v),(a^x,b^y)\in G$ عرفنا $(a^u,b^v)(a^x,b^y)=(a^{u+x},b^y)$ وفي حالة $v=1$ فإن G زمرة من الرتبة $2n$ فيها

$b_1 = (a^o, b), a_1 = (a, b^o)$ اعتبارها مولدتان لها كذلك $b_1a_1b_1^{-1} = a_1^{-1}, b_1^2 = e, a_1^n = e$ ومن ثم فإن G زمرة (دايهدرال) نونية ، ويمكننا التحقق من أن أي زمرة دايهدرال نونية تكون إيزوموفية للزمرة G .

تعريف 7.6

الزمرة G المتولدة بالعنصرين b, a والتي تحقق العلاقة $a^u = e$, $b^2 = a^2$, $bab^{-1} = a^{-1}$ تسمى الزمرة الكواتيرينية .

المجموعة H المكونة من المصفوفات الآتية :

$$\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{1} \end{pmatrix}, \pm\begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

هي زمرة من الرتبة 8 تحت عملية ضرب المصفوفات الاعتيادية ، وإذا أخذنا $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, b = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}$ نستطيع بسهولة أن نبين أن a و b يحققان شروط الزمرة الكراتيرينية ، ومن السهل ملاحظة أنها تكون أيزومورفية مع H .

نظرية 8.6

أي زمرة غير إبدالية G من الرتبة 8 تكون إما D_4 أو الزمرة الكواتيرينية .

البرهان

لأن G غير إبدالية ، فتكون G غير دائرية ، ومن ثم فإن G لا يمكن لها أن تحوي عنصراً من الرتبة 8 ، علاوة على ذلك إذا كان كل عنصر عدا المحايد فيها من الرتبة 2 فسوف تكون إبدالية ، وعلى ذلك يوجد عنصر $a(\neq e) \in G$ بحيث أن $O(a)$ ليس 2

أو 8 ، وعندئـــذ فـــإن $o(a)|o(G)$ يعطـــي أن $o(a)=4$ ، إذاً فـــإن الزمـــرة الجزئيـــة $H=(e,a,a^2,a^3)$ ذات الدليل 2 هي زمرة عادية في G .

اختر $b\in G$ بحيث أن $b\notin H$ فيكون :

$$G=H\cup bH=\{e,a,a^2a^3,b,ba,ba^2,ba^3) \qquad (1)$$

هذا يبين أن a و b يولدان G .

إذا كان $ab=ba$ فإن G تكون إبدالية ، فإذاً $ab\neq ba$.

الآن $bab^{-1}\in H$ ولأن H عادية ، فإن $o(bab^{-1})=o(a)=4$.

في H العنصر a^3 هو الوحيد من الرتبة 4 عدا a فإذاً $bab^{-1}=a^3=a^{-1}$ الآن G/H من الرتبة 2 ومن ثم فإن $(bH)^2=H\Rightarrow b^2\in H$.

هـذا يعطي أن $b^2=e$ أو $b^2=a$ أو $b^2=a^2$ أو $b^2=a^3$ فإذا كان $b^2=a$ أو $b^2=a^3$ فإن $o(b)=8$ وهذا غير ممكن لأن G ليست إبدالية ، إذاً $b^2=e$ أو $b^2=a^2$ وفي الحالة الأولى نحصل على أن G هي D_4 وفي الحالة الأخيرة نحصل على أن G هي زمرة كواترينونية .

ملاحظة

لأن $3=3,\,2+1=3,\,1+1+1=3$ هي التجزيئات الثلاث للعدد 3 فإنه يوجد ثلاث زمر إبدالية غير إيزومورفيزمية من الرتبة 8 والنظرية السابقة تعطي أنه يوجد زمرتان إبداليتان غير إيزومورفيتين من الرتبة 8 فإذاً يوجد 5 زمر غير إيزومورفية من الرتبة 8 .

مسائل

1. بأخذنا $p=2$ في النظرية 5.6 برهن أن علاقة التطابق $r^2 \equiv 1 (\bmod q)$ لها حلان فقط ، هما $r \equiv -1 (\bmod q), r \equiv 1 (\bmod q)$ نستنتج أنه أي زمرة من الرتبة $2q$ (q عدد أولي فردي) تكون إما دائرية أو زمرة (دايهدرال) D_q .
2. برهن أن أي زمرة غير إبدالية من الرتبة 6 تكون إيزومورفية لزمرة التناظرات S_3 .
3. برهن أن في S_n مجموع أطوال أي مجموعة من العناصر غير المحايدة من دورات منفصلة ثنائياً لا يمكن أن يتعدى n . استخدم حقيقة أن أي زمرة من الرتبة 15 تكون دائرية ، واستنتج أن A_5 ، A_6 ، A_7 ليس لها زمرة جزئية من الرتبة 15 رغم أن 15 تقسم رتبة كل واحدة منهن .
4. إذا كانت الزمرة G من الرتبة 12 غير إيزومورفية مع A_4 ، برهن أن G يجب أن تحوي عنصراً من الرتبة 6 .
5. إذا كانت الزمرة غير إبدالية من الرتبة 12 ليست إيزومورفية مع A_4 وتحوي على الأقل عنصرين من الرتبة 2 فإن G تكون (دايهدرال) D_6 .
6. بين أن الضرب المباشر $S_3 \times H$ حيث H زمرة دائرية من الرتبة 2 يكون إيزومورفيان مع D_6 .
7. بين أن عدد الزمر الإبدالية غير الأيزومورفية من الرتبة 12 هو 2 .

تمارين محلولة

تمرين 1 : ليكن $g\,,f$ تبديلان دوريان منفصلان في S_n من الرتبة $k\,,m$ على الترتيب ، بين أن $o(fg)=d$ حيث $d=[m,k]$.

الحل

$\because \qquad o(f)=m\,,o(g)=k \Rightarrow f^m=7\,,g^k=7$

وحيث أن $g\,,f$ منفصلتان فإن $fg=gf$ ، إذاً $(fg)^d=f^d g^d=I$ ولأن $k/d\,,m/d$ زد على ذلك أن $(fg)^r=e$ فيكون $f^r=g^{-r}$.

فإذا كانت f^r ليست هي التبديل المحايد ، فإنه يوجد $a\in s$ بحيث يكون $f^r(a)\neq a$ كما أن $f^r(a)$ ينتمي للدورة في f .

ولكن $f^r(a)=g^{-r}(a)$ يؤدي إلى أن $g^{-r}(a)$ تنتمي إلى دورة f ، وذلك لأن $g\,,f$ هما دورتان منفصلان وعليه فإن فرضنا خاطئ ، وعليه فإن $f^r=I=g^{-r} \Rightarrow f^r=I$ $k/r\,,g^r=I \Rightarrow m/r\,,$ الآن $d=[m,k]$ فيكون d/r ومنه $o(fg)=d$.

تمرين 2 : بين أن الزمرة ذات الرتبة 112 لا يمكن أن تكون بسيطة .

الحل

لتكن G زمرة من الرتبة 112 لاحظ $o(G)=112=2^4.7$.

اعتبر زمرة 2- سايلو الجزئية عدد زمرة 2 سايلو الجزئية هو $1+2k$ حيث $k\geq 0$ هو عدد صحيح بحيث يكون $(1+2k)/7$ هذا يعطي أن $k=0,3$.

في حالة $k=0$ يكون لدينا زمرة جزئية واحدة من الرتبة 16 ، وهذا يستوجب أن تكون عادية ، وبالتالي G لا يمكن أن تكون زمرة بسيطة .

في حالة $k=3$ يكون لدينا 7 زمر 2 سايلو جزئية من G وكلها مترافقة بعضاً لبعض .

لتكن H واحدة من زمر 2- سايلو الجزئية .

عدد المجموعات المصاحبة اليمينة للزمرة H هو $o(G)/o(H)=7$ لتكن هذه المجموعات هي $Hx_1\ ,\ Hx_2\ ,\ ..Hx_7$ نعـرف $f:G\to S_7$ بالصـورة $\forall \quad x\in G$, $f\,(\chi)=T_x$ حيـث

$$T_2(Hx_i)=Hx_ix^{-1}, \qquad \forall \quad i=1\,,2\,,...,7$$

من السهل التأكد أن $T_\chi\in S_7$ و f هو هومومورفيزم وأن $\ker f\subseteq H$.

إذا كانت G زمرة بسيطة فإن $\ker f=\{e\}$ لأن e هو محايد الزمرة G $G\neq \ker f$ وإلا أصبح $G=H$.

الآن حيث أن $\ker f=\{e\}$ فإن $G\cong f\,(G)$ حيث أن $f\,(G)$ هي زمرة جزئية من S_7 .

إذا كان $f\,(G)$ يضم كل التباديل الزوجية فإن $f\,(G)\subseteq A_7$ ولكن :

$$o[f\,(G)]=o(G)=112\Rightarrow 112|2520\,,o(A_7)=2520$$

وهذا غير صحيح وعليه فإن $f\,(G)$ تضم على الأقل تبديل فردي واحد .

مجموعة التباديل الزوجية في $f\,(G)$ تشكل زمرة جزئية عادية في $f(G)$ ذات الدليل 2 وهذا ضد ببساطة G نستنتج أن G لا يمكن أن تكون زمرة بسيطة .

تمرين 3 : ميز جميع الزمر G التي تحوي بالضبط زمرة جزئية فعلية واحدة .

الحل

من التمرين 24 في البند الثالث من الفصل الثاني ، G يجب أن تكون زمرة منتهية ليكن q,p عددان أوليان مختلفان ويقسمان $o(G)$ فبواسطة نظرية سايلو تكون G لها زمرة جزئية من الرتب q,p وهذا خلاف الفرض في التمرين ، إذاً $o(G)=p^n$ حيث p عدد أولي و n عدد صحيح أكبر أو يساوي 2 .

مرة أخرى من نظرية سايلو G لها زمر جزئية من الرتب p, p^{n-1} لأن G لها بالضبط زمرة جزئية فعلية واحدة ، إذاً $n-1=1$ أي أن $n=2$ نستنتج أن G هي زمرة إبدالية من الرتبة p^2 أما G زمرة دائرية أو G حاصل ضرب مباشر لزمرتين دائريتين كل واحدة منهما من الرتبة p في الحالة الثانية G لها أكثر من زمرة جزئية فعلية واحدة من الرتبة p ونحصل على تناقض آخر مع الفروض ، إذاً G هي زمرة دائرية من الرتبة p^2 حيث p عدد أولي .

تمرين 4

تعريف : الزمرة الجزئية H من الزمرة G تسمى زمرة جزئية أعظمية إذا كان :

i. $H \neq G$

ii. لا توجد أي زمرة جزئية k في G بحيث يكون $H \subset K \subset G$.

بين أن $<Q,+>$ ليس فيها زمرة جزئية أعظمية .

الحل

لتكن H زمرة جزئية أعظمية في $\lambda.Q$ سوف يوجد عدد نسبي $r/s(r,s \in Z, s \neq o)$ بحيث أن $r/s \notin H$ لأن Z زمرة جزئية في Q , $Z \neq Q$, $H \neq \{0\}$ لتكن $m/n \in H$ و $m \in Z$ و $n \in Z$ و $mn \neq o$.

الآن $m/n \in H \Rightarrow n.m/n \in H \Rightarrow m \in H$ من خاصية الأعظمية للزمرة H نستنتج أن $H+<r/s>=Q$ ومنه يكون $r/sms = h+tr/s$ لبعض $t \in Z, h \in H$ وهكذا $r/s = msh+tmr = (sh)m+(tr)m \in H$ لأن $sh, tr \in Z, m \in H$ وهذا تناقض .

تمرين 5

برهن أن مركز الزمرة G هو محتوى بشكل فعلي في كل زمرة جزئية ذات دليل مركب أعظمية في G .

الحل

لتكن H زمرة جزئية أعظمية في G بدليل مركب وليكن Z هو مركز الزمرة G وليكن Z غير محتوى في H فسوف يوجد $a \notin H, a \notin Z$ اعتبر $<H,a>$ الزمرة الجزئية المتولدة بواسطة a,H ولأن H أعظمية فإن $H \subseteq <H,a>$ ولأن $a \notin H$ فإن $<H,a>=H$ أي $g \in G$ يمكن كتابتها بالشكل $a^i h$ لبعض العناصر $i \in Z, h \in H$ (لاحظ أننا استخدمنا حقيقة أن $a \in Z$) .

الآن لأي $g \in G, y \in H$ فإن :

$$gyg^{-1} = \left(a^i h\right) y \left(a^i h\right)^{-1} = a^i hyh^{-1} a^{-i} = hyh^{-1}$$

لأن $a \in Z$ ولكن $h, y, h^{-1} \in H$ يؤدي إلى أن $gyg^{-1} \in H$ إذاً H هي زمرة جزئية عادية في G ولأن G/H هي ذات رتبة مركبة فإن لها زمرة جزئية غير تافهة ولتكن k/H أي أن $\{H\} \subset K/H \subset G/H$ هذا يعطينا أن $H \subset K \subset G$ وهذا يتعارض مع أعظمية H إذاً $Z \subseteq H$.

الآن إذا كانت $Z = H$ فإن H هي زمرة جزئية عادية من G وبنفس الإدعاء المعطى فيما ذكرناه سلفاًسوف نحصل على تناقض فيكون $Z \subset H$.

تمرين 6

إذا كانت G زمرة تامة ، فإن مركز $G/Z(G)$ يكون تافهاً .

الحل

من أجل التمييز سوف نكتب Z بالشكل $Z(G)$. ونفرض أن مركز $G/Z(G)$ ليست تافهاً ، وعليه يوجد $Za \in Z\left(\frac{G}{Z}\right)$ بحيث أن $a \notin Z$.

نعرف الراسم $f: G \to G$ بالشكل $f(x) = ax\,a^{-1}x^{-1}$ نرى أن $ax\,a^{-1}x^{-1} \in Z$ لجميع العناصر $x \in G$ لأن $Za \in Z\left(\frac{G}{Z}\right)$ فإن $ZaZx = ZxZa$.

$$\Rightarrow Zax = Zxa \Rightarrow (ax)(xa)^{-1} \in Z$$
$$\Rightarrow axa^{-1}x^{-1}Z$$

إذاً f هو راسم من G إلى Z نبين الآن أن f هو هومومورفيزم .

نلاحظ أن $f(xy) = axya^{-1}y^{-1}x^{-1} = \left(axa^{-1}x^{-1}\right)x\left(aya^{-1}y^{-1}\right)x^{-1}$

لأن $= \left(axa^{-1}x^{-1}\right)\left(aya^{-1}y^{-1}\right)x\,x^{-1}, \left(aya^{-1}y^{-1}\right) \in Z$

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

الآن $\ker f$ هو زمرة جزئية عادية في G .

إذا كان $\ker f = G$ فإنه لكل $f(x) = e, x \in G$ يؤدي إلى أن $axa^{-1}x^{-1} = e \Rightarrow ax = xa \Rightarrow a \in Z$ وهذا تناقض فيكون $\ker f \subset G$.

أخيراً لأن $f: G \to Z$ هو هومورفيزم فإن $G/\ker f \cong T$ حيث T هو زمرة جزئية من Z ولأن Z إبدالية فإن $G/\ker f$ هي إبدالية فإذاً $G \subseteq \ker f$ ولكن G تامة فإذاً $G = G'$ هذا يؤدي إلى أن $G = \ker f$ إذاً $aZ = Z$ نستنتج أن مركز G/Z محتوى Z فقط .

تمرين 7 (نظرية ويلسون)

إذا كان p عدد أولي فإن $(p-1)! \equiv -1 (\mathrm{mod}\, P)$.

الحل

اعتبر زمرة التناظرات S_p حيث أن $P^2 + P!, P/P!$ زمرة p سايلو في S_P من الرتبة P فإن عدد الزمر الجزئية P سايلو من S_P هو $1+kp$ ولأن أي زمرة جزئية p سايلو هي من الرتبة P فإن أي زمرتين جزئيتين p- سايلو لا يوجد عنصر مشترك عدا المحايد فيكون العدد الكلي للعناصر من الرتبة p يساوي $(1+kp)(p-1)$.

العناصر من الرتبة P في S_P هي بالضبط دورات بطول p إذاً عددها هو $(p-1)! = \left(\frac{1}{P}\right)P!/o!$ فيكون :

$$(p-1)! = (1+kp)(p-1) = p + kp^2 - kp - 1 \Rightarrow (p-1)! \equiv -1 (\mathrm{mod}\, p)$$

تمارين متنوعة

1- لأي مجموعة غير خالية H في G عرف $H^{-1} = \{\chi^{-1} | \chi \in H\}$.

برهن

i. H زمرة جزئية من G يؤدي إلى $H^{-1} = H$ ولكن عكس هذه النتيجة عموماً .

ii. إذا كانت H مجموعة غير خالية ، فإن H زمرة جزئية من G إذا وفقط إذا كان $HH^{-1} \subseteq H$.

2- بين أن الزمرة الجزئية H من الزمرة G هي زمرة جزئية عادية من G إذا وفقط إذا كان $\chi y \in H \Rightarrow y\chi \in H$ لكل $\chi, y \in G$.

3- أعطي مثالاً لزمرة غير إبدالية G يكون فيها $(\chi y)^3 = \chi^3 y^3$ لجميع العناصر χ, y في G .

إرشاد : افرض $S = \{(x , y , Z) | x , y , Z \in Z / < 3 >\}$ عرف $*$ على S بالشكل :

$$(x , y , Z) * (x' , y' , Z') = (x + x', y + y' , Z + Z' + Zx\, y')]$$

4- لتكن G زمرة إبدالية منتهية برهن أن عدد حلول $x^n = e$ حيث $n / o(G)$ و e هو المحايد في G هو من مضروب n .

5- بين أن A_6 ليس لها زمرة جزئية من الرتبة 120 .

إرشاد : استخدم بساطة A_6 .

6- بين أن زمرة من الرتبة 120 ليست بسيطة .

إرشاد : استخدم التمرين 5 أعلاه .

7- برهن أن زمرة من الرتبة $p^2 q$ حيث q, p عددان أوليان متمايزان زمرة غير بسيطة واستنتج أيضاً أنه إذا كان $p > q , (p^2 - 1)$ q فإن أي زمرة من الرتبة $p^2 q$ تكون إبدالية .

8- برهن أن $xax = b$ قابلة للحل بالنسبة لـ x في G إذا وفقط إذا كان ab هو مربع عنصر من عناصر G .

9- ميز جميع الزمر التي فيها كل عنصر غير المحايد a ويتبادل مع a, a^{-1}, e فقط . (الحل الزمر الدائرية من الرتبة $S_3, 3, 2, 1$) .

10- لتكن G زمرة رتبتها $2n$ افرض أن نصف العناصر كان من الرتبة 2 والباقي يشكل زمرة جزئية H رتبتها n ، برهن أن H من رتبة فردية وهي زمرة جزئية إبدالية من G . اعط مثالاً لزمرة تحقق الشرط أعلاه .

إرشاد : حاول في S_3 .

11- برهن أن كل زمرة منتهية تضم أكثر من عنصرين لها أو تومورفيزم غير تافه .

12- اعط مثالاً لأوتوموفيزم خارجي لزمرة G (نعني أوتومورفيزم غير داخلي على G) الذي يحوّل كل فصل ترافق للزمرة فوقياً على نفسه .

إ رشاد : خذ $G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \middle| a, b \in Z_8, (b, 8) = 1 \right\}$ بين أن G هي زمرة تحت عملية ضرب المصفوفات .

عرف $f : G \to G$ بالشكل $\left[f\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} 1 & a + \dfrac{b^{2-1}}{2} \\ 0 & b \end{pmatrix} \right]$.

13- برهن أن زمرة منتهية من الرتبة $2n$ والتي تحوي عنصراً من رتبته n لها على الأقل $t(n)+1$ من الزمر الجزئية العادية ، حيث $t(n)$ هو عدد قواسم العدد n .

14- لتكن G زمرة جمع إبدالية لأي مجموعة جزئية غير خالية S من G ، ليكن $D(S)$ مجموعة الفروق $x - y$ حيث $x, y \in S$.

بين أنه إذا كان B, A مجموعتين جزئيتين غير خاليتين من G بحيث كان $G = A \cup B$ فإنه إما أن $D(A) \supseteq B$ أو $D(B) \supseteq A$. بين إذا كان $G = A \cup B$ كان B, A غير منفصلتين فإن $D(A) = G$ أو $D(B) = G$.

15- لتكن S مجموعة جميع العناصر في G والتي رتبتها n وهو عدد صحيح موجب مثبت .

برهن أن الزمرة الجزئية المتولدة بالمجموعة S هي زمرة جزئية عادية في G .

16- لتكن G زمرة منتهية ، برهن أن G زمرة P دائرية إذا وفقط إذا كان G لها زمرة جزئية أعظمية وحيدة .

17- برهن أن الجذور النونية للواحد تكوّن فقط مجموعة الجذور النونية لعدد مركب والتي تشكل زمرة تحت عملية الضرب .

إرشاد : لتكن Z عدداً مركباً جذوره النونية تشكل زمرة تحت الضرب من الواضح أن G هي زمرة جزئية من العناصر غير الصفرية المركبة تحت عملية الضرب إذاً $\left[1 \in G \Rightarrow 1 = Z^{\frac{1}{n}} \Rightarrow Z = 1 \right.$.

18- افرض أن G زمرة منتهية وافرض أن لكل $d \geq 1$ و G لها على الأكثر d من العناصر من الرتبة d برهن أن G زمرة دائرية .

19- لتكن G زمرة منتهية من رتبة فردية ، برهن أن مجموعة مضروبات كل العناصر في G مأخوذة بأي ترتيب محتواه في الزمرة الجزئية للمبادلات .

20- لتكن G زمرة منتهية ، بين أن كل عنصر في G يمكن التعبير عنه كمربع لبعض عناصر G إذا وفقط إذا كان $o(G)$ فردياً .

21- إذا كان p عدداً أولياً يقسم n فإن العناصر الوحيدة في S_n والتي رتبتها p هي حاصل ضرب دورات p- منفصلة .

إرشاد : استخدم تمرين محلول بعد نظرية 6.1 .

22- بين أنه لا توجد زمر جزئية رتبها 15 و 20 للزمرة A_s .

إرشاد : كل زمرة رتبتها 15 دائرية و A_s ليس لها عنصر رتبته 15 .

23- لتكن S زمرة جزئية 2- سايلو زمرة A_s ، بين أن S لها 5 مرافقات في A_s .

7

الحلقات Rings

حتى الآن اعتبرنا مجموعات مع عملية ثنائية واحدة ، ولكن هناك مجموعات غير خالية مع أكثر من عملية ثنائية ، مثل مجموعة الأعداد الصحيحة ومجموعة الأعداد النسبية وغيرها .

ونود أن نقوم بإثراء بناء الزمرة وذلك بإمدادها بخواص إضافية أخرى وتتبع الفكرة من حقيقة أن الأعداد الصحيحة تتبع أنماطاً محددة بالنسبة لعمليتي الجمع والضرب الاعتياديتين الأمر الذي يقودنا إلى فكرة الحلقة التي تعرف بالشكل الآتي .

تعريف الحلقة

النظام $<R,+,.>$ حيث R مجموعة غير خالية + و . عمليتين معرفتين على المجموعة R تسمى حلقة إذا حققت البديهيات الآتية :

لأي $a,b,c \in R$

1. $(a+b)+c = a+(b+c)$
2. $a+b = b+a$
3. يوجد $o \in R$ بحيث أن $a+o=a$
4. لكل $a \in R$ يوجد $-a \in R$ بحيث أن $a+(-a)=o$
5. $(a.b).c = a.(b.c)$
6. $a.(b+c) = a.b+a.c$ (قانون التوزيع اليساري) .

$(b+c).a = b.a+c.a$ (قانون التوزيع اليمني) .

ملاحظات

1. . و + تسميان عمليتي الضرب والجمع على الترتيب .
2. الخواص من $R-1$ إلى $R-4$ تبين أن الحلقة R هي زمرة جمع إبدالية ، لذا فإن المحايد الجمعي 0 للحلقة يكون وحيداً وسوف نسميه صفر الحلقة ولنفس السبب أيضاً النظير الجمعي لكل عنصر $a \in R$ يكون $-a$ وحيداً ، وسوف نسميه المعكوس الجمعي أو سالب العدد .
3. لكل عنصرين a,b في الحلقة R سوف نرمز للمجموع $a+(-b)$ بالرمز $a-b$.
4. وللموائمة فإننا نكتب حاصل ضرب عنصرين ab بدلاً من $a.b$.
5. و ... على ما تم الاتفاق عليه في الزمر فلن يكون هناك لبس حول العمليات الثنائية الأساسية في الحلقة $<R,+,.>$ لذا سنقول اختصاراً الحلقة R ونعني بذلك أن R مجموعة غير خالية مع عمليتين ثنائيتين + و . بحيث يكون $<R,+,.>$ حلقة .

تعريف

الحلقة R التي يتحقق فيها $ab=ba$ لكل $a,b \in R$ تسمى حلقة إبدالية .

تعريف

العنصر e في الحلقة R يسمى محايد ضربي للحلقة R إذا كان $ae=ea=a$ لكل $a \in R$.

وعلى العموم فالحلقة يمكن أن يكون فيها محايد ضربي أو لا يكون ، وعلى أية حال يمكننا أن نثبت بسهولة إذا كانت R حلقة تحوي عنصراً محايداً ضربياً e فإن e يكون وحيداً .

ملاحظة

يتضح من تعريف المحايد الضربي أنه إذا كانت الحلقة R تضم عنصراً محايداً ضربياً e فإنه يمكن أنه لا يختلف عن المحايد الجمعي o ومع ذلك فإذا كان فيها عنصرين على الأقل فإن المحايد الضربي e يجب أن يختلف عن o .

مثال 1

مجموعة الأعداد الصحيحة Z هي حلقة تحت عمليتي الجمع والضرب المعتادتين وهي حلقة إبدالية بمحايد و العدد 1 هو محايدها ، كما أن الأعداد الحقيقية R هي حلقات إبدالية والأعداد المركبة C مجموعة كل الأعداد النسبية Q ومجموعة كل الأعداد الحقيقية R ومجموعة كل الأعداد المركبة C كل منها يشكل حلقة إبدالية تحت عمليتي الجمع والضرب المألوفتين في كل واحدة منهن .

مثال 2

مجموعة الأعداد الزوجية الصحيحة E تمثل حلقة تحت عمليتي الجمع والضرب الاعتياديتين وهي حلقة إبدالية بلا عنصر محايد إذ أنه لا يوجد عدد زوجي e يحقق $ey = ye = y$ لكل الأعداد الصحيحة الزوجية y .

مثال 3

المجموعة M التي تمثل جميع المصفوفات ذات الرتبة 2×2 على الأعداد الصحيحة تشكل حلقة غير إبدالية تحت عمليتي جمع وضرب المصفوفات ، والمصفوفة الصفرية هي المحايد الجمعي ومصفوفة الوحدة $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ هي المحايد الضربي للمجموعة M .

وإذا كان $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ فإن $B = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$ هو النظير الجمعي للعنصر A .

ولبيان أن M غير إبدالية يكفي أن نعثر على مصفوفتين B,A في المجموعة M بحيث أن $AB \neq BA$ ، فمثلاً إذا كان : $A=\begin{pmatrix}1 & 2\\ 0 & 3\end{pmatrix}$ ، $B=\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}$ فإن : $AB=\begin{pmatrix}3 & 0\\ 3 & 0\end{pmatrix}$ و $BA=\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$ ومن الواضح أن $AB \neq BA$.

مثال 4

اعتبر المجموعة $X=\{0,1,2,3,4,5\}$ فإن X تكون حلقة تحت عمليتي الجمع والضرب معيار 6 (انظر الفصل الأول) .

مثال 5

لتكن G زمرة جمع إبدالية تضم على الأقل عنصرين . نعرف عملية ضرب ثنائية على عناصر G كالآتي : $x.y=o$ لكل $x,y \in G$ فإن : $<G,+,.>$ تكون حلقة إبدالية بلا محايد .

مثال 6

لتكن F مجموعة كل الدوال المتصلة $f: \mathbb{R} \to \mathbb{R}$ فإذا عرفنا عمليتي الجمع والضرب لكل $f,g \in F$ كالآتي

$$(f+g)(x) = f(x)+g(x) \qquad \forall x \in \mathbb{R}$$
$$(f.g)(x) = f(x)\,g(x) \qquad \forall x \in \mathbb{R}$$

فإن $<F,+,.>$ هي حلقة إبدالية بمحايد ويكون محايدها الجمعي هو الدالة $W: \mathbb{R} \to \mathbb{R}$ بحيث أن $W(x)=o$ لكل $x \in R$.

والنظير الجمعي للعنصر f هو التطبيق $f: \mathbb{R} \to \mathbb{R}$ بحيث يكون $f'(x)=-f(x)$ لكل $x \in \mathbb{R}$ ، $F\lambda$ تكون حلقة إبدالية ، والمناقشة الآتية توضح أن :

لأي $(g.f)(x)=g(x)f(x), (f.g)(x)=f(x)g(x), f,g \in F$

وحيث أن R | $f(x)g(x) \in$ | R و R | ليتحقق منه خاصيته الإبدالية $f(x),g(x)=g(x)f(x)$ وإن $(f.g)(x)=(g.f)(x)$ لكل $x \in$ | R ومن ثم فإنه $\forall f,g \in F$ يكون $f.g=g.f$ وختاماً إذا كان $\theta :$ | $R \to$ | R تطبيقاً معرفاً بالشكل $\forall x \in$ | R $\theta(x)=1$ فإن $\forall x \in$ | R $(\theta.f)(x)=f(x)=(f.\theta)(x)$

ويكون $\theta.f=f.\theta=f$ أي أن θ هي المحايد الضربي .

2. نتائج أولية

نظرية 4.7

لكل a,b في الحلقة R يكون :

i. $ao=oa=o$

ii. $a(-b)=(-a)b=-ab$

iii. $(-a)(-b)=ab$

البرهان

i. لكل $a \in R, aO=a(0+0)$

$$=aO+aO$$

$$aO+(-aO)=(aO+aO)+(-aO)$$

$$O=aO+[aO+(-aO)]$$

$$=aO+O=aO$$

وبالمثل نثبت أن $Oa=0$

وبالتالي فإن $aO=Oa=0$ لكل $a \in R$

$$\begin{aligned} \text{ii} \ . \ & a\left[b+(-b)\right]=aO=0 \\ & \Rightarrow ab+a(-b)=O \\ & \Rightarrow a(-b)=-(ab) \end{aligned}$$

وبنفس الطريقة يمكن إثبات أن $(-a)b=-ab$ 　 $(-a)(-b)=-[a(-b)]=-(-b)$

$$=ab$$

ملاحظة (1) : إذا كانت R حلقة بمحايد ضربي 1 وكان $1=0$ فإن $R=(0)$.

البرهان : إذا كان $x\in R$ فإن $x=1x=ox=0$ بواسطة (i) فيكون $R=(0)$.

لذلك ولتجنب الحالة ... فإننا عندما نقول أن R حلقة بمحايد فإننا نعني أن المحايد الضربي لا يساوي 0 (صفر) .

ملاحظة (2)

i. نعني بالرمز nx المجموع $x+x+...+x$ ، n من المرات ، حيث n عدد صحيح موجب وتعني كما نعني بالرمز $-nx$ المجموع $(-x)+(-x)+...+(-x)$ ، $-n$ من المرات إذا كان n عدداً صحيحاً سالباً .

ii. إذا كان n عدداً صحيحاً موجباً فإن الرمز x^n يعني حاصل الضرب $xxx..x$ من المرات لذا فإن :

$$5x=x+x+x+x+x,\forall x\in R$$
$$(-5)x=(-x)+(-x)+(-x)+(-x)+(-x),\forall x\in R$$
$$x^7 = xxxxxxx \quad \forall \quad x\in R$$

3. أنواع خاصة من الحلقات

من المعلوم أنه إذا كان لدينا عددان صحيحان a,b وكان $ab=0$ فإن ذلك يعني أن $a=0$ أو $b=0$ وعلى العموم فإذا كان a,b عنصران في حلقة ما ، فمن المتوقع أنه إذا

كان $a.b=0$ فإن $a=0$ أو $b=0$ ولكن ذلك ليس صحيحاً دائماً في الحلقات ، فعلى سبيل المثال إذا كان A,B هما عنصران في ... M للمصفوفات في السعة 2×2 على الأعداد الصحيحة وكان $A=\begin{bmatrix}0 & 3\\ 0 & 9\end{bmatrix}$ ، $B=\begin{bmatrix}0 & 4\\ 0 & 0\end{bmatrix}$ فإن $A.B=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$.

في حين أن كلاً من B,A عناصر غير صفرية في الحلقة M حلقة المصفوفات المربعة على Z ، لذلك فإنه من الممكن العثور على عنصرين غير صفريين a,b في حلقة بحيث $a.b=0$.

تعريف 5.7 (القواسم الصفرية)

إذا كانت R حلقة فإن العنصر $a\in R$ يسمى قاسماً يسارياً للصفر إذا كان $ab=0$ لبعض العناصر غير الصفرية $b\in R$ العنصر $a\in R$ يسمى قاسماً يمينياً للصفر إذا وجد عنصر غير الصفر $b\in R$ بحيث يكون $ba=0$.

وإذا كانت R حلقة تضم عنصرين على الأقل ، فإن الحالة التافهة يكون الصفر فيها قاسماً يمينياً ويسارياً للصفر ويسمى القاسم التافه للصفر ، العنصر الغير صفري والذي يكون قاسماً يسارياً (يمينياً) للصفر يسمى قاسم قبلي يساري (يميني) للصفر ، العنصر غير الصفري والذي يكون إما قاسم يساري أو يميني للصفر يسمى قاسم فعلي للصفر .

أما إذا كانت R لا تحتوي على قواسم للصفر يسارية أو يمينية فإننا نقول أن R هي حلقة بدون قواسم صفرية .

تعريف 6.7

الحلقة الإبدالية R التي لا تحتوي على قواسم صفرية فعلية تسمى ساحة تامة ، أي أن الحلقة الإبدالية R هي ساحة تامة إذا كان لكل $ab=o,a,b\in R$ يعني أن $b=0$ أو $a=o$.

مثال 7

المجموعة Z تحت عمليتي الجمع والضرب المألوفتين هي ساحة تامة لأنه لكل عددين صحيحين a,b إذا كان $ab=0$ فإن $a=0$ أو $b=0$.

تعريف 7.7

العنصر a في الحلقة R والتي لها محايد 1 يسمى وحدة (أو قابل للعكس) إذا وجد عنصر b في R بحيث $ab=ba=1$.

مثال 10

في المثال 8 العنصر 5 هو وحده للحلقة X لأن :

$$3.3=1 \pmod 8$$

$$1.1=1 \pmod 8$$

$$7.7=1 \pmod 8$$

بينما $6,4,2,0$ ليست كذلك .

ملاحظة :

العنصر a في الحلقة R التي لها محايد يسمى عنصر غير وحده إذا كان a ليس بوحده ، في المثال 8 نجد أن كل من $6,4,2,0$ هو عنصر غير وحده .

مثال 11

اعتبر الحلقة $R=\{0,1,2,3,4,5,6\}$ تحت عمليتي الجمع والضرب معيار 7 بحيث أن $1.1=\pmod 7$ ، $2.4=1 \pmod 7$ ، $3.5=1 \pmod 7$ ، $6.6=1 \pmod 7$. فإن جميع عناصر الحلقة R غير الصفرية قابلة للعكس .

نظرية 7.8

في الحلقة R التي لها محايد 1 مجموعة العناصر التي هي وحدات تشكل زمرة جزئية من شبه الزمرة $< R, \ \bullet >$.

البرهان

نفرض أن S هي مجموعة العناصر التي هي وحده ، فمن الواضح أن $1.1 = 1$ فيكون $1 \in S$.

والآن نفرض أن $a, b \in S$ فإنه وبما أن كل من a, b هو وحده فإنه يوجد $c, d \in S$ بحيث يكون $ac = ca = 1$ و $bd = db = 1$ وهذا يعني أن $(ab)(dc) = a(bd)c = a1c = ac = 1$

وبصورة مشابهة فإن $(dc)(ad) = 1$ ينتج من ذلك أن العنصر ab وحده يكون $ab \in S$ ولكن $c = a^{-1}$ هو وحده فيكون $a^{-1} \in S$ وبالتالي فإن S زمرة جزئية من $< R, . >$.

تعريف 9.7 (الحلقة القاسمية)

في أي حلقة بمحايد ضربي إذا شكلت مجموعة العناصر غير الصفرية فيها زمرة تحت عملية الضرب سميت حلقة قاسمية .

تعريف 10.7 (الحقل)

الحلقة القاسمية الإبدالية تسمى حقلاً .

مثال 12

افرض أن M هي مجموعة كل المصفوفات 2×2 وذات الشكل $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ حيث أن b, a أعداد مركبة وأن $\bar{a}, \bar{b}$ هما مرافقي العددين a, b ، من اليسير بيان أن M حلقة بمحايد ضربي $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ تحت عمليتي الجمع والضرب .

فإذا كانت A هي أي مصفوفة غير صفرية في M فإنها تكون على صورة $A=\begin{pmatrix} x+yi & u+vi \\ -u+vi & x-yi \end{pmatrix}$ حيث x, y, u, v هي أعداد ليست جميعها أصفاراً .

فإذا أخذنا مثلاً $B=\begin{pmatrix} \dfrac{x-yi}{x^2+y^2+y^2+v^2} & \dfrac{-y+vi}{x^2+y^2+u^2+v^2} \\ \dfrac{u-vi}{x^2+y^2+u^2+v^2} & \dfrac{x+yi}{x^2+y^2+u^2+v^2} \end{pmatrix}$ فإن $B \in M$ كما أن $AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

وعليه أي مصفوفة غير صفرية في M هي وحده لذلك فإن M هي حلقة قاسمية ، ورغم ذلك فهي ليست حقلاً لأنه بأخذ $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \in M$ فإن :

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

أي أن

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \neq \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

فيكون M غير إبدالية تحت عملية الضرب .

مثال 13

في المثال 11 رأينا أن R حلقة إبدالية بمحايد وكل عنصر غير صفري فيها قابل للعكس ، لذلك فإن R حقل .

مثال 14

مجموعة الأعداد المركبة C تمثل حقلاً تحت عمليتي جمع وضرب الأعداد المركبة ، ومن الواضح أن C هي إبدالية والعنصر 1 هو المحايد الضربي ، كما أنه كل عدد مركب غير صفري $a+bi$ له معكوس ضربي يساوي $\dfrac{a-bi}{a^2+b^2}$.

بالمثل بما أن معكوس كل عدد نسبي غير صفري هو عدد نسبي ومعكوس أي عدد حقيقي غير صفري هو عدد حقيقي ، فإن IR,Q كلاهما حقل .

نظرية 11.7

الحلقة الإبدالية R تكون خالية من قواسم الصفر إذا وفقط إذا لكل $a \neq 0, a, b, c \in R$ فإن $ab = ac = b = c$.

البرهان

R حلقة خالية من قواسم الصفر وكان $a \neq 0, ab = ac$ حيث $a, b, c \in R$ فإن :

$$ab = ac \Rightarrow a(b-c) = 0$$

لكن $a \neq 0$ فرضاً ، كما أن R لا تحوي قواسم للصفر فيجب أن يكون $b - c = 0$ إذاً $b = c$.

والآن نفرض أن R حلقة يتحقق فيها الشرط السابق وهو أن $ab = ac \Rightarrow b = c$ وليكن $a, b \in R$ بحيث أن $a \neq 0, ab = 0$.

الآن $a0 = 0$ يعطينا $ab = ao$ و $a \neq 0$ وهذا من خلال الفرض يعطينا أن $b = 0$ إذاً حلقة بدون قواسم للصفر .

تعريف 12.7 (قوانين الحذف)

الحلقة R يقال لها أنها تحقق قانون الحذف اليساري إذا كان لكل $a, b, c \in R$ و $a \neq 0$

$$ab = ac \Rightarrow b = c$$

وبنفس التعريف يمكن إعطاء قانون الحذف اليميني .

ملاحظة

يجب الانتباه إلى أن المقصود بقانون الحذف ، هو قانون الحذف للعناصر غير الصفرية .

نظرية 13.7

كل ساحة تامة غير صفرية منتهية هي حقل .

البرهان

لتكن $R=\{a_1,a_2,...,a_n\}$ هي ساحة تامة غير صفرية و منتهية وفيها $n\geq 2, a_1\neq 0$.

نفرض أن $a(\neq 0)\in R$ فإن $aa_1,aa_2,aa_3,.......,aa_n$ هي كل عناصر R المختلفة وعددها n ، الآن قانون الحذف متحقق في R ، نستنتج أن لأي $a_x\in R$ فإن a_k هو أحد $aa_i\ (i=1,2,...,n)$ أي أن $a_k=aa_i$ لبعض قيم i ومن ثم فإنه يوجد $a_L\in R$ بحيث يكون $a=aa_2$ كما أنه لأي $b\in R$ يكون $ab=(aa_L)b=a(a_Lb)$ إذاً $b=a_Lb$ بما أن R إبدالية هنا ... يؤدي إلى أن a_L هو العنصر المحايد في R ولنرمز للعنصر a_L بالرمز e .

والآن العلاقة (1) تؤدي إلى وجود $a_j\in R$ بحيث أن $e=aa_j$ إذاً $a^{-1}=a_j\in R$ وعليه فإن R حقلاً .

ملاحظة

برهان آخر للنظرية السابقة وذلك باستخدام حقيقة أن كل شبه الزمرة المنتهية التي يتحقق قانون الحذف هي زمرة وهنا لدينا $R-\{0\}$ هي شبه زمرة منتهية ويتحقق فيها قانون الحذف اليساري واليميني .

نظرية 7.14

(a) الحلقة غير الصفرية المنتهية التي لا تحوي قواسم للصفر هي حلقة قاسمية .

البرهان

البرهان يشبه بالضبط برهان نظرية 13.7 مع اختلاف بسيط وهو بعد المعادلة (2) يتم إكمال البرهان بالطريقة التالية :

(لأن $a \neq 0$) $a = aa_L \Rightarrow a(a_L a - a) = a^2 - a^2 = 0 \Rightarrow a_L a = a,$ والآن لكل $x \in R$.

$$ax = (aa_L)x = a(a_L x) \Rightarrow x = a_L x$$

وأيضاً $xa = x(a_L a) = (xa_L)a \Rightarrow x = xa_L$ وعليه فإن a_L هو العنصر المحايد في R وأخيراً العلاقة (1) تعطي $a_L = aa_j$ لبعض القيم $aa_j \in R$ وأيضاً :

$$a(a_j a - a_L) = (aa_j)a - aa_L = a_L a - aa_L = 0 \Rightarrow a_j a = a_L$$

يؤدي إلى أن R هي حلقة قاسمية .

ملاحظة

من نظرية (*wedderbum*) الشهيرة كل حلقة قاسمية منتهية هي حقل ، فإننا نستطيع القول بأن كل حلقة غير صفرية ومنتهية ولا تحوي قواسم للصفر هي حقل .

تمارين محلولة

تمرين 1

لتكن R نظاماً يتحقق فيه كل شروط الحلقة مع إمكانية استثناء الشرط $a+b=b+a$ إذا وجد عنصر $c \in R$ بحيث كان $\forall a,b \in R \quad ac = bc \Rightarrow a = b$ برهن أن R هي حلقة .

الحل

$$(a+b)(c+c) = a(c+c) + b(c+c) = ac + (ac+bc) + bc$$

وأيضاً
$$(a+b)(c+c) = (a+b)c + (a+b)c = ac + (bc+ac) + bc$$

وهذا يعني أن
$$ac + bc = bc + ac$$
$$\Rightarrow (a+b)c = (b+a)c$$
$$\Rightarrow a+b = b+a$$

(بواسطة خاصية العنصر c) إذاً R هي حلقة .

تمرين 2

إذا كان في الحلقة R $x^3 = x$ لكل x في R ، برهن أن R إبدالية .

الحل :

لكل $x, y \in R$

$$\left(x^2 y - x^2 yx^2\right)^2 = x^2 yx^2 y - x^2 yx^2 yx^2 - x^2 yx^4 y + x^2 yx^4 yx^2 = 0$$

لأن $x^4 = x^2$

فإذاً $x^2 y - x^2 yx^2 = \left(x^2 y - x^2 yx^2\right)^3 = 0 \Rightarrow x^2 y = x^2 yx^2$

وبنفس الطريقة نحصل على $yx^2 - x^2 yx^2 = 0$

إذاً :

$$x^2 y = yx^2 \qquad (1)$$

وأيضاً :

$$\left(x^2 - x\right)^3 = x^2 - x \Rightarrow -3x + 3x^2 = 0 \Rightarrow 3x = 3x^2 \qquad (2)$$

أخيراً :

(بواسطة 2) $\left(x^2 - x\right)^2 = x^4 - 2x^3 + x^2 = 2x^2 - 2x^2 - 2x^3 = 2x^2 - 2x = x - x^3$

ولكن الآن بواسطة (1) فإن $\left(x^2 - x\right)^2 = y\left(x^2 - x\right)^2$ ومنها نحصل على :

$$\left(x - x^2\right)y = y\left(x^2 - x\right) \qquad (3)$$

وأيضاً من خلال (1) $xy^2 = yx^2$ هذه العلاقة مع العلاقة (3) نحصل على $xy = yx$ إذاً R هي إبدالية .

تمرين 3

إذا كانت R حلقة بمحايد وفيها $(xy)^2 = x^2 y^2$ لكل $x, y \in R$ فإن R حلقة إبدالية .

الحل

لكل $x, y \in R$

$$[x(y+1)]^2 = x^2(y+1)^2$$
$$\Rightarrow (xy+x)^2 = x^2(y^2+2y+1)$$
$$\Rightarrow (xy)^2 + xyx + x^2y + x^2 = x^2y^2 + 2x^2y + x^2$$
$$\Rightarrow xyx = x^2y \qquad (1)$$

باستبدال x بـ $x+1$ نحصل على

$$(x+1)y(x+1) = (x+1)^2 y$$
$$\Rightarrow (xy+y)(x+1) = (x^2+2x+1)y$$
$$\Rightarrow xyx + xy + yx + y = x^2y + 2xy + y$$
$$\Rightarrow yx = xy$$

(لأن من (1) فإن $xyx = x^2y$

إذاً R هي حلقة إبدالية .

تمرين 4

لتكن $S = \{g_1, g_2, \ldots, g_n\}$ شبه زمرة منتهية مع عملية الضرب ولتكن R حلقة لتعرف $R(S) = \left\{\sum_{i=1}^{n} a_i g_i \middle| a_i \in R, g_i \in S\right\}$ حيث أن $\sum_{i=1}^{n} a_i g_i$ هو رمز صوري ، لذا فإن :

$$\sum a_i g_i = \sum b_i g_i \Leftrightarrow a_i = b_i \qquad \forall \quad i = 1, 2, \ldots, n$$

نعرف .,+ على المجموعة $R(S)$ كالآتي

$$\sum a_i g_i + \sum_{i=1}^{n} b_i g_i = \sum_{i=1}^{n} (a_i + b_i) g_i$$

$$\left(\sum_{i=1}^{n} a_i g_i\right)\left(\sum_{j=1}^{n} b_j g_j\right) = \sum_{k=1}^{n} G_k g_k$$

حيث أن $C_k = \sum a_i b_j$ والمجموع مأخوذ على كل الأزواج a_i, b_j بحيث يكون $g_i g_j = g_k$.

اثبت أن $R(S)$ تمثل حلقة .

ملاحظة

$R(S)$ تسمى حلقة نصف الزمرة .

الحل

من الواضح أن $\left(\sum_i a_i g_i + \sum_i b_i g_i\right) + \sum_i C_i g_i = \sum_i (a_i + b_i) g_i + \sum_i C_i g_i$

$$= \sum_i [(a_i + b_i) + C_i] g_i$$

$$= \sum_i [a_i + (b_i + C_i)] g_i = \sum_i a_i g_i + \sum_i (b_i + c_i) g_i$$

$$\sum_i a_i g_i + \left(\sum_i b_i g_i + \sum_i c_i g_i\right)$$

و $\sum_i a_i g_i + \sum_i b_i g_i = \sum_i (a_i + b_i) g_i = \sum_i (b_i + a_i) g_i = \sum_i b_i g_i + \sum_i a_i g_i$

فإذا أخذنا $\forall_i \quad d_i = 0$ كان $\sum_i d_i g_i = 0$ يمثل الصفر بالنسبة إلى $R(S)$ أي أن $\sum d_i g_i$ العنصر المحايد لعملية الجمع لأنه عندئذ يكون :

$$\sum_i a_i g_i + \sum_i d_i g_i = \sum_i (a_i + d_i) g_i = \sum_i a_i g_i$$

كذلك $\sum (-a_i) g_i + \sum a_i g_i = \sum (-a_i + a_i) g_i = 0$.

ومنه نستنتج أن $< R(S), + >$ هي زمرة إبدالية .

نعني بالرمز $\sum_{g_j g_j = g_k} a_i b_i$ العنصر $C_k = \sum a_i b_j$ في الحلقة R ويكون المجموع مأخوذ على كل a_i, b_j بحيث أن $g_i g_j = g_k$ وبنفس الطريقة $\sum_{(g_i g_j) g_k = g_u} a_i b_j c_k$ و $\sum_{(g_i g_j) g_k = g_v} a_i b_j c_k$ تمثل أن العنصرين $\alpha_u = \sum a_i b_j c_k, \beta_v = \sum a_i b_j c_k$ في الحلقة R على الترتيب والمجموعين يعملان على الثلاثي $a_i b_j c_k$ بحيث أن $(g_i g_j) g_k = g_u$ و $(g_i g_j) g_k = g_v$ على حسب الترتيب .

الآن $\left[\left(\sum_i a_i g_i\right)\left(\sum_j b_j g_j\right)\right]\left(\sum_l c_l g_l\right)$

$$=\left(\sum_k a_k g_k\right)\left(\sum_l c_l g_l\right)$$

حيث
$$a_k = \sum_{g_i g_j = g_k} a_i b_j$$
$$= \sum_u \beta_u g_u$$

حيث
$$\beta_u = \sum_{g_k g_l = g_u} \alpha_k c_l = \sum_{g_k g_l = g_u}\left(\sum_{g_i g_j = g_k} a_i b_j\right) c_l$$
$$= \sum_{(g_i g_i) g_l = g_u} a_i b_j c_l \qquad (1)$$

مرة أخرى $\left(\sum a_i g_i\right)\left[\left(\sum_j b_j g_j\right)\left(\sum_l c_l g_l\right)\right]$

$$=\left(\sum a_i g_i\right)\sum_k \beta_k g_k$$

حيث $\left[\beta_k = \sum_{g_j g_l = g_k} b_j c_l\right]$

$$=\sum v_v g_v$$

حيث
$$v_v = \sum_{g_i g_k = g_v} a_i \beta_k = \sum_{g_i g_k = g_v} a_i\left(\sum_{g_i g_l = g_k} b_j c_i\right) = \sum_{g_i (g_i g_l) = g_v} a_i b_j c_l$$

لأن S هي شبه زمرة تحت عملية الضرب $g_u = g_v$ لكل $u, v = 1, 2, \ldots, n$ لذا :

$$\left[\left(\sum_i a_i g_i\right)\left(\sum b_i g_i\right)\right]\left(\sum c_l g_l\right)$$
$$=\sum_i a_i g_i\left[\left(\sum_j b_j g_j\right)\left(\sum_l c_l g_l\right)\right]$$

وهكذا $< R(S), . >$ تكون شبه زمرة .

أخيراً $\sum a_i g_i\left(\sum_j b_i g_i + \sum_j c_i g_i\right)$

$$=\sum_i a_i g_i\left(\sum_j (b_j+c_j) g_j\right)$$

$$=\sum_i a_i g_i\left(\sum_j d_j g_j\right)$$

عندما $\forall_J = 1,2,\dots,n$ $\quad d_j = b_j + c_j$ $\quad =\sum_k \alpha_k g_k$

حيث

$$\sum_{\substack{i,j\\ g_i g_j = g_k}} a_i d_j = \sum_{\substack{i,j\\ g_i g_j = g_k}} a_i (b_j + c_i)$$

$$= \sum_{\substack{i,j\\ g_i g_j = g_k}} a_i b_j + \sum_{\substack{i,j\\ g_i g_j = g_k}} a_i c_j$$

$$= \beta_k + r_k$$

حيث

$$\beta_k = \sum_{\substack{i,j\\ g_i g_j = g_k}} a_i b_j , r_k = \sum_{\substack{i,j\\ g_i g_j = g_k}} a_i c_j$$

وأيضاً

$$\left(\sum_i a_i g_i\right)\left(\sum_j b_j g_j\right) + \left(\sum_i a_i g_i\right)\left(\sum_i c_j g_i\right)$$

$$= \sum_k \beta_k g_k + \sum_k r_k g_k$$

$$= \sum_k (\beta_k + r_k) g_k$$

$$= \sum_k \alpha_k g_k$$

أيضاً

$$\sum_i a_i g_i\left(\sum_j b_j g_j + \sum_j c_j g_j\right) =$$

$$\left(\sum_i a_i g_i\right)\left(\sum_j b_j g_j\right) + \sum_i a_i g_i\left(\sum_j c_j g_j\right)$$

بنفس الطريقة نستطيع برهان أن :

$$\left(\sum_j b_j g_j + \sum_j c_j g_j\right)\left(\sum_i a_i g_i\right) = \left(\sum_j b_j g_j\right)\left(\sum_i a_i g_i\right) + \left(\sum_j c_j g_j\right)\left(\sum_i a_i g_i\right)$$

ومنه نستنتج أن $< R(S),+,. >$ تكون حلقة .

تمرين 5 (كاتلانسكي)

أثبت أنه إذا كان لعنصر ما في حلقة لها محايد أكثر من معكوس ضربي يميني ، فإن مجموعة المعكوسات الضربية اليمينية تكون مجموعة غير منتهية .

الحل

لتكن R حلقة بمحايد ضربي 1 وليكن $a \in R$ عنصراً له أكثر من معكوس ضربي يميني ، وافرض أن S هي مجموعة المعكوسات اليمينية للعنصر a أي أن $S = \{x \in R / ax = 1\}$ والآن لأي عنصر s في المجموعة S نأخذ المجموعة $T = \{xa - 1 + s / x \in S\}$ لأن

$$\begin{aligned} a(xa-1+s) &= (ax)a - a + as \\ &= 1a - a + as \\ &= as = 1 \end{aligned}$$

نحصل على $xa - 1 + s \in S$ إذاً $T \subseteq S$

نعرف $f : S \to T$ حسب $f(x) = xa - 1 + s$ كل $x \in S$.

من الواضح أن f فوقي وهو أحادي أيضاً لأن :

$$\begin{aligned} & f(x) = f(y) \Rightarrow xa - 1 + s = ya - 1 + s \\ & \Rightarrow xa = ya \Rightarrow (xa)x = (ya)x \Rightarrow x(ax) = y(ax) \Rightarrow x = y \end{aligned}$$

فإذاً إذا كانت S مجموعة منتهية فإن $|S| = |T|$ ونستنتج أن $T = S$ بما أن $s \in S, s \in T$ فإذاً $s = Za - 1 + s$ هذا يؤدي إلى أن $Za = 1$ ولكن $Z \in S$ فيكون $aZ = 1$.

هذا يؤدي إلى أن a عنصر له معكوس ضربي ، وهذا يعني أن a يجب أن يكون له معكوس يميني واحد وهذا يناقض الفرض فتكون S مجموعة غير منتهية .

تمرين 6

المجموعة الغير خالية R مع عمليتين ثنائيتين +,. والتي تحقق جميع شروط الحلقة باستثناء شرط التوزيع من جهة اليمين والتوزيع من جهة اليسار تسمى حلقة ناقصة إذا كان

$$(a+b).(c+d) = a.c + a.d + b.e + b.d$$

لكــل $a,b,c,d \in R$ بـين أن إذا كانـت $<R,+,.>$ تكـون حلقـة ناقصـة و $Z=0.0$ فـإن $32=0$ و $a.0=0.a=a.z=z.a=z$ لكـــل $a\in Z$ ، وإذا مـــا عرفنـــا $*$ علـــى المجموعـــة R بالشكل $x*y=x.y-z$ لكل $x,y\in R$ فبرهن أن $(R,+,*)$ هي حلقة وأن $x*z=z*x=0$ لكل $x\in R$.

الحل

$$0.0=(0+0).(0+0)=0.0+0.0+0.0+0.0 \Rightarrow Z=4Z=3Z=0$$

وأيضاً

$$a.0=(a+0).(0+0)=a.0+a.0+Z+Z \Rightarrow a.0+2Z=0$$
$$\Rightarrow a.0+3Z=Z \Rightarrow a.0=Z$$

وبنفس الطريقة يمكن إثبات أن

$$0.a=Z$$

وهذا يؤدي إلى أن

$$a^2.0=0.a^2=Z$$

وهكذا فإن

$$a.Z=a(a.0)=(a.a).0=a^2.0=Z$$

وبنفس الطريقة نستنتج أن

$$Z.a=Z$$

وأخيراً لكل $a,b,c\in R$

$$\begin{aligned}(a*b)*c&=(a.b-Z)*c=(a.b-Z).c-Z\\&=(a.b-Z).(c+0)-Z\\&=(a.b).c+(a.b).0-Z.c-Z.0-Z\\&=(a.b).c+Z-Z-Z-Z\\&=(a.b).c+Z\end{aligned}$$

لأن $3z=0$

مرة أخرى

$$\begin{aligned}a*(b*c)&=a*(b.c-z)\\&=a.(b.c-z)-z\\&=(a+0).(b.c-z)-z\\&=a.(b.c)-a.z+0(b.c)-0.z-z\\&=a.(b.c)-z+z-z-z\\&=a.(b.c)+z\end{aligned}$$

ولأن $(a.b).c = a.(b.c)$ نحصل على أن $*$ هي عملية تنسيقية وأيضاً :

$$\begin{aligned} a*(b+c) &= a.(b+c)-z \\ &= (a+0).(b+c)-z \\ &= a.b+a.c+0.b+0.c-z \\ &= a.b+a.c+z+z-z = a.b+a.c+z \end{aligned}$$

وأيضاً

$$\begin{aligned} (a*b)+(a*c) &= a.b-z+a.c-z \\ &= a.b+a.c-3z+z \\ &= a.b+a.c+z \end{aligned}$$

لأن $3z=0$ فإذاً

$$a*(b+c) = a*b+a*c$$

بـنفس الطريقـة نسـتطيع برهـان أن $(b+c)*a = b*a+c*a$ ونسـتنتج أن $<R,+,*>$ هـي حلقة .

أخيراً

$$x*z = x.z-z = z-z = 0$$

و

$$z*x = z.x-z = z-z = 0$$

تمارين

1. برهن أن المجموعة $Z[i]=\{a+bi : a,b\in Z\}$ هي حلقة تحت عمليتي جمع الأعداد المركبة وضربها .

   $Z[i]$ تسمى حلقة الأعداد الصحيحة لتجاوس .

2. برهن أن المجموعة $R=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} / a,b,d\in Q\}$ هي حقل .

3. هل المجموعة R' مجموعة كل الأعداد غير النسبية تشكل حلقة تحت عمليتي الجمع والضرب الاعتياديتين ؟ (الجواب لا) .

4. برهن أن لأي عدد أولي P تكون $Q(\sqrt{P})=\{a+b\sqrt{P} / a,b\in Q\}$ هي حلقة تحت عمليتي جمع وضرب الأعداد الحقيقية . هل هذه المجموعة تشكل حقلاً ؟ (الجواب نعم).

5. برهن أنه إذا كان a,b,c,d عناصر في الحلقة R فإن $(a+b)(c+d)=ac+ad+bc+bd$.

6. برهن أن الحلقة R تكون إبدالية إذا وفقط إذا $\forall a,b\in R \quad (a+b)^2=a^2+2ab+b^2$

7. لتكن R_n مجموعة كل المصفوفات من السعة $n\times n$ والتي عناصرها من حلقة R وعرفنا عمليتي الجمع والضرب لأي مصفوفتين $A=(a_{ij}), B=(b_{ij})$ كما يلي $A+B=(a_{ij}+b_{ij})$ ونعرف $AB=(c_{ij})$ حيث أن $c_{ij}=\sum_{k=1}^{n} a_{ik}b_{kj}$ بين أن المجموعة R_n تحت العمليات أعلاه تشكل حلقة ، هذه الحلقة تسمى حلقة المصفوفات $n\times n$ على الحلقة R وبين كذلك إذا كانت R حلقة بمحايد 1 فإن R_n غير إبدالية لكل $n\geq 2$.

8. لتكن S مجموعة غير خالية ولتكن F عائلة كل المجموعات الجزئية من S لأي $A,B \in F$ نعرف عمليتي الجمع والضرب كما يلي :

$$A+B = A \cup B - A \cap B$$

و :

$$AB = A \cap B$$

برهن أن F هي حلقة إبدالية بمحايد .

9. لتكن $G=\{g_1, g_2, ..., g_n\}$ هي زمرة منتهية بعملية ثنائية يشار لها بالضرب ولتكن R حلقة فإذا كان $R(G)=\{(a_1, a_2, ..., a_n)/ a_i \in R\}$ وعرفنا عمليتي الجمع والضرب على المجموعة $R(G)$ كالآتي :

$$(a_1, a_2, ..., ..., a_n)+(b_1, b_2, ..., ..., b_n) \\ = (a_1+b_1, a_2+b_2, ..., ..., a_n+b_n)$$

و

$$(a_1, a_2, ..., ..., a_n)(b_1, b_2, ..., ..b_n)(c_1, c_2, ..., ..., c_n)$$

حيث أن $c_j = \sum a_k b_L$ والمجموع مأخوذ على كل الأزواج a_k, b_L حيث $g_k g_L = g_j$ في الزمرة G ، اثبت أن $R(G)$ هي حلقة .

$R(G)$ تسمى حلقة زمرة G على R .

10. لتكن $H=\{a_0+a_1 i+a_2 j+a_3 k / a_0, a_1, a_2, a_3 \in / R\}$ تعرف المساواة على المجموعة H بالشكل :

$$a_0+a_1 i+a_2 j+a_3 k = b_0+b_1 i+b_1 j+b_3 k$$

إذا وفقط إذا كان $a_0=b_0, a_1=b_1, a_2, a_3=b_3$ نعرف عملية الجمع والضرب على H بالشكل :

$$(a_0+a_1 i+a_2 j+a_3 k)+(b_0+b_1 i+b_2 j+b_3 k) \\ = (a_0+b_0)+(a_1+b_1)i+(a_2+b_2)j+(a_3+b_3)k$$

و

$$(a_0+a_1 i+a_2 j+a_3 k)(b_0+b_1 i+b_2 j+b_3 k) \\ = (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3)+(a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2)i \\ +(a_0 b_2 + a_2 b_0 + a_3 b_1 - a_1 b_3)j+(a_0 b_3 + a_3 b_0 + a_1 b_2 - a_2 b_1)k$$

برهن أن H تكوّن حلقة قاسمية .

11. إذا كان R هو نظام يحقق جميع شروط الحلقة بمحايد مع إمكانية شرط التبديل الجمعي $a+b=b+a$ برهن أن هذا الشرط سيتحقق وبالتالي فإن R هي حلقة

إرشاد : وزع $(a+b)(1+1)$ في إتجاهين مختلفين .

12. في الحلقة R كان $x^2=x, \forall x\in R$ برهن أن :

i. $\forall x\in R \quad 2x=0$.

ii. R حلقة إبدالية .

13. اعطي مثالاً لحلقة R غير إبدالية وبدون محايد ضربي ، بحيث يكون فيها

$$(xy)^2=x^2y^2 \qquad \forall x,y\in R$$

إرشاد : خذ $R=\left\{\begin{pmatrix} a & b \\ 0 & 0\end{pmatrix} a,b\in Z\right\}$.

14. اثبت صواب أو اثبت خطأ العبارة :

$(xy)^3=x^3y^3$ لكل $x,y\in R$ فإن R تكون إبدالية .

15. اعط مثالاً لشبه حلقة لا تكون حلقة .

إرشاد : لتكن $X=\{0,4,24\}$ زمرة جمع دائرية رتبتها لكل $a,b,\in X$ عرف $ab=4$.

16. إذا كانت R حلقة كان $e\in R$ بحيث كان $ex=x\forall x\in R$ فإن e يسمى المحايد اليساري للحلقة R بين أنه إذا كانت R ذات محايد يساري وحيد فإنها تكون ذات محايد .

إرشاد : برهن أنه لكل $x\in R$, $x+e-xi$ هو محايد يساري للحلقة R .

17. لتكن R حلقة بمحايد e إذا كان لكل عنصر غير صفري $x\in R$ يوجد عنصر وحيد $y\in R$ بحيث أن $xy=e$ برهن أن x له معكوس ضربي .

إرشاد : بين أن $[x(e+y-yx)=e]$.

18. العنصر e في الحلقة R يسمى عنصر متساوي القوة إذا كان $e^2 = e$ وأيضاً العنصر x في الحلقة R يسمى عديم القوة إذا كان $x^n = 0$ لبعض عدد موجب n .

بين أنه في الحلقة R :

i. العنصر الغير صفري متساوي القوة لا يمكن أن يكون عنصراً عديم القوة .

ii. في الحلقة ذات المحايد والتي لا تحوي قواسم الصفر فإن العناصر متساوية القوى تكون فقط هي الصفر والمحايد .

19. في حلقة إبدالية R كان b,a عنصران عديمي القوة ، فإن العناصر $ar, a+b$ لكل $r \in R$ تكون كذلك عديمة القوة .

إرشاد : إذا كان $a^m = 0, b^n = 0$ فإن :

$$\left[(a+b)^{m+n} = a^{m+n} + c_1^{m+n} a^{m+n-1} b + \ldots + \ldots + \ldots + \ldots b^{m+n} = 0\right.$$

20. إذا كانت R حلقة لا تضم عناصر غير صفرية عديمة القوة فإن أي عنصر تساوي القوة e للحلقة R يكون $ex = xe \quad \forall x \in R$ اثبت ذلك .

إرشاد : لأي عنصر $x \in R$ $\left[(exe - ne)^2 = 0 = (ex - exe)^2\right.$

21. لتكن R حلقة تضم أكثر من عنصر واحد ، وليكن لكل عنصر $a \in R$ يوجد عنصر b وحيد في R بحيث يكون $aba = a$ برهن أن :

i. $R(i), bab = b$ حلقة قاسمية .

إرشاد : بين أن R لا تضم قواسم صفرية فعلية .

22. برهن أن كل حقل هو ساحة تامة .

23. ليكن P عدد أولي ولتكن D_p مجموعة الأعداد النسبية التي يمكن كتابتها على الشكل $a \mid b$ حيث أن $b = P^k$ لبعض الأعداد الصحيحة $k \geq 0$ بين أن D_p هي ساحة تامة تحت عمليتي الجمع والضرب الاعتياديتين اثبت صحة أو اثبت خطأ العبارة .

24. توجد ساحة تامة فيها 6 عناصر .

إرشـــاد : لـتكن D سـاحة تامـة مـن الرتبـة 6 لأن $<D,+,.>$ هـي حلقـة مـن الرتبـة 6 فإن زمرة الجمع من D تمثل زمرة إبدالية من الرتبة 6 إذاً فيها عنصران a,b ذوات رتبتين 2 , 3 علـى الترتيـب إذاً $2ab=0$ الآن $a\neq 0$ و $2b\neq 0$ فـإذاً $<b,+,.>$ لا يمكـن أن تكـون ساحة تامة .

25. برهن أن أي حقل منتهٍ يجب أن يكون رتبته عدد أولي .

إرشاد : إذا كان F حقلاً منتهياً بحيث كان هناك عددان أوليان مختلفان q,p يقسمان رتبة F فإنه وفق نظرية كوشي يكون $F\lambda$ تحتويان عنصران b,a من الرتبة q,p على الترتيب نسبة إلى عملية الجمع ، وعندئذ يكون $pab=0$.

26. بـين أن حلقـة الأعـداد الصـحيحة معيـار p هـي حقـل إذا وفقـط إذا كانـت p عـدد أولي .

4. الحلقات الجزئية والمثاليات

في الفصل الثاني ناقشنا فكرة الزمرة الجزئية H والتي هي مجموعة جزئية غير خالية من الزمرة G بحيث كانت H نفسها زمرة إيضاً تحت العملية الثنائية المعرفة على الزمرة G . نقدم الآن فكرة الحلقة الجزئية بنفس الطريقة التي قدمنا بها الزمرة الجزئية .

تعريف 14.7

المجموعة الجزئية غير الخالية S من الحلقة R تسمى حلقة جزئية إذا كان :

i. $a+b\in S, ab\in S$ لكل $a,b\in S$ بمعنى أن S مغلقة تحت عمليتي الجمع والضرب في R

ii. S حلقة تحت عمليتي الجمع والضرب إذا كانت S حلقة جزئية من R فإن R تسمى حلقة فوقية لـ S .

مثال 15

Z حلقة جزئية من Q .

مثال 16

المجموعة y المتكونة من كل المصفوفات ذات الرتبة 2×2 والشكل $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}$ حيث a,b,c أعداد صحيحة تكوّن حلقة جزئية من الحلقة M_2 والتي هي مجموعة كل المصفوفات ذات السعة 2×2 على مجموعة الأعداد الصحيحة Z .

نظرية 15.7

المجموعة غير الخالية S من الحلقة R هي حلقة جزئية من R إذا وفقط إذا كان $a-b\in S$ و $ab\in S$ لكل $a,b\in S$.

البرهان

لتكن S حلقة جزئية من R و $a,b\in S$ فمن تعريف S يكون $a+b\in S, ab\in S$ وأيضاً لأن S حلقة تحت عمليتي الجمع والضرب فإننا نستنتج أن $a-b\in S$.

من ناحية أخرى لتكن S مجموعة بحيث كان لكل $a,b\in S$ و $a-b\in S$ وأيضاً $ab\in S$.

الآن $a-b\in S$ لكل $a,b\in S$ يؤدي إلى أن S زمرة جزئية من $<R,+>$ إذاً S تكون مغلقة تحت عملية الجمع في R وهي زمرة إبدالية تحت عملية الجمع وأيضاً لأن S مغلقة على عملية الضرب نستنتج أن S هي شبه زمرة من الزمرة $<R,.>$ وقانون التوزيع متحقق في S لأنه متحقق أصلاً في R ، لذا فإن S حلقة تحت عمليتي الجمع والضرب الاعتياديتين ومنه فإن S هي حلقة جزئية من R .

تعريف 16.7

i. لتكن R حلقة ولتكن S حلقة جزئية من R وليكن $a,b\in R$ نقول أن a يطابق b يميناً معيار S (يرمز لذلك بالرمز $a\equiv rb \pmod s$) إذا وفقط إذا كانت $a-b\in S$ و $(a-b)d\in S$ لكل $d\in R$.

ii. بنفس الطريقة نقول أن a يطابق يساراً معيار S (يرمز لذلك بالرمز $a\equiv b \pmod s$) إذا وفقط إذا $a-b\in S$ و $d(a-b)\in S$ لكل $d\in R$.

iii. نقول أن a يطابق b معيار S إذا كانت a تطابق b يميناً ويساراً معيار S يرمز لذلك بالرمز $a\equiv b \pmod s$.

نظرية 17.7

التطابق اليميني معيار حلقة جزئية S هو علاقة تكافؤ على عناصر R .

البرهان

لتكن $a,b,c\in R$

1. **الانعكـــــاس** : لأن $(a-a)d=0, a-a=0$ لكـــل $\theta\in S, d\in R$ نحصـــل علـــى $a\equiv_r a(\bmod s)$.

2. **التناظر** : إذا كانت $a\equiv_r b(\bmod S)$ فإن $a-b\in S$ و $(a-b)d\in S$ لكل $d\in R$

$$\Rightarrow b-a=-(a-b)\in S$$

و $$(b-a)d=-(a-b)d\in S \quad \forall d\in R$$

$$\Rightarrow b \equiv ra\ (\bmod S)$$

3. **التعدي** : إذا كانت $a \equiv rb\ (\bmod S)$ و $b \equiv rc\ (\bmod S)$ فإن

$$(a-b)d\in S, b-c\in S, a-b\in S$$

و $$(b-c)d\in S$$

لكل $d\in R$ ولأن S حلقة جزئية فإن $$a-c=(a-b)+(b-c)\in S$$

و $$(a-c)d=(a-b)d+(b-c)d\in S, \forall d\in R$$

إذاً $$a \equiv rc\ (\bmod S)$$

وهذا يثبت صحة النظرية .

ملاحظة

بنفس الطريقة يمكن إثبات أن التطابق اليساري معيار S والتطابق معيار S هما علاقتي تكافؤ على R .

نظرية 18.7

إذا كانت S حلقة جزئية من R بحيث كان لأي $a\in S$ ، $y\in R$ ، $ay\in S$ فإنه لكل $x\in R$ تكون المجموعة الجزئية $x+S=\{x+s \mid s\in S\}$ فصل تكافؤ بالنسبة لعلاقة

التطابق اليميني معيار S وبالعكس إذا كان لكل $x \in R$ ، $x+S$ هي فصل تكافؤ بالنسبة لعلاقة التطابق اليميني معيار S فإن $ay \in S$ لكل $y \in R, a \in S$.

البرهان : لتكن S حلقة جزئية بحيث أن $ay \in S$ لكل $y \in R, a \in S$ نأخذ :

$$L = \{t \in R / t \equiv_r x (\bmod S)\}$$

فإذا كان $y \in L$ فإن $y \equiv_r x (\bmod S)$ $\Rightarrow y - x \in S \Rightarrow y \in x + S$

وبذلك فإن $L \subseteq x+S$ مرة أخرى $Z \in x+S$ يؤدي إلى أن $Z - x \in S$ فإنه لأي $y \in R$ فإن $(Z-x)y \in S$ من الفرضية ، هذا يعطي $Z \equiv rx \text{ (mod } S)$ أي أن $Z \in L$ وهذا يعني أن $x+S \subseteq L$ نستنتج أن $x+S=L$ وفي المقابل لكل $x \in R$ فإن $x+S$ هو فصل تكافؤ بالنسبة لعلاقة التطابق اليميني معيار S ، ولأن $0+S=S$ فإن $a \equiv r0 \text{ (mod } S)$ لكل $a \in S$

$$\Rightarrow \quad (a-0)y \in S \quad \forall y \in R$$
$$\Rightarrow \quad ay \in S \quad \forall y \in R$$

إذاً $ay \in S$ لكل $a \in S$ و $y \in R$

بالمثل إذا كانت T حلقة جزئية من R بحيث لكل $t \in T, y \in R$ كان $yt \in T$ فإن لكل $x+T, x \in R$ هو فصل تكافؤ بالنسبة لعلاقة التطابق اليسارية معيار T وبالعكس كذلك إذا كانت V حلقة جزئية من R بحيث لكل $r \in R, v \in V$ كان $rv \in V, vr \in V$ فإنه لكل $x+V=V+x, x \in R$ هو فصل تكافؤ لعلاقة التطابق معيار V والعكس صحيح .

كل ما ناقشناه سلفاً يمكن أن يقودنا للتعريف الآتي :

تعريف 19.7

المجموعة الجزئية غير الخالية I من الحلقة R تسمى مثالي يساري للحلقة R إذا كان :

$a,b\in I$ يؤدي إلى أن $a-b\in I$

$a\in I , r\in R$ يؤدي إلى أن $ra\in I$

تعريف 20.7

المجموعة الجزئية غير الخالية J من الحلقة R تسمى مثالي يميني بالنسبة للحلقة R إذا كان :

i. $a,b\in J$ يؤدي إلى أن $a-b\in J$.

ii. $a\in J$ يؤدي إلى أن $ar\in J$

تعريف 21.7

المجموعة الجزئية غير الخالية k من الحلقة R تسمى مثالي أو مثالي من الجانبين إذا كان K مثالي يساري ويميني في نفس الوقت ، أي بمعنى $a,b\in K$ يؤدي إلى أن $a-b\in K$ و $a\in K$ ، $r\in R$ يؤدي إلى أن $ar\in k$ و $ra\in K$.

ملاحظة : في حلقة R من الواضح أن (0) و R هما مثاليان يمينيان كما هما ومثاليان يساريان وأي مثالي غيرهما يميني أو يساري أو مثالي من الجانبين لا يساوي (0) و R يسمى فعلي يميني ، يساري ، من الجانبين على الترتيب .

مثال 17

مجموعة الأعداد الصحيحة الزوجية E هي مثالي للحلقة Z (حلقة الأعداد الصحيحة) لأن $2m-2n=2(m-n)\in E$ لكل $2m,2n\in E$ وأيضاً إذا كان $r\in Z$ فإن $r(2m)=2rm\in E$ لكل $2m\in E$.

مثال 18

لتكن R حلقة وليكن $a \in R$ المجموعة الجزئية $X = \{r \in R : ar = 0\}$ هي مثالي للحلقة R ولتبيان ذلك لاحظ أن $0 \in X$ فإذاً المجموعة X غير خالية وأيضاً إذا كان $x, y \in X$ فإن $ay = 0, ax = 0$

$$\Rightarrow \qquad a(x-y) = 0 \Rightarrow x - y \in X$$

وإذا كان $r \in R$ فإن $a(xr) = (ax).r = 0r = 0$ إذاً $xr \in X$.

مثال 19

في الحلقة M حلقة كل المصفوفات من السعة 2×2 على الأعداد الصحيحة إذا فرضنا أن المجموعة $L = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a, b \in Z \right\}$ فإن $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in L$ وبالتالي L مجموعة غير خالية

وأيضاً
$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} - \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a-c & 0 \\ b-d & 0 \end{pmatrix} \in L$$

وإذا كان $\begin{pmatrix} \alpha & \beta \\ \delta & \gamma \end{pmatrix} \in M$ فإن
$$\begin{pmatrix} \alpha & \beta \\ \varpi & \delta \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} \alpha a + \beta b & 0 \\ \partial c + \delta b & 0 \end{pmatrix} \in L$$

وهذا يبين أن L هي مثالي يساري للحلقة M ولكن L ليست مثالي يميني في الحلقة M لأن $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in L, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M$ ولكن $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin L$.

مثال 20

مرة ثانية لتكن M حلقة جميع المصفوفات من 2×2 على الأعداد الصحيحة

ولنأخذ
$$K = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in Z \right\}$$

من السهل التأكد أن المجموعة K تشكل مثالي يميني للحلقة M لكنها ليست مثالي يساري لأن $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in K, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in M$ لكن
$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin K$$

ملاحظة : من التعريف نستنتج أن كل مثالي يميني أو يساري أو كلاهما هو حلقة جزئية ، ولكن العكس ليس صحيح وهذا ما يوضحه المثال التالي :

مثال 21

Z هي حلقة جزئية من الحلقة Q ولكن Z ليست مثالية في Q لأن $\frac{1}{2}.3=\frac{3}{2}\in Q$ بالرغم من أن $\frac{1}{2}\in Q$ و $3\in Z$.

ملاحظة : إذا كان $B\subseteq A$ مثاليين في حلقة R وعلى الفور إذا فرضنا أن A نفسها حلقة A عندئذ يكون B مثالي كذلك في A . وسوف نوضح بمثال أن الآتي غير متحقق .

إذا كان $C\subseteq I\subseteq R$ بحيث كان C مثالي في I و I مثالي في R فإن C مثالي في R .

مثال 22

لتكن
$$R=\left\{\begin{pmatrix} a & b & c \\ d & e & f \\ o & o & g \end{pmatrix} \middle| a,b,c,d,e,f,g\in Z\right\}$$

فإن R هي حلقة تحت عمليتي جمع وضرب المصفوفات ، ولتكن :

$$A=\left\{\begin{pmatrix} 0 & 0 & x \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix} \middle| x,y\in Z\right\}$$

فإن A مثالي في R (تحقق فهم ذلك) .

افرض أن
$$B=\left\{\begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \middle| 4\in Z\right\}$$

فإن B مثالية في A لأن :

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\in B,\begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.\begin{pmatrix} 0 & 0 & v \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}=\begin{pmatrix} 0 & 0 & u-v \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\in B$$

وأيضاً $\begin{pmatrix}0&0&x\\0&0&y\\0&0&0\end{pmatrix}.\begin{pmatrix}0&0&u\\0&0&0\\0&0&0\end{pmatrix}=\begin{pmatrix}0&0&4\\0&0&0\\0&0&0\end{pmatrix}.\begin{pmatrix}0&0&x\\0&0&y\\0&0&0\end{pmatrix}=\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}\in B$

ندّعي أن B ليست مثالي في R .

لبيان ذلك نأخذ $\begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix}\in B6\begin{pmatrix}0&0&0\\1&0&0\\0&0&0\end{pmatrix}\in R$

فيكون $\begin{pmatrix}0&0&0\\1&0&0\\0&0&0\end{pmatrix}.\begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix}=\begin{pmatrix}0&0&0\\0&0&1\\0&0&0\end{pmatrix}\notin B$

إذا B ليست مثالي في R .

تعريف 22.7

الحلقة R يقال إنها بسيطة إذا كان :

i. يوجد $a,b\in R$ بحيث $ab\neq 0$.

ii. R لا تحوي مثاليات فعلية .

ملاحظة

إذا كانت R حلقة بمحايد $1(\neq 0)$ فإن لبيان أن R بسيطة فلا داعي للبحث عن الشرط الأول من التعريف لأنه يأخذ $b=1,a=1$ نجد أن $ab=1\neq 0$.

نظرية 23.7

الحلقة القاسمية هي حلقة بسيطة .

البرهان

لتكن $[A_1\neq(0)]$ هي مثالي في حلقة قاسمية R ولأن $A\neq(0)$ فإنه يوجد $a(\neq 0)$ في A ولأن R هي حلقة قاسمية فإن a هو وحدة في R أي أنه يوجد $b\in R$ بحيث يكون $ab=1$ إذاً $1\in A$ لأن $a\in A$ والآن لكل $r\in R$ نجد أن $r=1.r\in A$ نستنتج منه أن $A=R$ وعليه فإن R لا تحوي مثالي فعلي .

ملاحظة

لأي حلقة بمحايد 1 فأي مثالي I في R إذا يحوي 1 فإن $I=R$ ولرؤية هذا افرض أن $x\in R$ فإن $x=x1\in R$ لأن $1\in I$ لذلك فإن $R\subseteq I$ ولكن $I\subseteq R$ بالتالي $I=R$.

تمارين محلولة

تمرين 1

لتكن R حلقة بمحايد ، إذا كانت R لا تحوي مثاليات يمنى عدا R و (0) نبين أن R هي حلقة قاسمية .

الحل

يكفي أن نثبت أن $<R-\{0\},.>$ هي زمرة ، لتكن $x\neq 0\in R$ اعتبر $xR=\{xr\mid r\in R\}$ من الواضح أن $x=x.1\in R$ لذلك فإن R غير خالية وأيضاً :

$$xy-xz=x(y-z)\in xR$$

ولكل $s\in R$ فإن $(xr)s=x(rs)\in xR$ هذا يؤدي إلى أن xR هي مثالي يميني في R .

لأن $x(\neq 0)\in R$ فإن $xR=R$.

بما أن $1\in R$ إذاً يوجد $y\in R$ بحيث يكون $xy=1$ إذاً $<R-\{0\},.>$ هي شبه زمرة بمحايد ولأن كل عنصر فيها هو وحدة فإن $<R-\{0\},.>$ هي زمرة وبناء عليه فإن R حلقة قاسمية .

تمرين 2

برهن أن $M_2=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d\in Q\right\}$ هي حلقة بسيطة .

الحل

M_2 هي حلقة تحت عمليتي الجمع والضرب للمصفوفات (يمكن التأكد من ذلك بسهولة) لأن M_2 تحوي محايداً $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ فإن M_2 هي حلقة بسيطة إذا كانت لا تحوي مثاليات عدا M_2 و $\{0\}$ نفرض أن A هي مثالي في M_2 يختلف عن المثالي (0) .

توجد مصفوفة غير صفرية $X \in A$ ولتكن $X = (a_{ij}), a_{ij} \in Q, i, j = 1,2$ لأن :

$X \neq \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$ فإنه يوجد $a_{rs} \in Q$ بحيث أن $a_{rs} \neq 0$.

لتكن E_{ij} مصفوفة من السعة 2×2 فيها 1 في الصف i والعمود j وأصفار لبقية العناصر (E_{ij} تسمى مصفوفة الوحدة) اجعل $Y = E_{1r}, Z = E_{s1}, C = E_{2r}, D = E_{s2}$

فيكون $YXZ + CXD = \begin{pmatrix}a_{rs} & 0\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ 0 & a_{rs}\end{pmatrix} = \begin{pmatrix}a_{rs} & 0\\ 0 & 0\end{pmatrix} \in A$

لأن $a_{rs}^{-1} \in Q, a_{rs} \neq 0$ فإن المصفوفة $\begin{pmatrix}a_{rs}^{-1} & 0\\ 0 & a_{rs}^{-1}\end{pmatrix} \in M_2$

بما أن A هي مثالي في M_2 إذاً $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}a_{rs}^{-1} & 0\\ 0 & a_{rs}^{-1}\end{pmatrix}\begin{pmatrix}a_{rs} & 0\\ 0 & a_{rs}\end{pmatrix} \in A$

إذاً $A = M_2$ فتكون M_2 حلقة بسيطة .

تمرين 3

لتكن المجموعة A مجموعة غير خالية ، وليكن $P(A)$ رمزاً لحلقة مجموعة القوى (قارن مسألة 8 في نهاية البند الثالث من الفصل السابع) برهن أن المجموعة غير الخالية I والجزئية من $P(A)$ هي مثالية في $P(A)$ إذا وفقط إذا كان لكل $X, Y \in I$ فإن $P(X \cup Y) \subseteq I$.

الحل

نفرض أنه لكل $P(XUY) \subseteq I \, , XY \in I$

$$x\,,\, y \in I \Rightarrow x\Delta y = (X \cup Y) - (x \cap y)$$

هي مجموعة جزئية من $x \cup y$ هذا يؤدي إلى أن $x\Delta y \in P(x \cup y) \Rightarrow X\Delta Y \in I$

زد على ذلك أنه لأي $Z \in P(A)$ يكون :

$$X \cap Z \subseteq X \subseteq (X \cup Y) \Rightarrow x \cap z \in P(x \cup y) \Rightarrow x \cap z \in I$$

إذاً I هـي مثاليـة في $P(A)$ ، مـن ناحيـة أخـرى لـتكن I مثاليـة في $P(A)$ ولـتكن $T \in P(x \cup y)$ هذا يؤدي إلى أن $T \subseteq x \cup y$.

$x, y \in I$ و I هي مثالي في $P(A)$ فيكون $x \cap y \in I \, , x\Delta y \in I$ لأن :

$$T \cap (x \cap y) \in I \, , T \cap (x\Delta y) \in I \, , T \in P(A)$$

ولكـن $T = [T \cap (x\Delta y)] \Delta [T \cap (x \cap y)]$ (اثبـت ذلـك) لـذا فـإن $T \in I$ ومنـه ينـتج أن $P(x \cup y) \subseteq I$.

مسائل

1. لتكن R حلقة اثبت أن $C=\{x\in R \mid xy=yx\forall y\in R\}$ هي حلقة جزئية من R (C تسمى مركز R) .
2. إذا كانت R حلقة $a\in R$ اثبت أن $N(a)=\{r\in R \mid ar=ra\}$ هي حلقة جزئية من R وأن مركز الحلقة R هو حلقة جزئية من $N(a)$ ($N(a)$ تسمى منظم a في R) .
3. لتكن A مثالياً في R بحيث أن $A\neq R$ بين إذا كانت R تحوي على محايد فإن $1\notin A$
4. إذا كانت A و B مثاليتين في R نعرف $A:B=\{r\in R \mid rB\subseteq A\}$ بين أن $A:B$ هو مثالي في R .

لاحظ أن $rB=\{rb \mid b\in B\}$.

5. لكل عنصر a في R بين أن المجموعة $Y=\{r\in R \mid ra=0\}$ هي مثالي يساري في R .
6. لتكن R حلقة إبدالية ولتكن A مثال في R برهن أن :

$$\sqrt{A}=\left\{x\in R \,\middle|\, \exists ntz^{t}\ , x^{n}tAy\right\}$$

هي مثالي في R وأن :

i. $A\subseteq\sqrt{A}$

ii. $\sqrt{\sqrt{A}}=\sqrt{A}$

iii. وإذا كانت R تحوي محايداً وكان $\sqrt{A}=R$ فإن $A+R$.

إرشاد

$a,b\in\sqrt{A}\Rightarrow a^{m}\in A, b^{n}\in A$ حيث أن n,m أعداد صحيحة موجبة

$$\Rightarrow \qquad (a-b)^{m+n}=a^{m+n}-c_{1}^{m+n}a^{m+n-1}b+\ldots+(-1)^{m+n}b^{m+n}\in A\Rightarrow a-b\in\sqrt{A}$$

7. لتكن R حلقة إبدالية برهن أن مجموعة كل العناصر عديمة القوة في R هي مثالي في R .

8. لكل مثالي يساري I وكل مثالي يميني J في R برهن أن :

$$I_1 = \{x \in R \mid x \equiv r0 \pmod I\}$$
$$J_1 = \{x \in R \mid x \equiv L0 \pmod J\}$$

هما مثاليان في R .

9. برهن أن كل حلقة مصفوفات F_n على الحقل F هي حلقة بسيطة ، استنتج أن الحلقة البسيطة يمكن أن تحوي مثالي فعلي ذات جانب واحد .

10. إذا كانت I مثالي يميني فالحلقة R بين أن المجموعة I_3 مجموعة كل المصفوفات من السعة 3×3 على I هي مثالي يميني في الحلقة R_3 حلقة كل المصفوفات من السعة 3×3 على R .

11. برهن أنه إذا كانت R حلقة أكثر من عنصر بحيث أن $aR=R$ لكل عنصر a غير صفري في R فإن R تكون حلقة قاسمية .

إرشاد

أولاً بين أن R لا تحوي قواسم صفرية فعلية ، ليكن c,d عنصران غير صفريين في R فيكون $cR=R$ ، $R=R$ إذاً :

$$(cd)R = c(dR) = cR = R$$

هذا يعطي أن $cd \neq 0$ إذاً R حلقة بدون قواسم صفرية ، والآن $c(\neq 0) \in R = cR \Rightarrow c = cu$ لبعض العناصر $u \in R$ فيكون $cu = cu^2 \Rightarrow u = u^2$ و $u \neq 0$ ولأن $uR = R$ لأي $x = uy, x \in R$ و $y \in R$

$$\Rightarrow \quad ux = u^2 y = uy = x$$

لذا فإن u وحده أيسر في R ، الآن $u \in R = cR \Rightarrow \exists e \in R$ بحيث يكون $u = cd$ وأيضاً $u \in R = dR \Rightarrow \exists e \in R$ بحيث يكون :

$$u = de \Rightarrow e = ue = (cd)e = c(de) = cu = c$$

12. لتكن E حلقة الأعداد الزوجية الصحيحة ، برهن أن مجموعة كل المصفوفات $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ حيث أن a من النوع $4k$ (k عدد صحيح) هي مثالي في E_2 حلقة كل المصفوفات ذات السعة 2×2 على E .

13. برهن أن الحلقة R الإبدالية بمحايد هي حقل إذا وفقط إذا كان المثاليان الوحيدان فيها هما $R, \{0\}$.

14. إذا كانت R حلقة بحيث أنه لكل x تنتمي إلى R و $x^2 - x$ تنتمي إلى مركز الحلقة R فإن R هي حلقة إبدالية .

5. جبر المثاليات

نظرية 24.7

تقاطع مثاليان أيمنان أو أيسران في الحلقة R هو مثالي أيمن أو أيسر في الحلقة R .

البرهان

لتكن A,B مثاليان أيمنان في الحلقة R لأن $0\in A, 0\in B \Rightarrow 0\in A\cap B$

فإن $A\cap B$ غير خالية ، لتكن $v\in R, x, y\in A\cap B$ فإن :

$x, y\in A\cap B \Rightarrow x\in A, x\in B, y\in A, y\in B$

لأن A مثالي أيمن في R فإن $x-y\in A$.

و $xr\in A$ لكل $r\in R$ ولنفس السبب $x-y\in B$ و $xr\in B$ لكل $v\in R$ إذاً $x, y\in A\cap B$ هذا يؤدي إلى أن $x-y\in A\cap B$ و $xr\in A\cap B$ لكل $v\in R$ نستنتج أن $A\cap B$ هو مثالي أيمن في R .

بطريقة مشابهة يمكن إثبات أنه إذا كانت A ، B مثاليان أيسران في R فإن $A\cap B$ هو مثالي أيسر في R أيضاً .

نظرية 25.7

تقاطع أي عائلة غير خالية من مثاليات يُمنى أو يسرى في الحلقة R هي مثالية غير يسرى في الحلقة R .

البرهان

لتكن $F=\{A_i\} i\in A$ هي أي عائلة غير خالية من المثاليات اليمنى في R .

لتكن $A=\cap A_i$ لأن $\forall i\in A \quad 0\in A_i$.

نحصل على أن $0\in A$ ومنه $A\neq\phi$ وبنفس أسلوب النظرية السابقة نستطيع إثبات أنه :

$$x \in A, y \in A, r \in R \Rightarrow x-y \in A, xr \in A$$

إذاً A هو مثالي أيمن في R ، وبنفس الأسلوب يمكن إثبات المثالي الأيسر .

ملاحظة

إذا كانت B, A مثاليان في R فإن $A \cup B$ يمكن أن لا تكون مثالياً في R وهذا يمكن تبيانه بالمثال الآتي :

مثال 23

لتكن $A = \{2n \mid n \in Z\}$ ولتكن $B = \{3n \mid n \in Z\}$ مثاليان في الحلقة Z .

خذ $3 \in B, 2 \in A, A \cup B$ يؤدي إلى أن $2,3 \in A \cup B$ ولكن $3-2=1$ لا ينتمي إلى $A \cup B$ لأن 1 ليس من مضاعفات العدد 2 ولا من مضاعفات العدد 3 لذا فإن $A \cup B$ ليست مثالياً في Z .

الملاحظ في هذا المثال أن A لم تكن محتواه في B ولا B محتواه في A ، الآن يمكن أن نبرهن النظرية التالية :

نظرية 26.7

لأي مثاليان B, A في الحلقة R يكون $A \cup B$ مثالياً في R إذا وفقط إذا $A \subseteq B$ أو $B \subseteq A$.

البرهان

إذا كانت $A \subseteq B$ فإن $A \cup B = B$ هو مثالي في R ، مرة أخرى إذا كانت $B \subseteq A$ فإن $A \cup B = A$ هي مثالي في R وبالعكس ليكن $A \cup B$ مثالياً في R نفرض أن A ليست محتواه في B و B ليست محتواه في A ، فإنه يوجد عنصرين $x \in A-B$ و $y \in B-A$

$$x \in A, y \in B \Rightarrow x, y \in A \cup B$$

بما أن $A\cup B$ مثالياً فإن $x-y\in A\cup B$ ومنه إما $x-y\in A$ أو $x-y\in B$.

في حالة $x-y\in A$ يكون $y=x-(x-y)\in A$ هذا يناقض اختيارنا لـ y ، بنفس الطريقة إذا كانت $x-y\in B$ فإن $x=(x-y)+y\in B$ وهي أيضاً تناقض حقيقة كون $x\notin B$ لهذا فإن فرضنا خطأ والصحيح أن $A\subseteq B$ أو $B\subseteq A$ ولبيان أن اتحاد أكثر من مثاليين يمكن أن يكون مثالياً حتى ولو لم يكن أي منها غير مجازٍ في اتحاد الآخرين . اعتبر المثال الآتي :

مثال 24

لتكن $x=\{0,a,b,c\}$ هي مجموعة عناصر تحقق الشروط الآتية :

$2a=2b=2c=0$ و $a+b=a+b=c$ و $a+c=c+a=b$ و $b+c=c+b=a$ و $xy=0$

لكل $x,y\in X$ فإن X حلقة والمجموعات الجزئية $I=\{0,a\}$ و $J=\{0,b\}$ و $K=\{0,c\}$ ثلاث مثاليات في X ليس منها واحدة محتواة في اتحاد الاثنين الأخريين ولكن $X=I\cup J\cup K$ هو مثالي .

تعريف 27.7

لتكن A و B مثاليان في الحلقة R فالمجموعة $A+B=\{a+b\ |a\in A,b\in B\}$ تسمى مجموع المثاليين B,A .

نظرية 28.7

لأي مثاليين B,A في الحلقة R $A+B$ هو مثالي في R ويحوي كلاً من B,A .

البرهان

من الواضح $0=0+0\in A+B$ إذاً $A+B$ مجموعة غير خالية ، لتكن $x=a_1+b_1$ و $y=a_2+b_2$ حيث أن $a_1,a_2\in A$ و $b_1,b_2\in B$ فإن $x-y=(a_1-a_2)+(b_1-b_2)\in A+B$

لآن $a_1-a_2\in A$ و $b_1-b_2\in B$ وأيضـــاً لكـــل $r\in R$ لـــدينا $xr=a_1r+b_1r\in A+B$ ، $rx=ra_1+rb_1\in A+B$ لأن $a_1r,ra_1\in A$ و $b_1r,rb\in B$ إذاً $A+B$ هـو مثـالي في R أخـيراً لكـل $a\in A$ لأن $a=a+0$ و $0\in B$ نحصـل علـى أن $a\in A+B$ فينـتج أن $A\subseteq A+B$ وبنفس الطريقة فإن $B\subseteq A+B$ وهذا هو برهان النظرية .

تعريف 29.7

إذا كانت S مجموعة جزئية من الحلقة R فإنه يقال أن المثالي A في R مثالياً متولداً بالمجموعة S إذا كان :

i. $S\subseteq A$

ii. لكل مثالي B في R و $S\subseteq B$ يؤدي إلى $A\subseteq B$ سوف نرمز للمثالي A بالرمز $<S>$ ومن الممكن ملاحظة أن $<S>$ هو تقاطع جميع المثاليات في R والتي تحوي المجموعة S وعليه فإن $<S>$ وحيد وزيادة على ذلك إذا كانت متولدة بعنصر واحد منقول $S=\{a\}$ وعندها نقول أن A مثالي رئيسي وتكتب $A=<S>$ أو تكتب $A=<a>$ أو (a) أخيراً إذا كان A مثالي وتوجد مجموعة منتهية S حيث $S\subseteq A$ تولد A فإن A يسمى مثالي منتهى التولد .

نظرية 30.7

لأي مثاليين B,A في الحلقة R فإن $A+B=<A\cup B>$.

البرهان

بواسـطة النظريـة 29.7 فـإن $A+B$ هـو مثـالي في R بحيـث أن $A\subseteq A+B$ و $B\subseteq A+B$ فيكون $A\cup B\subseteq A+B$ ليكن x أي مثالي في R بحيث يكون $A\cup B\subseteq X$

إذا كان $z \in A+B$ فإن $Z = a + b$ بحيث أن $b \in B, a \in A$ الآن $a \in A \cup B$ و $b \in A \cup B$ يؤدي إلى أن $a, b \in x$ وبدوره يؤدي إلى أن $a+b \in x$ يؤدي إلى أن $z \in x$ إذاً $A+B \subseteq x$ نستنتج من التعريف أن $A+B = < A \cup B >$.

تعريف 31.7

لأي مثاليتين B, A في الحلقة R نعرف $AB = \left\{ \sum a_i b_i \;\middle|\; a_i \in A, b_i \in B \right\}$ AB تسمى حاصل ضرب المثاليتين B, A .

نظرية 32.7

لأي مثاليتين B, A في الحلقة R حاصل الضرب AB هو مثالي في R .

البرهان

من الواضح أن $0 = 00 \in AB$ إذاً AB مجموعة غير خالية إذا كان $x, y \in AB$ فإن $x = \sum_{i=1}^{n} a_i b_i$ و $y = \sum_{j=1}^{m} c_j d_j$ حيث أن $a_i, c_j \in A$ و $b_i, d_j \in B$ إذاً :

$$x - y = \sum_{i=1}^{n} a_i b_i - \sum_{j=1}^{m} c_j d_j = \sum_{k=1}^{m+n} x_k y_k$$

حيث أن $x_k = a_k \;\; \forall K = 1, 2, ..., n, x_{n+t} = -c_t \forall t = 1, 2, ..., m$

و $y_k = b_k \; \forall K = 1, 2, ..., n, y_n + t = d_t \; \forall t = 1, 2, ..., m$

ولأن $x_k \in A, y_k \in B \forall K = 1, 2, ..., m+n$ نحصل على $x - y \in AB$ وأيضاً إذا كانت $r \in R$ فإن

$$xr = \sum_{i=1}^{n} (a_i b_i) r$$
$$= \sum_{i=1}^{n} (a_i b_i) r$$

$$= \sum_{i=1}^{n} a_i (b_i r) \in AB$$

لأن $a_i \in A$ و $b_i r \in B$ لكل $i = 1,2,...,n$ وبنفس الطريقة :

$$rx = r\left(\sum_{i=1}^{n} a_i b_i\right) = \sum_{i=1}^{n} (ra_i) b_i \in AB$$

لأن $ra_i \in A$ و $b_i \in B$ لكل $i = 1,2,...,n$ إذاً AB هو مثالي في R .

تعريف 33.7 قوى المثال

ليكن A مثالي في الحلقة R نعرف $A^2 = AA$ أي أن $A^2 = \left\{\sum a_i b_i \mid a_i, b_i \in A\right\}$ وباستخدام الاستنتاج يمكن تعرف A^n لأي عدد صحيح موجب n .

تعريف 34.7 (مثالي عديم القوة)

المثالي A في الحلقة R يسمى عديم القوة إذا وجد عدد صحيح موجب n بحيث يكون $A^n = (0)$.

مثال 25

اعتبر M_2 حلقة كل المصفوفات من السعة 2×2 المثلثية العليا على مجموعة الأعداد الصحيحة ولتكن I المثالي في M_2 المتولد بالمصفوفة $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

من الواضح أن I هو مثالي عديم القوة لأن $I^2 = (0)$.

تعريف 35.7 مثالي العدم أو المثالي المتلاشي

المثالي I في الحلقة R يسمى مثالي العدم أو متلاشي إذا كان كل عنصر في I هو عنصر عديم القوة (أي أن لكل $a \in I$ يوجد عدد صح موجب n بحيث أن $a^n = 0$) .

مثال 26

المثـالي I المـذكور في المثـال 25 مـن الواضـح أنـه مثـالي عـديم القـوة لأن $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

ملاحظة

من الواضح أن كل مثالي عديم القوة هو مثالي متلاشي لأنه إذا كانت A مثالي عديم القوة فإنه يوجد عدد صحيح موجب n بحيث أن $A^n = (0)$ لذلك فإنه لكل $a \in A$ و $a^n \in A^n = (0)$ هذا يؤدي إلى أن $a^n = 0$ إذاً A هو مثالي متلاشي أو صفري والعكس غير صحيح كما توضح من المثال الآتي :

مثال 27

لتكن $Z_{p^n}(n > 1)$ هي حلقة الأعداد الصحيحة معيار P^n حيث أن P هو عدد أولي لتكن $F = \left\{\{\overline{a}_n\} \,\middle|\, a_n \in Z_{p^n}\right\}$ أي أن F هي عائلة كل المتتابعات $\{\overline{a}_n\}$ حيث أن $\overline{a}_n \in Z_{P^n}$.

نعرف الجمع والضرب على F كالآتي $\{\overline{a}_n\}\{\overline{b}_n\} = \{\overline{a_n b_n}\}, \{\overline{a}_n\} + \{\overline{b}_n\} = \{\overline{a_n + b_n}\}$

من الممكن التأكد أن F هي حلقة والمتتابعة $\{\overline{o}_n\}$ تمثل الصفر فيها حيث أن $\overline{0}_n$ هو صفر الحلقة Z_{P^n} وأن $-\{\overline{a}_n\} = \{-\overline{a}_n\}$.

الآن إذا كانت R مجموعة المتتابعات في F والتي تحوي عدداً منتهياً من الحدود غير الصفرية فإن R مثالي في F (تحقق من ذلك !) .

نعتبر أن R حلقة وأن I مثالياً فيها يحوي العناصر من النوع :

$$\left(P\overline{r}_1, P\overline{r}_2, \ldots, P\overline{r}_k, \overline{0}, \overline{0}, \ldots\right), \overline{r}_k \in Z_{P^k}$$

فإذا كان $a=\left(P\bar{r}_1, P\bar{r}_2, \dots, \dots P\bar{r}_k, \bar{o}, \bar{o} \dots, \dots\right) \in I$

من $\left(P\bar{r}_i\right)^i = \bar{o}, Z_{P^i}$ نحصل على أن $\left(P\bar{r}_i\right)^k = \bar{0}$ لكل $i \le k$.

ويكون $a^k = \left(\bar{0}, \bar{0}, \bar{0}, \dots, \dots\right)$ يؤدي إلى أن I مثالي صفري ، نتوقع أن يكون I مثاليا غير عديم القوة ولأجل هذا نبين أنه لكل عدد صحيح موجب n يوجد عنصر $a \in I$ بحيث يكون $a^n \ne 0$.

عرف $a = \{\bar{a}_k\} \dots \bar{a}_{n+1} = \bar{P}$ في $Z_{P^{n+1}}, \bar{a}_k = \bar{o} \forall k \ne n+1$ يكون :

$$a = \left(\bar{0}, \bar{0}, \bar{0}, \dots, \dots, \bar{P}, \bar{0}, \bar{0}, \dots, \dots\right)$$

لأن في الحلقة $Z_{P^{n+1}}$ العنصر $\bar{0} \ne {}^n\bar{P}$ من ذلك نحصل على أن :

$$a^n = \left(\bar{0}, \bar{0}, \bar{0}, \dots, \dots, \bar{P}^n, \bar{0}, \bar{0}, \dots, \dots\right) \ne 0$$

فيكون $I^n \ne (0)$ لكل عدد صحيح $n > 0$ نستنتج أن I مثالياً غير عديم القوة .

تمارين محلولة

تمرين 1

T, S هما حلقتان جزئيتان من الحلقة R فإذا كان $ST = \left\{\sum s_i t_i, s_i \in S, t_i \in T\right\}$

بين أنه إذا كان $ST = TS$ فإن ST هي حلقة جزئية من الحلقة R .

أعطي مثالاً لحلقتين جزئيتين T, S من الحلقة R حتى يصبح من غير الضروري أن تكون ST حلقة جزئية من حلقة R .

الحل

من الواضح أن ST غير خالية ، وأن $x, y \in ST \Rightarrow x - y \in ST$.

إذا كان $xy \in ST$ فإن $x = \sum_{i=1}^{m} s_i t_i$ و $y = \sum_{j=1}^{n} a_j b_j$ ، $s_i, a_j \in S$ و $t_i, b_j \in T$ وهذا يتطلب أن يكون $xy = \sum_{j=1}^{n} \sum_{i=1}^{m} s_i \left(t_i a_j\right) b_j$.

الآن $t_i a_j \in TS \Rightarrow t_i a_j \in ST \Rightarrow t_i a_j = \sum_{k=1}^{q(i,j)} \alpha^{(i)}{}_k \beta^{(i)}{}_k$ حيـــــــث $\overset{(i)}{\alpha_k} \in S$ و $\overset{(j)}{\beta_k} \in T$

و $q(i,j)$ هو عدد طبيعي يعتمد على j,i لذلك فإن :

$$xy = \sum_{j=1}^{n} \sum_{i=1}^{m} \sum_{k=1}^{q(i,j)} s_i \overset{(i)}{\alpha_k} \overset{(j)}{\beta_k} b_j$$

ولكن $K, J, i \quad \forall \quad S_i \overset{(i)}{\alpha_k} \in S\beta_k b_j^{(j)} \in T$ فيكون $xy \in ST$ من هذا يتضح أن ST هي حلقة جزئية من R .

للجزء الثاني خذ R حلقة المصفوفات من السعة 3×3 على Z ولتكن :

$$S = \left\{ \begin{matrix} 0 & 0 & 0 \\ a & 0 & 0 \\ b & c & 0 \end{matrix} \middle| a,b,c \in Z \right\}, T = \left\{ \begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ 0 & 0 & 0 \end{pmatrix} \middle| a,b \in Z \right\}$$

نستطيع أن نثبت أن T,S تكون حلقتان جزئيتان من R أي :

$$s = \begin{pmatrix} 0 & 0 & 0 \\ x & 0 & 0 \\ y & z & 0 \end{pmatrix} \in S, t = \begin{pmatrix} 0 & 0 & \alpha \\ 0 & \beta & 0 \\ 0 & 0 & 0 \end{pmatrix} \in T$$

$$st = \begin{pmatrix} 0 & 0 & 0 \\ x & 0 & 0 \\ y & z & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & \alpha \\ 0 & \beta & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & x\alpha \\ 0 & z\beta & yx \end{pmatrix} \qquad (1)$$

و ST هي مجموع عدد منتهٍ من عناصر النوع (1) .

الآن $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \in S$ و $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in T$ يــؤدي إلى أن $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ أيضــاً $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 2 & 0 \end{pmatrix} \in S$

و $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in T$ يؤدي إلى أن $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 4 & 1 \end{pmatrix} \in ST$ فإذا كانت ST حلقة جزئية من R فإن :

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 4 & 1 \end{pmatrix} \in ST$$

وبعبارة أخرى يكون $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 4 & 2 \end{pmatrix} \in ST$ وهذا يكون مناف لكون أن كل عنصر من ST يجب أن يكون من النوع (1) لذلك فإن ST ليست حلقة جزئية في R .

تمرين 2

المثاليان B, A في الحلقة R يسميان متعاظمين* إذا كان $A+B=R$.

برهن أنه إذا كانت B, A مثاليان متعاظمان في حلقة إبدالية R ذات محايد فإن $AB = A \cap B$.

الحل

بما أن A مثالياً في R و $AB \subseteq AR \subseteq A$ بالمثل بما أن B مثالياً في R و $AB \subseteq B$ فإن $AB \subseteq A \cap B$.

الآن لتكن $x \in A \cap B$ فإن $R = A + B \Rightarrow 1 = r + s$ لبعض العناصر $s \in B, r \in S$ هذا يعطي $x = x1 = x(r+s) = xr + xs$ ولكن $r \in A, x \in B \Rightarrow xr = rx \in AB$ وأن :

$$x \in A, s \in B \Rightarrow xs \in AB$$

فينتج أن $x \in AB$ أي أن $A \cap B \subseteq AB$ فإذاً $A \cap B = AB$.

---

* متعاظمين (Commercials) من النهاية العظمى .

مسائل

1. بين أنه إذا كان A مثالي أيمن و B مثالي أيسر للحلقة R فإن $AB \subseteq A \cap B$ وأعط مثالاً للحلقة R ومثاليان B, A في الحلقة R بحيث يكون $AB \neq A \cap B$.
2. برهن ما يلي :

i. إذا كانت B, A مثاليان أيمنان أو أيسران للحلقة R فإن AB هي مثالي أيمن أو أيسر للحلقة R .

ii. إذا كانت A مثالياً أيسر و B مثالياً أيمن للحلقة R فإن AB مثالي من الجانبين في الحلقة R ولكن BA ليست بالضرورة مثالياً حتى من جانب واحد في الحلقة R .

iii. إذا كان A مثالياً أيسر و B مثالياً أيمن في الحلقة R فإن $A+B$ ليس بالضرورة مثالياً من أي جهة للحلقة R .

iv. إذا كانت A مثالياً أيسر و B مثالياً أيمن للحلقة R بين أن $A \cap B$ ليست من الضروري λ مثالياً حتى من أي جهة في R .

إرشاد

(iii) و (iv) في الحلقة Z_2 للمصفوفات 2×2 على Z .

خذ $A = \left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} | \, x, y \in Z \right\}, B = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} | \, a, b \in Z \right\}$.

3. لتكن B, A مثاليان في الحلقة R بحيث أن $A \cap B = (0)$ المجموع $A+B$ يسمى المجموع المباشر لـ B, A ويرمز له بالرمز $A \oplus B$. بين أن كل عنصر في $A \oplus B$ يمكن التعبير عنه بشكل وحيد $a+b$, $b \in B, a \in A$.

4. إذا كان C, B, A مثاليات في الحلقة R بين أن $A(B+C)=AB+AC$.

5. برهن أنه إذا كانت R حلقة تحوي عنصراً غير صفري متساوي القوة (أي أن $e^2=e$) بحيث أن e ليست وحده يسارياً في R فإن R هي مجموع مباشر (انظر المسألة 3 السابقة) لمثاليات يمينية غير صفرية $S=\{a-ea \mid a\in R\}, eR$.

6. إذا كانت C, B, A مثاليات في حلقة بحيث أن $B\subseteq A$ برهن أن $A\cap(B+C)=B+(A\cap C)$ (هذا يسمى قانون التعويل) .

أعطي مثال تبين فيه بصورة عامة $A\cap(B+C)$ لا تساوي $B+(A\cap C)$.

إرشاد

انظر مثال 24 خذ $C=K, B=J, A=I$.

7. بالعودة إلى مسألة (4) في البند 4 إذا كانت C, B, A مثاليات في الحلقة R فبرهن ما يلي :

i. $(A\cap B):C=(A:C)\cap(B:C)$

ii. $A:(B+C)=(A:B)\cap(A:C)$

iii. $A:(BC)=(A:C):B$

8. بالعودة إلى مسألة 4 في البند 4 برهن ما يلي لكل مثاليات K, J, I في الحلقة R .

i. $I\subseteq J$ يؤدي إلى $I:K\subseteq J:K$ و $K:I\supseteq K:J$.

ii. $I:J^{n+1}=(I:J^n):J=(I:J):J^n$ لكل عدد صحيح موجب n .

iii. $I:J=I:(I+J)$.

9. لتكن R حلقة بمحايد ولتكن R_n حلقة كل المصفوفات سعة $n\times n$ على R . برهن ما يلي :

i. إذا كان I مثالي في R فإن I_n المجموعة الجزئية من R_n والتي تحوي المصفوفات سعة $n \times n$ والتي جميع عناصرها من I هي مثالي في R_n .

ii. كل مثالي في R_n هو من الشكل I_n لبعض مثالي I في R .

10. لتكن R حلقة وفيها الخاصية أن كل حلقة جزئية منها ضروري أن تكون مثالية فيها إذا كانت R لا تحوي قواسم صفرية فعلية برهن أن R إبدالية .

11. برهن ما يلي :

i. مجموع مثاليان عديمي القوة هو مثالي عديم القوة بينما مجموع عنصران عديمي القوة ليس بالضرورة أن يكون عنصر عديم القوة .

ii. بين أن في الحلقة الإبدالية R توجد مثالي صفري أو متلاشي A تحوي جميع المثاليات المتلاشية في R .

iii. إذا كانت R حلقة بسيطة فإن R_n بسيطة .

12. بالرجوع إلى مسألة 4 في البند 4 برهن إذا كانت R حلقة بمحايد و J, I مثاليان في R فإن $I : J = R \Leftrightarrow J \subseteq I$ أعطي مثالاً تبين فيه إذا كانت R بدون محايد فإن النتيجة ليست بالضرورة أن تكون صحيحة بصورة عامة .

تلميح : خذ $J = (6), I = (4), R = (2)$.

8

الهومومورفزمات وغمر الحلقات

Homomorphisms and Embedding of Rings

1. حلقات القسمة ، الحقول والهرمومرفزمات

من التعريف فإن الحلقة R هي زمرة جمع إبدالية ، فمن الضروري أن يكون المثالي N في الحلقة R فمن الضروري أن يكون زمرة جمع جزئية من $<R,+>$ ، يمكننا التحدث عن زمرة القسمة الجمعية $R/N=\{r+N/r\in R\}$ للزمرة $<R,+>$ ، ومن الملاحظ أيضاً أن كل $r+N$ هو فصل تكافؤ لعلاقة التطابق معيار N (نظرية 18.7) وهكذا فإن R/N هي مجموعة جميع فصول التكافؤ بالنسبة لعلاقة التطابق معيار N نودُّ أن نجعل R/N حلقة لهذا تعرف عملية الضرب كالآتي :

لأي $r+N, s+N \in R/N, (r+N)(s+N) = rs+N$

نلاحظ أن R/N هي زمرة إبدالية تحت عملية الجمع $\oplus$ المعطاة بالشكل :

$$(r+N)\oplus(s+N)=(r+s)+N$$

$\oplus$ هي بطبيعة الحال تعريفاً جيداً ، فإننا نتحقق من أن عملية الضرب معرفة تعريفاً جيداً ، أيضاً لهذا الغرض نفرض أن :

$s+N = s_1+N , r+N = r_1+N$ لبعض $r, r_1, s, s_1 \in R$ هذا يؤدي

$r-r_1=n, s-s_1=n_1$ لبعض $n, n_1 \in N$ $\Rightarrow \quad r=n+r_1 , s=n_1+s_1$

$$\Rightarrow \quad rs = nn_1+ns_1+r_1n_1+r_1s_1$$

ولأن $n, n_1 \in N$ كما أن N هي مثالي في R ، $nn_1 + ns_1 + r_1 n_1 \in N$ فإن $rs - r_1 s_1 \in N$
ومن ثم $rs + N = r_1 s_1 + N$ أي أن $(r+N).(s+N) = (r_1+N).(s_1+N)$
هذا يبين أن عملية الضرب معرفة تعريفاً جيداً على R/N .

نظرية 1.8

لتكن R حلقة ولتكن N مثالياً في R فإن R/N حلقة تحت عملية الجمع والضرب المعرفتين كالآتي :

لكل $r+N, s+N \in R/N$

$(r+N)+(s+N) = (r+s)+N$ و $(r+N).(s+N) = rs+N$

البرهان

من التعريف فإن R/N مغلقة بالنسبة لعمليتي الجمع والضرب وليكن $r, s, t \in R$

(1) $< R/N, + >$ زمرة إبدالية .

(2) الضرب تنسيقي $(r+N)[(s+N).(t+N)] = (r+N)(st+N) = r(st)+N$

(لأن $(rs)t = r(st)$ في R)

$$
\begin{aligned}
&= (rs)t+N \\
&= (rs+N)(t+N) \\
&= [(r+N)(s+N)](t+N)
\end{aligned}
$$

(3) قانوني التوزيع $(r+N)[(s+N)+(t+N)] = (r+N)[(s+t)+N]$

$$
\begin{aligned}
&= r(s+t)+N \\
&= (rs+rt)+N \\
&= (rs+N)+(rt+N) \\
&= (r+N)(s+N)+(r+N)(t+N)
\end{aligned}
$$

وبنفس الطريقة يمكن إثبات أن :

$$[(s+N)+(t+N)](r+N) = (s+N)(r+N)+(t+N)(r+N)$$

إذاً $< R/N, +, . >$ حلقة .

تعريف 2.8

لتكن R حلقة وليكن N مثالي في R عندئذ يكون النظام $< R/N, +, . >$ حلقة حيث $R/N = \{r+N / r \in R\}$ و +،. عمليتين ثنائيتين معرفتين على R/N بالشكل $(r+N)+(s+N)=(r+s)+N$ و $(r+N)\,(s+N)=rs+N$ لجميع $r, s \in R$.

هذه الحلقة تسمى حلقة القسمة للحلقة R بالنسبة للمثالي N .

اصطلاح

سوف نرمز عادة للعنصر $x+N$ في R/N بالرمز $\bar{x}$ بهذا يكون N، رمزاً إلى الصفر في R/N ونجد من التعريف أنه لأي $\bar{x}, \bar{y} \in R/N$ ، $\bar{x}+\bar{y}=\overline{x+y}$ ، و $\bar{x}\bar{y}=\overline{xy}$.

مثال 1

لتكن $N=\{6n / n \in Z\}$ فإن N هو مثالي في Z عناصر Z/N هي المجموعات المشاركة $N, 1+N, 2+N, 3+N, 4+N, 5+N$ وبناءاً على الاصطلاح فإننا نرمز للعناصر هذه بالرموز $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}$ على الترتيب فيكون $< Z/N, +, . >$ حلقة علماً بأن كلاً من الجمع والضرب هما معيار 6 انظر الجدولين الآتيين :

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$
	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

تعريف 3.8 (المثالي الأولي)

لتكن R حلقة إبدالية ، المثالي P للحلقة R يسمى مثالياً أولياً إذا كان $\forall \quad a, b \in R, ab \in P \Rightarrow a \in P \text{ or } b \in P$.

مثال 2

في الساحة التامة D, (0) هو مثالي أولي لأن لكل $a,b \in D$ فإن $b=0$ أو $ab \in (0) \Rightarrow ab = 0 \Rightarrow a = 0 \text{ or } b = 0$ لأن D ساحة تامة .

مثال 3

في Z المثالي $(3)=\{3n \mid n \in Z\}$ هو مثالي أولي لأن

$$ab \in (3) \Rightarrow 3 \mid ab \Rightarrow 3 \mid a \text{ or } 3 \mid b$$

$$\Rightarrow a \in (3) \quad \text{أو} \quad b \in (3)$$

في الحقيقة فإن كل مثالي $(P)=\{pn / n \in Z\}$ حيث p عدد أولي هو مثالي أولي في Z .

نظرية 4.8

المثالي P في الحلقة الإبدالية R هو مثالي أولي إذا وفقط إذا كان R/P ساحة تامة.

البرهان

لتكن R/P ساحة تامة فيكون لأي $a,b\in R$

$ab\in p \Rightarrow \overline{ab}=\overline{0} \Rightarrow \overline{a}\overline{b}=\overline{0}$

حيث أن $\overline{a}=a+p$ (لأن R/P ساحة تامة) $\overline{b}=\overline{0}$ أو $\overline{a}=\overline{0} \Rightarrow$

$b\in p$ أو $\Rightarrow a\in p$ إذاً p هي مثالي أولي ، وبالمقابل ليكن P مثالياً أولياً فيكون :

$\overline{a}\overline{b}=\overline{0}\Rightarrow\overline{ab}=\overline{0}\Rightarrow ab\in P$

$b\in P$ أو $\Rightarrow a\in P$

$\overline{b}=\overline{0}$ أو $\Rightarrow\overline{a}=\overline{0}$

وأيضاً R/P إبدالية لأن R إبدالية .

نستنتج أن R/P حلقة إبدالية لا تحوي قواسم فعلية للصفر إذاً R/P هي ساحة تامة .

تعريف 5.8 (المثالي الأعظمي)

المثالي M في الحلقة R يسمى مثالياً أعظمي في الحلقة R إذا كان :

i. $M\neq R$

ii. لا يوجد مثالي J في R بحيث يكون $M\subset J\subset R$ من (ii) إذا كان $M(\neq R)$ مثالي أعظمي فإنه لكل مثالي J في R يكون $M\subseteq J\subseteq R$ محقق فقط عندما $J=M$ أو $J=R$.

مثال 4

في حلقة قاسمية D ,(0) هو مثالي أعظمي وإذا كان $D\neq(0)$ فإن $1\in D$ و $1\neq 0$.

لتكن J أي مثالي غير صفري في D فإنه يوجد $n(\neq 0)$ في J . ولكن D حلقة قاسمية إذاً $x^{-1}\in D$ يعطي أن $1=xx^{-1}\in J$ ونستنتج أن $J=D$ إذاً (0) هو مثالي أعظمي .

مثال 5

في الحلقة E حلقة الأعداد الصحيحة الزوجية المثالي (4) هو مثالي أعظمي وحيث أن $2\notin(4)$ فإن $E\neq(4)$ وإذا كان J مثالي في E بحيث كان $(4)\subset J$ فإنه يوجد عنصر $x\in J$ بحيث أن $x\notin(4)$ بمعنى أن x عدد صحيح زوجي لا يقبل القسمة على 4 نستنتج أن $x=4n+2$ لعدد صحيح n .

الآن $2=x-4n\in J$ لأن $4n\in(4)\subset J$ و $x\in J$ إذاً كل مضاعف صحيح زوجي للعدد 2 هو في المثالي J إذاً $E=J$ وهذا برهان المطلوب .

نظرية 6.8

المثالي M في الحلقة الإبدالية R بمحايد هو مثالي أعظمي إذا وفقط إذا R/M حقل .

البرهان

لتكن M مثالياً أعظمي في R لأن R إبدالية فإن R/M إبدالية وأيضاً 1 هو محايد R نستنتج أن 1 هو محايد $M\neq R.R/M$ لذا $I\neq\bar{0}$ ولكي نبين أن R/M هو حقل يكفي أن نثبت أن كل عنصر غير صفري في R/M هو وحدة أي له معكوس ضربي ، ليكن $\bar{x}(\neq\bar{0})\in R/M$ فيكون $x\notin M$.

اعتبر أن $xR=\{xr/r\in R\}$ ، أن xR مثالي في R وكذلك $x=x1\in R$ هذا يؤدي إلى أنه يوجد $r\in R,m\in M$ بحيث أن $1=m+xr$ هذا بدوره يؤدي إلى أن :

$$1+M=xr+M\Rightarrow\bar{1}=\overline{xr}=\bar{x}\bar{r}$$

لذلك فإن $\bar{x}$ هو وحده ويكون R/M حقلاً بالاتجاه الآخر لأن محايد الحقل يختلف عن الصفر $\bar{1}\neq\bar{0}$ أي أن $1\notin M$ إذاً $M\neq R$ ليكن I هو أي مثالي في R بحيث أن $M\subset I$. نختار $a\in I$ بحيث $a\notin M$ فيكون $\bar{a}\neq\bar{0}$ إذاً $\bar{a}$ له معكوس ضربي في R/M وبناء عليه فإنه يوجد $\bar{b}\in\bar{R}=R/M$ بحيث أن $\overline{ab}=\bar{1}$ هذا يعطي $1-ab\in M$ إذاً $1-ab\in I$ لأن $M\subset I$ هذا يؤدي إلى أن $1=(1-ab)+ab\in I$ لأن $ab\in I$ (مثالي و $a\in I$) إذاً $I=R$.

ملاحظة

إذا كان M أي مثالي أعظمي في حلقة إبدالية R بمحايد ضربي فإن R/M حقل (نظرية 6.8) وأيضاً نعلم أن أي مثالي أعظمي في حلقة إبدالية بمحايد يكون مثالياً أولياً على أية حال فإن عكس العبارة ليس صحيحاً .

مثال 6

اعتبر المثالي (0) في Z لأن Z ساحة تامة فإن (0) مثالياً أولياً في Z ولكن (0) ليس مثالياً أعمياً في Z لأن $Z\subset(2)\subset(0)$.

مثال 7

المثالي (4) في E حلقة الأعداد الزوجية الصحيحة هو مثالي أعظمي (انظر مثال 5) ولكنه ليس أولياً لأن $2.2\in(4)$ ولكن $2\notin(4)$. إذاً في الحلقة الإبدالية بدون محايد المثالي الأعظمي ليس بالضرورة أولياً .

تمارين محلولة

تمرين 1

لتكن R حلقة كل الدوال المتصلة ذات القيم الحقيقية على الفترة المغلقة $[0,1]$ ولتكن $M=\left\{f\in R/f\left(\frac{1}{3}\right)=0\right\}$ بين أن M هو مثالي أعظمي في R .

الحل

الدالة $W:[0,1]\Rightarrow IR$ المعرفة بالشكل $W(x)=0$ لكل $x\in R$ تنتمي إلى M إذاً M مجموعة غير خالية .

خذ $f,g\in M$ فيكون $(f-g)\left(\frac{1}{3}\right)=f\left(\frac{1}{3}\right)-g\left(\frac{1}{3}\right)=0\Rightarrow f-g\in M$

وأيضاً لتكن $h\in R,f\in M$ فإن $hf\left(\frac{1}{3}\right)=h\left(\frac{1}{3}\right)f\left(\frac{1}{3}\right)=h\left(\frac{1}{3}\right).0=0\Rightarrow hf\in M$

بما أن R إبدالية فإن $hf=fh\in M$ إذاً M هو مثالي في R ومن الواضح أن $M\neq R$ لأن $\theta\in R$ المعرفة بالشكل $\theta(x)=1$ لا تنتمي إلى M .

ليكن N مثالياً في R بحيث أن $M\subset N$ فإنه يوجد $\lambda\notin M,\lambda\in N$ هذا يعني أن $\lambda\left(\frac{1}{3}\right)\neq 0$ اجعل $\lambda\left(\frac{1}{3}\right)=C$ حيث $C\neq 0$.

اعتبر $\mu\in R$ معطى بالشكل $\mu=\lambda-\beta$ حيث $\beta(x)=C$ لكل $x\in[0,1]$ فيكون :

$$\mu\left(\frac{1}{3}\right)=\lambda\left(\frac{1}{3}\right)-\beta\left(\frac{1}{3}\right)=c-c=0\Rightarrow\mu\in M\Rightarrow\mu\in N$$

إذاً $\beta=\lambda-\mu\in N$. عرف $\gamma\in R$ بالشكل $\gamma(x)=\frac{1}{2}$ لكل $x\in[0,1]$ فيكون

$\forall x\in[0,1]$ $\quad \gamma\beta(x)=\gamma(x)\beta(x)=1=\theta(x)\Rightarrow\gamma\beta=\theta\in N$

لكن θ هو المحايد في R إذاً $N=R$ وبناء عليه فإن M مثالي أعظمي في R .

تمرين 2

لأي مثـاليين B, A في الحلقـة R بحيـث أن $A \subseteq B$ بـرهن إنـه إذا كـان كـلاً مـن A/B , B هـو مثـالي عـديم القـوة (متلاشـيان) يتطلـب أن يكـون A مثاليـاً عـديم القـوة (متلاشياً) .

الحل

لتكن $\frac{A}{B}, B$ عديمي القوة ، فإن (B) $\left(\frac{A}{B}\right)^n = (B), B^m = (0)$ لبعض الأعداد الصحيحة $0 < n, m$.

$$\left(\frac{A}{B}\right)^n = (B) \Rightarrow A^n \subseteq B \Rightarrow \left(A^n\right)^m \subseteq B^m \Rightarrow A^{mn} = (0)$$

إذن A مثالي عديم القوة .

الآن افرض $\frac{A}{B}, B$ متلاشيان وليكن $a \in B$ فيكون $a + B \in \frac{A}{B}$ لأن $\frac{A}{B}$ متلاشي فإنه يوجد عدد صحيح $n > 0$ بحيث يكون $(a+B)^n = B$ يؤدي إلى أن $a^n \in B$.

ومـرة أخـرى لأن B متلاشـي فإنـه يوجـد عـدد صـحيح $m > 0$ بحيـث أن $\left(a^n\right)^m = 0 \Rightarrow a^{mn} = 0$ هذا يبين أن a عنصر عديم القوة إذاً A هو مثالي متلاشي في R .

مسائل

1. R حلقة منتهية إبدالية غير صفرية ، بين أن كل مثالي أولي للحلقة R هي مثالي أعظمي .
2. أعط مثال لحلقة بدون محايد ولا تحوي مثالياً أعظمياً وفيها الضرب غير تافه (نقصد بالضرب التافه أن $\forall x, y \in R \quad xy = 0$.

إرشاد

خذ $R = \{(a,b) | a,b \in Q\}$ عرف $(a,b)+(c,d)=(a+c,b+d)$ و $(a,b).(c,d)=(0,ac)$ استخدم الحقيقة أن $<Q,+>$ لا تحوي زمرة جزئية أعظمية .

3. برهن أنه في Z المثالي (n) هو مثالي أعظمي إذا وفقط إذا كان n عدداً أولياً حيث $(n)=\{nx | x \in Z\}$.
4. برهن أن المثالي I في الحلقة R مثالي أعظمي إذا وفقط إذا كان

i. $I \neq R$.

ii. لكل $a \in R$ حيث $a \notin I$ يكون لدينا $I + <a> = R$.

5. تعريف المثالي M في الحلقة R تسمى مثالي أصغري في R إذا كان :

i. $M \neq \{0\}$

ii. لكل $<c> = I, c \neq 0 \in I$.

6. لتكن R حلقة كل الدوال الحقيقية المتصلة على الفترة المغلقة $[0,1]$ إذا كان M مثالياً أعظمياً في R فأثبت أنه يوجد عدد حقيقي $0 \leq \delta \leq 1, \delta$ بحيث أن $M = \{f \in R | f,(\delta) = 0\}$

إرشاد

استخدم نظرية هاين بوريل .

7. أعط مثالاً لحلقة غير إبدالية R ومثالياً I في R بحيث يكون :

i. $\frac{R}{I}$ حلقة قاسمية .

ii. $\frac{R}{I}$ حقل .

[إرشاد $R=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,b\in Q\right\}$ ، خذ $I=\left\{\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \middle| x\in Q\right\}$ **]** .

8. لتكن R حلقة ، إذا وجد عدد صحيح موجب n بحيث كان $na=0$ لأي $a\in R$ فإن أصغر عدد صحيح موجب يحمل هذه الخاصية يسمى مميز الحلقة R وإذا لم يوجد هذا العدد الصحيح الموجب أي أن $\forall a\in R \quad na=0$ يؤدي إلى أن $n = 0$ و R تسمى حلقة بمميز صفر .

اصطلاح

$Char\, R$ يعني مميز الحلقة R برهن أنه إذا كان n عدداً صحيحاً موجباً فإن :

a. المجموعتان $J_n = \{a \in R \mid na = 0\}, I_n = \{na \mid a \in R\}$ كلتاهما مثاليات في R .

b. $Char\left(R/I_n\right)$ تقسم n .

c. إذا كان $Char\, R\neq 0$ فإن $Char\, R$ تقسم $n\, Char\left(R/J_n\right)$.

2. الهومومورفزمات

تعريف 7.8

الراسم f من الحلقة R إلى الحلقة R' تسمى هومورفيزم حلقة أو اختصاراً هومومورفيزم إذا تحققت الخصائص الآتية لأي $a,b \in R$.

i. $f(a+b)=f(a)+f(b)$

ii. $f(a.b)=f(a)-f(b)$

ملاحظة

من الواضح أن (i) يبين أن هومومورفيزم الحلقة هو هومورفيزم كل زمرة بالنسبة إلى زمرة الجمع $<R,+>$ كما أنه يحافظ على الضرب .

الهومومورفيزم

$f:R \rightarrow R'$ يسمى إبيمورفيزم إذا كان f فوقياً ويسمى مونومورفيزم إذا كان أحادياً ويسمى أيزموموفيزم إذا كان كلاهما معاً .

والهومومورفيزم f من الحلقة وإليها يسمى إندومورفيزم ، فإذا كان f إيزمورفيزم من الحلقة وإليها سمي أوتومورفيزم .

مثال 8

لتكن S حلقة جزئية من R عرف $f:S \rightarrow R$ بحيث $f(x)=X, \forall x \in S$ فإنه من الواضح لأي $x,y \in S$ $\quad f(x+y)=x+y=f(x)+f(y)$

و $f(xy)=xy=f(x)f(y)$ إذا f هو هومومورفيزم حلقة من S إلى R (يسمى راسم الاحتواء) .

مثال 9

ليكن A مثالياً في R عرف $f:R\to R/A$ بالشكل $f(r)=r+A,\forall r\in R$ فإن f هي هومومورفيزم لأن $f(r+s)=(r+s)+A=(r+A)+(s+A)=f(r)+f(s)$

وأيضاً $f(rs)=rs+A=(r+A).(s+A)=f(r).f(s)$ وأيضاً f فوقي إذاً f هو إيبيمورفيزم وهو ليس أحادي إذا كان $A\neq(0)$ ولرؤية هذا خذ $a(\neq 0)$ في A فإن $f(0)=0+A=A$ و $f(a)=a+A=A$ إذاً $f(0)=f(a)$ ولكن $a\neq 0$ هذا يثبت أن f ليس أحادياً ، هذا الراسم الهومومورفيزم الطبيعي .

مثال 10

لتكن $R_1=\left\{\begin{pmatrix}a&0\\0&0\end{pmatrix}\middle| a\in R\right\}$ حيث R هي حلقة . عرف $f:R_1\to R$ بالشكل :

$$f\begin{pmatrix}a&0\\0&0\end{pmatrix}=a\,,\forall\begin{pmatrix}a&0\\0&0\end{pmatrix}\in R_1$$

فإن f إيزومورفيزم وهذا يمكن التحقق منه كالآتي :

$$f\left[\begin{pmatrix}a&0\\0&0\end{pmatrix}+\begin{pmatrix}b&0\\0&0\end{pmatrix}\right]=f\begin{pmatrix}a+b&0\\0&0\end{pmatrix}=a+b=f\begin{pmatrix}a&0\\0&0\end{pmatrix}+f\begin{pmatrix}b&0\\0&0\end{pmatrix}$$

وأيضاً

$$f\left[\begin{pmatrix}a&0\\0&0\end{pmatrix}.\begin{pmatrix}b&0\\0&0\end{pmatrix}\right]=f\begin{pmatrix}ab&0\\0&0\end{pmatrix}=ab=f\begin{pmatrix}a&0\\0&0\end{pmatrix}.f\begin{pmatrix}b&0\\0&0\end{pmatrix}$$

مرة أخرى

$$f\begin{pmatrix}a&0\\0&0\end{pmatrix}=f\begin{pmatrix}b&0\\0&0\end{pmatrix}\Rightarrow a=b\Rightarrow\begin{pmatrix}a&0\\0&0\end{pmatrix}=\begin{pmatrix}b&0\\0&0\end{pmatrix}$$

إذاً f أحادي .

أخيراً من الواضح أن f فوقي ومن ثم فهو إيزومورفيزم .

مثال 11

إذا كان $M=\{a+b\sqrt{2}\,|\,a,b\in Z\}$ فإن M حلقة تحت عمليتي الجمع والضرب الاعتياديتين للأعداد الحقيقية .

عـــرف $f: M \to M$ بحيـــث $f\left(a+b\sqrt{2}\right)=a-b\sqrt{2}$ لأي $a+b\sqrt{2}$ في M ، f هـــو أومومورفيزم (تحقق من ذلك) .

الآن سوف نتفحص بعض النظريات على هومورفيزم بحلقات والتي تشابه إلى حد كبير النظريات التي برهنت حول هومومورفيزم الزمر ، ورغم أن برهان هذه النظريات ضروري بقدر أهميتها في الزمر فإننا مع ذلك نطمئن إلى الحاجة إليها من ناحية توضيح براهين بعض النتائج .

نظرية 9.8

لتكن $f: R \to R_1$ هومومورفيزم حلقة ، فيكون :

i. $f(0)=0$

ii. $f(-a)=-f(a)$ لكل $a \in R$

البرهان

لأي $x \in R$
$$f(x)=f(x+0)=f(x)+f(0)$$

لأن $f(x) \in R_1$ يكون لدينا أيضاً $f(x)=f(x)+0$ ومن قانون الحذف بالنسبة للجمع يكون لدينا $f(0)=0$.

الآن :

$$a+(-a)=0 \Rightarrow f(a+(-a))=f(0)=0 \Rightarrow f(a)+f(-a)=0 \Rightarrow f(-a)=-f(a)$$

نتيجة 10.8

لأي $f(x-y)=f(x)-f(y), x, y \in R$.

البرهان

$$f(x-y)=f(x+(-y))=f(x)+f(-y)=f(x)+[f(y)]=f(x)-f(y)$$

تعريف 11.8

لـتكن $f:R\to R_1$ هومومورفيزمـاً نعـرف نـواة f بأنهـا المجموعـة $\{r\in R \mid f(r)=0\}$ سوف نرمز لنواة f بالرمز $\ker f$.

نظرية 12.8

نواة هومومورفيزم من الحلقة R إلى الحلقة R_1 هي مثالي في R .

البرهان

لـتكن $f:R\to R_1$ هومومـورفيزم لأن $f(0)=0\in\ker f$ فـإن $\ker f$ مجموعـة غـير خالية

$$x,y\in\ker f\to f(x)=0\,,\,f(y)=0$$

إذاً

$$f(x-y)=f(x)-f(y)=0\Rightarrow x-y\in\ker f$$

كما أن

$$r\in R\,,x\in\ker f\Rightarrow f(xr)=f(x).f(r)=0$$

لأن $f(x)=0$ وبـنفس الطريقـة $f(rx)=0$ يـؤدي إلى أن $xr\in\ker f$ وكـذلك $rx\in\ker f$ وعلى ذلك فإن $\ker f$ مثالي في R .

نظرية 13.8

لتكن $f:R\to R_1$ هومومورفيزم ولتكن A مثالي في R فإن $f(A)$ يكون مثالي في $f(R)$.

البرهان

لاحظ أن

$$f(A)=\{x\in R \mid \exists a\in A, x=f(a)\}$$

من الواضح $0\in f(A)$ لأن $0=f(0)$ إذاً $f(A)$ مجموعة غير خالية .

لتكن $x,y\in f(A)$ فإن $y=f(b),x=f(a)$ لبعض عناصر b,a في A إذاً :

$$x-y=f(a)-f(b)=f(a-b)\Rightarrow x-y\in f(A)$$

لأن $a-b \in A$.

إذا كان $r_1 \in f(A)$ فإنه يوجد $r \in R$ بحيث أن $r_1 = f(r)$ إذاً :

$$r_1 x = f(r) f(a) = f(ra)$$

$$\Rightarrow \qquad r_1 x \in f(A) \qquad\qquad (\text{لأن } ra \in A)$$

وبنفس الطريقة $xr_1 \in f(A)$ إذاً $f(A)$ مثالي في $f(R)$.

نظرية 14.8 (النظرية الأساسية للهومومورفيزم)

لأي مثالي A في الحلقة R ، R/A صورة هومورفيزم للحلقة R وبالعكس إذا كان f هو هومومورفيزم فوقي في الحلقة R على R_1 فإن R_1 أيزومورفي إلى حلقة قسمة للحلقة R ، في الحقيقة $R_1 \cong R/\ker f$.

البرهان

لأن الهومورفيزم الطبيعي $f : R \to R/A$ المعطى بالشكل $\forall x \in R \quad f(x) = x + A$ هو راسم فوقي ، فإن R/A صورة هومومورفية للحلقة R وبالعكس ، ليكن f هومومورفيزم من R فوقياً على الحلقة R نفرض أن $A = \ker f$ عندئذ يكون A مثالياً في R .

عرف $\bar{f} : R/A \to R_1$ بالشكل $\bar{f}(\bar{r}) = f(r)$ لكل $\bar{r} = r + A \in R/A$.

الآن لأي $\bar{r}, \bar{s} \in R/A$ يكون لدينا $\bar{r} = \bar{s} \Leftrightarrow r - s \in A = \ker f \Leftrightarrow f(r-s) = 0$

$$\Leftrightarrow \qquad f(r) = f(s) \Leftrightarrow \bar{f}(r) = \bar{f}(\bar{s})$$

ويبين أيضاً أن f أحادي .

هذا يبين أن f معرف تعريفاً جيداً ، كذلك :

$$\bar{f}(\bar{r} + \bar{s}) = \bar{f}(\overline{r+s}) = f(r+s) = f(r) + f(s) = \bar{f}(\bar{r}) + \bar{f}(\bar{s})$$

وأيضاً $\bar{f}(\bar{r}\bar{s}) = \bar{f}(\overline{rs}) = f(rs) = f(r).f(s) = \bar{f}(\bar{r}).\bar{f}(\bar{s})$

هـذا يعطـي أن $\overline{f}$ مونومـورفيزم ، وختامـاً لأن $\overline{f}(\overline{R})=f(R)=R_1$ نحصـل علـى أن $\overline{f}$ فـوقي أيضاً ، إذاً $\overline{f}:R/A\to R_1$ هو أيزومورفيزم وأن $R/A\cong R_1$ أي أن $R_1\cong R/A$.

نظرية 15.8

لـيكن N مثاليـاً في R فإنـه يوجـد تقـابلاً أحـادي بـين مثاليـات R المحتويـة N والمثاليات في R/N .

البرهان

ليكن f هو الهومومورفيزم الطبيعي من R إلى R/N وليكن A مثالي في R يحوي N فإن :

$$f(A)=\{f(a)|\,a\in A\}=\{a+N|\,a\in A\}=A/N$$

هـو مثـالي في R/N (نظرية 13.8) اعتـبر أي مثـاليين B,A في R يحـويان N بحيـث يكـون $f(A)=f(B)$ أي أن $A/N=B/N$ فسـوف يكـون لأي $a\in A$ يوجـد $b\in B$ بحيـث أن $a+N=b+N$ هذا يؤدي $a-b\in N\subseteq B\Rightarrow a=(a-b)+b\in B$

تبعاً لذلك يكون $A\subseteq B$ وبنفس الطريقة يمكن أن نبين أن $B\subseteq A$ فنحصل على $A=B$ أي أن الراسم $A\to f(A)$ من F مجموعة كل المثاليات في R المحتوية على N إلى المجموعة $\overline{F}$ مجموعة كل المثاليات في R/N أحادي .

ولبيـان أنـه فـوقي لـه نظهـر أن أي مثـالي في R/N هـو مـن الشـكل $f(A)$ لمثـالي $A\in F$ ، ليكن X هو أي مثالي في R/N عرف $A=\{x\in R|\,f(x)\in X\}$ حيث أنه لأي $n\in N$ فإن $f(n)=\overline{0}\in X$ فإننا نحصل على $n\in A$ أي أن $N\subseteq A$ واضح أن أي عنصر في X هو من الشـكل $f(a)$ وحيـث $a\in A$ فـإذا بيّنّـا أن A هـو مثـالي في R فسـوف نحصـل علـى $X=f(A)$ مـع $A\in F$ وهـذا يعطـي أن $A\Leftrightarrow f(A)$ هـو تقابـل أحـادي بـين $\overline{F},F$ لـيكن $r\in R,a,b\in A$ فيكون $f(a),f(b)\in X$ $f(r)\in R/N,$ ومن ثم :

$$f(a-b)=f(a)-f(b)\in X\,,\, f(ar)=f(a)f(r)\in X$$

و $f(ra)=f(r)f(a)\in X$ لأن X مثالي في R/N فينتج من ذلك أن :

$$a-b\in A, ar\in A, ra\in A$$

و A مثالي في R لذلك يكون $A\in F$ وهذا يبرهن النظرية .

النظرية التالية هي تعميم ظاهري للنظرية السابقة والبرهان يسير بالضبط على نفس الخطوط فقط علينا استبدال g بـ f وأخذ $N=\ker g$.

نظرية 16.8

إذا كانت g هومومورفيزم من حلقة R إلى حلقة R_1 فإنه يوجد تقابل أحادي بين عائلة المثاليات في R المحتوية على $\ker g$ وعائلة كل المثاليات في R_1 معطى بالشكل $A\Leftrightarrow g(A)$.

نظرية 17.8 (نظرية الإيزومورفيزم الثانية)

إذا كان $B\subseteq A$ مثاليان في حلقة R فإن $R/A\cong(R/B)/(A/B)$.

البرهان

عرف الراسم $f:R/B\to R/A$ بالعبارة $f(r+B)=r+A,\forall r\in R$ بذلك يكون f معرفاً تعريفاً جيداً لأن $r+B=s+B\Rightarrow r-s\in B\subseteq A\Rightarrow r+A=s+A$

ونترك للقراء بيان أن f هو أبيمورفيزم بنواة هي A/B .

نظرية 18.8 (نظرية الإيزمورفيزم الثالثة)

إذا كان B,A مثاليان في الحلقة R فإن $\frac{A+B}{A}\cong\frac{B}{A\cap B}$.

الرهان

عرف $P:B\to\frac{A+B}{A}$ بالشكل $f(b)=\bar{b}$ لكل $b\in B$.

افرض أن $b_1, b_2 \in B$ فيكون :

i. $f(b_1+b_2)=\overline{b_1+b_2}=\overline{b_1}+\overline{b_2}=f(b_1)+f(b_2)$

ii. $f(b_1 b_2)=\overline{b_1 b_2}=\overline{b_1}\,\overline{b_2}=f(b_1).f(b_2)$

إذاً f هو هومومورفيزم .

الآن $\bar{x} \in \frac{A+B}{A}$ يؤدي إلى أن $x=a+b$ لبعض العناصر $a \in A, b \in B$ إذاً :

$\bar{x}=a+b+A=b+a+A=b+A$

لأن $a \in A$ أي أن $\bar{x}=\bar{b}=f(b)$ أي أن f فوقي .

ختاماً $\ker f = A \cap B$ لأن :

$b \in \ker f \Leftrightarrow \bar{b}=\bar{0} \Leftrightarrow b \in A \Leftrightarrow b \in A \cap B \qquad$ (لأن $b \in A$)

من نظرية الهومومورفيزم الأساسية نجد $\frac{B}{A \cap B} \cong \frac{A+B}{A}$ أي أن $\frac{A+B}{A} \cong \frac{B}{A \cap B}$.

مسائل

1. لتكن R حلقة إبدالية فيها $PX=0$ لكل $x\in R$ و P عدد أولي ، عرف $f:R\to R$ بالصورة $f(x)=x^P$ بين أن f هومومورفزم .
2. إذا كان f هومومورفيزم من الحلقة R على الحلقة R' مع $\ker f=N$ برهن كلاً من النتائج الآتية :

i. إذا كان A مثالي يميني أو يساري في R فإن $f(A)$ هو مثالي يميني (يساري) في R' .

ii. إذا كان B مثالي يميني (يساري) في R' فإن $\bar{f}^1(B)=\{r\in R|\ f(r)\in B\}$ هو مثالي يميني (يساري) في R يحوي N .

iii. إذا كان B, A مثاليان في R بحيث كان $N\subseteq B, N\subseteq A$ فإن $A\subset B$ إذا وفقط إذا $f(A)\subset f(B)$.

3. إذا كان f هومومورفيزم من حلقة R إلى حلقة S و g هومومورفيزم من S إلى حلقة T بين أن gf هو هومومورفيزم من R إلى T .
4. أكمل برهان نظرية 17.8 .
5. لتكن B, A حلقتان جزئيتان من الحلقة R بحيث أن لكل $b\in B, a\in A$ كان ba, ab ينتميان إلى A برهن ما يلي :

i. $A+B$ حلقة جزئية في R .

ii. $A\cap B, A$ هما مثاليان في $B, A+B$ على الترتيب .

iii. $\frac{A+B}{A}\cong\frac{B}{A\cap B}$.

كيف تكون هذه النتيجة تعميماً لنظرية الهومومورفيزم الثانية ؟

أعط مثالاً تبين فيه أن مجموع حلقتين جزئيتين يمكن ألا يكون حلقة جزئية .

إرشاد

خذ $S=\left\{\begin{pmatrix}0 & a\\ 0 & 0\end{pmatrix} \mid a\in Z\right\}, T=\left\{\begin{pmatrix}0 & 0\\ b & 0\end{pmatrix} \mid b\in Z\right\}$ فإن T,S حلقتان جزئيتان من Z حلقة كل المصفوفات من السعة 2×2 على Z ولكن $S+T$ ليس حلقة جزئية على Z_2 .

6. الهومومورفيزم f من الحلقة R إلى حلقة S يقال له هومومورفيزم صفري إذا كان $f(R)=0$ أثبت أن هومومورفيزم من حقل إلى أي حلقة إما أن يكون مونومورفيزم أو هومومورفيزم صفري .
7. إذا كان $f:R\to R_1$ هو هومومورفيزم فوقي و R حلقة ذات محايد يساوي 1 فأثبت أن $f(1)$ هو محايد الحلقة $f(R)$.
8. افرض أن $f:R\to S$ هو إيبيمورفيزم فإذا كان B,A مثاليان في R و V,U مثاليان في S فأثبت أن :

i. $f(A+B)=f(A)+f(B)$
ii. $f(AB)=f(A)f(B)$
iii. $f^{-1}(U+V)=f^{-1}(U)f^{-1}(V)$
iv. $f^{-1}(UV)\supseteq f^{-1}(U)f^{-1}(V)$

أعط مثالاً تبين فيه أنه بوجه عام يكون $P^{-1}(UV)\neq f^{-1}(U)f^{-1}(V)$.

إرشاد

لتكن R زمرة جمع إبدالية بها أكثر من عنصر ، عرف $xy=0,\forall x,y\in R$ فتكون R حلقة ، خذ $S=\{0\}$ وعرف $f:R\to S$ بالشكل $f(x)=0,\forall x\in R$ خذ $U=V=\{0\}$ فيكون $UV=\{0\}, f^{-1}(UV)=R$ بينما $f^{-1}(U)f^{-1}(V)=RR=\{0\}$.

9. بين أن $f: C \to R_2$ معطاة بالشكل $f\ (a + b_i) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ هي هومومورفيزم حيث أن R_2 هي حلقة كل المصفوفات من السعة 2×2 على R .

10. لتكن $(P) = \{Pn \mid n \in Z, P \neq 0\}$ بين أن $Z/(P)$ حقل إذا وفقط إذا كان P هو عدد أولي .

إرشاد

أي ساحة تامة غير صفرية ومنتهية هي حقل .

11. (فيرمات) ليكن P عدداً أولياً ، برهن أنه لكل $a \in Z$ غير قابل للقسمة على P يكون $a^{P-1} = 1 (\operatorname{mod} P)$.

إرشاد

$Z/(P)$ هو حقل ومن ثم فإن $\bar{a} \neq \bar{0}$ والعناصر غير الصفرية في الحقل تشكل زمرة تحت عملية الضرب .

12. إذا كان P عدداً أولياً فردياً فبين أنه في $Z/(P)$ يوجد بالضبط عنصران $\bar{x}$ بحيث أن $\bar{x}^2 = \bar{1}$ من هذا نستنتج نظرية ويلسون القائلة (إذا كان P عدداً أولياً فإن $(P-1)! \equiv -1 (\operatorname{mod} P)$.

13. A مثالي في حلقة إبدالية R ، لتكن $\sqrt{A}$ معرفة كما في الفصل السابع البند 4 مسألة 6 بين أن $R/\sqrt{A}$ ليس فيها عناصر غير صفرية عديمة القوة .

14. في حلقة R عرف S بأنها مجموعة $\{ab - ba \mid a, b \in R\}$ بين أنه لأي مثالي A في R فإن حلقة R/A تكون إبدالية إذا وفقط إذا $S \subseteq A$.

15. المثالي Q في الحلقة R الإبدالية يسمى مثالي ابتدائي إذا كان :

i. $Q \neq R$.

ii. لكل $ab \in Q, a, b \in R$ وأن $a \notin Q$ يستدعى أن $b^n \in Q$ لبعض الأعداد الصحيحة الموجبة n ، بين أن Q مثالي ابتدائي في R إذا وفقد إذا كل قاسم صفري في R/Q عديم القوة .

16. المثالي A في الحلقة الإبدالية R يسمى مثالياً شبه أولي إذا كان $\forall a \in R, a^2 \in A \Rightarrow a \in A$ بين أن A هو مثالي شبه أولي في R إذا وفقط إذا R/A ليس بها عناصر غير صفرية عديمة القوة .

17. إذا كانت I مثالياً في R برهن أن حلقة المصفوفة $(R/I)_n$ أيزومورفية مع R_n/I_n .

إرشاد

عرف $f : R_n \to (R/I)_n$ بالشكل $f(a_{ij}) = (a_{ij} + I) \forall a_{ij} \in R_n$.

3- حقل القواسم ونظرية الغمر

بعض أنواع الحلقات تكون أسهل دراسة وابنيتها تكون معرفة من أنواع أخر ، فإذا استطاع أحد غمر حلقة ما R في حلقة أخرى S بحيث يكون بناء الأخيرة معروف أكثر من الأولى فإنه باستخدام خواص S نستطيع أن نقول الكثير حول خصائص R ، وقد استخدمنا الغمر لحلقة ما في أخرى استخداماً بالغ الجمال في تطوير نظرية الحلقة .

هناك العديد من طرق غمر حلقة في أخرى ، وهنا في هذا البند سنحصر أنفسنا على ثلاثة طرق فقط :

I. غمر حلقة في حلقة بمحايد .

II. غمر ساحة في حقل .

III. غمر حلقة في حلقة الأندومورفيزم لزمرة إبدالية .

I. غمر حلقة في حلقة بمحايد

لتكن R حلقة اعتبر $R\times Z=\{(r,n)|\, r\in R, n\in Z\}$ ، $R\times Z$ يمكن جعلها حلقة معرفين عليها عملية جمع وضرب كالآتي :

لكل $(r,n),(s,m)\in RxZ$

$$(r,n)+(s,m)=(r+s,n+m)$$
$$(r,n)(s,m)=(rs+ns+mr,nm)$$

يمكننا التأكد من أن $R\times Z$ هي حلقة بمحايد يساوي $(0,1)$.

نظرية 19.8

أي حلقة يمكن غمرها في حلقة بمحايد .

البرهان

لتكن R حلقة فمن الملاحظ سابقاً أن يكون :

$$R_1 = R \times Z = \{(r,n) \mid r \in R, n \in Z\}$$

هي حلقة . نعرف $f : R \to R_1$ بالشكل $\forall r \in R \quad f(r) = (r,0)$.

واضح أن f هو هومومورفيزم كما أن f أحادي لأن :

$$f(r) = f(s) \Rightarrow (r,0) = (s,0) \Rightarrow r = s$$

إذاً $R \cong f(R) \subseteq R_1$ وعلى ذلك فإن R قابل للغمر في R_1 والتي لها محايد يساوي $(0,1)$.

ملاحظة

الغمر الذي نوقش في النظرية السابقة جميل جداً إذ ينطوي على أن $f(R)$ مثالياً في R_1 .

للتأكد من هذا لاحظ أنه لأي $(s,n) \in R_1, (r,0) \in f(R)$ فإن :

$$(r,0)(s,n) = (rs + 0s + nr, on) = (sr + nr, 0) \in f(R)$$

وكذلك $(s,n)(r,o) = (sr + nr, 0) \in f(R)$ وهكذا فإن R بتشخيص r مع $(r,0)$ تصبح مثالياً في R_1 .

II. غمر ساحة في حقل

كل حلقة جزئية من حقل هي ساحة تامة ، ومن الطبيعي أن يسأل أحد إذا أعطينا ساحة تامة فهل يمكننا إيجاد حقل يحوي هذه الساحة التامة كحلقة جزئية منه ؟

أو بكلام آخر يمكن غمر ساحة تامة في حقل ؟

والسؤال في غاية الأهمية لمن يبحث عن حل للمعادية الخطية $a \neq 0, ax = b$ في ساحة تامة D من الطبيعي أن الحل إذا كان موجوداً في D فإنه يجب أن يكون وحيداً (لماذا ؟) على أنه من الممكن دائماً ألا يكون هناك في D فمثلاً في $3x = 5, Z$ ليس لها حل في Z ولكن في حقل $ax = b, a \neq 0, F$ دائماً لها حل هو $a^{-1}b$ وعلى ذلك فإذا غمرنا الساحة D في حقل F فإن المعادلة $ax = b, a \neq 0$ بمعاملات من D سيكون لها على الأقل حل في F ، والآن

نسعى لبناء الحقل الذي يغمر ساحة تامة مسترشدين بطريقة بناء الأعداد النسبية من الأعداد الصحيحة .

لتكن D ساحة تامة تحوي على الأقل عنصرين وليكن $D_0 = D - \{0\}$ اعتبر :

$$D \times D_0 = \{(a,b) \mid a,b \in D, b \neq 0\}$$

عرف العلاقة N على $D \times D_0$ كالآتي :

لكل $(a,b),(c,d) \in D \times D_0$ فإن $(a,b),(c,d)$ إذا وفقط إذا $ad = bc$.

قضية 20.8

العلاقة '~' هي علاقة تكافؤ على $D \times D_0$.

البرهان

لتكن $(a,b),(c,d),(e,f) \in D \times D_0$.

i. **الانعكاس** : لأن $ab = ba$ اجعل $c = a, d = b$ في تعريف '~' نرى أن $(a,b) \sim (a,b)$

ii. **التناظر** : $(a,b) \sim (c,d) \Rightarrow ad = bc \Rightarrow cb = da \to (c,d) \sim (a,b)$.

iii. **التعدي** : $(a,b) \sim (c,d), (c,d) \sim (e,f)$

$$\Rightarrow \quad ad = bc, cf = de$$
$$\Rightarrow \quad adf = bcf$$
$$\Rightarrow \quad adf = bde$$
$$\Rightarrow \quad af = be$$ (لأن $cf = de$)

$$\Rightarrow \quad (a,b) \sim (e,f)$$ (لأن $d \neq 0$ وقانون الحذف يتحقق)

إذاً ~ هي علاقة تكافؤ على $D \times D_0$.

ملاحظة

من تعريف علاقة التكافؤ يمكننا أن نرى على الفور أنه لأي أعداد غير صفرية c,b,a في D يكون $(0,a) \sim (0,b), (a,a) \sim (b,b), (ac,bc) \sim (a,b)$

لتكن a/b هو فصل تكافؤ للعنصر (a,b) من خواص فصول التكافؤ يتضح أن $a/b=c/d$ إذا وفقط إذا $ad=bc$.

والآن إذا كان F هو عائلة صفوف التكافؤ a/b في $D\times D_0$ فسوف نبين أنه تحت عمليتي جمع وضرب مناسبتين فإن F يصبح حقل وعلى الفور فإن عمليتي الجمع والضرب للأعداد النسبية تفي بالغرض ، لذا نعرف لكل $a/b, c/d\in F$ أن $a/b+c/d=(ad+bc)|bd$ وأن $(a/b)(c/d)=ac/bd$. لاحظ أن D هي ساحة تامة لذا فإن $b\neq 0, d\neq 0 \Rightarrow bd\neq 0$ وبالتالي $(cd+bc)/bd\in F$ و $ac/bd\in F$ ولكي تكون تعريفاتنا ذات معنى فيجب علينا أن نبين أنها مستقلة عن اختيارنا لما يمثل فصول التكافؤ الداخلة في العمليات أو بعبارة أخرى يجب أن نبين أنه إذا كان $c/d=c'/d', a/b=a'/b'$ فإن $ac/bd=a'c'/b'd', (ad+bc)/bd=(a'd'+b'c')/b'd'$.

قضية 21.8

عمليتي الجمع والضرب في التعريف السابق معرفتان تعريفاً جيداً .

البرهان

ليكن $c/d=c'/d', a/b=a'/b'$ فإن :

$$cd'=c'd\,, ab'=a'b \qquad (1)$$

الآن

$$(1)\Rightarrow ab'dd'=a'bdd'\,, bb'cd'=bb'c'd$$

$$\Rightarrow \quad ab'dd'+bb'cd'=a'bdd'+bb'c'd$$

$$\Rightarrow \quad (ad+bc)b'd'=(a'd'+b'c')bd$$

$$\Rightarrow \frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$$

فإذاً الجمع معرف تعريفاً جيداً . أخيراً

$$(1)\Rightarrow \quad ab'cd'=a'bc'd$$

$$\Rightarrow \quad (ac)(b'd')=(bd)(a'c')$$

$$\Rightarrow \quad \frac{ac}{bd}=\frac{a'c'}{b'd'}$$

أي أن الضرب معرف تعريفاً جيداً أيضاً والقضية محققة .

نظرية 22.8

$<F,+,.>$ هو حقل و D يمكن أن تغمر في F .

البرهان

البرهان من الملاحظة التالية للقضية 20.8 نجد أنه لأي $a\neq 0\in D$ فإن :

$$\frac{0}{a}\neq\frac{a}{a},\frac{0}{a},\frac{a}{a}\in F,$$

لذا فإن F فيه عنصران على الأقل وكما نلاحظ أنه لأي عنصران غير صفريان a,b في D فإن $\frac{0}{a}=\frac{0}{b}$ وأيضاً إذا كان $c\neq 0$ فإن $\frac{ac}{bc}=\frac{a}{b}$.

1. **العملية تنسيقية**

لأي $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in F$

$$\begin{aligned}\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}&=\frac{ad+bc}{bd}+\frac{e}{f}\\&=\frac{(ad+bc)f+(bd)e}{(bd)f}\\&=\frac{a(df)+(cf+de)b}{b(df)}\\&=\frac{a}{b}+\frac{cf+de}{df}\\&=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)\end{aligned}$$

2. **العملية إبدالية**

لأي $\frac{a}{b},\frac{c}{d}\in F$

$$\begin{aligned}\frac{a}{b}+\frac{c}{d}&=\frac{ad+bc}{bd}\\&=\frac{bc+ad}{db}\\&=\frac{c}{d}+\frac{a}{b}\end{aligned}$$

3. وجود عنصر صفري

الآن لأي $U \neq 0$ في D فإن $\frac{0}{u} \in F$ حيث أن $\frac{a}{b}+\frac{0}{u}=\frac{au}{bu}=\frac{a}{b}$.

فإذاً $\frac{0}{u}$ هو العنصر الصفري في F لنرمز له بالرمز 0 .

4. وجود المعكوس الجمعي

لأن

$$\frac{a}{b}+\left(\frac{-a}{b}\right)=\frac{ab-ba}{b^2}=\frac{0}{b^2}$$

و

$$\frac{0}{u}=\frac{0}{b^2}\Rightarrow\frac{a}{b}+\left(\frac{-a}{b}\right)=0$$

إذاً

$$-\left(\frac{a}{b}\right)=\frac{-a}{b}\in F$$

5. التنسيق الضربي

لأي $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in F$

$$\left(\frac{a}{b}.\frac{c}{d}\right)\left(\frac{e}{f}\right)=\left(\frac{ac}{bd}\right)\left(\frac{e}{f}\right)=\frac{(ac)e}{(bd)f}$$
$$=\frac{a(ce)}{b(df)}=\frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right)$$

6. التبديل الضربي

لأي $\frac{a}{b},\frac{c}{d}\in F$

$$\frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}.\frac{a}{b}$$

7. وجود المحايد الضربي

الآن إذا كان $U\neq 0\in D$ فإن $\frac{u}{u}\in F$ بحيث أن $\frac{a}{b}.\frac{u}{u}=\frac{au}{bu}=\frac{a}{b}$.

هذا يعطي أن $\frac{u}{u}$ هو المحايد الضربي والذي سنرمز له بالرمز 1 .

8. وجود معكوس ضربي للعناصر غير الصفرية

الآن

$$\frac{a}{b}\neq 0\Rightarrow a\neq 0, b\neq 0\Rightarrow\frac{b}{a}\in F$$
$$\frac{a}{b}.\frac{b}{a}=\frac{ab}{ab}=\frac{u}{u}=1$$

إذاً $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$.

9. التوزيع

لكل $\frac{a}{b},\frac{c}{d},\frac{e}{f}\in F$

$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\left(\frac{cf+de}{df}\right)=\frac{a(cf+de)}{b(df)}$$

وأيضاً

$$\frac{a}{b}\frac{c}{d}+\frac{a}{b}.\frac{e}{f}=\frac{ac}{bd}+\frac{ae}{bf}=\frac{(ac)bf+(ae)bd}{(bd)(bf)}=\frac{[(ac)f+(ae)d]b}{(bdf)b}$$
$$=\frac{a(cf+de)}{bdf}$$

أي أن الضرب بتوزيع على الجمع وينتج أن $<F,+,.>$ هو حقل .

في النهاية نعرف $f:D\to F$ كالآتي

خذ $a(\neq 0)\in D$ ولكل $x\in D$ ضع $f(x)=\frac{xa}{a}$ ليكن $x,y\in D$ فإن :

$$f(x)=f(y)\Rightarrow\frac{xa}{a}=\frac{ya}{a}$$
$$\Rightarrow\qquad xa^2=ya^2\Rightarrow x=y$$

إذاً f راسم أحادي وأيضاً :

$$f(x+y)=\frac{(x+y)a}{a}=\frac{(x+y)a^2}{a^2}=\frac{xa}{a}+\frac{ya}{a}=f(x)+f(y)$$

كما أن

$$f(xy)=\frac{xya}{a}=\frac{(xa)(ya)}{a^2}=\frac{xa}{a}.\frac{ya}{a}=f(x)f(y)$$

وهذا يبين أن f هي مونومورفزم من D إلى F إذاً D مغمورة في F .

تعريف 23.8

لتكن D ساحة تامة تحوي أكثر من عنصر ، فإن حقل قواسم D هو الثنائي (F,σ) حيث F هو حقل و σ هي مونومورفزم من D إلى F بحيث أن كل عنصر $Z\in F$ يمكن التعبير عنها بالشكل $\sigma(x)/\sigma(y)$ لبعض العناصر $x,y\in D$ حيث $y\neq 0$.

ملاحظة

عندما لا يوجد حقل المونومورفزم σ فإن F وحدها يشار لها بأنها حقل قواسم D

.

والآن لأن $D \cong \sigma(D) \subseteq F$ فسوف نتعود على تشخيص D مع صورتها $\sigma(D)$ ونلاحظ أن D هي نفسها حلقة جزئية من F .

في تلك الحالة فإن كل $a \in D$ يتحدد بصورته $\sigma(a)$ وعندئذ فإن كل عنصر $Z \in F$ سيكون بالصيغة $y \neq 0, xy \in D, x/y$.

نظرية 24.8

إذا كانت D ساحة تامة تضم على الأقل عنصرين ، فإن لها حقل قواسم إذا كان $(F_1 , \sigma_1), (F_2 , \sigma_2)$ حقلين قواسم فإنه يوجد إيزومورفيزم η من F_1 على F_2 بحيث أن $\eta \sigma_1 = \sigma_2$.

البرهان

في النظرية (8-22) أنشأنا الحقل F بحيث كان $f : D \to F$ مع كون $f(x) = xa/a$ لكل عنصر $a, x \in D$ عنصر غير صفري مثبت في D .

وكذلك رأينا أن f كان مونومورفزم ، الآن كل عنصر $Z \in F$ هو على شكل x/y حيث $x, y \in D, y \neq 0$ إذاً $Z = (xa/a)(a/ya) = f(x)/f(y)$ ولذلك (F, f) هو حقل قواسم D ، لتكن $(F_2 , \sigma_2), (f_1 , \sigma_1')$ حقلي قواسم D نعرف $1: F_1 \to F_2$ كما يلي :

خذ $Z \in F_1$ فمن التعريف يكون $\dfrac{\sigma_1(x)}{\sigma_1(y)}$ = لبعض $y \neq 0, x, y \in D$.

بوضع $\dfrac{\sigma_2(x)}{\sigma_2(y)}$ = $\eta(Z)$ فإن η تكون معرفة تعريفاً جيداً لأنه إذا كان :

$$Z = \frac{\sigma_1(x)}{\sigma_1(y)} = \frac{\sigma_1(u)}{\sigma_1(v)}$$

لبعض قيم $y \neq 0, v \neq 0, x, y, u, v \in D$ (σ_1 لأن أحادية) $\sigma_1(xv) = \sigma_1(uy) \Rightarrow xv = uy$

$\Rightarrow \quad \sigma_2(xv) = \sigma_2(uy) \Rightarrow \sigma_2(x, \sigma_2, v) = \sigma_2(u)\sigma_2(y)$

$\Rightarrow \quad \dfrac{\sigma_2(x)}{\sigma_2(y)} = \dfrac{\sigma_2(u)}{\sigma_2(v)}$

إذاً η معرفة تعريفاً جيداً .

والآن إذا كان $Z = \dfrac{\sigma_1(x)}{\sigma_1(y)}, t = \dfrac{\sigma_1(u)}{\sigma_1(v)} \in F$ فإن :

$$\eta(Z+t) = \eta\left[\frac{\sigma_1(x)}{\sigma_1(y)} + \frac{\sigma_1(u)}{\sigma_1(v)}\right] = \eta\left[\frac{\sigma_1(xv+yu)}{\sigma_1(yv)}\right]$$
$$= \frac{\sigma_2(xv+yu)}{\sigma_2(yv)} = \frac{\sigma_2(x)}{\sigma_2(y)} + \frac{\sigma_2(u)}{\sigma_2(y)} + \frac{\sigma_2(u)}{\sigma_2(v)}$$
$$= \eta(z) + \eta(t)$$

كذلك

$$\eta(zt) = \eta\left[\frac{\sigma_1(x)}{\sigma_1(y)} . \frac{\sigma_1(u)}{\sigma_1(v)}\right] = \eta\left[\frac{\sigma_1(xu)}{\sigma_1(yv)}\right]$$
$$= \frac{\sigma_2(xu)}{\sigma_2(yv)} = \frac{\sigma_2(x)\sigma_2(u)}{\sigma_2(y)\sigma_2(v)} = \eta(z)\eta(t)$$

وهذا يبرهن أن η هو هومومورفيزم .

والآن سنبين أن η فوقي ، ليكن $z' \in F$ فمن التعريف $z' = \dfrac{\sigma_2(x')}{\sigma_2(y')}$ لبعض $y' \neq 0, x', y' \in D$ من الواضح أن $\dfrac{\sigma_1(x')}{\sigma_1(y')}$ بحيث يكون $\eta\left[\dfrac{\sigma_1(x')}{\sigma_1(y')}\right] = z'$ وهذا يبين أن η فوقي .

أخيراً لتكن $z \in \ker \eta$ $\qquad \Rightarrow \quad \eta(z) = 0 \Rightarrow \dfrac{\sigma_2(x)}{\sigma_2(y)} = 0$

حيث $z = \dfrac{\sigma_1(x)}{\sigma_1(y)}$

(σ_2 لأن أحادي) $\qquad \Rightarrow \quad \sigma_2(x) = 0 \Rightarrow x = 0$

$\Rightarrow \quad \sigma_1(x) = 0 \Rightarrow z = \dfrac{\sigma_1(x)}{\sigma_1(y)} = 0$

لذا فإن $\ker\eta=(0)$ و η راسم أحادي ، فيكون η أيزومورفزم في F على F_2 .
ومن تعريف η لكل $x\in D$ فإن $\eta[\sigma_1(x)]=\sigma_2(x)$ نحصل على $\eta\sigma_1=\sigma_2$ وهذا يتمم البرهان .

نظرية 25.8

إذا كان الحقل K يحوي ساحة تامة غير صفرية D فإن K يحوي حقل قواسم للحلقة D .

البرهان

ليكن $F=\left[\frac{a}{b}:a,b\in D,b\neq 0\right]$ (لاحظ أننا نعني أن $\frac{a}{b}$ هو ab^{-1}) ولأن D غير صفرية ، فإنه يوجد $a(\neq 0)\in D$ إذاً $1=\frac{a}{a}\in F$ والآن لأي $y=\frac{c}{d},x=\frac{a}{b}$ يكون $xy=\frac{ac}{bd}\in F,x-y=\frac{ad-bc}{bd}\in F$ وهكذا تكون F هي حلقة جزئية من K وتحوي 1.
والآن إذا كان $x\neq 0$ فإن $x'=\frac{b}{a}\in F,a\neq 0$ بحيث $xx'=\frac{a}{b}\frac{b}{a}=(0)$ أي أن $x^{-1}=x'\in F$ وهذا يثبت أن F هي حقل .
نأخذ $z(\neq 0)\in D$ نستطيع كتابة $z=za/a$ (كما في الملاحظة السابقة) ، $(za)/a\in F$ وهكذا لدينا $D\subseteq F$ ومن التعريف يتضح لنا أن F هو قواسم للحلقة محتوي K وهذا يبرهن النظرية .

III. غمر حلقة في حلقة إندومورفزم لزمرة إبدالية

لتكن V زمرة جمع إبدالية سنشير بالرمز $Hom(V,V)$ أو بالرمز $EndV$ لمجموعة كل الأندومورفيزمات على V .

بداية سوف نبين أن $Hom(V,V)$ هي حلقة تحت عمليتي جمع وضرب معرفتين تعريفاً مناسباً ، نعرف الجمع والضرب على $Hom(V,V)$ كما يلي لكل $f+g,f,g\in Hom(V,V)$ هي الراسم من V إلى v والمعطى بالشكل :

$(f+g)(v)=f(v)+g(v), v\in V$

وأن fg هي الراسم المركب من V إلى v ، أي أن $fg(v)=f[g(v)]$ لكل $v\in V$.

نظرية 26.8

$Hom(V,V)$ حلقة بمحايد .

البرهان

نعتمد عمليتي الجمع والضرب كما سبق ثم نبين أنه لكل $fg\in Hom(V,V)$ فإن $fg, f+g$ كلاهما ينتمي إلى $Hom(V,V)$ لكل $u,v\in V$ يكون :

$$\begin{aligned}(f+g)(u+v)&=f(u+v)+g(u+v)\\&=[f(u)+f(v)]+[g(u)+g(v)]\\&=[f(u)+g(u)]+[f(v)+g(v)]\\&=(f+g)(u)+(f+g)(v)\end{aligned}$$

(لأن V زمرة إبدالية)

لذلك فإن $f+g\in Hom(V,v)$ وكذلك فإن

$$\begin{aligned}(f.g)(u+v)&=f[g(u+v)]\\&=f[g(u)+g(v)]\\&=f[g(u)]+f[g(v)]\\&=(fg)(u)+(fg)(v)\end{aligned}$$

ولذلك $fg\in Hom(v,v)$

(1) العملية تنسيقية

لكل $f,g,h\in Hom(V,v)$ ولكل $v\in V$:

$$\begin{aligned}[(f+g)+h](v)&=(f+g)(v)+h(v)\\&=[f(v)+g(v)]+h(v)\\&=f(v)+[g(v)+h(v)]\\&=f(v)+(g+h)(v)\\&=[f+(g+h)](v)\end{aligned}$$

وهذا يؤدي إلى $(f+g)+h=f+(g+h)$

(2) العملية + إبدالية

لكل $f, g\ Hom(V, v)$ ولكل $v \in V$ فإن

$$\begin{aligned}(f+g)(v) &= f(v)+g(v)\\ &= g(v)+f(v)\\ &= (g+f)(v)\end{aligned}$$

$$\Rightarrow \qquad f+g=g+f$$

(3) وجود عنصر صفري

واضح أن الراسم $0 : v \to V$ المعرف بالعبارة $0(v)=0$ كل $v \in V$ هو العنصر الصفري في $Hom(v, V)$ لأن لكل $f \in Hom(v, V)$.

$$(f+0)(v) = f(v)+0(v) = f(v)$$

وهذا يعطي $f+0=f$.

(4) وجود النظير الجمعي

لأي $f \in Hom(\forall, V)$ تعرف $-f : v \to V$ بالشكل $(-f)(v) = -f(v)$ لكل $v \in V$

كما أن $u, v \in V$

$$\begin{aligned}(-f)(u+v) &= -f(u+v)\\ &= -[f(u)+f(v)]\\ &= -f(u)+[-f(v)]\\ &= (-f)(u)+(-f)(v), -f \in Hom(v, v)\end{aligned}$$

وأيضاً لكل $[f+(-f)](v) = f(v)+[-f(v)], v \in V$

$$\begin{aligned}&= 0\\ &= 0(v)\end{aligned}$$

ولذلك فإن الراسم $-f$ هو النظير الجمعي للراسم f .

(5) عملية الضرب تنسيقية

لكل $f, g, h \in Hom(V, V)$ ولكل $v \in V$

$$\Rightarrow \qquad [(fg)h](v) = (fg)[h(v)] = f\{g[h(v)]\}$$

وبنفس الطريقة نجد أن $[f(gh)](v)=f\{g[h(v)]\}$

إذاً $(fg)h=f(gh)$

(6) توزيع الضرب على الجمع

لكل $f,g,h\in Hom(v,v)$ ولكل $v\in V$ $[f(g+h)](v)=f[(g+h)(v)]$

$$\begin{aligned}&=f[g(v)+h(v)]\\&=f[g(v)]+f[h(v)]\\&=fg(v)+fh(v)\\&=fg+fh\end{aligned}$$

$$\Rightarrow \qquad f(g+h)=fg+fh$$

وبصورة مشابهة يكون $(g+h)f=gf+hf$.

(7) وجود المحايد الضربي

الراسم الذاتي $I:V\to V$ من الواضح أنه هومومورفيزم زمرة لـ V لذا $I\in Hom(v,v)$ كذلك لأي $f\in Hom(V,V)$ يكون :

$$fI(v)=f[I(v)]=f(v) \qquad \forall v\in V$$

ومنها نحصل على أن $fI=f$ وبصورة مشابهة يمكن أن نبين $If=f$ أي أن I هو المحايد الضربي للحلقة $Hom(V,V)$ ينتج عن ذلك أن $Hom(V,V)$ حلقة بمحايد ضربي .

نظرية 27.8

كل حلقة بعنصر محايد ضربي يمكن غمرها في حلقة إندوموفيزم لزمرة جمع إبدالية .

البرهان

لتكن R حلقة بمحايد وليكن V هو زمرة جمع R^+ في R .

نعرف $f:R\to Hom(V,V)$ بواسطة $[f(r)](v)=rv$ لكل $v\in V$ واضح أن $v\in V$ وأن :

$$[f(r)](u+v)=r(u+v)=ru+rv=[f(r)](u)+[f(r)](v)$$

لكل $u,v\in Hom(v,v)$ لذلك $f(r)\in Hom(v,v)$ وهكذا يصبح تعريفنا محقق .

الآن لأي $r,s\in R$ ولكل $v\in V$ يكون
$$[f(r+s)](v)=(r+s)V$$
$$=rv+sv=[f(r)](v)+[f(s)](v)$$
$$=[f(r)+f(s)](v)$$
$$\Rightarrow \quad f(r+s)=f(r)+f(s)$$

وأيضاً
$$[f(rs)](v)=(rs)v=r(sv) \qquad (\text{لأن } r,s,v\in R)$$
$$=[f(r)](sr)=f(r)\{[f(s)](v)\}=[f(r)f(s)](v)$$
$$\Rightarrow \quad f(rs)=f(r)f(s)$$

إذاً f هو هومومورفيزم .

نهاية
$$f(r)=f(s)\Rightarrow [f(r)](v)=[f(s)](v)$$
$$\Rightarrow \quad rv=sv \quad \forall v\in V$$
$$\Rightarrow \quad r1=s1 \quad (\text{لأن } 1\in V=R^{+})$$

وهكذا يكون
$$f(r)=f(s)\Rightarrow r=s$$

نستنتج أن f راسم أحادي ويكون
$$R\cong f(R)\subseteq Hom(V,V)$$

بعبارة أخرى R مغمورة في $Hom(V,V)$.

نتيجة 28.8

كل حلقة يمكن غمرها في حلقة أندومورفيزم لزمرة جمع إبدالية .

البرهان

لتكن R حلقة عندئذ توجد حلقة R_1 بمحايد ومونومورفزم $f:R\rightarrow R_1$ (نظرية 19.8) كما توجد زمرة جمع إبدالية V ومونومورفيزم $g:R_1\rightarrow Hom(V,V)$ (نظرية 27.8) وهكذا يكون $gf:R\rightarrow Hom(V,V)$ هو هومومورفيزم ، وبما أن كلاً من g,f أحادي فإن gf كذلك أحادي ، هذا يعطينا أيضاً $R\cong gf(R)\subseteq Hom(V,V)$ وبذلك يكون R قابل للغمر في $Hom(V,V)$.

ملاحظة

من الآن فصاعداً سوف نستخدم الرمز R^+ لزمرة الجمع للحلقة R ، وهكذا نكون قد برهنا أن الحلقة R بمحايد قابلة للغمر في $Hom(R^+, R^+)$.

9

حلقات كثيرة الحدود

Polynomial Rings

1. كثيرات الحدود

في المرحلة المدرسية يتعرف طالب الرياضيات على مفهوم كثيرات الحدود وجمعها وضربها وكذا تحليلها إلى عوامل ، كما أنه يكون مشدوداً نحو إيجاد حلول لمعادلات كثيرات الحدود .

بعد ذلك وفي بداية التعليم الجامعي فإن الطالب يتعرض لدراسة دوال كثيرات الحدود ونهاياتها واتصالها .

ونحن هنا نناقش كثيرات الحدود ولكننا أساساً لن نتعرض لأي من المفاهيم المذكورة سلفاً بل سنعالج كثيرات الحدود كأعضاء في حلقة وندرس الخصائص الجبرية لتلك الحلقة .

اعتبر الحلقة S والحلقة R الجزئية منها وليكن $u \in S$ بحيث أن $ru = ur$ لكل $r \in R$ دع $R[u]$ يرمز لمجموعة كل العناصر في S ذات الشكل $a_0 + a_1u + a_2u^2 + ... + a_nu^n$ حيث $i = 0,1,2,...,n$ و n عدد صحيح موجب فباستخدام الحقيقية $au^k = u^ka$ لكل $a \in R$ وكل عدد صحيح موجب k يمكن استنتاج أن $R[u]$ مجموعة غير خالية وهي مغلقة تحت عمليتي الطرح والضرب بما يعني أن $R[u]$ هي حلقة جزئية من S .

فإذا كان $a_0 + a_1u + a_2u^2 + ... + a_nu^n = 0$ حيث $ai \in R(i = 0,1,2,...,n)$ وبحيث كان واحداً على الأقل من ai ليس صفراً فإننا نقول أن u جبري على R أما إذا كان لكل اختيار من $a_0, a_1, a_2, .. an$ (عناصر من R) .

$a_0+a_1u+a_2u^2+..a_nu^n \neq 0$ حيث يكون أحدها على الأقل $a_i \neq 0$ $(i>0)$ فإن u تسمى متسامياً على R فمثلاً إذا أخذنا الحلقتين Q,R فإن $\sqrt{2}\in R$ وباستخدام الحقيقة $\left(\sqrt{2}\right)^2=2\in Q$ يمكن ملاحظة أن كل عنصر في المجموعة $Q\left[\sqrt{2}\right]$ يأخذ الشكل $a+b\sqrt{2}\,,a,b\in Q$ ولأن $2-1\left(\sqrt{2}\right)^2=0$ فيكون لدينا $\sqrt{2}$ عدداً جبرياً على Q .

اعتبر π نعلم أن π ليس عدداً جبرياً أي أنه ليس جذراً لأي كثيرة حدود ذات المعاملات النسبية فإن π متسامياً على Q .

إذا أخذنا أي عنصر $a_0+a_1\pi+a_2\pi^2+...+a_n\pi^n \in Q[\pi]$ فإننا نحصل على متتابعة لا نهائية $(a_0,a_1,a_2,.....,a_n,0,0,...)$ عناصرها من Q جميع حدودها بعد الموقع n تكون أصفاراً وبالعكس إذا أخذنا أي متتابعة لا نهائية $(b_0,b_1,.....,b_n,0,0,....,..)$ عناصرها من Q بحيث فقط عدد منته من حدودها غير الصفرية فسوف نحصل على عدد صحيح غير سالب m بحيث يكون $b_i=0$ لكل $i\geq m+1$ هذه المتتابعة تحدد عنصراً $b_0+b_1\pi+b_2\pi^2+...+b_m\pi^m \in Q[\pi]$ كما نلاحظ أن أي عنصرين :

$$c_0+c_1\pi+c_2\pi^2+...$$

و

$$d_0+d_1\pi+d_2\pi^2+...$$

$c_i,d_i\in Q$ يكونان متساويان إذا وفقط إذا $c_i=d_i$ لكل i وإلا فإن π يكون جبرياً على Q لذلك فإن كل عنصر $a_0+a_1\pi+a_2\pi^2+...+a_n\pi^n$ يتحدد بطريقة وحيدة بالتعبير عنه لمتتابعة لا نهائية $(a_0,a_1,a_2,.....,a_n,0,0,....,..)$ عناصرها من Q ، مرة أخرى نعود إلى الحالة العامة لكل من S,R في هذه الحالة إذا كان $u\in S$ هو يتسامى على R ، فإن كل عنصر $a_0+a_1u+...+a_nu^n, a_i\in R$ يتحدد بطريقة وحيدة بالمتتابعة اللانهائية $(a_0,a_1,a_2,.....,a_n,0,0,...)$ عناصرها من R .

دعنا ننظر المسألة من زاوية أخرى لداعي التيسير دعنا نفرض أن R حلقة وأنها ذات محايد $1(\neq 0)$ والمسألة هي ، هل توجد حلقة S تحوي R

S يكون فيها عنصراً x يكون إبدالياً مع كل عناصر R ويكون متسامياً على R ؟
هذه هي المسألة التي سنأخذها أولاً ، في هذا البند لنقدم إجابة وافية .

نأخذ مفتاحاً لذلك من الملاحظة السابقة وهي أنه إذا كان يتحدد بصورة وحيدة بواسطة المتتابعة اللانهائية $(a_0, a_1, a_2, ..., a_k, 0, 0, ...)$ عناصرها من R هذا يقودنا إلى تعريف كثيرة الحدود على R كالآتي :

تعريف 1.9

أي متتابعة لا نهائية $(a_0, a_1, a_2, ..., a_n, a_n + 1, ...)$ من الحلقة R تسمى كثيرة حدود على R إذا كانت جميع عناصرها باستثناء عدد منته تساوي أصفاراً و بعبارة أخرى المتتابعة اللانهائية $(a_0, a_1, a_2, ..., a_n, ..., ...)$ من عناصر R تسمى كثيرة حدود من R إذا وجد عدد صحيح غير سالب n بحيث كان $\forall_i \geq n+1 \quad a_i = 0$.

كل عنصر a_j في كثيرة الحدود $(a_0, a_1, a_2, ..., ...)$ يسمى المعامل ذو الترتيب j بالحد الثابت وإذا كان n هو العدد الصحيح الأكبر غير السالب بحيث $a_n \neq 0$ فإن a_n يسمى المعامل القائد في كثيرة الحدود .

تعريف 2.9 (مجموع وحاصل ضرب كثيرتي الحدود)

لتكن $g = (b_0, b_1, b_2, ..., ...), f = (a_0, a_1, a_2, ..., ...)$ أي كثيرتي حدود على الحلقة R فإن مجموعهما $f + g$ وحاصل ضربهما fg يعرفان كالآتي :

$$f + g = (a_0 + b_0, a_1 + b_1, a_2, + b_2, ..., ...)$$
$$fg = (c_0, c_1, c_2, ..., ...)$$

حيث
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_2 \, , c_1 = a_0 b_1 + a_1 b_0 \, , c_0 = a_0 b_0$$

وبصورة عامة
$$G_K = a_0 b_k + a_1 b_{k-1} + ... + ... + ... + a_k b_0 = \sum_{i+j=k} a_i b_j$$

(لكل $K \geq 0$)

يبقى أن نبين هل أن حاصل جمع وحاصل ضرب كثيرتي حدود على R هي كثيرة حدود على R وهذا ما تقرره النظرية الآتية :

نظرية 3.9

المجموعة T من كل كثيرات الحدود على الحلقة R المرحلة تحت عمليتي الجمع والضرب المعرفتين كالآتي :

لكل عنصر في $f=(a_0,a_1,a_2,\ldots,\ldots)$ و $g=(b_0,b_1,b_2,\ldots,\ldots)$ في T

$f+g=(a_0+b_0,a_1+b_1,a_2+b_2,\ldots,\ldots)$ و $fg=(c_0,c_1,c_2,\ldots,\ldots)$ حيث $c_k=\sum_{i+j=k} a_i b_j$

لكل $k \geq 0$.

البرهان

لتكن b_n, a_n معاملات g, f حسب الترتيب بحيث أن $a_i = 0 \quad \forall \quad i \geq n+1$ و $b_j = 0 \quad \forall \quad j \geq m+1$.

إذا كان $s=\max\{m,n\}$ فإن $a_t=b_t=0$ لكل $t>s$ إذاً $a_t+b_t=0$ لكل $t>s$ ومن ثم $f+g \in T$ مرة أخرى نفرض أن $k>m+n$ فإنه إذا كان $i+j=k$ فإما $i>m$ أو $j>n$ فيكون $a_i b_j=0$ لكل j,i تحقق $i+j=k$ عندما $k>m+n$ هذا يعطي أن $c_k=0$ لجميع قيم $k \geq m+n+1$ لذا فإن $fg \in T$.

الآن بما أن R هي حلقة فإنه من السهل التحقق من أن $<T,+>$ هي حلقة إبدالية وأن $(0,0,0,\ldots,\ldots)$ هو المحايد الجمعي ولكل $f=(a_0,a_1,a_2,\ldots,\ldots)\in T$ يكون $f=(-a_0,-a_1,-a_2,\ldots,\ldots)$ هو النظير الجمعي لكثيرة الحدود f ومن الواضح أن $f \in T$ وزيادة على ذلك $<T,.>$ هي شبه زمرة لأن $<R,.>$ هي شبه زمرة ، أخيراً يمكن التأكد بسهولة من قانون التوزيع يساراً و يمينياً لعملية الضرب على الجمع وعليه فإن $<T,+,.>$ هي حلقة .

نظرية 4.9

إذا كانت T حلقة كثيرة الحدود على الحلقة R فإن $R' = \{(a,0,0,\ldots) \mid a \in R\}$ هي حلقة جزئية من T أيزومورفية مع R تحت التطبيق $a \to (a,0,0,\ldots,\ldots)$ وعلى ذلك إذا كان R ذات محايد يساوي 1 فإن $(1,0,0,\ldots,\ldots)$ هو محايد للحلقة T .

البرهان

افرض أن $f : R \to T$ معرفة بالشكل $f(a) = (a,0,0,\ldots), \forall a \in R$ لكل $a, b \in R$

$$f(a+b) = (a+b,0,0,\ldots,\ldots) = (a,0,0,\ldots,\ldots) + (b,0,0,\ldots,\ldots)$$
$$= f(a) + f(b)$$

و

$$f(ab) = (ab,0,0,\ldots,\ldots)$$
$$= (a,0,0,\ldots,\ldots)(b,0,0,\ldots,\ldots) = f(a)f(b)$$

كما أن f أحادية لأن $f(a) = f(b) \Rightarrow (a,0,0,\ldots,\ldots) = (b,0,0,\ldots) \Rightarrow a = b$

إذاً $R \cong f(R) = R'$ هذا ثبت الجزء الأول من النظرية .

أخـيراً إذا كانـت R ذات محايـد يسـاوي 1 فـإن $f(1) = (1,0,0,\ldots,\ldots) \in T$ ولكـل $(a_1, a_2, a_3, \ldots, \ldots) \in T$ يكون :

$$(a_1,a_2,a_3,\ldots,\ldots)(1,0,0,\ldots,\ldots) = (a_1,a_2,a_3,\ldots,\ldots) = (1,0,0,\ldots,\ldots)(a_1,a_2,a_3,\ldots,\ldots)$$

أي أن $(1,0,0,\ldots,\ldots)$ هي المحايد في T .

ملاحظة

لكل $a \in R$ ليكن a رمزاً لكثيرة الحدود $(a,0,0,\ldots,\ldots,\ldots)$ ولتكن R بمحايد يساوي $1(\neq 0)$.

نعرف $x = (0,1,0,0,\ldots,\ldots)$ فإن :

$$\bar{a}x = (a,0,0,\ldots,\ldots)(0,1,0,0,\ldots,\ldots) = (0,a,0,0,\ldots,\ldots) = (0,1,0,0,\ldots)(a,0,0,\ldots,\ldots) = x\bar{a}$$

عليه فإن x إبدالي مع جميع عناصر R' أي مع كل عنصر من R إذا رمزياً لصورة a بالرمز $\bar{a}$ بتطبيق صيغة الضرب لكثيرات الحدود فإننا نجد أن $x^2=(0,0,1,0,0,\ldots,\ldots)$ و $x^3=(0,0,0,1,0,0,\ldots,\ldots)$ وبصورة عامة $x^4=(0,0,0,\ldots,\ldots,0,1,0,\ldots,\ldots)$ حيث أن 1 في الموقع $n+1$ وأيضاً لكل $a\in R$ $\quad \bar{a}x^n=(0,0,0,\ldots,\ldots,a,0,\ldots,\ldots)$

حيث a في الموقع $n+1$ لتكن $f=(a_0,a_1,a_2,\ldots,\ldots)$ كثيرة حدود على R حيث يوجد عدد صحيح غير سالب n بحيث أن $\forall i\geq n+1 \quad a_i=0$ نرى أن :

$$\begin{aligned}&(a_0,a_1,a_2,\ldots,\ldots,a_n,0,0,\ldots,\ldots)=(a_0,0,0,\ldots,\ldots)+(0,a_1,0,0,\ldots,\ldots)+\\&(0,0,a_2,0,\ldots,\ldots)+\ldots+\ldots+\ldots+(0,0,\ldots,0,a_n,0,\ldots,\ldots)\\&=\bar{a}_0+\bar{a}_1x+\bar{a}_2x^2+\ldots+\bar{a}_nx^n\end{aligned}$$

زد علـى ذلـك أن $f=0$ إذا وفقـط إذا كـان $a_i=0$ لكـل فـإن $\bar{a}_0+\bar{a}_1x+\bar{a}_2x^2+\ldots+\bar{a}_nx^n=0$ إذا وفقط إذا كل $a_i=0$ وحيث أن $R\cong R'$ تحت الراسم $a\to\bar{a}$ من R إلى R' عندئذ فإننا نزاوج R مع R' وكل $a\in R$ بكثيرة حدود $\bar{a}$ نحصل على أن R حلقة جزئية من T .

الآن $x\in T$ حيث $ax=xa$ لكل $a\in R$ كل عنصر في T على الشكل :

$$f=a_0+a_1x+a_2x^2+\ldots+\ldots+a_nx^n$$

و $f=0$ إذا وفقط إذا كان $a_i=0$ لكل i وبناء عليه فإن x متسامٍ على R وأن x متسامي على R .

ونبين أن الحلقة T وحيدة في إطار إيزومورفيزم لذا نذكر النظرية الآتية :

نظرية 5.9

لتكن R أي حلقة و S,S حلقتين غامرتين للحلقة R نفرض وجود $u\in S$ و $u'\in S'$ بحيث أن u',u إبداليان مع كل عنصر في R فإن $R[u]\cong R[u']$ تحت الراسم $f:R[u]\to R[u']$ المعرف كالآتي $f\left(a_0+a_1u+a_2u^2+\ldots\right)=a_0+a_1u'+a_2(u')^2+\ldots$

حيث u', u متساميان على R .

البرهان

أولاً نوضح أن f معرفة تعريفاً جيداً ليكن :

$$a_0 + a_1u + a_2u^2 + \ldots = b_0 + b_1u + b_2u^2 + \ldots$$

فإن $(a_0 = b_0) + (a_1 - b_1)u + (a_2 - b_2)u^2 + \ldots = 0$

$$\Rightarrow \quad a_0 = b_0 \,, a_1 = b_1 \,, a_2 = b_2 \,, \ldots$$

لأن u متسامي على R ، هذه بدوره يؤدي إلى أن :

$$a_0 + a_1u' + a_2(u')^2 + \ldots = b_0 + b_1u' + b_2(u')^2 + \ldots$$

فيكون $f(a_0 + a_1u + a_2u^2 + \ldots) = f(b_0 + b_1u + b_2u^2 + \ldots)$

ينتج أن f معرف تعريفاً جيداً .

الآن لتكن $a_0 + a_1u + a_2u^2 + \ldots, b_0 + +b_1u + b_2u^2 + \ldots \in R[u]$

فإن $f\left[(a_0 + a_1u + a_2u^2 + \ldots) + (b_0 + b_1u + b_2u^2 + \ldots)\right]$

$$= f\left[(a_0 + b_0) + (a_1 + b_1)u + (a_2 + b_2)u^2 + \ldots\right]$$
$$= (a_0 + b_0) + (a_1 + b_1)u' + (a_2 + b_2)(a_2 + b_2)(u'^2) + \ldots$$
$$= f(a_0 + a_1u + a_2u^2 + \ldots) + f(b_0 + b_1u + b_2u^2 + \ldots)$$

كما أن $f\left[(a_0 + a_1u + a_2u^2 + \ldots)(b_0 + b_1u + b_2u^2 + \ldots)\right]$

$$= f\left[a_0b_0 + (a_0b_1 + a_1b_0)u + (a_0b_2 + a_1b_1 + a_2b_0)u^2 + \ldots\right]$$
$$= a_0b_0 + (a_0b_1 + a_1b_0)u' + (a_0b_2 + a_1b_1 + a_2b_0)(u')^2 + \ldots$$
$$= \left[a_0 + a_1u' + a_2(u')^2 + \ldots\right]\left[b_0 + b_1u' + b_2(u')^2 + \ldots\right]$$
$$= f(a_0 + a_1u + a_2u^2 + \ldots)f(b_0 + b_1u + b_2u^2 + \ldots)$$

لذا فإن f هومومورفيزم .

مرة أخرى $f(a_0 + a_1u + a_2u^2 + \ldots) = f(b_0 + b_1u + b_2u^2 + \ldots)$

$$\Rightarrow \quad a_0 + a_1u' + a_2(u')^2 + \ldots = b_0 + b_1u' + b_2(u')^2 + \ldots$$

$\Rightarrow \quad (a_0-b_0)+(a_1-b_1)u'+(a_2-b_2)(u')^2+...=0$

$\Rightarrow \quad a_0=b_0, a_1=b_1, a_2=b_2,...$

$\Rightarrow \quad a_0+a_1u+a_2u^2+...=b_0+b_1u+b_2u^2+...$ (لأن n متسامي على R)

هذا يعي أن f أحادي .

أخيراً كل عنصر في $R[u']$ هو من النوع $a_0+a_1u'+a_2(u')^2+...$ حيث $a_0,a_1,a_2,...\in R$

ومن الواضح أن ذلك التركيب تساوي $f(a_0+a_1u+a_2u^2+...)$ أي أن f فوقي .

إذا نستنتج أن $R[u]\cong R[u']$.

دعنا نعُد إلى T, R سالفي الذكر وسمي $x=(0,1,0,...,0,...)$ غير محدد على R وإذا كانت R لا تحوي محايداً فإن R يمكن إغمارها داخل حلقة S بمحايد $1(\neq 0)$ فيكون $T\subseteq S[x]$ حيث $x=(0,1,0,0,...)\in S[x]$ ولكن $x\notin T$.

على أية حال كل عضو T يظل من الشكل :

$$a_0+a_1x+a_2x^2+...+a_nx^4 \qquad a_i\in R$$

وسوف نبقى على الإشارة إلى T بالرمز $R[x]$ وعندئذ يجب التأكيد على أن $x\notin R[x]$.

نظرية 6.9

i. إذا كانت R حلقة إبدالية فإن $R[x]$ تكون إبدالية أيضاً .

ii. إذا كانت R ليس لها قواسم صفرية فعليه $R[x]$ ليس لها قواسم صفرية فعلية.

البرهان

i. لتكن :

$$f(a_0,a_1,a_2,...), g=(b_0,b_1,b_2,...)\in R[x]$$

فإن

$$fg=(c_0,c_1,c_2,...,...)$$

حيث

$$c_k=a_0b_k+a_1b_{k-1}+a_2b_{k-2}+...+a_kb_0$$

لكل $k \geq 0$ كذلك $gf = (d_0, d_1, d_2, ..., ...)$ حيث $d_k = (b_0 a_k + b_1 a_{k-1} + ... + b_k a_0)$ لكل $k \geq 0$ لأن R إبدالية فإن $a + b_{k-t} = b_{x-t} a_t, \forall k = 0,1,...,k$ لذا $c_k = d_k$ لكل $k \geq 0$ أي أن $fg = gf$ ونستنتج أن $R[x]$ تبديلية .

ii. لتكن $g \neq 0, f \neq 0$ فإنه يوجد عددان صحيحان غير سالبين n, m بحيث أن لتكن $b_m \neq 0, b_j = 0 \quad \forall J \geq m+1$ و $a_n \neq 0, a_i = 0 \quad \forall i \geq n+1$

فإن $fg = (c_0, c_1, c_2, ..., ..)$:

$$\begin{aligned} c_{m+n} &= a_0 b_{m+n} + a_1 b_{m+n-1} + ... + a_{n-1} b_{m+1} + a_n b_m + a_{n+1} b_{m+1} + ... + ... + a_{m+n} b_0 \\ &= a_n b_m \\ &\neq 0 \end{aligned}$$

(لأن $a_i = 0$ لكل $n \geq n+1$ و $b_j = 0$ لكل $j \geq m+1$)

لن $R, b_m \neq 0, a_n \neq 0$ ليس لها قواسم صفرية فعلية ، منه نستنتج أن $fg \neq 0$ وهذا برهان أن $R[x]$ ليس لها قواسم صفرية فعلية .س

نتيجة 7.9

إذا كانت R ساحة تامة فإن $R[x]$ هي ساحة تامة أيضاً .

تعريف 8.9

لتكن $f = (a_0, a_1, a_2, ..., ...)$ أي كثيرة حدود غير صفرية على الحلقة R فإن درجة f يرمز لها بالرمز $\deg f$ هو أكبر عدد صحيح غير سالب n بحيث أن المعامل النوني a_n فيها لا يساوي الصفر ، إذاً فإن f كثيرة الحدود الغير صفرية فإنها تحوي على الأقل عاملاً غير واحداً غير صفري ولأن f لها عدد منته من العوامل غير الصفرية فإنه يمكن إيجاد عدد صحيح غير سالب n يكون له $a_n \neq 0$ و $\forall i \geq n+1 \quad a_i = 0$.

فإذاً

$$\begin{aligned} f &= (a_0, a_1, a_2, ..., a_n, 0, 0, ...) \\ &= a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \end{aligned}$$

ومن ثم $\deg f = n$.

من الملاحظ أننا لم نعرف درجة كثيرة الحدود الصفرية وبالطبع فإن بعض المؤلفين يعرف درجة كثيرة الحدود الصفرية بأنها تساوي $-\infty$.

نظرية 9.9

لأي كثيرتي حدود غير صفريتين $f=(a_0,a_1,a_2,\dots,\dots)$ و $g=(b_0,b_1,b_2,\dots,\dots)$ على الحلقة R يتحقق ما يلي :

i. إذا كانت $f+g\neq 0$ فإن $\deg(f+g)\leq \max\{\deg f,\deg g\}$.

ii. إذا كانت $fg\neq 0$ فإن $\deg(fg)\leq \deg f+\deg g$.

iii. إذا كانت R هي حلقة بدون قواسم صفرية فعلية فإن $\deg(fg)=\deg f+\deg g$.

البرهان

لتكن $\deg g=m,\deg f=n$ فإن $an\neq 0,b_m\neq 0$ لكل $i>n$ و $b_j=0$ لكل $j>m$.

i. من تعريف الجمع فإن $f+g=(c_0,c_1,c_2,\dots,\dots)$ حيث $c_i=a_i+b_i\,,\forall i\geq 0$ الآن لأي $i>\max\{n,m\}$ لدينا $i>n,i>m$ فإذاً $b_i=0,a_i=0$ بالتالي $c_i=0$ ومن التعريف يكون $\deg(f+g)\leq \max\{n,m\}$.

ii. لتكن $fg=(d_0,d_1,d_2,\dots,\dots)\neq 0$ حيث $d_k=\sum_{i+j=k}a_ib_j\ \forall_k\geq 0$ إذا كان $k>m+n$ فإن لأي عددين صحيحين غير سالبين j,i ، $i+j=k\Leftarrow i<n$ أو $j>m$ هذا يؤدي إلى أن $b_j=0$ أو $a_i=0$ وفي كل حالة يكون $a_ib_j=0$ إذاً $d_k=0,\forall k>m+n$ ويكون $\deg(fg)\leq m+n=\deg f+\deg g$.

iii. نعلم أن $d_{n+m} = a_n b_m \neq 0$ وحيث R هي حلقة بدون قواسم صفرية فعلية ، نستنتج أن $\deg(fg) \geq m+n$ كما رأينا في (ii) $\deg(fg) \leq m+n$ نستنتج أن $\deg(fg) = \deg f + \deg g$.

نعطي الآن مثالين لنبين أن المساواة غير متحقق في الجزأين (i) و (ii) في النظرية السابقة .

مثال 1

اعتبر الحلقة $R = Z/(6)$ عناصرها هي $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}$ خذ $f = \bar{1} + \bar{2}x$ و $g = \bar{5} + \bar{4}x + \bar{3}x^2$ هاتان كثيرتي حدود من الدرجة 1 و 2 على الترتيب وهما عنصران من $R[x]$ الآن $fg = \bar{5} + \bar{2}x + \bar{5}x^2$ من الدرجة 2 في هذه الحالة فإن $\deg(fg) = 2$ وهي لا تساوي $\deg f + \deg g$.

مثال 2

خذ كثيرتي الحدود $f = 1 + 2x - 3x^2$ و $g = 4 - 3x + 3x^2$ في $Z[x]$ فإن $\deg f = 2$ و $\deg g = 2$.

ولكن $f + g = 5 - x$ وهي كثيرة حدود من الدرجة 1 في هذه الحالة $\deg(f+g)$ لا تساوي $\max\{\deg f, \deg g\}$.

ملاحظة : في أي حلقة R إذا كان $f = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ و $g = b_0 + b_1x + b_2x^2 + ... + b_mx^n$.

كثيرتي حدود من الدرجة m,n على الترتيب بحيث كان a_n أو b_m ليس قاسماً للصفر ، فإن $\deg fg = \deg f + \deg g$ وذلك لأن معامل x^{n+m} في fg هو $a_n b_m \neq 0$ لأن أياً من b_m, b_n ليس قاسماً صفرياً .

2. التحليل في $R[x]$

إن قابلية تحليل الأعداد الصحيحة إلى عوامل أولية ذات شبه كبير في نظرية تحليل كثيرات الحدود على حقل هذا التناظر سوف يدرس في الفصل القادم في إطار أعم ، ولكننا ننهي هذا الفصل بنظرية خوارزمية القسمة في $R[x]$ حيث R هي حلقة إبدالية بمحايد .
سوف نرى أن هذه النظرية تلعب دوراً قيادياً في تطوير نظرية التحليل في $F[x]$ حيث F هو حقل وأيضاً في النظرية العامة للحقول .

نظرية 10.9 (خوارزمية القسمة في $R[x]$)

لتكن R حلقة إبدالية بمحايد و g كثيرة حدود غير صفرية في $R[x]$ من الدرجة n ومعاملها القائد هو وحده أي له نظير ضربي في R عندئذ لكل $f \in R[x]$ توجد كثيرتي حدود وحيدتان r, h في $R[x]$ بحيث أن $f = hg + r$ حيث أن إما $r = 0$ أو $\deg r < \deg g$.

البرهان

أولاً نتحقق من وجود r, h إذا كان $f = 0$ فإنه يمكن أخذ $r = 0, h = 0$ وتتحقق النتيجة ببساطة .
الآن إذا كانت f غير صفرية فإننا نطبق الاستنتاج على $\deg f$ مستخدمين حقيقة أن النتيجة تحققت عندما $f = 0$ كما رأينا أعلاه . لتكن النتيجة متحققة لكل كثيرات الحدود لدرجة أقل من درجة f ولتكن $\deg f = m$ في حالة كون $m < n$ بأخذ $r = f, h = 0$ نحصل على $f = hg + r$ نفرض أن $m \geq n$ عندئذ يمكن أن نكتب :

$$f = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m, b_m \neq 0 \qquad (1)$$

$$g = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \;, (\text{وحدة في } R \;\; a_n) \qquad (2)$$

حيث أن a_n^{-1} موجود و $m \ge n$ فإن (2) تعطي :

$$b_m a_n^{-1} x^{m-n} g = b_m a_n^{-1} a_0 x^{m-n} + b_m a_n^{-1} a_1 x^{m-n+1} + \ldots + b_m a_n^{-1} x^{m-1} + b_m x^m \qquad (3)$$

وبطرح (3) من (1) وباستخدام حقيقة أن كثيرتي الحدود هما من نفس الدرجة m ولهما نفس الحد القائد b_m نحصل على أن $f - b_m a_n^{-1} x^{m-n} g$ كثيرة حدود صفرية أو ذات درجة أما من m فإذا كانت كثيرة الحدود صفرية كان $h = b_m a_n^{-1} x^{m-n}, r = 0$ وهذا يحقق الشروط المعطاة أما إذا كانت كثيرة الحدود غير صفرية فمن فروض الاستنتاج فإنه يوجد $h, r \in R[x]$ بحيث أن :

$$f - b_m a_n^{-1} x^{m-n} g = h_1 g + r \qquad (4)$$

بحيث أن $r = 0$ أو $\deg r < \deg g$ وعلى الفور فإن $(u)r$ تعطي $f = hg + r$ حيث :

$$h = b_m a_n^{-1} x^{m-n} + h_1 \qquad (5)$$

وهذا يحقق الجزء الأول من النظرية .

الآن نبين وحدانية كل من r, h .

لتكن $f = hg + r = h_1 g + r_1$ حيث $h, h_1, r, r_1 \in R[x]$ وتحقق الشروط المعطاة فإن :

$$(h - h_1) g = r_1 - r \qquad (6)$$

إذا كان $h - h_1 \ne 0$ فإن $\deg[(h - h_1) g] = \deg(h - h_1) + \deg g \ge \deg g$

كما أن $r_1 - r \ne 0$ (بواسطة ملاحظة مثال (2)) ولكن عندئذ $\deg(r_1 - r) < \deg g$ والتي تناقض المعادلة (6) فيكون $h = h_1$ وينتج أن $r = r_1$ لأنه في أي حقل كل عنصر غير صفري هو وحده فإن النظرية السابقة تعطي الآتي :

نتيجة 11.9

إذا كان F حقلاً فإنه لأي كثيرتي حدود $g \ne 0, f, g \in F[x]$ فإنه يوجد كثيرتي حدود وحيدتان $h, r \in F[x]$ بحيث يكون $f = hg + r$ وأنه إما $r = 0$ أو $\deg r < \deg g$.

ملاحظة

كثيرات الحدود r,h في النظرية السابقة يسميان خارج القسمة والباقي حسب الترتيب ، بينما g,f يسميان القاسم والمقسوم حسب الترتيب ، في حالة $r=0$ نقول أن g نقسم f أو أن g عامل من عوامل f أو f يقبل القسمة على g ونشير لذلك بالرمز $f \mid g$.

تمارين

1. أكمل برهان النظرية 3.9 .

إرشاد : الخطوات الصعبة في البرهان هي فقط للتحقق من خاصية التجميع (التنسيق) بالنسبة للضرب وتوزيع الضرب على الجمع .

لتكن $f=(a_0,a_1,a_2,\ldots,\ldots,\ldots)$ ، $g=(b_0,b_1,b_2,\ldots,\ldots,\ldots)$ ، $h=(c_0,c_1,c_2,\ldots,\ldots,\ldots)\in T$.

لإثبات أن $(fg)h=f(gh)$ نتبع ما يلي :

لتكن المركبة x في fg هو $d_k=\sum_{i+j=k} a_i b_j$ المركبة r في $(fg)h$ هو $\sum_{L+k=r} d_k c_L$

$$=\sum_{L+k=r}\left(\sum_{i+j=k} a_i b_j\right)c_L=\sum_{i+j+L=r}(a_i b_j)c_L$$

بحيث أن المجموع الأخير يجري على كل الثلاثيات الصحيحة الواقعة في $0\le i,j,L\le r$ والتي تحقق المعادلة $i+j+L=r$ بالمثل وأن المركبة r في $f(gh)$ تساوي :

$$\sum_{i+k=r} a_i\left(\sum_{j+L=k} b_i c_L\right)=\sum_{i+j+L=r} a_i(b_j c_L)$$

هذا يعطي $(fh)h=f(gh)$

الآن لإثبات أن $f(g+h)=fg+fh$ نلاحظ أن المركبة r في $f(g+h)$ هو $\sum_{i+j=r} a_i(b_j+c_L)$ وأن المركبة r في $fg+fh$ هو $\sum_{i+j=r} a_i b_j+\sum_{i+j=r} a_i c_j$ إذاً $f(g+h)=fg+fh$.

2. لتكن R حلقة بمحايد و $A=<x^2>$ هو مثالي في $R[x]$ متولدة بـ x^2 ، بين أن $\frac{R[x]}{A}=\{\overline{a_0+a_1x}|a_0+a_1\in R\}$ وأنه إذا كانت R حلقة منتهية ما استنتج أن $\frac{R[x]}{A}$ هي حلقة منتهية كذلك .

3. لتكن R هي حلقة تحقق من المجموعة S المكونة من كل كثيرات الحدود في $R[x]$ والتي فيها الحد الثابت يساوي صفراً تشكل حلقة جزئية من $R[x]$.
4. لكل مثالي A في الحلقة R . برهن أن مجموعة كل كثيرات الحدود في $R[x]$ والتي حدودها الثابتة اختيارية بينما بقية المعاملات تنتمي إلى A هي حلقة جزئية من $R[x]$.
5. لكل مثالي A في الحلقة R بين أن $A[x]$ هو مثالي في $R[x]$ وبرهن أن $\frac{R[x]}{A[x]} \cong \frac{R}{A}[x]$.
6. إذا كانت T, S حلقتين جزئيتين من R بحيث أن $ST \subseteq T$ و $TS \subseteq T$ اثبت أن مجموعة ل كثيرات الحدود هذه في $R[x]$ والتي حدودها الثابتة من S وبقية المعاملات من T هي حلقة جزئية من $R[x]$.
7. لتكن R حلقة إبدالية بمحايد بين أن كل كثيرة حدود $f \in R[x]$ هي وحدة إذا وفقط إذا كان الحد الثابت في f هو وحده وبقية المعاملات هي عناصر عديمة القوة .
8. لتكن R حلقة إبدالية بمحايد لكل كثيرة حدود $f = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \in R[x]$ A_f المثالي في R المتولد بالعناصر $a_0, a_1, a_2, ..., .. a_n$ يسمى مضمون f وباستخدام حقيقة أن أي مثالي فعلي في R يكون محتوى في مثالي أعظمي . اثبت أنه إذا كان لأي كثيرتي حدود g, f ، $A_g = R, A_f = R$ فإن $A_{fg} = R$.
9. لتكن g, f كثيرتي حدود غير صفريتين على R فاثبت ما يلي :
   - **(a)** إذا كان $\deg f \neq \deg g$ فإن $f + g \neq 0$ و $\deg(f+g) = \max\{\deg f, \deg g\}$.
   - **(b)** إذا كان $\deg f = \deg g$ و $f + g \neq 0$ فإن $\deg(f+g) \leq \deg f$.
10. برهن صحة الصورة المعممة لخوارزمية القسمة ، لتكن R هي أي حلقة إبدالية بمحايد ولتكن $g \neq 0, f, g \in R$ و α هو المعامل القائد في g . برهن أنه يوجد كثيرتي حدود r, h في $R[x]$ وعدد صحيح موجب k بحيث يكون $\alpha^k f = hg + r$ حيث $r = 0$ أو $\deg r < \deg g$ وإذا كانت α ليس قاسماً صفرياً برهن أن الثابت k يحقق الشرط المعطى r, h هما وحيدان . كيف عممت هذه النتيجة خوارزمية القسمة ؟

11. لتكن R حلقة إبدالية فإذا كانت $f=a_0+a_1x+a_2x^2+...+a_nx^n$ في $R[x]$ هي قاسم صفري برهن أنه يوجد $b(\neq 0)$ في R بحيث يكون $ba_0=ba_1=...=ba_n=0$.

إرشاد : اختر كثيرة حدود $g=c_0+c_1x+...+c_mx^m$ من أقل درجة m بحيث يكون $fg=0$ فيكون $a_nc_m=0$ اعتبر a_ng فإذا كانت غير صفرية فإن درجتها أقل من m و لا يزال $f(a_ng)=0$ هذا يبين أن $a_ng=0$ ثم تطبيق الاستنتاج على R لإثبات أن $a_{n-r}g=0$ لكل $0\leq r\leq n$.

12. لتكن R حلقة إبدالية بمحايد ولتكن S حلقة جزئية من R وتحوي محايد R ولتكن $f\in R[x]$ إذا وجدت كثيرة حدود $g\in s[x]$ التي معاملها القائد هو وحده في S بحيث أن $fg\in S[x]$ فاثبت أن $f\in S[x]$.

13. لأي حلقة R بين أن $\frac{R[x]}{<x>}\cong R$.

إرشاد : عرف $f:R[x]\to R$ بالشكل $f(a_0+a_1x+a_2x^2+...+a_nx^n)=a_0$.

14. اثبت أن زمرة الجمع في $Z[x]$ إيزومورفية للزمرة G للأعداد النسبية الموجبة تحت الضرب .

إرشاد : استخدم الحقيقة أن مجموع الأعداد الأولية قابلة للعد .

عرف $f[z(x)]\to C$ حسب $f\left(\sum_{i=b} a_ix^i\right)=\prod_{i=0} p_n^{a_i}$.

10

نظرية التحليل في الساحات التامة

Factorization Theory in Integral Domains

في نظرية الأعداد قد نصادف النظرية الأساسية للحساب والتي تنص على أن أي عدد صحيح $n > 1$ يمكن التعبير عنه كحاصل ضرب قوى أعداد أولية مختلفة ، وأن هذا التعبير وحيد كحد الترتيب .

في هذا الفصل نهدف إلى تعميم هذه النتيجة للعناصر في ساحات تامة خاصة معينة تلك التي استحدثت تعاريفها من خواص حلقة الأعداد الصحيحة ، كذلك في هذا الفصل سوف نهتم أساساً بالحلقات الإبدالية ذات العنصر المحايد .

1. قابلية القسمة

تعريف 1.10

لتكن R حلقة إبدالية وليكن b, a عنصرين في R . يقال أن العنصر b يقسم a (رمزياً $b \mid a$) إذا كان $a = bc$ لعنصر $c \in R$ ، b يسمى عامل للعنصر a زيادة على ذلك يقال أن b عامل فعلي للعنصر a إذا كان c, b كلاهما غير وحده .

إثبات النظرية الآتية بسيطة ولذا تم حذفه .

نظرية 2.10

لتكن R حلقة إبدالية بعنصر محايد وليكن c, a, b أي ثلاث عناصر في R فإن :

i. $a \mid a$

ii. إذا كان $b \mid c , a \mid b$ فإن $a \mid cx , a \mid c$ لكل $x \in R$.

i. إذا كان $a \mid b \, , a \mid c$ فإن $a /(b \pm c)$.

ملاحظة : من التعريف ينتج أن كل عنصر في الحلقة R هو عامل للصفر .

تعريف 3.10

لتكن R حلقة إبدالية بعنصر محايد ، يقال للعنصر a في R أنه مرافق للعنصر $b \in R$ إذا كان $a = bu$ لوحدة ما $u \in R$.

ملاحظة : $a \sim b$ **يرمز إلى أن العنصر** a **مرافق للعنصر** b .

نظرية 4.10

إذا كانت R حلقة إبدالية بعنصر محايد ، فإنه يتحقق الآتي :

i. علاقة الترافق هي علاقة تكافؤ على R .

ii. إذا كانت R حلقة تامة و a, b عنصرين غير صفريين في R فإن $a \sim b$ إذا وفقط إذا كان $a \mid b \, , b \mid a$.

iii. إذا كان a, b عنصرين غير صفريين في R فإن $a \mid b \, , b \mid a$ إذا وفقط إذا كان $<a> = <b>$.

البرهان

i. لجميع $x \in R$ فإن $x = 1x$ أي أن $x \sim x$ أي أن $\sim$ علاقة انعكاسية .

إذا كان $a \sim b$ فإن $a = bu$ لوحده $u \in R$ هذا يؤدي إلى أن $b = au^{-1} \Rightarrow au^{-1} \Rightarrow b \sim a$ لأن u^{-1} أيضاً وحده .

عليه فإن $\sim$ متماثلة أو متناظرة .

وأخيراً إذا كان $b \sim c , a \sim b$ فإن $b = cv , a = bu$ لبعض $u , v \in R$ حيث u , v عناصر وحده ، هذا يعطينا أن $a = cvu$ على أي حال لأن كلاً من u , v وحده في R هذا يؤدي إلى أن uv أيضاً وحده في R عليه فإن $a \sim c$ وهذا يؤدي إلى أن $\sim$ متعدية ، إذاً $\sim$ علاقة تكافؤ.

ii. إذا كان $a \sim b$ فإن $a = bu$ لوحده ما $u \in R$ والذي يؤدي إلى أن $b \mid a$ كذلك $b = au^{-1}$ يؤدي إلى أن $a \mid b$.

بالعكس إذا كان $b \mid a , a \mid b$ فإن $a = bd , b = ac$ لبعض $c , d \in R$ عليه فإن $b = hdc \Rightarrow dc = 1$ لأن $b \neq 0$ و R حلقة تامة .

وعليه فإن d وحدة إذاً $a \sim b$.

iii. $a \mid b \Rightarrow b = ac$ لبعض $c \in R$ هذا يؤدي إلى أن :

$$b \in < a > \Rightarrow < b > \subseteq < a >$$

وبالمثل فإن $b \mid a \Rightarrow < a > \subseteq < b >$ وبالتالي يكون $<b> = <a>$ وبالعكس $b \mid a$.

على نفس المنوال فإن $< a > = < b > \Rightarrow a \in < b > \Rightarrow a = br \Rightarrow b \mid a$ (لبعض $r \in R$) $<b> = <a>$ يعطي $a \mid b$ لاحظ أن المرافق الوحيد للعنصر 0 هو الصفر .

مثال 1

في Z العددان $3 , -3$ مترافقان لأن -1 وحده ، في الحقيقة الوحدتان الوحيدتان في Z هما $1 , -1$ عليه كل عدد صحيح غير صفري n له مرافقان هما $n , -n$.

مثال 2

في $Z \mid (8)$ الوحدات هي فقط $\bar{7} , \bar{5} , \bar{3} , \bar{1}$ مرافقي $\bar{2}$ هما $\bar{6} , \bar{2}$.

مثال 3

في $Z[i] = \{ a + bi \mid a , b \in Z , i = \sqrt{-1} \}$ (حلقة أعداد جاوس) .

الوحدات هي $1 , -1 , i , -i$ عليه المرافقات للعدد $2 + 3i$ هي $2 + 3i , -2 - 3i , 2i - 3 , 3 - 2i$

تعريف 5.10

يقال للعنصر p في الحلقة الإبدالية بمحايد R أنه أولي إذا كان :

i. $p \neq 0$ و p ليس وحده .

ii. لكل a,b في R فإن $p \mid ab$ يؤدي إلى أن $p \mid b$ أو $p \mid a$.

تعريف 6.10

العنصر p في الحلقة الإبدالية بمحايد يقال له غير قابل للتحليل إذا كان :

i. $p \neq 0$ و p ليس وحده .

ii. حيثما كان $p = ab$ فإن واحداً من b,a يجب أن يكون وحده بمعنى آخر p ليس له عوامل فعلية .

مثال 4

في Z كل عدد أولي هو عنصر أولي وكل عدد أولي هو عنصر غير قابل للتحليل .

مثال 5

في $Z\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \mid a,b \in Z\right\}$ ، $\sqrt{-5}$ هو عنصر أولي لأنه إذا كان $\sqrt{-5} \mid \left(a + b\sqrt{-5}\right)\left(c + d\sqrt{-5}\right)$ لبعض العناصر $a,b,c,d \in Z$ فإن :

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

لبعض العناصر $x, y \in Z$ عليه فإن $\left(a - b\sqrt{-5}\right)\left(c - d\sqrt{-5}\right) = \left(-\sqrt{-5}\right)\left(x - y\sqrt{-5}\right)$

لذا فإن $\left(a^2 + 5b^2\right)\left(c^2 + 5a^2\right) = 5\left(x^2 + 5y^2\right) \Rightarrow 5 \left| \left(a^2 + 5b^2\right)\left(c^2 + 5a^2\right)\right.$

ولكن $5 \mid 5b^2c^2 + 5a^2d^2 + 25b^2d^2$ بالتالي فإن $5 \mid a^2c^2$ الآن 5 عدد أولي لذا فإنه أما $5/a^2$ أو $5/c^2$ في حالة $5/a^2$ فإن $5/a$ وفي الحالة الثانية $5 \mid c$.

دع $a \mid 5$ ولأن $5=(-\sqrt{5})(-\sqrt{-5})$ فإن $\sqrt{-5}\,|\,a$ وهكذا فإن $\sqrt{-5}\,\big|\,(a+\sqrt{-5}b)$ وبالمثل في حالة $5|c$ نحصل على أن $\sqrt{-5}\,\big|\,(c+\sqrt{-5}d)$ إذاً $\sqrt{-5}$ عنصر أولي في $Z\left[\sqrt{-5}\right]$.

مثال 6

بالعودة ثانية إلى $Z\left[\sqrt{-5}\right]$ يمكن التحقق من أن الوحدات في $Z\left[\sqrt{-5}\right]$ هما فقط $-1,1$. ندعي أن 3 غير قابلة للتحليل في $Z\left[\sqrt{-5}\right]$ إذا لم يكن كذلك فإنه يمكن التعبير عنه بالصورة $3=\left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)$ لبعض $a,b,c,d\in Z$ حيث كلاً من $a+b\sqrt{-5}$ و $c+d\sqrt{-5}$ ليس وحده عندئذ يكون :

$$3=\left(a-b\sqrt{-5}\right)\left(c-d\sqrt{-5}\right)\Rightarrow 9=\left(a^2+5b^2\right)\left(c^2+5d^2\right)$$

عليه إما $a^2+5b^2=1$ و $c^2+5d^2=3$ أو $a^2+5b^2=3$ و $c^2+5d^2=3$ أو $a^2+5b^2=9$ و $c^2+5d^2=1$ ، بما أن $1<5$ فإن الحلول العددية الصحيحة للمعادلة $a^2+5b^2=1$ هي $b=0,a=\pm1$ كذلك $a^2+5b^2=3$ ليس لها حلول عددية صحيحة . في حالة $a^2+5b^2=9$ ، $c^2+5d^2=1$ نحصل على $d=0,c=\pm1$ عليه فإن $3=\left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)$ يؤدي إما إلى $a+b\sqrt{-5}=\pm1$ أو $c+d\sqrt{-5}=\pm1$ ولكن $-1,1$ هما وحدة في $Z\left[\sqrt{-5}\right]$ (لماذا ؟) عليه فإن 3 قابل للتحليل في $Z\left[\sqrt{-5}\right]$. لاحظ أن 3 ليس عنصراً أولياً لأن $3 \mid 9 = \left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right)$ ولكن 3 لا يقسم أياً من $\left(2+\sqrt{-5}\right)$ أو $\left(2-\sqrt{-5}\right)$ بعكس ذلك فإن $2\pm\sqrt{-5}=3\left(x+y\sqrt{-5}\right)$ لبعض $x,y+Z$ هذا يؤدي إلى أن $3x=2$ ولكن $3x=2$ ليس لها حل في Z .

مثال 7

في $Z[i]$ حلقة أعداد جاوس الصحيحة (انظر مثال 3) ، $1+i$ عنصر غير قابل للتحليل . افرض أن $1+i=\left(a+b_i\right)\left(c+d_i\right),a,b,c,d\in Z$ فإن :

$$1-i=(a-b_i)(c-d_i)\Rightarrow 2=(a^2+b^2)(c^2+d^2)$$

عليه إما $a^2+b^2=2$ أو $a^2+b^2=1$ في حالة $a^2+b^2=1$ نحصل على $(a+ib)(a-ib)=1$ يـــؤدي إلى أن $a+bi$ وحـــده . في حالـــة $a+b^2=2$ يكـــون $c^2+d^2=1$ أي أن $(c+di)(c-di)=1$ يؤدي إلى أن $c+di$ وحده إذاً $1+n$ غير قابلة للتحليل في $Z[i]$.

قضية 7.10

في ساحة تامة بمحايد D كل عنصر أولي يكون غير قابل للتحليل .

البرهان

ليكن p عنصراً أولياً في الحلقة D فمن التعريف $p\neq 0$ و p ليس وحده . افرض أن $p=ab$ لبعض العناصر $a,b\in D$ فيكون $p|ab$ ولكن p عنصر أولي فإما $p \mid a$ أو $p \mid b$.

افرض $p \mid a$ فيكون $a=pk$ لبعض $k\in D$.

هذا يعطي $p=pkb$ وهكذا فإن $kb=1$ و b وحده بالمثل إذا كان $p \mid b$ فإن a وحده بالتالي p غير قابلة للتحليل .

مثال 8

في $Z \mid (6)$ 2 عنصر أولي ولكنه ليس غير قابل للتحليل بما أن :

$$\bar{2} \mid \overline{ab} \Rightarrow 6 \mid (ab-2) \Rightarrow ab-2=6k$$

لبعض $k\in Z$ هذا يؤدي $2 \mid ab$ يؤدي إلى أن $2 \mid a$ أو $2 \mid b$ وبدوره يؤدي إلى أن $\bar{2} \mid \bar{a}$ أو $\bar{2} \mid \bar{b}$ والذي يؤدي إلى أن $\bar{2}$ عنصر أولي ولكن $\bar{2}=\bar{2}.\bar{4}$ حيث أن إما من $\bar{2},\bar{4}$ ليس بوحده .

هذا يثبت أن $\bar{2}$ عنصر قابل للتحليل . لاحظ أن $Z \mid (6)$ ليس حلقة تامة .

ملاحظة : بصورة عامة عكس القضية 7.10 غير صحيح . انظر مثال 6 قضية 8.10 لتكن R حلقة إبدالية بمحايد و $a \in R$ فإن المثالي الرئيسي $<a>$ يساوي المجموعة $\{ar + na \mid r \in R, n \in Z\}$.

البرهان

لتكن $X = \{ar + na \mid r \in R, n \in Z\}$ سوف نبين أن X هو المثالي المولد بالعنصر a من الواضح $a = a0 + 1a \in X$ عليه فإن X مجموعة غير خالية ليكن $ar + na, as + ma \in X$ حيث $m, n \in Z, r, s \in R$ فإن :

$$(ar + na) - (as + ma) = a(r - s) + (n - m)a \in X$$

إضافة إلى ذلك إذا كان $s \in R$ فإن $(ar + na)s = a(rs) + a(ns) = a(rs + ns) + 0a \in X$ هذا يبين أن X مثالي يميني في R لأن R إبدالية فإن X مثالي يساري أيضاً ، إذاً x مثالي في R بحيث أن $\{a\} \subseteq X$ ليكن y أي مثالي آخرين R يحوي $\{a\}$ بما أن $a \in y$ و y مثالي للحلقة R فإن $na \in y, ar \in y$ لكل $r + R$ و $n \in Z$ هذا يؤدي إلى أن $ar + na \in y$ لكل $r \in R$ وكل $n \in Z$ إذاً $X \subseteq y$ بالتالي يكون $X = <a>$.

نتيجة 9.10

في الحلقة R الإبدالية بمحايد $<a> = Ra = aR$.

البرهان : افرض أن هو المحايد للحلقة R فإنه يمكننا كتابة $ar + na = a(r + n1) = as$ لبعض $s \in R$ لأن $1 \in R$ يؤدي إلى أن $n1 \in R$ وبالتالي فإن $<a> = \{as \mid s \in R\}$ أي أن $<a> = aR = Ra$.

تعريف 10.10

الحلقة الإبدالية بمحايد R تسمى حلقة مثاليات رئيسة (PIR) إذا كان كل مثالي فيها رئيسي . إضافة إلى ذلك إذا كانت R ساحة تامة فإن R تسمى ساحة مثاليات رئيسية (PID) .

مثال 9

كل حقل هو PID الآن المثاليان الوحيدان لحقل ما F هما (0) والحقل F نفسه . بما أن لكل $x \in F$ فإن $x = x1$ يؤدي إلى أن $x \in (1)$ فإن $F = (1)$ إذاً كل مثالي في F هو مثالي رئيسي بعبارة أخرى فإن F هو PID . على أية حال فإن النظرية التالية تمدنا بأمثلة على PID التي ليست حقلاً .

نظرية 11.10

(a) Z عبارة عن PID .

(b) لأي حقل F حلقة كثيرات الحدود $F(x)$ هي PID .

البرهان

لاحظ أنه في كل جزء يكفي البرهنة على أن كل مثالي غير صفري هو مثالي رئيسي.

(a) ليكن A مثالي غير صفري للحلقة Z دع $a(\neq 0) \in A$ بدون أن نفقد العمومية يمكن أن نفرض أن a موجب (لأنه غير ذلك يكون $-a \in A$ و $-a$ عدد موجب) . ليكن n أصغر عدد صحيح موجب في A . سوف نبين أن $A = < a >$. من الواضح أن $< a > \subseteq A$ ليكن q أي عدد صحيح في A حسب خوارزمية القسمة في Z يوجد عددان صحيحان r, h بحيث $q = hn$ حيث إما $r = 0$ أو $0 < r < n$ إذا كان $0 < r < n$ فإن $r = q - hn \in A$ لأن $q, n \in A$ وهذا يناقض حقيقة أن n هو أصغر عدد صحيح موجب ينتمي

إلى A . عليه فإن $r=0$ أي أن $q = hn \Rightarrow q \in (n)$ هذا يبين أن $A \subseteq (n)$ لذا فإن $A = <n>$ والمطلوب الأول للنظرية قد تحقق .

(b) ليكن A مثالي غير صفري للحلقة $F[x]$ ولتكن g كثيرة حدود غير صفرية وهي الأقل درجة بين كثيرات الحدود في A فيكون $A \subseteq <g>$ الآن إذا كان $t \in A$ فإنه في نتيجة 11.9 يوجد كثيرتي حدود r,h بحيث أن $t = hg + r$ حيث يكون إما $r=0$ أو $\deg r < \deg g$ ولكن $r = t - hg \in A$ لأن $t, g \in A$ و A مثالي في $F(x)$ عليه إذا كان $r \neq 0$ فإن $\deg r$ لا يمكن أن يكون أقل من $\deg g$ حسب اختيارنا لكثيرة الحدود g .

إذاً $A = <g>$ هذا يكمل برهان النظرية . والآن سوف نبين أن عكس القضية 7.10 يتحقق عندما تكون الساحة التامة هي (PID) ساحة مثاليات رئيسية .

نظرية 12.10

كل عنصر غير قابل للتحليل في PID هو عنصر أولي .

البرهان

ليكن P عنصر غير قابل للتحليل في ساحة مثاليات R من التعريف $P \neq 0$ و P ليس وحده ، ليكن p/ab و $p\chi a$ ، سوف نبين أن p/b . الآن $<p>+<b> = <d>$ لعنصر $d \in R$ لأن R هي PID هذا يؤدي إلى أن $<b> \subseteq <d>$ والذي بدوره يؤدي إلى أن $p = dx$ لعنصر ما $x \in R$ ولكن P عنصر غير قابل للتحليل فإما أن يكون d وحده أو x وحده . إذا كان العنصر a هو الوحدة فإنه يوجد $r, s \in R$ بحيث :

$$1 = pr + bs \Rightarrow a = apr + abs \Rightarrow p \mid a$$

لأن $p \mid ab$ و $p \mid apr$ هذا خلاف فرضيتنا ذلك يشدد على أن x وحده عليه $d = px^{-1}$ أي أن $<d> = <p>$ عندئذ يكون $<p> + <b> = <p>$ مؤدياً إلى أن $<b> \subseteq <p>$ أي أن p/b وهكذا فإن القضية محققة .

ملاحظة

القضية السابقة تبين حالاً أن $Z\left[\sqrt{-5}\right]$ ليس PID لأن $3=Z\left[\sqrt{-5}\right]$ غير قابلة للتحليل ولكن 3 ليس عنصراً أولياً .

نظرية 13.10

إذا كان R عبارة في PID وليس حقلاً فإن أي مثالي حقلي A في R هو مثالي أعظمي إذا وفقط إذا كان مولداً بعنصر غير قابل للتحليل في R .

البرهان

بما أن R ليس حقلاً ، يوجد عنصر $a(\neq 0)\in R$ بحيث أن a ليس وحده فيكون $R\subset<a>\subset(0)$ وعليه فإن (0) ليس مثالياً أعظمياً ليكن A مثالياً أعظمياً في R ، فكما رأينا سابقاً $A\neq 0$. الآن $A=<p>$ لعنصر ما $p(\neq 0)\in R$ لأن R هي PID . زيادة على ذلك $A\neq R$ يؤدي إلى أن P ليس وحدة . نبين الآن أن p عنصر غير قبل للتحليل . لنفرض أن $p=ab$ لبعض العناصر $p\in<a>,a,b\in R$ هذا يؤدي إلى أن $A\subseteq<a>$ بما أن A مثالي أعظمي إما أن يكون $A=<a>$ أو $R=<a>$ في حالة $R=<a>$ فإن $1=ac$ لعنصر ما $c\in R$ والذي يعني أن a وحدة . في حالة $R=<a>$ فإن $a\in<p>$ يؤدي إلى أن $a=pq$ لبعض $q\in R$ فنحصل على أن $p=pqb$ وبدوره يعطي $qb=1$ أي أن b وحدة وبالتالي فإن p غير قابل للتحليل .

بالعكس افرض $A=<p>$ حيث p عنصر غير قابل للتحليل .

بما أن p ليس وحدة فإن $A\neq R$ بفرض $A\subset J$ مثالي للحلقة R فبما أن R هي PID فإن $J=<x>$ لعنصر ما $x\in R$ و $x\notin A$ (وإلا فإن $J=A$) الآن $<p>\subset<x>\Rightarrow x\mid p$ أي أن $p=xy$ لبعض $y\in R$ ولأن p عنصر غير قابل للتحليل .

فإما أن x وحدة أو y وحدة . فإذا كان y وحدة فإن $x=py^{-1}\in A$ وهذا تناقض . هذا يدعم أن x وحدة ، أي أن $J=[x]=R$ إذاً A مثالي أعظمي في R .

مثال 10

في Z المثالي $<p>$ أعظمي إذا وفقط إذا كان p عدداً أولياً ، هذا يتبع حقيقة أنه في Z كل عنصر غير قابل للتحليل هو عدد أولي وبالعكس .

مثال 11

في $Q[x]$ المثالي $(x+2)$ مثالي أعظمي لاحظ أن $Q[x]$ عبارة عن PID (نظرية 11.10) وأن $x+2$ عنصر غير قابل للتحليل في $Q[x]$ لأنه إذا كان $x+2=fg$ فإن $\deg f+\deg g=1$ مما يعني أن $\deg f=0$ أو $\deg g=0$ فنفرض أن $\deg g=0$ فإن $\deg f=1$ وبوضع $f=a_0$ حيث $a_0\neq 0\in Q$ ووضع $g=b_0+b_0y$ حيث $b_1\neq 0,b_0b_1\in Q$ فإن $x+2=a_0(b_0+b_1x)$ والذي يؤدي إلى أن $a_0b_1=1,a_0b_0=2$ فيكون a_0 وحدة أي أن f وحدة . بالمثل إذا أخذنا $\deg g=0$ فإن g يكون وحدة ، لذا فإن $x+2$ عنصر غير قابل للتحليل ومن النظرية السابقة يكون $<x+2>$ مثالي أعظمي .

تعريف 14.10 (HCF)

لتكن R حلقة إبدالية إذا كان a,b غير صفريين في R فإنه يقال للعنصر غير الصفري c في R أنه عامل مشترك أكبر (HCF) للعنصرين b,a في R إذا كان :

i. $c\mid a$, $c\mid b$ في R .

ii. لأي $d\neq 0\in R$ إذا كان $d\mid a$, $d\mid b$ في R فإن $d\mid c$ في R .

تعريف 15.10 (LCM)

العنصر غير الصفري d في الحلقة الإبدالية R يقال أنه مضاعف مشترك أصغر (LCM) للعنصرين غير الصفريين a,b في R إذا كان :

i. $d \mid a, d \mid b$.

ii. لأي $(x \neq 0)$ في R إذا كان $x \mid a, x \mid b$ في R فإن $x \mid d$ في R .

التعريفين السابقين يمكن ... بصورة طبيعية لأي عدد منته من العناصر غير الصفرية في R .

مثال 12

في Z العدد 3 هو عامل مشترك أصغر للعددين 6 ,9 لاحظ أن $6 = 3.2$ و $9 = 3.3$ عليه $3 \mid 6$ و $3 \mid 9$ أضف لذلك أنه إذا كان $a(\neq 0)$ عدداً صحيحاً بحيث $a \mid 6$ و $a \mid 9$ فإن $a \mid 9 - 6$ أي أن $a \mid 3$ لذا فإن 3 يحقق الشرطين (i) , (ii) في تعريف HCF بالمثل يمكن بيان أن 3– هو HCF لعددين 6 , 9 كذلك 18 هو LCM لعددين 6 , 9 . الآن $18 = 6.3$ و $18 = 9.2$ يؤدي إلى أن $6 \mid 18$ و $9 \mid 18$ زد على ذلك افرض أن $x(\neq 0)$ عدد صحيح بحيث $6 \mid x , 9 \mid x$ الآن $2 \mid 6$ يؤدي إلى أن $2 \mid x$ وأن $9 - 4.2 = 1 \Rightarrow 9x - 4.2x = x$ ومرة أخرى فإن $2 \mid x$ يؤدي إلى أن $x = 2k$ لعدد صحيح k , $9 \mid x$ يؤدي إلى أن $x = 9\ell$ لعدد صحيح ℓ ، هذا يبين أن $18k - 4.18\ell$ ومن ثم يكون $18 \mid k$ أي أن 18 هو LCM للعددين 6 , 9 .

وبنفس الطريقة يمكن البرهنة على أن 18– هو LCM للعددين 6 , 9 .

مثال 13

الحلقة $Z/(12)$ عناصرها هي $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\bar{9},\overline{10},\overline{11}$ ، $\bar{2}$ هو عامل مشترك أكبر للعنصرين $\bar{8},\bar{6}$ لاحظ أن $\bar{3}.\bar{2} = \bar{6}$ و $\bar{4}.\bar{2} = \bar{8}$ إضافة إلى ذلك إذا كان $\bar{x} \neq \bar{0}$ في $Z/(12)$ وكان $\bar{x} \mid \bar{8}, \bar{x} \mid \bar{6}$ فإن $\bar{x} \mid (\bar{8} - \bar{6})$ فيكون $\bar{x} \mid \bar{2}$ إذاً $\bar{2}$ هو HCF للعنصرين $\bar{8},\bar{6}$ لاحظ أن $\overline{10}.\bar{3} = 6$ و $\overline{10}.\bar{2} = \bar{8}$ عليه $\overline{10} \mid \bar{6}$, $\overline{10} \mid \bar{8}$ كذلك إذا كان $Z/12 \ni \bar{y}(\neq \bar{0})$ وكان $\bar{y} \mid \bar{6}$ و $\bar{y} \mid \bar{8}$ فإن $\bar{y} \mid (\bar{6} - \bar{8}.\bar{2})$ أي أن $\bar{y} \mid \overline{10}$ إذاً $\overline{10}$ هو

أيضاً HCF لـ $\bar{8},\bar{6}$ ندعي أن $\bar{8},\bar{6}$ ليس لها LCM في $Z/(12)$ لو فرضنا أن $\bar{x}$ هو LCM للعنصرين $\bar{8},\bar{6}$ فإن $\bar{x}\mid\bar{8}$ | $\bar{x},\bar{6}$ ويكون $\bar{x}=\overline{6n}$ لعنصر ما $\bar{n}\in Z/(12)$ إذاً $\bar{x}$ يساوي $\bar{0}$ أو $\bar{6}$ هذا يؤدي إلى أن $\bar{6}=\overline{89}$ للعنصر $\bar{9}\in Z/(12)$ لأن LCM لا يساوي صفراً أبداً ولكن $\overline{8m}\equiv 0,\bar{4},\bar{8}$ لكل $\bar{m}\in Z/(12)$ وهذا تناقض بالتالي $\bar{8},\bar{6}$ ليس لها LCM في $Z/(12)$ هذا يبين أن $\bar{8},\bar{6}$ عنصرين ما ، قد يكون لهما HCF وليس بينهما LCM .

مثال 14

في $Z[x]$ حلقة كثيرات الحدود على Z كثيرة الحدود $x+2$ هي HCF لكثيرتي الحدود $2x+4, x^2+2x$ في حين $2x^2+4x$ هي LCM لهما ، من الواضح $(x+2)\mid(2x+4),(x+2)\mid(x^2+2x)$.

إذاكان $f(\neq 0)+Z[x]$ وكان $f\mid(x^2+2x)$ و $f\mid(2x+4)$ فإن $2x+4=fg$ لبعض $g\in Z[x]$ بما أن Z ساحة تامة $\deg f+\deg g=\deg(2x+4)=1$ عليه فإما أن $\deg f=0$ أو $\deg g=0$ في حالة $\deg f=0$ فإن $f=a_0$ حيث $a_0\neq 0$ وعندئذ $f\mid(x^2+2x)\to x^2+2x=a_0(b_0+b_1x+b_2x^2)(b_2\neq 0)$ لأن $\deg(x^2+2x)=2$ هذا يعطي أن $a_0b_2=1$ ويؤدي إلى أن a_0 وحدة في Z يؤدي كذلك إلى أن a_0 يساوي 1 أو -1 إذاً f يساوي 1 أو -1 عليه فإن $f\mid(x+2)$.

في حالة $\deg f=1$ ضع $f=a_0+a_1x, a_1\neq 0$ الآن :

$$f/(2x+4)\Rightarrow 2x+4=(a_0+a_1x)c_0,c_0\neq 0\Rightarrow a_0c_0=4\Rightarrow a_0\neq 0$$

ومرة أخرى
$$f/(x^2+2x)\Rightarrow x^2+2x=(a_0\in a_1x)(d_0+d_1x),d_1\neq 0$$

لأن $\deg(x^2+2x)=2$ يؤدي إلى أن $a_0d_0=0$ و $a_0\neq 0$ وبدوره يؤدي إلى $d_0=0$ إضافة لذلك $a_1d_1=1$ يعني أن a_1 وحدة عليه فإن $a_1=\pm 1$ لذا فإن $d_1=\pm 1$ وختاماً عندما

$a_0 d_1 = 2$ يكـــون $a_0 = 2$ عنــــدما $d_1 = 1$ و $a_0 = -2$ عنـــــدما $d_1 = -1$ إذاً $f = x+2$ أو $f = -x-2$ في كلا الحالتين يكون $f \mid (x+2)$.

عليه فإن $x+2$ هو HCF لكثير من الحدود $x+2x$ و $2x+4$ نترك للقارئ التحقق من إثبات العبارة أن كثيرة الحدود $2x^2 + xy$ هي LCM كثيرة الحدود $x^2 + 2x$ و $2x+4$.

نلاحظ في الأمثلة السابقة أن زوج من العناصر غير الصفرية b,a في حلقة ما قد يكون لها أكثر من HCF وأن وجود HCF لهما لا يضمن وجود LCM .

وهناك ملاحظة مشابهة حول LCM ووجود بصورة متقابلة مع HCF كذلك لن نفقد ملاحظة أنه إذا وجد في ساحة تامة بمحايد أكثر من HCF واحد أو LCM فإنها تكون مرافقة .

ونتحقق من ذلك بالنظرية الآتية .

نظرية 16.10

ليكن D ساحة تامة بمحايد إذا كان b,a عنصرين غير صفريين في D ويوجد لهما HCF فإن أي اثنين في HCF للعنصرين b,a يكونان هما مترافقين بالمثل إذا كان b,a لهما LCM فإن أي اثنين من LCM يكونان مترافقين .

البرهان

سنقدم البرهان في حالة HCF ونترك برهان الحالة الثانية للقرار .

ليكن d,c أي اثنين من H,F للعنصرين b,a فبما أن c/a و c/b و d هو HCF للعنصرين b,a فإن $d \mid c$ بالمثل $c \mid d$ لذا فإن d,c مرافقان (نظرية 4.10 (ii)) .

اصطلاح : العامل المشترك HCF أكبر للعنصرين b,a يرمز له بالرمز (a,b) كما يرمز للمضاعف مشترك أصغر بالرمز $[a,b]$.

أخيراً نعطي مثالاً لنبين أنه قد لا يوجد عامل مشترك أكبر لعنصرين غير صفريين في ساحة تامة بمحايد .

مثال 15

اعتبر الحلقة $R = Z\left[\sqrt{-5}\right] = \{a + b\sqrt{-5} \mid a , b \in Z\}$ عندئذ $3 \mid -3+3\sqrt{-5}\,,3 \mid 9, 9,-3+3\sqrt{-5} \in Z\left[\sqrt{-5}\right]$.

أولا نبين أن العوامل الفعلية للعدد 9 هي $-3,3,-2,-\sqrt{-5},-2+\sqrt{-5},2+\sqrt{-5},2-\sqrt{-5}$

افرض أن $9=\left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)$ حيث $c+d\sqrt{-5}\,,a+b\sqrt{-5}$ ليست وحدة ، هذا يعطي أن $81=N\left[\left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)\right]$ حيث $N\left(x+y\sqrt{-5}\right)=x^2+5y^2$ أي أن $81=\left(a^2+5by\right)\left(c^2+5d^2\right)$ لذا فإن $a^2+5b^2=1,3,9,27,81$ في حالة $a^2+5b^2=1$ فإن $b=0,a=\pm1$ إذاً $a+b\sqrt{-5}$ وحدة وهذا تناقض .

$a^2+5b^2=3$ ليس لها حل صحيح (برهن ذلك !) .

$a^2+5b^2=9$ لها $a=\pm2$ ، $b=\pm1$ أو $a=\pm3$ ، $b=0$ كحلول صحيحة ، مرة ثانية $c^2+5d^2=9$ يعطي $d=\pm1,c=\pm2$ أو $d=0,c=\pm3$ نحصل من ذلك على أن $\pm3,\pm2\neq\sqrt{-5}$

العوامل فعلية الست للعدد 9

مرة أخرى $a^2+5b^2=27$ ليس لها حل .

أخيراً $a^2+5b^2=81$ يؤدي إلى أن $c^2+5d^2=1$ وبدوره يؤدي إلى أن $c+d\sqrt{-5}$ وحدة وهذا غير معقول إذا تحقق جزئياً .

الآن أي من العوامل $,-5\sqrt{-5},2-\sqrt{-5},-2\sqrt{-5},-2+\sqrt{-5}$ ، $-2+\sqrt{-5}$ لا يمكن أن يكون HCF لـ 9 و $-3+3\sqrt{-5}$ لأن غير ذلك يعني أن $2+\sqrt{-2} \mid 3$ أو $\left(2-\sqrt{-5}\right) \mid 3$ وهذا مستحيل كما رأينا في مثال 6 .

إضافة إلى ذلك لا يمكن أن يكون 9 هو HCF لنفسه وللعدد $-3+3\sqrt{-5}$ لأن $9/-3+3\sqrt{-5}$ يؤدي إلى أن $-3+3\sqrt{-5}=9\left(u+v\sqrt{-5}\right)$ لبعض $u,v\in Z$ يؤدي إلى أن $9u=-3$ لها حل في الأعداد الصحيحة ، وهذا مجافٍ للعقل .

لذا إذا كان 9 و $-3+3\sqrt{-5}$ لهما HCF فيجب أن يكون 3 هو العدد (لاحظ مرافق HCF هو أيضاً HCF فرضه كذلك الآن $2+\sqrt{-5}$ هو عامل للعدد 9 وكذلك :

$$\left(-3+3\sqrt{-5}\right)=\left(2+\sqrt{-5}\right)\left(1+\sqrt{-5}\right)\Rightarrow\left(2+\sqrt{-5}\right)\left(-3+3\sqrt{-5}\right)$$

عليه فإن $3\mid\left(2+\sqrt{-5}\right)$ لأن 3 هو HCF للعنصرين 3 و $-3+3\sqrt{-5}$ حسب فرضنا ولكن في هذه الحالة يكون $3=\left(2+\sqrt{-5}\right)\left(8+9\sqrt{-5}\right)$ و :

$$3=\left(2-\sqrt{-5}\right)\left(p-9\sqrt{-5}\right)\Rightarrow 9=q\left(p^3+5q^2\right)\Rightarrow p^2+5q^2=1$$

$$\Rightarrow\qquad p=\pm1,q=0\Rightarrow 5=\pm\left(2+\sqrt{-5}\right)$$

وهو غير معقول إذاً 9 و $-3+3\sqrt{-5}$ ليس لها HCF .

نظرية 17.10

إذا كانت R هي PID فإن كل زوجين من العناصر غير الصفرية b,a للحلقة R لهما HCF و LCM زيادة على ذلك إذا كان $d=(a,b)$ فإن $d=ax+by$ لبعض $x,y\in R$.

البرهان

اعتبر $<a>+<b>$ بما أن R هي PID ، $<a>+<b>=<c>$ لبعض $c\in R$ ومن ثم فإن $<a>\subseteq<c>$ و $<b>\subseteq<c>$ وهو ما يؤدي إلى أن $c\mid a$ و $c\mid b$.

افرض $d(\neq0)\in R$ بحيث يكون d/a و d/b فإن $<a>\subseteq<d>$ وأيضاً :

$$<b>\subseteq<d>\Rightarrow<a>+<b>\subseteq<d>\Rightarrow<c>\subseteq<d>\Rightarrow d/c$$

إذاً c هو عامل مشترك أكبر HCF للعنصرين b,a .

الآن (لبعض $x, y \in R$) $c \in <a> + <b> \Rightarrow c = ax+by$ ومرة ثانية نعتبر $<a> \cap <b>$ فيما أن R هي PID فإن $<a> \cap <b> = <\ell>$ لبعض $\ell \in R$. الآن $<\ell> \subseteq <a>$ و $<\ell> \subseteq <b>$ يؤدي إلى أن $a \mid \ell$ و $a \mid \ell$ ليكن $m(\neq 0) \in R$ بحيث $a \mid m$ و $b \mid m$ يؤدي إلى أن :

$$<m> \subseteq <b>, <m> \subseteq <a>$$
$$\Rightarrow \quad <m> \subseteq <a> n <a> = <\ell> \Rightarrow \ell \mid m$$

إذاً ℓ هو LCM للعنصرين b, a .

نتيجة 18.10

لتكن R هي PID فإن أي n من العناصر غير الصفرية $a_1, a_2, ..., a_n \in R$ لها HCF و LCM .

البرهان

نطبق الاستنتاج على n .

تعريف 19.10

يقال لعنصرين غير صفريين في حلقة إبدالية بمحايد أنهما أوليان نسبياً (كلاهما مع الآخر) إذا كان HCF لها هو وحدة .

نتيجة 20.10 (تطابق بيزوت)

لتكن R عبارة عن PID العنصران غير الصفريين b, a في R يكونان أوليين نسبياً مع بعضهما إذا وفقط إذا وجد $x, y \in R$ بحيث كان $ax+by=1$.

البرهان

إذا كان b, a أوليان نسبياً فبما أن 1 مرافق لأي عنصر وحدة في R فإن 1 هو HCF للعنصرين b, a عليه يوجد $x, y \in R$ بحيث $ax+by=1$ (نظرية 17.10) وبالعكس

يكـن $x, y \in R$ بحيـث كـان $ax+by=1$ فـإذا كـان d هـو HCF للعنصـرين $b\,, a$ عندئـذ $d \mid c$ و $d \mid b$ يـؤدي إلى $d \mid (ax+by) \Rightarrow d \mid 1$ لـذا فـإن $1=dc$ لعنصـر مـا $c \in R$ بعبارة أخرى فإن d وحدة ويكون b, a أوليان نسبياً .

نتيجة 21.10

إذا كان R عبارة عن PID فإن n من العناصر غير الصفرية $a_1, a_2, ..., a_n$ في R تكون أولية نسبياً (أي أن HCF لها هو وحده) إذا وفقط إذا وجد $x_1, x_2, ..., x_n \in R$ بحيث كان $a_1x_1 + a_2x_2 + ... + a_nx_n = 1$.

البرهان

يشبه برهان نتيجة 20.10 .

مسائل

1. بين أن أي مرافق لعامل مشترك أكبر (HCF) لعنصرين غير صفريين b, a في حلقة إبدالية بمحايد هو أيضاً عامل مشترك أكبر لهما ، اثبت صحة ذلك للمضاعف المشترك الأصغر (LCM) .

2. إذا كان $a_1, a_2, ..., a_n$ و r عناصر غير صفرية لساحة تامة R ، برهن أنه إذا كان للعناصر $a_1, a_2, ..., a_n$ لها HCF فإن العناصر $ra_1, ra_2, ..., ra_n$ عامل مشترك أكبر HCF وأن $(ra_1, ra_2, ..., ra_n) = r(a_1, a_2, ..., a_n)$. اثبت كذلك أنه إذا كان للعناصر $a_1, a_2, ..., a_n$ مضاعف مشترك أصغر LCM فإن العناصر $ra_1, ra_2, ..., ra_n$ مضاعف مشترك أصغر LCM وأن $[ra_1, ra_2, ..., ra_n] = r[a_1, a_2, ..., a_n]$.

إرشاد

افرض $c = (ra_1, ra_2)$ الآن $r \mid ra_1$ و $r \mid ra_2$ يؤدي إلى $r \mid c$ ويؤدي إلى $c = d$ لبعض $d \in R$ الآن وضح أن $d \mid a_1$ و $d \mid a_2$ لأن $c \mid ra_1$ و $c \mid ra_2$ إضافة إلى ذلك إذا كان $x \mid a_1$ و $x \mid a_2$ فإن $rx \mid ra_1$ و $rx \mid ra_2$ يؤدي إلى أن $rx \mid c$ وهكذا فإن $x \mid d$. مرة ثانية إذا كان $\ell = [a_1, a_2]$ فمن الواضح $r\ell \mid ra_1$ و $r\ell \mid ra_2$ فإذا كان $x \mid ra_1$ و $x \mid ra_2$ فإن $r \mid x \Rightarrow x = rs$ لعنصر $s \in R$ هذا يعطي $s \mid a_1$ و $s \mid a_2$ إذاً $\ell \mid s$ بالتالي $x \mid r\ell$.

3. اثبت أنه في ساحة تامة بمحايد ، كل عنصرين غير صفريين لهما HCF إذا وفقط إذا كان كل عنصرين غير صفريين لهما LCM .

4. اثبـت أنـه إذا كانـت R هـي PID وكـان a,b عنصـرين غـير صـفريين في R فـإن $[a,b][a,b]=abu$ لوحدة $u\in R$.

5. اثبت أن الساحة التامة بعنصر محايد R هي حقل إذا وفقط إذا كان $R[x]$ هي PID استنتج أن $Z[x]$ ليس PID .

6. لتكن R حلقة إبدالية بمحايد ، ليكن $a,e\in R$ بحيث $e^2=e$ اثبت أن :

i. إذا كان $<a>=<e>$ فإن e,a مترافقان .

ii. إذا كـان e,a^m مترافقـان لعـدد صـحيح موجـب m فـإن لجميـع الأعـداد الصحيحة $m\le n$ يكون $e\,,a^n$ مترافقين أيضاً .

7. أوجد HCF و LCM فيما يلي إذا كانا موجودين :

i. $\bar{9}$ و $\overline{18}$ في $Z/(20)$.

ii. x^2+3x و $3x+9$ في $Z[x]$.

iii. x^2+5x+6 و $x^2+7x+12$ في $Z[x]$.

iv. $\bar{7}$ و $\bar{6}$ في $Z/(14)$.

v. $3x^5-8x^4-x^2+6x-2$ و $x^9-3x^8+x^7-2x^2+6x-2$ في $Z[x]$.

إجابة

i. $HCF=\bar{9}$ و $LCM=\overline{18}$.

ii. $HCF=x+3$ $\quad i \quad$ $LCM=3x^2+9x$

iii. $HCF=y+3$ $\quad$ $LCM=x^3+9x^2+26x+2i$

iv. $HCF=I$ $\quad i$ لا يوجد LCM .

v. $HCF=x^2-3x+1$ $\quad$ $LCM=(x^2-3x+1)(3x^3-x^2-2)(x^2-2)i$

استحضر أن أي مرافق إلى HCF هو HCF وأي مرافق لـ LCM هو LCM .

8. ليكن C,B,A مثاليات غير صفريات للحلقة R فإذا كانت R هي PID فاثبت أن :
   a. $A(B\cap C)=AB\cap AC$.
   b. $A=<a>$ و $B=<b>$ يؤدي إلى أن $AB=<ab>$.
9. اثبت أنه إذا كانت R هي PID فإن $AB=A\cap B$ إذا وفقط إذا كان A,B مترافقان أعظمياً على فرض أن B,A مثاليان غير صفريان في R .
10. ليكن P عنصراً أولياً في حلقة إبدالية بمحايد R اثبت أنه إذا كان $p \mid a_1a_2..a_n$ فإنه يجب أن يكون هناك على الأقل i واحدة $1\le i\le n$ بحيث يكون $p \mid a_i$.
11. ليكن a عنصراً غير صفري في PID وليكن $a \mid bc$ ، $(a,b)=1$ اثبت أن $a \mid c$.
12. إذا كان في PID ثلاث عناصر غير صفرية a,b,c بحيث $a \mid c$ و $b \mid c$ كذلك $(a,b)=1$ فاثبت أن $ab \mid c$.
13. اثبت أن $<2>+<x>$ ليس مثالياً رئيسياً في $Z[x]$.
14. اثبت أنه في حلقة الأعداد الزوجية E كل مثالي هو مثالي رئيسي .
15. لتكن R هي PID و a,b,c ثلاث عناصر غير صفرية في R اثبت الآتي :
   i. $(a,b)=1,(a,c)=1$ يؤدي إلى $(a,bc)=1$.
   ii. $(a,(b,c))=((a,b),c)$.
   iii. $(a,1)=1$.
16. اثبت أنه في حلقة إبدالية بمحايد مرافق العنصر الأول (غير القابل للتحليل) هو عنصر أولي (غير قابل للتحليل) .
17. إذا كان p عنصر أولياً في ساحة تامة بعنصر محايد يقسم عنصراً أولياً آخر q فاثبت أن q,p مترافقان .

2. ساحات إقليدس

نعلم أنه إذا كان b, a عددين صحيحين $(b \neq 0)$ فإنه يوجد عددان صحيحان c و d بحيث $a = bc + d$ حيث $d = 0$ أو $0 < d < |b|$ في هذا البند نحاول تعميم هذا المفهوم .

تعريف 22.10

يقال لساحة تامة غير صفرية R أنها ساحة أقليدية إذا توجد دالة δ من $R - \{0\}$ إلى Z بحيث يكون :

1. $\delta(a) \geq 0$ لكل $a \in R - \{0\}$.

2. لكل $a, b \in R - \{0\}$ فإن $\delta(ab) \geq \delta(a)$.

3. لكل $a \in R$ و $b \in R - \{0\}$ يوجد $q, r \in R$ بحيث يكون $a = qb + r$ حيث إما $r = 0$ أو $\delta(r) < \delta|b|$.

ملاحظة

الشرط 3 يسمى خوارزمية أقليدس والدالة δ تسمى دالة القيمة على R لاحظ كذلك من الشرط (2) أنه يمكن كتابة $\delta(ab) \geq \delta(b)$.

مثال 16

حلقة الأعداد الصحيحة Z هي ساحة أقليدس حيث نأخذ $\delta(a) = |a|$ لكل $a \in Z - \{0\}$ من الواضح δ يحقق (1) , (2) , (3) .

مثال 17

كل حقل F هو ساحة أقليدس نأخذ $\delta(a) = 1$ لكل $a \in F - \{0\}$ لجميع العناصر غير الصفرية $a, b \in F$ فإن $ab \neq 0$ عليه $\delta(ab) = 1 = \delta(a)$ كذلك إذا كان $a \in F$ و b أي عنصر غير صفري في F يمكننا كتابة $a = (ab^{-1})b + 0$ إذاً (3) أيضاً صحيحة .

مثال 18

الحلقـة $Z(i) = \{a + bi \mid a , b \in Z , i = \sqrt{-1}\}$ لأعـداد جـاوس الصـحيحة هـي ساحة تامة ، نفرض $\delta : Z[i] \to Z$ كالآتي $\delta(a + bi) = a^2 + b^2$ لجميع $a + bi$ من الواضح أن (1) متحققة ولكل عنصرين غير صفريين $a+b_i , c+d_i \in Z[i]$ ،

$$\begin{aligned}\delta[(a+b_i)(c+d_i)] &= \delta[(ac-bd)+(ad+bc)i] \\ &= (ac-bd)^2 + (ad+bc)^2 \\ &= (a^2+b^2)(c^2+d^2) \geq a^2+b^2\end{aligned}$$

لأن $c^2 + d^2 \geq 1$ عليه فإن $\delta[(a+b_i)(c+d_i)] \geq \delta(a+b_i)$ وهكذا فإن (2) تتابع كالآتي :

ليكن $a + bi \in Z[i]$ و $c + di (\neq 0)$ في $Z[i]$ (أي أن d , c ليستا صفرين في وقت واحد) .

اعتـبر $\dfrac{a + bi}{c + di}$ هـذا عنصـر في حقـل الأعـداد المركبـة ، والآن $\dfrac{a + bi}{c + di} = p + q_i$ حيـث $p = \dfrac{ac+bd}{c^2+d^2}$ و $q = \dfrac{bc-ad}{c^2+d^2}$ هما عددان نسبيان .

يوجـد عـددان صـحيحان n , m بحيـث أن $|p - m| \leq \dfrac{1}{2}$ و $|q - n| \leq \dfrac{1}{2}$ (لاحـظ أن $p = [p] + \theta$ حيث $[p]$ هو الجزء الصحيح للعدد p و θ هو الجزء الكسري له .

إذا كان $0 \leq \theta \leq \dfrac{1}{2}$ نأخذ $m = [p]$ وإذا كان $\dfrac{1}{2} < \theta < 1$ نأخذ $m = [p] + 1$) .

ليكن $p - m = \alpha$ و $q - n = \beta$ فإن $|\alpha| \leq \dfrac{1}{2}$ و $|\beta| \leq \dfrac{1}{2}$. الآن :

$$\begin{aligned}a+bi &= (p+qi)(c+di) \\ &= (c+di)(m+d+n+\beta)i] = (c+di)[(m+ni)+\alpha+\beta i] \\ &= (m+ni)(c+di)+(c+di)(\alpha+\beta i) \\ &= (m+ni)(c+di)+v = q'(c+di)+r\end{aligned}$$

حيـــــــث $q' = m+ni \in Z[i]$ و $r = (c+di)(\alpha+\beta i)$ الآن $a+bi , c+di , m+ni \in Z[i]$ لأن $a, b, c, d, m, n \in Z$ عليه $r = (a+bi) - (m+ni\ell c+di) \in Z[i]$.

كذلك إذا كان $r \neq 0$ فإن $\alpha(r) = (c^2+d^2)(\alpha^2+\beta^2) \leq (c^2+d^2)\left(\dfrac{1}{4}+\dfrac{1}{4}\right)$

$$\Rightarrow \qquad \delta(r) \le \frac{1}{2}\left(c^2+d^2\right) < \left(c^2+d^2\right) \Rightarrow \delta(r) < d\left(c+di\right)$$

هـذا يعطـي أن $(a+bi)=q'(c+di)+r$ حيـث $r=0$ أو $\delta(r)<\delta(c+di)$ إذاً $Z[i]$ سـاحة إقليدس .

مثال 19

إذا كان F حقلاً ، فإن حلقة كثيرات الحدود $F[x]$ على F هي ساحة إقليدس $F[x]$ ساحة تامة لأن F ساحة تامة .

نعلم أن درجة كل كثيرة حدود غير صفرية هو عدد صحيح غير سالب عليه نعرف $\delta : F[x]-\{0\} \to Z$ حسب $\delta(f)=\deg f$ لكل $f \in F[x]-\{0\}$ بما أن F ساحة تامة فإن لكل $f, g \in F[x]-\{0\}$ يكون $\delta(fg)=\deg fg=\deg f+\deg g \ge \deg f=\delta(f)$ عليه فإن الشرط (2) للساحة الإقليدية قد تحقق ، وأخيراً حسب خوارزمية القسمة في $F[x]$ إذا كان $f \in F[x]$ ، $g(\ne 0) \in F[x]$ فإنه يوجد كثيرتي حدود $r \in h \in F[x]$ بحيث $f=hg+r$ حيث إما $r=0$ أو $\deg r < \deg g$ أي أنه إما $r=0$ أو $\delta(r)<\delta(g)$ لذا فإن الشرط (3) أيضاً تحقق في $F[x]$ إذاً $F[x]$ ساحة إقليدية .

نظرية 23.10

كل ساحة إقليدية هي PID .

البرهان

لتكن R ساحة إقليدية إذا كان $A \ne (0)$ مثالي في R عندئذ يوجد عنصر غير صفري $a \in A$ ضع $M=\{\delta(x) | x(\ne 0) \in A\}$ من الواضح $\delta(a) \in M$ ومن ثم فإن M مجموعة غير خالية من أعداد صحيحة غير سالبة وحسب خاصية الترتيب الحسن للأعداد

الصحيحة غير السالبة فإن M فيها أصغر عنصر . ليكن $b(\neq 0)\in A$ بحيث $\delta(b)$ هو العنصر الأصغر في M ندعي أن $A=<b>$ فمن الواضح أن $<b>\subseteq A$ والآن إذا كان $y\in A$ فإنه طالما R ساحة إقليدية فإنه يوجد عنصران $q,r\in R$ بحيث $y=qb+r$ وفيها إما $r=0$ أو $\delta(r)<\delta(b)$ والآن $r=y-qb\in A$ لأن $b\in A, y\in A$ و A مثالي في R فإذا كان $r\neq 0$ فإن $\delta(r)\geq\delta(b)$ بناء على اختيار b وهذا يتنافى مع الشرط (1) لذا فإن $r=0$.
ويكون $qb\in<b>$ وعليه $A\subseteq<b>$ وبالتالي $A=<b>$ وهكذا فإن كل مثالي في R هو مثالي رئيسي وعرضاً نكون قد أثبتنا أن $A=bR$.

وأخيراً نبين أن R لها محايد ، بما أن R نفسها مثالي في R فإنه يوجد عنصر $c\in R$ بحيث أن $R=cR$. الآن بما أن $c\in R$ فإن $c=ce$ لعنصر ما $e\in R$ عندئذ لأي $x\in R$ ، $x=cy$ لبعض $y\in R$ يؤدي ذلك إلى أن $xe=cye=cey=cy=x$ إذاً العنصر e هو المحايد في R بالتالي R هي PID .

ملاحظة (1)

لاحظ أننا أثبتنا أن كل ساحة إقليدية لها عنصر محايد .

ملاحظة (2)

عكس نظرية 23.10 غير صحيح إذ الحلقة $R=\left\{a+b\left(\frac{1+\sqrt{-19}}{2}\right) \mid a,b\in Z\right\}$ هي PID ولكنها ليست ساحة إقليدية (انظر ملحق 1) .

مسائل

1. اثبت أن الحلقات الآتية هي ساحات إقليدية :

(i) $Z\left[\sqrt{2}\right]=\left\{a+b\sqrt{2}\middle|a,b\in Z\right\}$.

(i) $Z\left[\sqrt{-2}\right]=\left\{a+b\sqrt{-2}\middle|\, a,b\in Z\right\}$.

(iii) $Z\left[\sqrt{3}\right]=\left\{a+b\sqrt{3}\middle|\, a,b\in Z\right\}$.

2. اثبت أن $Z\left[\sqrt{-5}\right]=\left\{a+b\sqrt{-5}\middle|\, a,b\in Z\right\}$ ليست ساحة إقليدية .

إرشاد : استخدم حقيقة أن كل ساحة إقليدية هي PID .

3. بدون استخدام نظرية 17.10 اثبت أن كل عنصرين غير صفريين b,a في ساحة إقليدية يكون لهما HCF .

إرشاد : اعتبر المجموعة $\left\{M=\left\{\lambda a+\mu b\middle|\lambda,\mu\in D\right\}\right.$ وبين أنها مثالي رئيسي .

4. اثبت أن عنصراً غير صفري a في ساحة إقليدية D يكون وحدة إذا وفقط إذا كان $\delta(a)=\delta(1)$.

5. لتكن D ساحة إقليدية . اثبت :

i. $\delta(a')=\delta(-a)$ لكل $a(\neq 0)\in D$.

ii. إذا كان a عنصر غير صفري في D بحيث $\delta(a)=0$ فإن a وحدة .

6. (a) إذا كان a,b عنصران غير صفريان في ساحة إقليدية ، برهن ما يأتي :

(1) إذا كان b,a مترافقان فإن $\delta(a)=\delta(b)$.

(2) إذا كان $a \mid b$ و $\delta(a)=\delta(b)$ فإن b,a مترافقان .

(3) $\delta(ab)>\delta(b)$ إذا وفقط إذا كان a غير وحدة .

(b) أعط مثالاً لعنصرين a,b بحيث $\delta(a)=\delta(b)$ ولكن b,a غير مترافقين .

7. أثبت ما يلي في ساحة إقليدية D :

i. إذا كان $a(\neq 0)\in D$ وحدة ، فإن $a=p_1p_2...p_n$ حاصل ضرب عناصر أولية.

ii. إذا كان $a=p_1p_2...p_n=q_1q_2..q_m$ هما تمثيلين للعنصر a كضرب عناصر أولية ، أثبت أن $n=m$ وأنه يوجد تبديل σ للمجموعة $\{1,2,...,n\}$ بحيث $p_i \sim q_{\sigma(i)}$ لقيم $i=1,2,...,n$.

إرشاد : استخدم الاستنتاج على $\delta(a)$.

8. إذا كان D ساحة إقليدية ، أثبت أن لكل عدد صحيح n يحقق $\delta 1+n\geq 0$ فإن الدالة $f_n : d-\{0\}\to Z$ المعرفة بالصورة $f_i(a)=\delta(a)\sim$ هي تقييم ساحة إقليدية على D.

9. إذا كان n عدداً صحيحاً موجباً وعرفنا $\delta(a)=|a|^n$ لجميع $a(\neq 0)$ في Z فاثبت أن δ هو تقييم إقليدي على Z .

10. أثبت أنه لأي مثالي فعلي A في الحلقة $Z[i]$ فإن حلقة القسمة $Z[i] \mid A$ حلقة منتهية.

11. لتكن R ساحة إقليدية و a,b عنصران غير صفريين في R نعلم أنه يوجد q,r في R بحيث أن $a=bq+r$ وفيها إما $r=0$ أو $\delta(r)<d(b)$ أثبت أن لجميع أزواج العناصر غير الصفرية a,b في R يكون r,q وحيدان إذا وفقط إذا كان لجميع العناصر غير الصفرية :

$x, y \in R$

$x+y\neq 0$

يؤدي إلى أن $\delta(x+y)\leq \max\{\delta(x),\delta(y)\}$

[إرشاد : إذا كان $\{\delta(x), \delta(y)\} > \max\{\delta(x), \delta(y)\}$ ، يمكن كتابة $x = 1(x + y) - y$ و $x = \circ(x + y) + x$] .

12. لتكن R ساحة إقليدية و δ تقييم إقليدي لـ R ولتكن $F = \{a \in R | \delta(a) = \delta(1) \cup \{0\}\}$ إذا كانت F مغلقة تحت عملية الجمع . أثبت أن F حقل جزئي في R .

3- ساحات التحليل الوحيد

النظرية الأساسية للحساب تبين أن كل عدد صحيح أكبر من 1 يمكن التعبير عنه كحاصل ضرب عدد منته في الأعداد الأولية وأن هذا التعبير وحيد بغض النظر عن الترتيب، ينطوي العمل في هذا البند على دراسة تلك الحلقات التي لها خاصية مقابلة للنظرية الأساسية للحساب .

تعريف 24.10

يقال لساحة تامة بعنصر محايد أنها ساحة تحليل وحيد (UFD) أو ساحة جاوسية إذا كان :

1. كل عنصر غير صفري غير وحدة a في R يمكن كتابته كحاصل ضرب عدد منته من العناصر غير القابلة للتحليل في R .
2. إذا كان $a = p_1p_2...p_r$ و $a = q_1q_2..q_s$ تعبيرين (تحليلين) للعنصر a كحاصل ضرب عناصر غير قابلة للتحليل ، فإن $r = s$ ويوجد تبديل δ للمجموعة $\{1, 2, 3, ..., r\}$ بحيث يكون p_i مرافقاً لـ $q \sim (i)$ لكل $i = 1, 2, ..., r$ (أي إنه يوجد تناظر أحادي بين العناصر p_i ومجموعة عناصر q_j بحيث يكون العنصران المتقابلان مترافقين) .

عليه فإن الشرطين (1) و (2) يبينان أنه في (UFD) كل عنصر غير صفري وغير وحده يمكن التعبير عنه كحاصل ضرب عناصر غير قابلة للتحليل وهذا التعبير وحيد غير الترتيب والترافق ، يمكن أن نؤكد أن أي تعبيرين لعنصر غير صفري وغير بوحده كحاصل ضرب عناصر غير قابلة للتحليل يكونان متكافئين ساحة تحليل وحيد .

مثال 20

الحلقة Z هي ساحة تحليل وحيد (UFD) لأن كل عدد صحيح يختلف عن $1, 0, -1$ يمكن التعبير عنه كحاصل ضرب عدد منته من الأعداد الأولية وهذا التعبير وحيد

بعيداً عن الترتيب والإشارة (لاحظ أن الأعداد الأولية في Z ما هي إلا عناصر غير قابلة للتحليل وسوالبها أيضاً أعداد غير قابلة للتحليل أي أن $3,-3$ كلاهما غير قابل للتحليل .

مثال 21

كل حقل هو ساحة ذات تحليل وحيد (UFD) لأنه خلاف ذلك نجد عنصراً غير صفري وغير بوحدة في F لا يمكن التعبير عنه كحاصل ضرب عناصر غير قابلة للتحليل، ولكن في الحقل لا يوجد عنصر غير صفري ليس بوحدة . إذاً F هو ساحة تحليل وحيد UFD .

قضية 23.10

في ساحة التحليل الوحيد (UFD) كل عنصر غير قابل للتحليل يكون أولياً .

البرهان

ليكن R ساحة تحليل وحيد (UFD) و p عنصر غير قابل للتحليل في R . افرض أن $p \mid ab$ لبعض العناصر a,b في R فيكون $ab = cp$ لعنصر $c \in R$ ، بما أن $p \neq 0$ و p ليس بوحدة فإن واحدة على الأقل من بين b,a ليس بوحدة . ليكن a وحدة فيكون a^{-1} موجوداً و $b = cpa^{-1}$ وهذا يعطي $p \mid b$. وبالمثل إذا كان b وحدة فإن $p \mid a$ وبفرض كلاً من b,a ليس وحدة فإنه يمكن كتابة :

$$a = p_1 p_2 \ldots p_n , b = q_1 q_2 .. q_m$$

كحاصل ضرب عناصر غير قابلة للتحليل فإذا كان c وحدة كان ab مرافقاً للعنصر p وبالتالي فهو غير قابل للتحليل . هذا بدوره يؤدي على أنه إما a وحدة أو b وحدة ، وهذا تناقض . إذاً c ليس بوحدة ، عليه يمكن كتابة $c = r_1 r_2 .. r_s$ كحاصل ضرب عناصر غير قابلة للتحليل ونتيجة لذلك نحصل على أن $p_1 p_2 \ldots p_n q_1 q_2 .. q_m = r_1 r_2 .. r_s p$

وهـذه المعادلـة تبـين أنـه إمـا أن p مرافـق لأحـد p_i أو لأحـد q_i وعليـه فـإن $p \mid a$ أو $p \mid b$. إذاً في من الحالتين فإما $p \mid a$ أو $p \mid b$ إذن p عنصر أولي .

ملاحظة

رأينـا في مثـال 6 أن 3 عنصـر غـير قابـل للتحليـل في $Z\left[\sqrt{-5}\right]$ ولكنـه لـيس عنصـراً أولياً، وعلى ضوء النتيجة السابقة التي بُرهنت نحصل على أن $Z\left[\sqrt{-5}\right]$ ليس ساحة تحليل وحيد (UFD) .

قضية 26.10

في أي حلقـة R اتحـاد أي سلسـلة تصـاعدية مـن المثاليـات $A \subseteq A_2 \subseteq A_3 \subseteq \ldots \subseteq A_n \subseteq \ldots$ هو مثالي في R .

البرهان

ضـع $A = \bigcup_i A_i$ بمـا أن $A_i \subseteq A$ لكـل i فـإن A مجموعـة غـير خاليـة ، لـيكن $r \in R, a, b \in A$ فإن $a \in A_i, b \in A_j$ لبعض i, j . الآن إمـا $i \le j$ أو $j \le i$ وتحديداً نفرض أن $i \le j$. بما أن $A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots$ فإن $A_i \subseteq A_j$ بالتالي يكون $a, b \in A_j$ هذا يؤدي إلى أن $a - b \in A_j$ ، $ar \in A_j$ ، $ra \in A_j$ لأن A_j مثـالي في R . إذاً $a - b \in A$ ، $ar \in A$ ، $ra \in A$ لأن $A_j \subseteq A$ ويكون A مثالياً في R .

قضية 27.10

في سـاحة مثاليـات رئيسـة (PID) لكـل سلسـلة تصـاعدية مـن المثاليـات $A_1 \subseteq A_2 \subseteq A_3 \in \ldots \subseteq A_n \subseteq \ldots$ يوجد عدد صحيح t يحقق $A_m = A_t$ لكل $t \le m$.

البرهان

ليكن $A = \underset{i}{U} A_i$ فمن قضية 26.10 يكون A مثاليان في R ولأن R هي PID فإن $A =< a >$ لبعض $a \in A$ الأن $a \in A_t$ لبعض t ، بالتالي يكون $A =< a >\subseteq A_t$ ، لذا فإن لكل عدد صحيح $m \geq t$ يكون $A \subseteq A_t \subseteq A_m \subseteq A$ يؤدي إلى أن $A_m = A_t$ بالتالي القضية محققة .

قضية 28.10

لكل عنصر a غير صفري وليس بوحدة R في ساحة مثاليات رئيسة PID يوجد عنصر غير قابل للتحليل p بحيث p/a .

البرهان

ليكن a عنصراً غير صفري وليس بوحدة في الحلقة R والتي هي (PID) اعتبر المثالي $I_1 =< a >$ إذا كان I_1 أعظمي فإن a غير قابل للتحليل (نظرية 13.10) ولا يوجد شيء للإثبات إذا كان I_i مثالي غير أعظمي ، فإنه يوجد مثالي I_2 للحلقة R بحيث $I_1 \subset I_2 \subset R$ إذا كان I_2 مثالي أعظمي فإنه يتولد بعنصر غير قابل للتحليل وليكن p_1 هذا يعطي

$$I_1 =< a >\subset I_2 =< p_1 \Rightarrow p_1 \mid a$$

وبهذا تحقق بالمطلوب ، ... ذلك يمكن إيجاد مثالي I_3 للحلقة R بحيث $I_1 \subset I_2 \subset I_3 \subset R$ بالتالي I_n يولد بعنصر غير قابل للتحليل وليكن p هذا يؤدي إلى أن :

$$I_1 =< a >\subset I_n =< p >\Rightarrow p \mid a$$

وبهذا تتحقق القضية .

نظرية 29.10

كل ساحة مثاليات رئيسة (PID) هي ساحة تحليل وحيد (UFD) .

البرهان

ليكن a عنصراً غير صفري وليس بوحدة في الحلقة R والتي هي PID يوجد عنصر غير قابل للتحليل p_1 وهو أيضاً أولي لعنصر ما (حسب نظرية 12.10) بحيث p_1 / a أي أن $a = a_1 p_1$ لعنصر ما $a_1 \in R$ عليه يكون $< a > \subseteq < a_1 >$ إذا كان $< a_1 > = < a >$ فإن $a_1 = ar$ لعنصر ما $r \in R$ وبالتالي $a = arp_1 \Rightarrow rp_1 = 1$ هذا يؤدي إلى أن p_1 وحدة ، وذلك لا يجوز لأن p_1 عنصر غير قابل للتحليل .

ومن ثم فإن $< a > \subset < a_1 >$ الآن إذا كان a_1 وحدة فإن a مرافق لعنصر غير قابل للتحليل بالتالي فإنه غير قابل للتحليل ولا يوجد شيء للبرهان .

أما إذا كان a_1 ليس بوحدة ، فإنه يوجد عنصر غير قابل للتحليل p_2 بحيث أن $p_2 \mid a_2$ أي أن $a_1 = a_2 p_2$ لعنصر ما $a_2 \in R$ هذا يعطي أن $a = a_2 p_1 p_2$ و $< a > \subset > a_2 >$.

إذا كان a_2 وحدة فإننا نتوقف ، وإذا لم يكن a_2 وحدة يمكن قبل السابق كتابة $a_2 = a_3 p_3$ لعنصر ما غير قابل للتحليل p_3 عنصر آخر a_3 غير وحدة في R فيكون للمرة الثانية $< a_2 > \subset < a_3 >$ بهذه الطريقة نحصل على سلسلة تصاعدية فعلية من المثاليات $< a > \subset < a_1 > \subset < a_2 > \subset < a_3 > \subset \ldots$ وهي سلسلة في ساحة مثاليات رئيسة (PID) يجب أن تكون منتهية (قضية 27.10) .

إذن لعددها n فإن a_{n+1} يجب أن يكون وحدة لأن $a_n = a_{n+1}\, q_{n+1}$ لعنصر غير قابل للتحليل q_{n+1} في R فيجب أن يكون a_n نفسه غير قابل للتحليل إذاً :

$$a = a_1 p_1, a_1 = a_2 p_2 , \ldots a_{n-1} = p_n a_n = p_n p_{n+1}$$

حيث $a_n = p_{n+1}$ هذا يعطي أن :

$$a = p_1 p_2 \ldots p_{n+1} \qquad (1)$$

وهو حاصل ضرب عدد منته من العناصر غير القابلة للتحليل ، إذاً كل عنصر غير صفري وغير وحدة يمكن التعبير عنه كحاصل ضرب عدد منته من العناصر غير القابلة للتحليل .

افرض أن :

$$a = q_1 q_2 .. q_m \qquad (2)$$

هو تعبير آخر للعنصر a كحاصل ضرب عدد منته من العناصر غير القابلة للتحليل ، نحاول أن نبين أن الشرطين (1) و (2) متكافئان ، لذا نطبق الاستنتاج على $n+1$.

لاحظ إنه عندما $n=0$ النتيجة متحققة ببساطة ، نفرض أن النتيجة متحققة لجميع العناصر غير الصفرية والتي هي ليست وحدة ، ويمكن التعبير عنها كحاصل ضرب عناصر غير قابلة للتحليل عددها أقل من $n+1$. الآن في (2) فإن $a_1 \mid a \Rightarrow a_1 \mid p_1 p_2 ... p_{n+1}$.

بما أن كل عنصر غير قابل للتحليل (PID) هو أولي فإننا نحصل على أن $q_1 \mid p_i$ لبعض i ، بما أن p_i غير قابل للتحليل فيكون لدينا $q_1 = u_i p_i$ لوحدة ما i بإعادة ترتيب الدليل للعناصر p_i يمكن فرض $i=1$ عندئذ من (1) و (2) ينتج أن :

$$p_1 p_2 p_3 ... p_{n+1} = u_1 p_1 q_2 .. q_m \Rightarrow p_2 p_3 ... p_{n+1} = q'_2 q'_3 .. q'_m$$

حيث $q'_2 = u_1 q_2$ و $q'_i = q_i$ لكل $i \geq 3$.

إذا وضعنا $b = p_2 p_3 ... p_{n+1}$ فإننا نرى أن :

$$b = p_2 p_3 ... p_{n+1} \qquad (3)$$

$$b = q'_2 q'_3 .. q'_m \qquad (4)$$

تعبيرات للعنصر b كحاصل ضرب عناصر غير قابلة للتحليل ، وإن (3) لها حدود عددها n ، بما أن $n < n+1$ فإن فروض الاستنتاج تعطي أن $n = m-1$ أي أن $n+1 = m$ ويوجد تناظر أحادي بين العناصر $p_i \; (i = 2, ..., n+1)$ والعناصر $q'_j \; (j = 2, 3, ..., n+1)$ بحيث تكون العناصر المتناظرة مترافقة ، حيث أنه كما رأينا من قبل أن $q1 = u_1 p_1$ حيث u_1 وحدة فإن q_1 هو أيضاً مرافق p_1 .

في (1) و (2) ينتج أن عدد العوامل فيهما متساوي ويوجد تناظر أحادي بين العناصر p_i , q_j بحيث تكون العناصر المتقابلة مترافقة ، هذا يثبت النظرية .

بما أن كل ساحة إقليدية هي ساحة مثاليات رئيسة (PID) فإننا نحصل على النتيجة التالية :

نتيجة 30.10

كل ساحة إقليدية هي ساحة تحليل وحيد (UFD) .

بما أنه لكل حقل F تكون حلقة كثيرات الحدود $F(x)$ وحلقة الأعداد الجاوسية كلتاهما PID فمن النظرية السابقة نحصل على أن كلها ساحة تحليل وحيد (UFD) .

قضية 31.10

في (UFD) كل زوج من العناصر غير الصفرية لهما عامل مشترك أكبر (HCF) و (LCM) مضاعف مشترك أصغر .

البرهان

ليكن R هو UFD و $a,b\in R$ عنصران غير صفريين ، اعتبر الحالة عندما يكون واحداً من a,b وحدة وليكن a مثلاً ، بما أنه يوجد a^{-1} و $b=aa^{-1}b$ فإن $a \mid b$ بالتالي a هو عامل مشترك أكبر (HCF) و b هو مضاعف مشترك أصغر LCM للعنصرين b,a .

لذا نفرض أن كلاً من b,a ليس بوحدة ، نفرض أن p عنصر غير قابل للتحليل بحيث يكون $q \mid a$ عنصر غير قابل للتحليل بحيث $q \mid b$ فإذا كان q مرافق لـ p فإن $q=wp$ لعنصر وحدة $w\in R$ ، عندئذ يكون $p=w^{-1}q$ ويكون $p \mid b$ فإذا كان p لا يقسم b فإنه على الأقل $b \mid p^0 = 1$ وتأخذ هذا بعين الاعتبار يمكن كتابة :

$$a = up_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \qquad (1)$$

$$b = vp_1^{\beta 1} p_2^{\beta 2} \ldots p_k^{\beta_k} \qquad (2)$$

لعنصرين كلاهما وحدة $u,v\in R$ (على سبيل المثال في Z ، $2=1.2^1.3^0$ و $-3=(-1)(2^0).3^1$) لأي عنصر d فإن $d \mid a$ إذا وفقط إذا كان $d = wp_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\delta_k}$

لعنصر وحدة w ، $0 \le \delta_i \le \alpha_i$ ، $1 \le i \le k$ بأخذ هذا بعين الاعتبار يمكن بسهولة التحقق من أنه إذا كان $\lambda_i = \min(\alpha_i, \beta_i)$ ، $\mu_i = \max(\alpha_i, \beta_i)$ فإن $c = p_1^{\lambda_1} p_1^{\lambda_2} p_3^{\lambda_3} .. \lambda_k^{\lambda_k}$ هو عامل مشترك أكبر (HCF) للعنصرين b, a و $d = p_1^{\mu_1} p_2^{\mu_2} ... p_k^{\mu_k}$ هو مضاعف مشترك أصغر (LCM) للعنصرين b, a .

قضية 32.10

أي عدد منته في العناصر غير الصفرية $a_1, a_2, ..., a_n$ في ساحة تحليل وحيد (UFD) لها HCF و LCM .

قضية 32.10

أي عدد منته من العناصر غير الصفرية $a_1, a_2, ..., a_n$ في ساحة تحليل وحيد UFD لها (HCF) و (LCM) .

الآن ندرس حلقة كثيرات الحدود على ساحة ذات تحليل وحيد (UFD) ونبرهن عدداً من النتائج في صور قضايا ونظريات وهي بحد ذاتها لها أهمية كبيرة .

تعريف 33.10

لتكن R ساحة تحليل وحيد(UFD) و $f = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ كثيرة حدود غير صفرية في $R[x]$ إذا كان d هو عامل مشترك أكبر (HCF) للمعاملات $a_0, a_1, a_2, ..., a_n$ في كثيرة الحدود f فإن المثالي dR يسمى سعة f ويرمز بـ $c(f)$.

لاحظ أن $c(f)$ وحيد لأنه إذا كان d' أي عامل مشترك أكبر HCF آخر للعناصر $a_0, a_1, a_2, ..., a_n$ فإن d' يكون مرافقاً لـ d ويكون $d' = d_n$ لوجود $u \in R$ هذا

يعطي $d'R = duR = dR$ لأن $uR = R$ إذاً $c(R)$ وحيد . لاحظ كذلك أنه إذا كان a عنصراً يقسم كل معامل في f فإن a/d حيث d هو عامل مشترك أكبر (HCF) لمعاملات f .

ملاحظة

بعض المؤلفين يعرف أي عامل مشترك أكبر (HCF) لمعاملات كثيرة الحدود بأنه سعتها . بما أن العامل المشترك الأكبر (HCF) ليس وحيداً ، فهذا التعريف لا يعطي عنصراً واحداً ، في الحقيقة في الأعمال الحديثة فإن التعريف السابق ذائع الانتشار .

تعريف 34.10

ليكن R هو UFD فإن كثيرة الحدود غير الصفرية $f \in R[x]$ يقال أنها كثيرة حدود بدائية إذا كان HCF لمعاملاتها هو وحدة .

الآن ليكن $d \in R$ فإن $dR = R$ إذا وفقط إذا كان له وحدة ، عليه يمكننا القول أن كثيرة الحدود $f \in R(x)$ تكون بدائية إذا وفقط إذا كان $c(f) = R$.

مثال 22

إذا كان $f = 2 + 6x + 10x^2 + 18x^3 \in Z[x]$ ، فإن $c(f) = E$ مجموعة جميع الأعداد الزوجية ، بما أن $E \neq Z$ فإن f ليس بدائية (لاحظ أن (HCF) للأعداد $2,6,10,18$ يساوي 2 وهو ليس وحدة في Z .

مثال 23

في $Z[x]$ كثيرة الحدود $g = 3 + 5x + 4x^3 + 15x^4$ بدائية لأن (HCF) للأعداد $15,4,5,3$ هو 1 .

قضية 35.10

إذا كان R هو ساحة غير وحيدة (UFD) فإن كل كثيرة حدود غير صفرية في $R[x]$ عبارة عن حاصل ضرب كثيرة حدود بدائية على R وعنصر في R .

البرهان

لتكن $f=a_0+a_1x+a_2x^2+..a_nx^u$ كثيرة حدود غير صفرية في $R[x]$ حيث R هو ساحة تحليل وحيد (UFD) إذا كان d هو عامل مشترك أكبر (HCF) للعناصر $a_0,a_1,a_2,...,a_n$ في R فإن $a_i=db_i$ لبعض $b_i\in R$ لكل $i=1,2,...,n$ بما أن d هو عامل مشترك أكبر (HCF) للعناصر $a_0,a_1,..a_m$ هو 1 (HCF) للعناصر $b_0,b_1,...,b_n$ هذا يبرهن أن $f=d(b_0+b_1x+b_2x^2+...+b_nx^n)=d$ حيث $g=b_0+b_1x+..b_nx^n$ و HCF للعناصر $b_0,b_1,b_2,...,b_n$ هو 1 إذاً g وبذا نتثبت القضية .

نظرية 36.10 (جاوس)

حاصل ضرب كثيرتي حدود بدائي على ساحة تحليل وحيد (UFD) هي كثيرة حدود بدائية .

البرهان

ليكن R هو ساحة تحليل وحيد (UFD) ولنفرض أن :

$$f=a_0+a_1x+a_2x^2+...+a_nx^n \qquad (1)$$

$$g=b_0+b_1x+b_2x^2+...+b_mx^m \qquad (2)$$

هما كثيرتي حدود بدائيتان على R فإن :

$$fg=c_0+c_1x+c_2x^2+...+c_{m+n}x^{m+n} \qquad (3)$$

حيث $c_k=\sum_{i+j=k}a_ib_j$ عندما $0\le k\le m+n$.

إذا كان $d=(c_0,c_1,c_2,...,c_{n+m})$ عنصراً ليس بوحدة فإنه يوجد عنصر غير قابل للتحليل p بحيث $p\mid d$ من الواضح أن $p\mid c_k$ لكل k .

بما أن (HCF) للعناصر $a_0, a_1, a_2, ..., a_n$ ليس وحدة (لأن f بدائية) فإن p لا يمكن أن يقسم جميع a_i ليكن t أصغر ترقيم بحيث $p \nmid a_t$ بالمثل يكون u أصغر ترقيم بحيث $p \nmid b_u$.

اعتبر :

$$c_{t+u} = (a_0 b_{t+u} + a_1 b_{t+u-1} + ... + a_{t-1} b_{u+1})$$
$$+ a_t b_u + (a_{t+1} b_{u-1} + a_{t+2} b_{u-2} + ... + a_{t+1} b_0) \qquad (4)$$

حسب اختيارنا فإن $p \mid a_0, p \mid a_\mu, p \mid a_2, ..., p \mid a_{t-1}$

هذا يؤدي إلى أن $p \mid ca_0 b_t + a_1 b_{t+u-1} + ... + a_{t-1} b_{u+1}$ بالمثل:

$$p \mid a_{t+1} b_{u-1} + a_{t+2} b_{u-2} + ... + a_{t+u} b_0$$

وبما أنه أيضاً $p \mid c_{t+4}$ ، (4) يعطي $p \mid a_t b_n$ فهذا يؤدي إلى أن $p \mid a_t$ أو $p \mid b_u$ لأن u عدد أولي (قضية 25.10) وهذا تناقض ، إذاً fg بدائية .

نتيجة 37.10

لكثيرتي حدود غير صفريتين f و g على UFD فإن $c(fg) = c(f)c(g)$.

البرهان

ليكن R هو ساحة تحليل وحيد (UFD) و $f, g \in R[x]$ كثيرتي حدود غير صفريتين إذا كان كل من d', d عامل مشترك أكبر (HCF) لمعاملات f و g على الترتيب فإن :

$$f = df_1 \qquad (1)$$

و $g = d'$ حيث g_1, f_1 وكثيرتي حدود بدائيتان $c(g) = d'R, c(f) = dR$ وبالتالي $fg = (dd')f_1 g_1$ الآن ولأن $f_1 g_1$ بدائيتان (نظرية 36.10) فإن dd' هو HCF لمعاملات fg بالتالي $c(fg) = dd'R = (dR)(d'R) = c(f)c(g)$ لأن R إبدالية .

ملاحظة

النتيجة السابقة تعطي على الفور أنه إذا كان $f = gh$ واحدة من h, g ليس بدائية فإن f ليست بدائية .

تعريف 38.10

لتكن R ساحة تامة لعنصر محايد يقال لكثيرة الحدود f ذات الدرجة الموجبة أنها كثيرة حدود غير قابلة للتحليل على R إذا لم نقدر على التعبير عنها كحاصل ضرب كثيرتي حدود أخرتان على R كلتاهما درجتها موجبة ، أية كثيرة حدود درجتها موجبة إذا لم تكن غير قابلة للتحليل فإنه يقال عنها قابلة للتحليل .
وبوضوح أية كثيرة حدود ذات درجة تساوي 1 على ساحة تامة R تكون غير قابلة للتحليل على R .

مثال 24

x^2+1 ، x^2-2 ، x^2+x+1 جميعها غير قابلة للتحليل في $Z[x]$.

مثال 25

x^2+3 غير قابلة للتحليل في $R[x]$.

مثال 26

x^2+1 قابلة للتحليل في $c[x]$ حيث $(x+i)(x-i) = x^2+1$ لأن $i = \sqrt{-1} \in c$.

قضية 39.10

لأية ساحة تامة R بمحايد الوحدات في $R[x]$ هي بدقة وحدات R .

البرهان

من الواضح أن الوحدة في R هي وحدة في $R[x]$ لأن $R \subseteq R[x]$ ولهما نفس المحايد .

بالعكس افرض أن $f \in R[x]$ وحدة في $R[x]$ فإنه يوجد $g \in R[x]$ بحيث أن $fg=1$ هذا يؤدي إلى أن $\deg f + \deg g = 0 \Rightarrow \deg f = \deg g = 0$ يؤدي إلى أن g,f كثيرتي حدود ثابتتين ، عليه فإن f وحدة في R وبهذا نثبت القضية .

قضية 40.10

إذا كان R هو ساحة تحليل وحيد (UFD) فإن $f \in R[x]$ عنصر غير قابل للتحليل إذا وفقط إذا كان إما f عنصر غير قابل للتحليل في R أو f عنصر بدائي غير قابل للتحليل في $R[x]$.

ملحوظة

ننصح القارئ أن يستحضر في ذهنه الفرق بين عنصر غير قابل للتحليل في $R[x]$ وبين كثيرة حدود غير قابلة للتحليل في $R[x]$.

البرهان

ليكن $f \in R[x]$ عنصراً غير قابل للتحليل إذا كان $f \in R$ من البديهي أن f عنصر غير قابل للتحليل في R ، وإذا كان $f \notin R$ فنفرض أن $f = gh$ لبعض العناصر $g,h \in R[x]$. بما أن f عنصر غير قابل للتحليل في $R[x]$ فواحدة من b,g يجب أن تكون وحدة في $R[x]$ لذا فإن واحدة من h,g يجب أن تنتمي إلى R (قضية 39.10). ويكون $\deg g = 0$ أو $\deg h = 0$ هذا يعني أن f كثيرة حدود غير قابلة للتحليل في $R[x]$

ولأن $f=df_1$ حيث $d\in R$ و f_1 كثيرة حدود بدائية (قضية 35.10) و $\deg f_1=\deg f>0$
فإن f_1 ليست وحدة وتكون d هي الوحدة وبالتالي تكون f بدائية.

بالعكس أي عنصر غير قابل للتحليل في R هو عنصر غير قابل للتحليل في $R[x]$
لتكن f كثيرة حدود بدائية غير قابلة للتحليل في $R[x]$ وليكن $f=gh$ لبعض $g,h\in R[x]$
بما أن f كثيرة حدود غير قابلة للتحليل فإن إما $\deg g=0$ أو $\deg h=0$ وللتحديد ضع
$\deg g=0$ عندئذ $g=\alpha(\neq 0)\in R$ وعليه $f=\alpha h$.
بما أن $c(f)=1R$ فإننا نحصل على أن $\alpha/1$ إذاً α وحدة في R وعليه في $R[x]$ هذا يعطي
أن f عنصر غير قابل للتحليل في $R[x]$.

ملاحظة

ليكن k حقل القواسم لساحة تامة R اعتبر أن أي عنصر y في الحلقة السائدة
على k إذا كان y متسامياً مع R ولبيان ذلك اعتبر كثيرة الحدود غير الصفرية
$(a_n\neq 0)$, $f=a_0+a_1y+\dots+a_ny^n$ والأمر لجميع $a_i=\dfrac{c_i}{d_i}, i=0,1,2,\dots,n$ لبعض
$c_i,d_i\in R$ حيث $d_i\neq 0$ ضع $d=d_0d_1d_2..d_n$ فيكون :

$$df=da_0+da_1y+\dots+da_iy^i+\dots+da_ny^n$$

كما أنه لأي $i=0,1,2,\dots,n$ يكون :

$$da_i=d_0d_1..d_i\frac{c_i}{d_i}=d_0d_1..d_{i-1}d_{i+1}..d_nc_i\in R$$

عليه $df(y)\in R[y]$ فإذا كان $f(y)=0$ فإن $df(y)=0$ لأن y متسام على R ،
$df(y)\neq 0$ إذن $f(y)\neq 0$ أي أن y متسام على k .

ملاحظة

عندما يكون R حقلاً فطالما أن أي عنصر غير صفري في R هو وحدة ، فإنه لا يمكن أن يكون عنصراً غير قابل للتحليل ، والقضية السابقة تعطي أن العناصر غير القابلة للتحليل في $R[x]$ هي بالضبط كثيرات الحدود غير القابلة للتحليل في $R[x]$.

قضية 41.10

إذا كان R هو UFD و k حقل قواسمها ، فإن كثيرة الحدود البدائية غير القابلة للتحليل في $R[x]$ هي أيضاً كثيرة حدود غير قابلة للتحليل في $k[x]$.

البرهان

افرض f كثيرة حدود بدائية غير قابلة للتحليل في $R[x]$ حيث R هي (UFD) افرض كذلك أن $f=gh$ لبعض العناصر h,g في $k[x]$ حيث $\deg g>0$ و $\deg h>0$ بما أن k هو حقل قواسم R فإنه يوجد عنصران غير صفريان d,d' في R بحيث يكون $d'h,dg$ كلاهما في $R[x]$ (انظر ملاحظة 1) . هذا يعطي أن $dd'f=(dg)(d'h)$.

والآن $dg=\alpha g_1$ و $d'h=\beta h$ حيث h_1,g_1 كثيرتي حدود بدائيتان في $R[x]$ و $\alpha,\beta\in R$.

عندئذ $dd'f=(\alpha\beta)g_1h_1$ حيث f و g_1h_1 بدائيتان في $R[x]$ ، هذا يؤدي إلى $udd'=\alpha\beta$ لوحدة u في R كما يؤدي إلى أن $f=ug_1h_1$ على أية حال f كثيرة حدود غير قابلة للتحليل في $R[x]$ فإما أن $\deg ug_1=0$ أو $\deg h_1=0$ ولكن $\deg ug_1=\deg g>0$ و $\deg h_1=\deg h>0$ وبهذا انتهينا إلى تناقض .

ملاحظة

على ضوء ملاحظة 2 المذكورة قبل القضية السابقة ، يمكننا القول أن كل كثيرة حدود بدائية غير قابلة للتحليل في $R[x]$ هي عنصر غير قابل للتحليل في $k[x]$ حيث k حقل قواسم R و R هي ساحة تحليل وحيد UFD ساحة تحليل وحيد .

قضية 42.10

إذا كان R هو UFD و k حقل قواسمها ، فإن :

1. كل عنصر غير قابل للتحليل في R هو عنصر أولي في $R[x]$.
2. إذا كان f كثيرة حدود بدائية في $R[x]$ و $h \in R[x]$ بحيث f / h في $K[x]$ فإن $f \mid h$ في $R[x]$.

البرهان

1. خذ p عنصراً غير قابل للتحليل في R و f و كثيرتي حدود غير صفريتين في $R[x]$ بحيث يكون $p \mid fg$ في $R[x]$ فيكون $fg = ph$ لكثيرتي حدود $h \in R[x]$.

الآن افـــرض أن $c(f) = dR$ ، $c(g) = d'R$ و $c(h) = \ell R$ لـــبعض العناصــــر $d, d', \ell' \in R$ ، فيكـــون $f = df_1$ ، $g = dg_1$ و $h = \ell h_1$ حيـــث f_1, g_1, h_1 كثـــيرات حـــدود بدائية في $R[x]$ عندئذ يكون $fg = ph \Rightarrow dd'f_1 g_1 = p\ell g_1 \Rightarrow dd'R = p\ell R$

لأن $c(fg) = dd'$ و $c(ph) = p\ell R$ وهذا بدوره يؤدي إلى أن $dd' = p\ell u$ لوحدة $u \in R$ وهذا بـدوره يـؤدي إلى أن $p \mid dd'$ في R وحيـث أن كـل عنصـر غـير قابـل للتحليـل في R هـو عنصـــر أولي فنحصـــل علـــى أن $p \mid d$ أو $p \mid d'$ في R ونفـــس الشـــيء يتحقـــق في $R[x]$. مـــن جهـــة أخـــرى $d \mid f$ و $d' \mid g$ في $R[x]$ بالتـــالي فـــإن $p \mid f$ أو $p \mid g$ في $R[x]$ وهذا يبرهن أن p عنصر أولي في $R[x]$.

2. بما أن $f \mid h$ في $K[x]$ فإنه يوجد $g \in K[x]$ بحيث $h = fg$ ولأن K هـو حقـل قواسـم R فإنه يوجد $d(\neq 0) \in R$ بحيث يكون $dg \in R[x]$.

إذاً $dh = dfg$ ، الآن يمكـن كتابـة $h = \alpha h_1$ و $dg = \beta g_1$ حيـث $\alpha, \beta \in R$ و h_1, g_1 كثـيرتي حدود بدائيتان في $R[x]$ ، هذا يعطي أن $d\alpha h_1 = f\beta g1 = \beta(fg_1)$ وحيث أن fg_1, h_1 كثيرتي

حدود بدائيتان في $R[x]$ ، $\beta , d\alpha$ مترافقان في R فإن $\beta = d\alpha u$ لوحدة $u \in R$ كما يعطي بدوره أن $h_1 = ufg_1$ إذاً $h_1 \mid f$ في $R[x]$ ولكن $h \mid h_1$ في $R[x]$ فيكون $h \mid f$.

نتيجة 43.10

إذا كان R هي ساحة تحليل وحيد (UFD) فإن كل عنصر غير قابل للتحليل في $R[x]$ هو عنصر أولي في $R[x]$.

البرهان

ليكن $f \in R[x]$ عنصر غير قابل للتحليل فتكون إما f عنصراً غير قابل للتحليل في R أو هي كثيرة حدود بدائية في $R[x]$ (قضية 40.10) في الحالة الأولى تكون f عنصراً أولياً في $R[x]$.

(قضية 42.10) في الحالة الثانية تكون f كثيرة حدود غير قابلة للتحليل في $K[x]$ حيث K حقل قواسم R (قضية 41.10) وحيث أن k حقل و f عنصر غير قابل للتحليل في $k[x]$.

على أية حال $k[x]$ هو (PID) (نظرية 11.1) ومن ثم فإن عنصر أولي في $k[x]$.

الآن افرض أن $gh \mid f$ في $R[x]$ فيكون $gh \mid f$ في $k[x]$ ولكن يكون f عنصر أولي في $k[x]$ فإما أن يكون $g \mid f$ في $k[x]$ أو $h \mid f$ في $k[x]$ باستخدام قضية 42.10 نحصل على أنه $g \mid f$ في $R[x]$ أو $h \mid f$ في $R[x]$ إذاً f عنصر أولي في $R[x]$.

والآن أعددنا العدة لاقتحام الهدف ، النظرية الشهيرة ساحات التحليل الوحيد (UFD) .

نظرية 44.10

إذا كان R هو UFR فإن $R[x]$ هي (UFD) .

البرهان

من الواضح أن $R[x]$ ساحة تامة بعنصر محايد . نبرهن أولاً أنه كل عنصر في $R[x]$ غير صفري غير وحدة يمكن كتابته كحاصل ضرب عدد منته من العناصر غير القابلة للتحليل في $R[x]$.

افرض أن f عنصر غير صفري وليس وحدة في $R[x]$ ، فإذا كان $f \in R$ فقد انتهينا لأن R هو UFD والعناصر غير القابلة للتحليل في R هي عناصر غير قابلة للتحليل في $R[x]$ لمناقشة الحالة التي فيها $f \notin R$ أولاً نثبت يقيننا لكثيرات الحدود f في $R[x]$ ذات الدرجة الموجبة باستخدام الاستنتاج على $\deg f$.

فإذا كانت $\deg f = 1$ ، فإن كثيرة حدود بدائية غير قابلة للتحليل وعليه فهي عنصر غير قابل للتحليل في $R[x]$ نفرض $\deg f = n > 1$ وأن يقيننا صحيح لجميع كثيرات الحدود البدائية ذات الدرجة $< n$.

مرة ثانية إذا كان f غير قابلاً للتحليل نكون قد بلغنا الهدف ، وعليه نفرض أن f قابلة للتحليل ، عندئذ تكون $f = gh$ لبعض العناصر $f, g \in R[x]$ حيث $\deg g < n$ و $\deg h < n$ وحيث أن f كثيرة حدود بدائية فإن h, g هي أيضاً كثيرتي حدود بدائيتين درجة كل منهما أقل من n ، عليه حسب فروض الاستنتاج يكون كلا h, g قابلة للتعبير عنهما كحاصل ضرب عدد منته من العناصر غير القابلة للتحليل في $R[x]$ ، نتيجة لذلك يكون $f = gh$ هو عبارة عن حاصل ضرب عدد منته من العناصر غير القابلة للتحليل في $R[x]$.

أما إذا كانت f ليست بدائية يمكن كتابة $f = df_1$ حيث f_1 كثيرة حدود بدائية في $R[x]$ و d ليس وحدة في R كما لوحظ من قبل كلا f_1, d يمكن التعبير عنهما كحاصل ضرب عدد منته من العناصر غير القابلة للتحليل في $R[x]$ إذاً $R[x]$ يحقق الشرط الأول لساحة تامة بمحايد كي يكون (UFD) ساحة تحليل وحيد .

الآن افرض أن $f = f_1 f_2 ... f_m$ و $f = g_1 g_2 ... g_n$ تعبيرين لكثيرة الحدود f كحاصل ضرب عدد منته من العناصر غير القابلة للتحليل .

من $R[x]$ نطبق الاستنتاج الرياضي على m عندما $m = 1$ ، $f = f_1 = g_1 g_2 ... g_n$ بما أن $g_1 \mid f_1$ فإذا كان $1 < n$ فإن $tg_2 ... g_n = 1$ لعنصر $t \in R$ هذا يؤدي إلى أن g_n وحدة وهو ما لا يقبله عقل ، عليه $n = 1$ و $f_1 = g_1$ افرض $m > 1$ وافرض أن أي تحليلين لجميع العناصر غير الصفرية التي ليست وحدة في $R[x]$ والتي يمكن كتابتها كحاصل ضرب لعدد أقل من m العناصر غير القابلة للتحليل في $R[x]$ يكونان متكافئين .

الآن $g_1 \mid f \Rightarrow g_1 \mid f_1 f_2 ... f_m$ وحيث أن g_1 عنصر أولي في $R[x]$ (نتيجة 43.10) فإن $g_1 \mid f_1$ لبعض i .

وبما أن f_i أيضاً عنصر غير قابل للتحليل فيكون لدينا $g_1 = u_i f_i$ لوحدة u_i في $R[x]$ والذي ينتمي إلى R وبإعادة ترتيب f_i يمكن فرض أن $i = 1$.

إذاً ينتج أن $f_1 f_2 f_5 ... f_m = u_1 f_1 g_2 g_3 ... g_n \Rightarrow f_2 f_3 ... f_m = g'_2 g'_3 ... g'_n$

حيث $g'_2 = n_2 g_2$ و $g'_k = g_k$ لكل $k \geq 3$ إذا وضعنا $h = f_2 f_3 ... f_m$ فإننا نجد أن $h = f_2 f_3 ... f_m$ و $h = g'_2 g'_5 ... g'_n$ تعبيران للعنصر h كحاصل ضرب عناصر غير قابلة للتحليل وأن التحليل الأول فيه $m-1$ من العناصر غير القابلة للتحليل فينتج من فروض الاستنتاج أن التحليلين متكافئان أي أن $n-1 = m-1$ (عليه $n = m$) .

ويوجد تقابل أحادي بين العناصر $i=2,...,m, f_i$ و $j=2,...,m, g'_j$ بحيث تكون العناصر المتقابلة مترافقة .

مرة أخرى حيث أن $g_1 = u_1 f_1$ و u_1 وحدة ، g_1 مرافق لـ f_1 ، إذاً يوجد تقابل أحادي بين العناصر f_i للترقيم $i=1,2,...,m$ و g_j للترقيم $j=1,2,...,m$ بحيث تكون العناصر المتقابلة مترافقة ، هذا يبين أن $R[x]$ يحقق الشرط (2) لساحة تحليل وحيد (UFD) بالتالي $R[x]$ هي ساحة تحليل وحيد (UFD) .

مثال 27

لأن Z هي UFD فإن $Z[x]$ هو UFD (نظرية 44.10) ندعي أن $Z[x]$ ليس PID ، لبيان صواب هذا الادعاء اعتبر المثالي $I =< x > + < 4 >$ فإذا كان I مثالي رئيسي أمكننا إيجاد كثيرة حدود $f \in Z[x]$ بحيث يكون $I =< f >$ أي أن $< f >=< 4 > + < x >$ هذا يعطي $< 4 >\subseteq< f >$ ويكون $f \mid 4$ في $Z[x]$ أي أن $4 = fg$ لعنصر ما $g \in Z[x]$.

على أية حال فإن $\deg 4 = 0 \Rightarrow \deg f = 0 \Rightarrow f \in Z$.

نفرض أن $f = \alpha(\neq 0) \in Z$ فيكون $< \alpha >=< 4 > + < x >$ زيادة على ذلك أن $< x >\subseteq< \alpha >$ يؤدي إلى أن $x = \alpha h$ لعنصر ما $h \in Z[x] \Rightarrow \deg h = 1 \Rightarrow h = \beta x + \delta$ لبعض العناصر $\beta, \delta \in Z$ حيث $\beta \neq 0$ الآن $x = \alpha h \Rightarrow \alpha\beta = 1$ عليه يكون :

$$1 \in < \alpha > \Rightarrow 1 \in < x > + < 4 > \Rightarrow 1 = xt + 4v$$

لبعض العناصر $t, v \in Z[x]$ ، ولكن هذا بدوره يؤدي إلى أن 4 يقسم 1 في Z .

ضع $\beta_i \in Z, v = \beta_0 + \beta_1 x + ... + \beta_m x^m$ و $1 = xt + 4v$ وقارن المعاملات ، وهذا مستحيل فيكون I مثالياً غير رئيسي ويكون $Z[x]$ ليس PID .

والآن في نهاية الفصل نذكر ونبرهن اختباراً لعدم قابلية كثيرة حدود للتحليل في $Z[x]$ على Q.

نظرية 45.10 (معيار أيزنستين لعدم قابلية التحليل)

ليكن $f = a_0 + a_1x + ... + a_nx^n$ كثيرة حدود في $Z[x]$ إذا وجد عدد أولي p بحيث كان $p \mid u_i$ لكل $i = 0,1,2,...,n-1$ و $p \nmid a_n$ و $p^2 \nmid a_0$ فإن f غير قابلة للتحليل على Q.

البرهان

لاحظ أن الشروط المعطاة تؤدي إلى أن $\deg f > 0$ نبين أولاً أن f كثيرة حدود غير قابلة للتحليل في $Z[x]$ وغير ذلك افرض أن $f = gh$ حيث $g, h \in Z[x]$ بحيث يكون $\deg g < \deg f$ و $\deg h < \deg f$.

ليكن

$$g = b_0 + b_1x + b_0x^2 + ... + b_sx^3, b_s \neq 0$$
$$h = c_0 + c_1x + c_2x^2 + ... + c_tx^t, c_t \neq 0$$

الآن $f = gh \Rightarrow a_0 = b_0c_0$ يؤدي على أن $p \mid c_0$ أو $p \mid b_0$ لأن $p \mid u_0$ ، وحيث أن $p^2 \nmid u_0$ فإن p لا يقسم كلاً من c_0, b_0 ولكي نكون محددين افرض أن $p \mid b_0$ و $p \nmid c_0$ فللمرة الثانية يكون $f = gh \Rightarrow a_n = b_5c_t$.

وحيث أن $p \nmid a_n$ يكون $p \nmid b_5$ لذا فإن b_k هو أول عامل لكثيرة الحدود و (في اليسار) لا يقبل القسمة على p ، من الواضح $0 < k$ و $k \leq s < n$.

الآن $a_k = b_kc_0 + b_{k-1}c_1 + ... + ... + b_0c_k$ بحيث يكون $p \mid a_k, p \mid b_0, p \mid b_2, ..., p \mid b_{k-1}$ بالتالي p / b_kc_0 وحيث أن $p \nmid c_0$ و p عدد أولي فإن $p \mid b_k$ ، هذا تناقض يحله أن تكون f غير قابلة للتحليل في $Z[x]$ الآن يمكننا كتابة $f = df_1$ حيث $d \in Z$ و f_1 كثيرة

حدود بدائية في $Z[x]$ إذاً f_1 أيضاً غير قابلة للتحليل تامة في $Z[x]$ هذا يجعل f_1 غير قابلة للتحليل في $Q[x]$ لأن Z هو ساحة تامة تحليل وحيد (UFD) و Q حقل قواسمها (قضية 41.10) ولكن $f_1=\left(\frac{1}{d}\right)f\in Q[x]$ فتكون f أيضاً غير قابلة للتحليل في $Q[x]$.

مثال 28

كثيرات الحدود $x^4-4x+2, x^3-9x+15$ و $7x^4-2x^3+6x^2-10x+18$ جميعها غير قابلة للتحليل في $Q[x]$. في حالة كثيرة الحدود x^4-2x+2 ، $p=2$ يحقق معيار إيزنستين وفي حالة $x^3-9x+15$ ، $p=3$ وأخيراً لكثيرة الحدود $7x^4-2x^3+6x^2-10x+18$ ، $p=3$ يتحقق معيار إيزنستين .

مثال 29

اعتبر كثيرة الحدود $f(x+1)=x^2+1$ فإن $f(x)=x^2+2x+2$ بأخذ $p=2$ نجد أن معيار إيزنستين يمكن تطبيقه على $f(x+1)$. بما أن $f(x)=g(x)h(x)$ إذا وفقط إذا كان $f(x+0)=g(x+a)h(x+a)$ لكل $a\in Z$ فإن x^2+1 غير قابلة للتحليل على Q .

لاحظ أن بصورة عامة إذا كان R هو (UFD) و $f\in R[x]$ فلأي $a\in R$ تكون كثيرة الحدود $f(x)$ غير قابلة للتحليل على R إذا وفقط إذا كان $f(x+a)$ كثيرة حدود غير قابلة للتحليل على R ، بما أن $f(x)=h(x)g(x)\Rightarrow f(x+a)=g(x+a)h(x+a)$ و $\deg g(x)=\deg(x+a)$ ، $\deg h(x)=\deg h(x\in a)$ فإنه أحياناً يمكن تطبيق معيار إيزنستين بنجاح إذا كتبنا $x+n$ بدلاً من x في كثيرة حدود على Z حيث n أي عدد صحيح مناسب (عادة نأخذ $n=\pm1,\pm2$) .

مثال 30

لأي عدد أولي p كثيرة الحدود $x^{p-1}+x^{p-2}+...+x^2+x+1$ غير قابلة للتحليل على Q .

ليكن $\frac{x^p - 1}{x - 1} = x^{p-1}x^{p-2} + ... + x^2 + x + 1 = f(x)$ عندئذ :

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + C_1^p x_1^{p-1} + ... C_r^p x^{p-r} + ... + C_{p-1}^p x}{x}$$
$$= x^{p-1} + C_1^p x^{p-2} + ... + C_r^p x^{p-r} + ... + C_{p-1}^p$$

وحيث أن p عدد أولي ، $p \mid C_r^p$ لكل $1 \leq r \leq p-1$ (برهن) كذلك $C_{p-1}^p = p$ فيكون $p^2 \nmid C_{p-1}^p$.

واستناداً إلى معيار إيزنستين فإن $f(x+1)$ كثيرة حدود غير قابلة للتحليل في $Q[x]$ وينتج أن $f(x)$ غير قابلة للتحليل في $Q[x]$

مسائل

1. في $Z\left[\sqrt{-5}\right]=\left\{a+b\sqrt{-5}\mid a,b\in Z\right\}$ بين أن $1+2\sqrt{-5},3$ أوليان ولكن ليس لهما LCM كذلك بين أنه في $Z\left[\sqrt{-5}\right]$ العنصران $21\left(1-2\sqrt{-5}\right)$ و $7\left(1+2\sqrt{-5}\right)\left(1-2\sqrt{-5}\right)$ ليس لهما HCF .
2. بين أن مجموعة كثيرات الحدود في $Z[x]$ ذات المعاملات الزوجية لـ x تشكل حلقة جزئية في R تحقق من أن $2x,2$ لهما عامل مشترك أصغر (HCF) وليس لهما مضاعف مشترك أصغر (LCM) في R .
3. بين أن $Z\left[\sqrt{-6}\right]=\left\{a+b\sqrt{-6}\mid a,b\in Z\right\}$ ليس ساحة تحليل وحيدة (UFD) .

إرشاد : $10=2.5=\left(2+\sqrt{-6}\right)\left(2-\sqrt{-6}\right)$

4. بين أن $Z\left[\sqrt{-7}\right]$ ليس ساحة تحليل وحيدة (UFD) .

إرشاد : $16\;=\;2.2.2.2$ كذلك $16=\left(3+\sqrt{-6}\right).\left(3-\sqrt{-7}\right)$.

5. إذا كان R هو ساحة تحليل وحيدة (UFD) و f كثيرة حدود ذات درجة موجبة في $R[x]$. اثبت أن $f=d_1f_1$ لعنصر $d_1\in R$ و f_1 كثيرة حدود بدائية في $R[x]$ إذا كان $f=d_1f_1=d_2f_2$ حيث $f_1,f_2,d_1d_2\in R$ كثيرتي حدود بدائيتان . برهن أن d_2,d_1 مترافقان في R وأن f_1,f_2 مترافقان في $R[x]$.
6. اثبت أنه إذا كان p عدداً أولياً فإنه لجميع $1\le r\le p-1x$ فيكون p قاسماً للعدد C_r^p .
7. إذا كان R هو ساحة تحليل وحيد (UFD), k حقل قواسمها اثبت ان كثيرتي الحدود البدائيتان f و في $R[x]$ تكونان مترافقتين في $R[x]$ إذا وفقط إذا كانتا مترافقتين في $k[x]$.

8. لتكن a,b,c ثلاثة عناصر غير صفرية في حلقة R هي ساحة تحليل وحيد (UFD)

اثبت الآتي
$$(a,[b,c])=[(a,b),(a,c)]$$
$$[a,(b,c)]=([a,b],[a,c])$$

أي أن عملية العامل المشترك الأكبر (HCF) توزيعية على (LCM) والعكس بالعكس .

9. اثبت أنه في ساحة تحليل وحيد (UFD) جميع المثاليات الأولية الأصغرية هي مثاليات رئيسية وهي بالضبط المثاليات المولدة بعناصر غير قابلة للتحليل .

10. اثبت أنه إذا كان p عدداً أولياً فإن $x^{p(p-1)}+x^{p(p-2)}+\ldots+x^{p}+1$ غير قابلة للتحليل على Q .

إرشاد : كثيرة الحدود المعطاة هي $\dfrac{x^{p^2}-1}{x^{p}-1}$.

11. إذا كان كل من C,B,A هي مثاليات في PID ولتكن R اثبت أن :

أ- $A\cap(B+C)=A\cap B+A\cap C$

ب- $A+(B\cap C)=(A+B)\cap(A+C)$

12. R هو ساحة تحليل وحيد (UFD) و p مثالي أولي في R بحيث كان p مولَّداً بعنصر x ليس بوحدة . اثبت أنه لا يوجد مثالي أولي Q في R بحيث $R \subseteq Q \subseteq (0)$.

إرشاد : بين أولاً إذا وجد مثل Q هذا فإن $Q=Ax$ مثالي A في R ومن ثم بين أنه بإمكاننا إيجاد عنصر غير قابل للتحليل p يجعل $x \mid p^{n}$ لجميع الأعداد الحقيقية $1\leq n$.

13. إذا كان R هو ساحة تحليل وحيد (UFD) و a,b,c عناصر غير صفرية في R . برهن ما يأتي :

i. إذا كان $a \mid c$ و $b \mid c$ و $(a,b)=1$ فإن $ab \mid c$.

ii. إذا كان $a \mid bc$ و $(a,b)=1$ فإن $a \mid c$.

تمارين متنوعة محلولة

تمرين 1

اثبت أن كلاً من x^2+1 و x^2+x+4 غير قابلة للتحليل على F حقل الأعداد الصحيحة معيار 11 . كذلك اثبت أن $\frac{F[x]}{<x^2+1>}$ و $\frac{F[x]}{<x^2+x+4>}$ حقلان إيزومورفيان كلاهما يحوي 121 عنصراً .

الحل

عناصر F هي $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\bar{9},\overline{10}$ وللتبسيط سوف نحذف العلامة (-) أي من كثيرتي الحدود x^2+1 و x^2+x+4 لا يتحقق بعناصر في F نتيجة لذلك فليس لأي منهما عامل خطر في $F[x]$ هذا يبين أن كلتاهما غير قابلة للتحليل على F أي عنصر في $\frac{F[x]}{<x^2+1>}$ هو من النوع $f[x]+<x^2+1>$ حيث $f(x)\in F[x]$.

ومن خوارزمية إقليدس في $F[x]$ يكون $f(x)=g(x)(x^2+1)+r(x)$ حيث $g(x),v(x)\in F[x]$ بحيث $r(x)=0$ أو $\deg\delta(x)<2$.

في كلتا الحالتين يكون $r(x)=\alpha x+\beta$ حيث $\alpha,\beta\in F$ وهكذا فإن $f(x)+<x^2+1>=\alpha x+\beta+<x^2+1>$.

والآن يمكننا اختيار α في 11 طريقة ولكل اختيار للعدد α فإن هناك 11 اختيار للعنصر β لذا فإن عدد العناصر في $\frac{F[x]}{<x^2+1>}$ هو 121 . بالمثل يمكن إثبات أن $\frac{F[x]}{<x^2+x+4}$ لـ 121 عنصراً . بما أن كلاً من $x^2+1<x^2+x+4$ غير قابلة للتحليل فإن كلاً من $<x^2+x+4>,<x^2+1>$ مثالي أعظمي في $F[x]$ أي أن كلاً من $\frac{F[x]}{<x^2+1>}$ و $\frac{F[x]}{<x^2+x+4>}$ هو حقل .

وأخيراً عرف $\theta : \frac{F[x]}{< x^2 + x + 4 >} \to \frac{F[x]}{< x^2 + 1 >}$.

بالصورة $\theta\left[\alpha x + \beta + < x^2 + 1 >\right] = \alpha x + (\beta - 5\alpha) + < x^2 + x + 4 >$

يمكن التحقق من أن θ هو هومومورفزم حلقة . بما أن $\frac{F[x]}{< x^2 + 1 >}$ حقل فإن θ أحادي .

كذلك لأن كلا الحقلين له نفس العدد في العناصر فإن θ فوقي إذاً :

$$\frac{F[x]}{< x^2 + 1 >} \cong \frac{F[x]}{< x^2 + x + 4 >}$$

تمرين 2

اثبت أنه لأي عدد صحيح $n > 1$ فإن الحلقة $Z/(n)$ ليس لها عناصر غير صفرية عديمة القوة إذا وفقط إذا كان n لا يقبل القسمة على مربع أي عدد صحيح موجب أكبر من واحد .

الحل

افرض أن $Z/(n)$ ليس لها عناصر عديمة القوة . حسب النظرية الأساسية للحساب فإن $n = p_1^{\lambda_1} p_2^{\lambda_2} ... p_k^{\lambda_k}$ حيث p_i هي أعداد أولية مختلفة لكل $i = 1, 2, ..., k$ و $\lambda_i > 0$ أعداد صحيحة . اعتبر العدد الصحيح $p_1 p_2 ... p_k$. ليكن $\beta = \max\{\lambda_1, \lambda_2, ..., \lambda_k\}$ فيكون

$$[p_1 p_2 ... p_k + (n)]^\beta = p_1^\beta p_2^\beta ... p_k^\beta + (n) = (n)$$

لأن $n \mid p_1^\beta p_2^\beta ... p_k^\beta$ عليه نحصل على أن $p_1 p_2 ... p_k + (n)$ هو عنصر عديم القوة في $Z/(n)$ حسب فرضيتنا ، هذا يعني أن $p_1 p_2 ... p_k + (n) = (n) \Rightarrow n \mid p_1 p_2 ... p_k$ بالتالي $\lambda_i \leq 1$ لكل i وبما أن $1 \leq \lambda_i$ لكل $i\lambda$ يكون لدينا $\lambda i = 1$ أي أن $n = p_1 p_2 ... p_k$ بالتالي n لا يقبل القسمة على مربع أي عدد صحيح .

بالعكس افرض $n = p_1 p_2 ... p_t$ لأعداد أولية مختلفة $p_j, j = 1, 2, ..., t$ وليكن $m + (n)$ عنصراً عديم القوة في Z | n فيكون $[m + (n)]^\alpha = (n)$ لعدد ما $1 \leq \alpha$.

هذا يؤدي إلى أن $m^{\alpha} \in (n)$ أو $n \mid m^{\alpha}$ يؤدي إلى أن $p_j \mid m^{\alpha}$ لكل j .

$$\Rightarrow \qquad p_i \mid m, V_i \Rightarrow p_1 p_2 \ldots p_5 \mid m \Rightarrow n \mid m \Rightarrow m + (n) = (n)$$

إذاً $Z/(n)$ لا يحوي عناصر عديمة القوة .

تمرين 3

إذا كانت R حلقة إبدالية بمحايد بين أن مركز حلقة المصفوفات R_n تحوي جميع المصفوفات القياسية في R_n .

الحل

لغرض الملائمة سوف ندخل مفهوم مصفوفة الوحدات $E_{ij}, i, j = 1, 2, \ldots, n, E_{ij}$ يرمز إلى مصفوفة عناصرها في جميع المواقع تساوي صفراً أما العنصر في الموقع (i, j) فإنه يساوي 1 العنصر المحايد للحلقة R لاحظ أن $E_{ij} E_{ki} = 0$ حيثما $j \neq k$ و $E_{ik} E_{k\ell} = E_{i\ell}$ إضافة إلى ذلك كل مصفوفة في R_n يمكن كتابتها بصورة وحيدة بالصورة :

$$\sum_{j=1}^{n} \sum_{i=1}^{n} \alpha_{kj} E_{ij}, \alpha_{nj} \in F, \alpha_{ij} \in F$$

افرض أن (مركز R_n)

$$\sum_{j=1}^{n} \sum_{k=1}^{n} \alpha_{ij} E_{ij} \in C_n R_n$$

اعتبر $E_{ik} \in R_n$

$$\left(\sum_{j=1}^{n} \sum_{i=1}^{n} \alpha_{ij} E_{ij} \right) E_{\ell k} = E_{\ell k} \left(\sum_{j=1}^{n} \sum_{i=1}^{n} \alpha_{ij} E_{ij} \right)$$

$$\Rightarrow \qquad \sum_{i=1}^{n} \alpha_{i\ell} E_{ik} = \sum_{j=1}^{n} \alpha_{kj} E_{\ell j}$$

وذلك لكل $j \neq k$ ، $E_{\ell j}$ لا يظهر في الطرف الأيسر فيكون $\alpha_{kj} = 0$ مثل $j \neq k$ بما أن $E_{\ell k}$ انتقيناها اختيارية .

هذا يبين أن جميع المدخلات غير قطرية في $\sum_{j=1}^{n} \sum_{i=1}^{n} \alpha_{ij} E_{ij}$ تساوي صفراً ، وعليه فكل عنصر في مركز R_n هو من النوع $\sum_{i=1}^{n} \alpha_{ij} E_{ij}$ مرة أخرى مع المصفوفة $\sum_{k=1}^{n} \sum_{\ell=1}^{n} E_{ik}$

$$\left(\sum_{i=1}^{n}\alpha_{ii}E_{ii}\right)\left(\sum_{k=1}^{n}\sum_{\ell=1}^{n}E_{\ell k}\right)=\left(\sum_{k=1}^{n}\sum_{\ell=1}^{n}E_{ik}\right)\left(\sum_{i=1}^{n}\alpha_{ii}E_{ii}\right)$$

$$\Rightarrow \qquad \sum_{k=1}^{n}\sum_{i=1}^{n}\alpha_{ii}E_{ik}=\sum_{k=1}^{n}\sum_{\ell=1}^{n}\alpha_{kk}E_{\ell k}$$

لأي دليل k فإن معامل $E_{\ell k}$ في الطرف الأيمن هو α_{kk} في حين أن معامل $E_{\ell k}$ في الطرف الأيسر هو $\alpha_{\ell\ell}$ عليه يكون $\alpha_{\ell\ell}=\alpha_{kk}$ ولكننا عينّا k,ℓ بصورة اختيارية فنحصل على $\alpha_{11}=\alpha_{22}=\ldots=\alpha_{nn}=\lambda$ حيث λ عدد اختياري إذا $\sum_{i=1}^{n}\alpha_{ii}E_{ii}=\lambda\sum_{i=1}^{n}E_{ii}$

وهذا يبين أن كل عنصر في مركز R_n هو مصفوفة قياسية . وأخيراً نفرض أن $\lambda\sum_{i=1}^{n}E_{ii}$ أي مصفوفة قياسية في R عندئذ يكون :

$$\left(\lambda\sum_{i=1}^{n}E_{ii}\right)\left(\sum_{\ell=1}^{n}\sum_{k=1}^{n}\alpha_{\ell k}E_{\ell k}\right)=\lambda\sum_{k=\ell}^{n}\sum_{i=1}^{n}\alpha_{ik}E_{ik}$$

$$=\sum_{k=1}^{n}\sum_{i=1}^{n}\lambda\,\alpha_{ik}E_{ik}=\sum_{k=1}^{n}\sum_{\ell=1}^{n}(\lambda\,\alpha_{\ell k})E_{\ell k}$$

(وذلك بتبديل دليل الجمع من i إلى ℓ) .

كذلك $$\left(\sum_{\ell=1}^{n}\sum_{k=1}^{n}\alpha_{\ell k}E_{\ell k}\right)\left(\lambda\sum_{i=\ell}^{n}E_{ii}\right)=\sum_{k=1}^{n}\sum_{\ell=1}^{n}(\alpha_{\ell k})E_{\ell k}$$

بما أن R إبدالية ، $\alpha_{\ell k}\,\lambda=\lambda\,\alpha_{\ell k}$ فإن $\lambda\sum_{i=1}^{n}E_{ii}\in Centr\,R_n$ أي أن مركز R_n يحتوي على جميع المصفوفات القياسية في R_n .

تمرين 4

مثالي يميني لحلقة R يسمى مثالي يميني أصغري في R إذا كان (i) $A\neq(0)$ و (ii) لأي مثالي يميني B في R ، $0\subseteq B\subseteq A$ يؤدي إلى أن إما $B=(0)$ أو $B=A$ فإذا كان R

لها مثالي يميني أصغري A ولأي ثابت r كان $rA \neq (0)$ ، بين أن rA مثالي أصغري يميني أيضاً .

الحل

تذكر أن $rA = \{ra / a \in A\}$ عليه $0 = r0 \in rA$ ، rA ليست خالية إذا كان $ra , ra' \in A$ حيث $a , a' \in A$ ، $ra - ra' = r(a - a') \in rA$ لأن $a - a' \in A$ لأي $x \in R$ فإن $(ra)x = r(ax) \in rA$ لأن $ax \in A$ (A مثالي يميني في R) .

عليه rA مثالي يميني في R . الآن حسب الفروض $rA \neq 0$ ليكن B أي مثالي يميني في R بحيث يكون $(0) \subseteq B \subseteq rA$ يمكننا بيان أنه إذا كان $B \neq 0$ فإن $B = rA$.

بما أن $B \neq (0)$ فإنه يوجد $b(\neq 0) \in B$ لأن $B \subseteq rA$ فإن $b = ra$ لعنصر ما $a \in A$ افرض أن $x = \{s \in A / rs \in B\}$ بما أن $0 \in x$ ، x غير خالية ، كذلك :

$$a_1, a_2 \in x \Rightarrow ra_1, ra_2 \in B \Rightarrow ra_1 - ra_2 \in B$$
$$\Rightarrow \quad r(a_1 - a_2) \in B \Rightarrow a_1 - a_2 \in x$$

ومرة ثانية لأي $x \in R$ ، $ra_1 \in B \Rightarrow (ra_1)x \in B$ لأن B مثالي يميني في R فهذا يؤدي إلى أن $r(a_1x) \in B \Rightarrow a_1x \in x$ إذاً x مثالي يميني في R محتوي في A إضافة إلى ذلك بما أن $x \neq 0, a \in x$ من أصغرية A نجد أن x يساوي A أي $rA \subseteq B$ بالتالي $B = rA$ وبناء عليه فإن rA مثالي أصغري في R .

11

الفضاءات المتجهة

Vector Spaces

في الهندسة التحليلية والميكانيكا يصادف أحدنا مفهوم المتجه على أنه كمية متجهة (مقدار اتجاهي) . لسنا بحاجة للعودة إلى ذلك التعريف . من وجهة النظر الجبرية فإن المتجهات المعرفة هكذا لها الخواص البارزة الآتية :

1- في الفضاء الإقليدي الثلاثي البعد ، يتحدد متجه ما بطريقة وحيدة بواسطة مركباته الثلاثة (ξ, η, λ) (نسبة لنظام إحداثي محدد سلفاً) ، وبالعكس لكل ثلاثي مرتب معطى من الأعداد الحقيقية (ξ, η, λ) يوجد متجه v له الإحداثيات ξ, η, λ . من المألوف أن نكتب $v = (\xi, \eta, \lambda)$ قاصدين أن v متجه مركباته هي ξ, η, λ . وبصورة مشابهة في الفضاء الإقليدي ثنائي البعد أي متجه له إحداثيان ويحدد بطريقة وحيدة بواسطة إحداثية . إضافة إلى ذلك فإن الأعداد الحقيقية تسمى قياسيات (Scalars) .

2- هناك ثلاث عمليات أساسية على المتجهات ، نعني بها جمع المتجهات ، ضرب متجه بقياس والضرب القياسي للمتجهات . فإذا كان $v = (\xi, \eta, \lambda)$ ، $v' = (\xi', \eta', \lambda')$ متجهان في R^3 ، الفضاء الإقليدي الثلاثي البعد ، α قياسي (عدد حقيقي) فإننا نعرف مجموعها $v + v' = (\xi + \xi', \eta + \eta', \lambda + \lambda')$ وضرب v في α $\alpha v = (\alpha\xi, \alpha\eta, \alpha\lambda)$ ، والضرب القياسي لهما (v, v') كالآتي :

$$(v, v') = \xi\xi' + \eta\eta' + \lambda\lambda'$$

العمليتــان الأولى والثانيــة للمتجهــات تلعبــان دوراً مهمــاً في الهندســة التحليليــة والميكانيكا . في هذا الفصل نحاول أن نعطي معالجة للمتجهات في إطار أكثر تعميماً .

إن دراسة المتجهات في إطار عمليتي الجمع والضرب بعدد حقيقي يمكن تعميمها في ناحيتين الأولى : ليس بالضرورة أن نقصر دراستنا على الأزواج المرتبة أو الثلاثيات المرتبة ، وبدلاً من ذلك يمكننا أخذ المرتبات النونية . والثانية لا نحتاج أن نقيد أنفسنا بإحداثيات هي أعداد حقيقية ، فالإحداثيات يمكن أن تؤخذ من أي حقل أو بصورة أعم من أية حلقة قاسمية (division ring) .

والآن نعطي تعريفاً مجرداً لفضاء متجهي ومن ثم نرى كيف يعمم هذا التعريف مفهوم المتجه المذكور سلفاً في الهندسة التحليلية والميكانيكا .

1– تعريف وخواص أولية

تعريف 1-11 النظام $(V, D, \oplus, .)$

حيث V مجموعة غير خالية ، D حلقة قاسمية ، $\oplus$ عملية ثنائية على V و . راسم من $D \times V$ إلى V يتحدد بواسطته لكل عنصر $v \in V$ وكل عنصر $\alpha \in D$ عنصراً $\alpha . v \in V$ ، يسمى فضاء متجهاً يسارياً على D إذا تحققت الشروط التالية :

1 – V . $< V, \oplus >$ زمرة أبيلية .

2 – V . لجميع $x, y \in V$ ، $\alpha, \beta \in D$ يكون

$$\alpha . (x \oplus y) = \alpha . x \oplus \alpha . y \qquad \text{(i)}$$

$$(\alpha + \beta) . x = \alpha . x \oplus \alpha . y \qquad \text{(ii)}$$

$$(\alpha\beta) . x = \alpha . (\beta . x) \qquad \text{(iii)}$$

$$1 . x = x \qquad \text{(iv)}$$

كل عنصر في V يسمى متجه ، كل عنصر في D يسمى قياسي أو لا متجهي .

بصورة مشابهة إذا أخذنا $v.\alpha$ بدلاً من $\alpha.v$ في التعريف السابق فإننا نحصل على فضاء متجهي يميني على D .

ملاحظة بصورة مناظرة للمتفق عليه في الزمر والحلقات عندما لا يكون هناك أي احتمال للالتباس فإننا نقول أن V فضاء متجهي على حلقة قاسمية D ، طالما كان النظام $(V, D, \oplus, \boldsymbol{.})$ فضاءً متجهاً على D ، في هذا الكتاب نحن مهتمون بدراسة الفضاءات المتجهة على الحقول فقط . ومع ذلك نؤكد أن معظم النتائج المبرهنة هنا حول الفضاءات المتجهة على حقول يمكن تعميمها بصورة مناسبة لتشمل الفضاءات المتجهة على حلقات قاسمية .

ملاحظة من أجل التيسير ، في المستقبل نستخدم الرمز نفسه "+" لكل من عمليتي الجمع في V والجمع في D .

مثال 1

لأي حقل F ، إذا كان $V = \{(\alpha_1, \alpha_2) : \alpha_i \in F\}$ ، فإن V فضاء متجهي على F تحت عمليتي الجمع للمتجهات وضرب متجه بقياس المعرفتين كالآتي :

$$(\alpha_1, \alpha_2) + (\beta_1, \beta_2) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2)$$
$$\alpha(\alpha_1, \alpha_2) = (\alpha\alpha_1, \alpha\alpha_2)$$

مثال 2

لتكن V زمرة الجمع لكثيرات الحدود في متغير واحد على حقل F . لكل $\alpha \in F$ و $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ إذا عرفنا :

$$\alpha f(x) = \alpha\alpha_0 + \alpha\alpha_1 x + \ldots + \alpha\alpha_n x^n$$

عندئذ يصبح V فضاءً متجهاً على F .

مثال 3

لتكن V مجموعة جميع الدوال الحقيقية المتصلة المعرفة على الفترة المغلقة $[0, 1]$.

لكل $f, g \in V$ ، $\alpha \in I\!R$ نعرف $f + g$ ، αf كالآتي :

$$(f + g)(x) = f(x) + g(x)$$

$$(\alpha f)(x) = \alpha f(x), \quad \forall\, x \in [0,1]$$

تحت هـاتين العمليتـين فـإن V يشـكل فضـاءً متجهـاً علـى $I\!R$ (لأن مجمـوع دوال متصـلة وحاصل ضرب دالة متصلة في قياسي يعطيان دوالاً متصلة) .

مثال 4

لأي حقـل F ولأي عـدد صـحيح موجـب n ، مجموعـة جميـع المرتبـات النونيـة $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ لعناصر في F ، هـو فضاء متجهي على F تحت عمليتي جمع المتجهات وضربها في قياس المعرفتين هكذا :

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) + (\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n)$$
$$\alpha(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n)$$

عـادة يرمز لهذا الفضـاء المتجهي بالرمز $F^{(n)}$ أو F^n . وكمـا أشرنا في البداية فإننـا مهتمـون بالفضـاءات المتجهة على حقول فقط . القضية التالية تثبت انه لا فرق بين فضاء متجهي يساري أو يميني على حقل ما .

قضية 11-2

إذا كـان V فضـاءً متجهـاً يسـارياً على حقـل F ، فـإن V هـو فضـاء متجهي يمين أيضاً وبالعكس .

البرهان

بمـا أن V فضـاء متجهي يسـاري على F فسـوف يكـون لكـل $v \in V$ ، $\alpha \in F$ عنصراً وحيداً $\alpha . v$ معرفاً في V كما أن

$$\alpha . (u + v) = \alpha . u + \alpha . v$$
$$(\alpha + \beta) . u = \alpha . u + \beta . u$$
$$(\alpha\beta) . u = \alpha . (\beta . u)$$
$$1 . u = u$$

لكل $u, v \in V$ و $\alpha, \beta \in F$.

وبتعريف $v\,.\,\alpha$ يساوي $\alpha\,.\,v$ لكل $\alpha \in F$ ، $v \in V$ فإن لكل $\alpha, \beta \in F$ ، $u, v \in F$ يكون

$$(u + v)\,.\,\alpha = \alpha\,.\,(u + v) = \alpha\,.\,u + \alpha\,.\,v = u\,.\,\alpha + v\,.\,\alpha$$
$$u\,.\,(\alpha + \beta) = (\alpha + \beta)\,.\,u = \alpha\,.\,u + \beta\,.\,u = u\,.\,\alpha + u\,.\,\beta$$
$$u\,.\,(\alpha\beta) = (\alpha\beta)\,.\,u = (\beta\alpha)\,.\,u \qquad (\text{لأن } \alpha\beta = \beta\alpha)$$
$$= \beta\,.\,(\alpha\,.\,u) = \beta\,.\,(u\,.\,\alpha) = (u\,.\,\alpha)\,.\,\beta\,.$$
$$u\,.\,1 = 1\,.\,u = u$$

ومن ثم فإن V زمرة إبدالية تحت الجمع بحيث لكل $v \in V$ ، $\alpha \in F$ ، يكون $v\,.\,\alpha$ هو العنصر الوحيد المعرف في V والذي يحقق الشروط التالية :

لكل $u, v \in V$ ، $\alpha, \beta \in F$.

$$(u + v)\,.\,\alpha = u\,.\,\alpha + v\,.\,\alpha$$
$$u\,.\,(\alpha + \beta) = u\,.\,\alpha + u\,.\,\beta$$
$$u\,.\,(\alpha\beta) = (u\,.\,\alpha)\,.\,\beta$$
$$u\,.\,1 = u$$

وعليه فإن V فضاء متجهي يميني على F .

وبالمثل إذا كان V فضاءً متجهاً يمينياً على F فإن V هو فضاء متجهي يساري أيضاً .

وهذا يكمل البرهان . □

من الآن فصاعداً سوف نقصر اهتمامنا على الفضاءات المتجهة على حقول . وبذلك لا نميز بين فضاء متجهي يساري ويميني . وعلى أي حال سوف نستمر في كتابة القياسيات على يسار المتجه في عملية ضرب ، قياسي في متجه .

اصطلاح سوف نستخدم F ليشير إلى أن V فضاء متجهي على الحقل F .

ملاحظة 1 للتبسيط مستقبلاً سوف نكتب αv بلاً من $\alpha\,.\,v$.

ملاحظة 2 فيما يلي نعطي مثلاً لتبيان أن الشرط $V - 2$ (iv) والذي يعني أن $1\,.\,x = x$ لكل $x \in V$ هو شرط مستقل عن الشروط المتبقية $V - 1$ و $V - 2$ (i) ، (ii) ، (iii) .

مثال 5

اعتبر $V = \{(\alpha, \beta, \gamma) : \alpha, \beta, \gamma \in IR\}$. عرف :

$$(\alpha, \beta, \gamma) + (\alpha', \beta', \gamma') = (\alpha + \alpha', \beta + \beta', \gamma + \gamma')$$
$$\lambda(\alpha, \beta, \gamma) = (\lambda\alpha, \lambda\beta, 0), \quad \forall\, \alpha, \beta, \gamma, \alpha', \beta', \gamma' \in IR$$

يمكننا الآن التأكد من أن الشروط $V-1$ ، $V-2$ (i) ، (ii) و (iii) محققة .

والآن $(3, 2, 6) \in V$ ولكـــن $1\,(3, 2, 6) = (3, 2, 0) \neq (3, 2, 6)$ وبالتـــالي فـــإن V ليس فضاءً متجهاً على IR .

قضية 3-11

ليكن V فضاء متجهي على الحقل F وليكن O_V ، O_F العنصران المحايدان لعمليتي الجمع لكل من F, V فتكون العبارات الآتية متحققة :

(1) $\alpha O_V = O_V$ لكل $\alpha \in F$

(2) $O_F v = O_v$ لكل $v \in V$

(3) $-v = (-1)v$ لكل $v \in V$

(4) $(-\alpha)v = \alpha(-v) = -(\alpha v)$ لكل $v \in V, \alpha \in F$

(5) إذا كان $\alpha v = O_V$ فإنه إما $\alpha = O_F$ أو $v = O_V$

البرهان

(1) بما أن $O_V = O_V + O_V$ يكون لدينا :

$$\alpha O_V = \alpha(O_V + O_V) = \alpha O_V + \alpha O_V$$ (حسب $V-2$)

$$\Rightarrow \alpha O_V = O_V$$ (حسب قانون الحذف للزمرة $< V, + >$)

(2) $$O_F = O_F + O_F \Rightarrow O_F v = O_F v + O_F v$$

$$\Rightarrow O_F v = O_F$$ (حسب قانون الحذف للزمرة $< V, + >$)

(3) الآن $[1+(-1)]v = 1.v + (-1)v$

كذلك $O_V = O_F v = [1+(-1)]v = 1v + (-1)v = v + (-1)v$

وبالتالي $(-1)v = -v$.

(4) بما أن $O_V = O_F v = [\alpha + (-\alpha)]v = \alpha v + (-\alpha)v$

نحصل على $(-\alpha)v = -(\alpha v)$.

وبما أن $O_V = \alpha O_V = \alpha[v + (-v)] = \alpha v + \alpha(-v)$

نحصل أيضاً على أن $\alpha(-v) = -(\alpha v)$ وبالتالي $(-\alpha)v = \alpha(-v) = -(\alpha v)$.

(5) لـــيكن $\alpha v = O_V$ ، فـــإذا كـــان $\alpha \neq O_F$ فإنـــه يوجـــد α^{-1} في F وأن

$$v = 1v = (\alpha^{-1}\alpha)v = \alpha^{-1}O_V = O_V$$

عليه فإن $v = O_V$ أو $\alpha = O_F$

ملحوظـة سـوف نسـتخدم الرمـز نفسـه o أو O ليمثـل المتجـه الصـفري O_V أو الصـفر القياسي O_F لأي فضاء متجهي V_F .

ويجب أن يكون واضحاً لدى قراء هذا الكتاب لأي شيء تم استخدام 0 ، O في المواقع الخاصة .

2- الفضاءات الجزئية Subspaces

تعريف 11-4

يقـال لمجموعة جزئية غير خالية W مـن الفضـاء المتجهي V_F أنها فضاء جزئي مـن V إذا تحققت الشروط :

$S-1$. $a + b \in W$ لكل $a, b \in W$

$S-2$. $\alpha a \in W$ لكل $a \in W, \alpha \in F$

وعلى الفور ينتج من التعريف أن (0) و V كلاهما فضاء جزئي للفضاء V وهذه هي الفضاءات الجزئية التافهة . أي فضاء جزئي W للفضاء V_F والذي يختلف عن كل من (0) و V يسمى فضاء جزئي فعلي من الفضاء V .

قضية 11-5

إذا كان W فضاءً جزئياً من فضاء متجهي V_F ، فإن $< W, + >$ زمرة جزئية للزمرة $< V, + >$ ويكون W فضاءً متجهاً على F تحت عمليتي جمع المتجهات وضربها في قياسي المستحدثين .

البرهان

لكل $x, y \in W$ يكون $(-1)y \in W$ حسب $S - 2$ وعليه وحسب $S - 1$ فإن $x + (-1)y \in W \Rightarrow x - y \in W$ وهذا يبرهن أن $< W, + >$ زمرة جزئية من الزمرة $< V, + >$. عناصر W تحقق الخاصية $V - 2$ في تعريف 11-1 لأن $W \subseteq V$ والخاصية نفسها تتحقق في V وكذلك العمليات من W جميعها مستحدثة من العمليات في V وبالتالي فإن W فضاء متجهي على F تحت عمليتي جمع المتجهات والضرب في قياسي المستحدثتين .

مثال 6

اعتبر $/R^3 = \{(a_1, a_2, a_3) \mid a_i \in /R\}$ فإذا كان :

$$W_1 = \{(0, a_2, a_3) \mid a_2, a_3 \in R\}$$
$$W_2 = \{(a_1, a_2, a_3) \mid a_1 + a_2 + a_3 = 0\}$$

فإنه يمكننا أن نرى بسهولة أن كلاً من W_1 ، W_2 يحقق الشروط في تعريف الفضاء المتجهي الجزئي . وبالتالي فإن W_1 ، W_2 كلاهما فضاء جزئي من الفضاء $/R^3$.

مثال 7

ليكن C مجموعة جميع الأعداد المركبة . فإن C فضاء متجهي على حقل الأعداد الحقيقية . وأن $W = \{ib \mid b \in IR, i = \sqrt{-1}\}$ هو فضاء جزئي من C .

نظرية 11-6

المجموعة الجزئية غير الخالية W من الفضاء المتجهي V_F هي فضاء جزئي من الفضاء V_F إذا وفقط إذا تحقق الشرط الآتي :

$a, b \in W$ ، $\alpha, \beta \in T$ يؤدي إلى أن $\alpha a + \beta b \in W$.

البرهان

ليكن W فضاءً جزئياً من الفضاء V و $a, b \in W$ ، $\alpha, \beta \in F$ فإن $\alpha a \in W$ ، βb (تعريف 11-4 ، $S-2$) .

ومن ثم فإن $\alpha a + \beta b \in W$ (تعريف 11-4 ، $S-1$) .

بالعكس افرض W تحقق الشرط المعطى . فإذا كان $a, b \in W$ ، فيأخذ $\alpha = 1$ $\beta = 1$ نحصل على $a + b = 1a + 1b \in W$. مرة أخرى بأخذ $\beta = 0$ و α عنصراً اختيارياً فإننا نحصل على $\alpha a = \alpha a + 0b \in W$. وعليه فإن W فضاء جزئي من الفضاء V .

نظرية 11-7

تقاطع أية عائلة من فضاءات جزئية لفضاء متجهي يكون فضاءً جزئياً .

البرهان

لتكن $\{W_\lambda \mid \lambda \in \wedge\}$ عائلة لفضاءات جزئية من الفضاء المتجهي V_F ولتكن $W = \bigcap_{\lambda \in \wedge} W_\lambda$.

بما أن $O \in W_\lambda$ لكل $\lambda \in \wedge$ فإن $O \in W$. عليه فإن W مجموعة جزئية غير خالية من الفضاء V .

الآن $a, b \in W$ ، $\alpha, \beta \in F$:

$$\Rightarrow a \in W_\lambda, b \in W_\lambda \quad \forall \lambda \in \wedge \qquad (W = \bigcap_{\lambda \in \wedge} W_\lambda \text{ لأن})$$

بما أن كل W_λ فضاء جزئي من الفضاء V حسب نظرية 11-6 ، $\alpha a + \beta b \in W_\lambda$ لكل $\lambda \in \wedge$ ومنها $\alpha a + \beta b \in W$ وبالتالي فإن W فضاء جزئي من الفضاء V . □

النظرية السابقة تبين أن تقاطع أي فضائين جزئيين من فضاء متجهي V_F هو فضاء جزئي من الفضاء V_F . لقد سبق وأن برهنا أن اتحاد زمرتين جزئيتين لزمرة ليس بالضرورة أن يكون زمرة جزئية والنتيجة المناظرة صحيحة للفضاءات الجزئية .

مثال 8

اعتبر الفضاء المتجهي $IR^2 = \{(a, b) : a, b \in IR\}$ فإن $W_1 = \{(a, 0) : a \in IR\}$ ، $W_2 = \{(0, b) : b \in IR\}$ فضاءان جزئيان للفضاء IR^2 . ليكن $W = W_1 \cup W_2$.

الآن $(1, 0) \in W_1$ ، $(0, 1) \in W_2$ ولكن $(1, 1)$ ليس عنصراً في أي من W_1 و W_2 ومن ثم فإن $(1, 1) = (1, 0) + (0, 1) \notin W$ وهكذا فإن W ليست مغلقة تحت عملية جمع المتجهات . وبالتالي فإن $W_1 \cup W_2$ ليس فضاءً جزئياً من IR^2 .

تعريف 11-8

لتكن X مجموعة جزئية لفضاء متجهي V_F . يقال لفضاء جزئي W من الفضاء V أنه مولد (generated) بالمجموعة X إذا كان :

(i) $X \subseteq W$.

(ii) لأي فضاء جزئي W' من V ، $X \subseteq W'$ يؤدي إلى أن $W \subseteq W'$.

اصطلاح سوف نستخدم $< X >$ رمزاً للفضاء الجزئي المولد بالمجموعة X . بالإضافة إلى ذلك إذا كانت X تحوي العناصر $x_1, x_2, \ldots, x_n$ فإننا ببساطة نكتب $< X > = < x_1, x_2, \ldots, x_n >$.

نظرية 11-9

لأي مجموعة غير خالية $X = \{x_1, x_2, \ldots, x_n\}$ ، الفضاء الجزئي المولد بالمجموعة X هو مجموعة جميع المتجهات بالصيغة $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$ حيث $\alpha_i \in F$ ، $i = 1, 2, \ldots, n$.

البرهان

لتكن W مجموعة جميع المتجهات في V بالصيغة $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$ ، حيث $\alpha_i \in F$ ، $i = 1, 2, \ldots, n$ بأخذ $\alpha_1 = 1$ $\alpha_i = 0$ لكل $i \geq 2$ نجد أن $x_1 \in W$ وبالمثل فإنه يمكننا بيان أن $x_2, x_3, \ldots, x_n$ هي عناصر في W وهكذا فإن $X \subseteq W$. وإذا فرضنا أن W' فضاء جزئي من الفضاء V بحيث أن $X \subseteq W'$. عندئذ لكل i ، $\alpha_i \in F, x_i \in X \subseteq W' \Rightarrow \alpha_i x_i \in W'$.

وهذا يؤدي إلى أن $\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n \in W'$ وبالتالي فإن $W \subseteq W'$.
وهكذا نجد أن W مجموعة جزئية من V تحقق الشرطان (i) و (ii) في تعريف 11-8 ، عليه فإن البرهان يكتمل إذا بينا أن W فضاء جزئي من V . لذا نفرض أن :

$$a = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n, b = \beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_n x_n$$

أي عنصرين في W وأن $\alpha, \beta \in F$ عندئذ يكون :

$$\alpha a + \beta b = (\alpha\alpha_1 + \beta\beta_1)x_1 + (\alpha\alpha_2 + \beta\beta_2) + \ldots + (\alpha\alpha_n + \beta\beta_n)x_n \in W$$

وعليه فإن W فضاء جزئي من V وبهذا يكمل البرهان . □

تعريف 11-10

لأي عدد منته من المتجهات $x_1, x_2, \dots, x_n$ في فضاء متجهي V_F وقياسيات $\alpha_1, \alpha_2, \dots, \alpha_n$ في F فإن المتجه $\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$ يسمى تركيباً خطياً للمتجهات $x_1, x_2, \dots, x_n$.

وهكذا فإن نظرية 11-9 تبين لنا أنه إذا كانت X مجموعة جزئية منتهية غير خالية من V_F فإن الفضاء الجزئي $< X >$ هي مجموعة جميع التراكيب الخطية لعناصر X .

تعريف 11-11

لكل فضائين جزئيين W_1 و W_2 من الفضاء المتجهي V_F . فإن مجموعهما $W_1 + W_2$ يعرف بأنه المجموعة $W_1 + W_2 = \{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\}$

نظرية 11-12

لأي فضائين جزئيين W_1 و W_2 من فضاء متجهي V_F فإن $W_1 + W_2$ هو فضاء جزئي من V_F مولد بالمجموعة $W_1 \cup W_2$.

البرهان

نبرهن أولاً أن $W_1 + W_2$ فضاء جزئي من V_F . من الواضح أن $O = O + O \in W_1 + W_2$ وهكذا فإن $W_1 + W_2 \neq \phi$ افرض $x, y \in W_1 + W_2$ و $\alpha, \beta \in F$. فإن $x = w_1 + w_2$ ، $y = w_1' + w_2'$ لبعض $w_1' \in W_1$ و $w_2, w_2' \in W_2$

وهكذا فإن

$$\begin{aligned} \alpha x + \beta y &= (\alpha w_1 + \alpha w_2) + (\beta w_1' + \beta w_2') \\ &= (\alpha w_1 + \beta w_1') + (\alpha w_2 + \beta w_2') \qquad (1) \end{aligned}$$

الآن $\alpha w_2 + \beta w_2' \in W_2, \alpha w_1 + \beta w_1' \in W_1$

وبالتالي (1) تبين أن $\alpha x + \beta y \in W_1 + W_2$. وهكذا فإن $W_1 + W_2$ فضاء من V_F .

ونبرهن الآن أن $W_1 + W_2$ مولدة بالمجموعة $W_1 \cup W_2$ بما أن $O \in W_2$ فإن لكل $w_1 \in W$ يكون $w_1 = w_1 + O \in W_1 + W_2$. وهكذا فإن $W_1 \subseteq W_1 + W_2$ وبالمثل فإن $W_2 \subseteq W_1 + W_2$. وبالتالي :

$$W_1 \cup W_2 \subseteq W_1 + W_2 \qquad (2)$$

ليكن W أي فضاء جزئي من V يحوي $W_1 \cup W_2$ عندئذ لكل $w_1 \in W_1$ ، $w_2 \in W_2$ فإن $w_1, w_2 \in W_1 \cup W_2$:

$$\Rightarrow w_1, w_2 \in W \Rightarrow w_1 + w_2 \in W$$

لأن W مغلقة تحت عملية جمع المتجهات ، وهذا يؤدي إلى :

$$W_1 + W_2 \subseteq W \qquad (3)$$

(تعريف 11-11) . من (2) و (3) نستنتج أن $W_1 \cup W_2$ يولد $W_1 + W_2$. □

مثال 9

لأي حقل F ، اعتبر الفضاء المتجهي $F^{(3)}$. العناصر $e_1 = (1, 0, 0)$ ، $e_2 = (0, 1, 0)$ و $e_3 = (0, 0, 1)$ هي في $F^{(3)}$. ليكن $x = (\alpha_1, \alpha_2, \alpha_3) \in F^{(3)}$ فإن :

$$x = \alpha_1(1, 0, 0) + \alpha_2(0, 1, 0) + \alpha_3(0, 0, 1) = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3$$

إذاً كل عضو في $F^{(3)}$ هو تركيب خطي من e_1, e_2, e_3 ، وبالتالي فإن $\{e_1, e_2, e_3\}$ تولد $F^{(3)}$. بصورة عامة إذا أخذنا $F^{(n)}$ وعرفنا المتجهات $e_1 = (1, 0, 0, \ldots, 0)$ ، $e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 0, 1)$ فإن المجموعة المكونة من المتجهات $e_1, e_2, \ldots, e_n$ تولد $F^{(n)}$.

مثال 10

اعتبر $/R^3$ فإن $x_1 = (1, 1, 0), x_2 = (1, 2, 0) \in /R^3$ ، ليكن W الفضاء الجزئي المولد بالمجموعة $\{x_1, x_2\}$. عندئذ $x_1, x_2 \in W \Rightarrow x_2 - x_1 = (0, 1, 0) \in W$

$$\Rightarrow (1, 0, 0) = x_1 - (0, 1, 0) \in W$$

وهكذا فإن $e_1 = (1, 0, 0), e_2 = (0, 1, 0) \in W$ ، ويؤدي إلى :

$$\alpha_1 e_1 + \alpha_2 e_2 = (\alpha_1, \alpha_2, \theta) \in W$$

لكل $\alpha_1, \alpha_2 \in /R$.

لتكن $W' = \{(\alpha_1, \alpha_2, 0) \mid \alpha_1, \alpha_2 \in /R\}$. نجد أن W' فضاء جزئي من $/R^3$ ، وكما رأينا أعلاه فإن $W' \subseteq W$.

بما أن $e_1, e_2 \in W'$ فإن $x_2 = e_1 + 2e_2 \in W', x_1 = e_1 + e_2 \in W'$ وهكذا فإن $W = < x_1, x_2 > \subseteq W'$. إذاً $W = W'$.

تمارين محلولة

تمرين 1

ليكن F حقلاً و V مجموعة غير خالية مع عملية ثنائية $\oplus$. لكل $\alpha \in F$ ، $v \in V$ إذا كان هناك عنصر وحيد $\alpha \times v$ في V معرف بحيث تتحقق البديهيات التالية فأثبت أن $< V, \oplus, \times >$ فضاء متجهي على F .

(1) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ لكل $a, b \in V$

(2) $\lambda \times (a \oplus b) = \lambda \times a \oplus \lambda \times b$ لكل $a, b \in V, \lambda \in F$

(3) $(\lambda + \mu) \times a = \lambda \times a + \mu \times a$ لكل $a \in V, \lambda, \mu \in F$

(4) $(\lambda\mu) \times a = \lambda \times (\mu \times a)$ لكل $a \in V, \lambda, \mu \in F$

(5) $O \times a = O \times b$ لكل $a, b \in V$

(6) $1a = a$ لكل $a \in V$

الحل

ضع $z = O \times a$. عندئذ استناداً إلى (5) فإن z مستقلة عن a .

لكل $v \in V$ فإن :

$$\begin{aligned} v &= 1 \times v && (\text{حسب } (6)) \\ &= (1 + O) \times v \\ &= 1 \times v \oplus O \times v && (\text{حسب } (3)) \\ &= v \oplus z \end{aligned}$$

وهكذا فإن z هو العنصر المحايد الأيمن للعملية الثنائية $\oplus$. إضافة إلى ذلك لكل $v \in V$ فإن

$$\begin{aligned} z = O \times v = [1 + (-1)] \times v &= 1 \times v \oplus (-1) \times v \\ &= v \oplus (-1) \times v \end{aligned}$$

هـذا يبرهن أن $(-1) \times v$ هـو المعكـوس الأيمـن للعنصـر v وبـدوره يـؤدي إلى أن $< V, \oplus >$ زمرة تحت العملية $\oplus$.

والآن :

$$\begin{aligned} (1 + 1) \times (a \oplus b) &= 1 \times (a \oplus b) \oplus 1 \times (a \oplus b) && (\text{حسب } (3)) \\ &= [1 \times a \oplus 1 \times b] \oplus [1 \times a \oplus 1 \times b] && (\text{حسب } (2)) \\ &= a \oplus b \oplus a \oplus b && (\text{حسب } (6)) \end{aligned}$$

مرة أخرى :

$$\begin{aligned} (1 + 1) \times (a \oplus b) &= (1 + 1) \times a \oplus (1 + 1) \times b && (\text{حسب } (2)) \\ &= 1 \times a \oplus 1 \times a \oplus 1 \times b \oplus 1 \times b && (\text{حسب } (3)) \\ &= a \oplus a \oplus b \oplus b && (\text{حسب } (6)) \end{aligned}$$

عليه فإن $a \oplus b \oplus a \oplus b = a \oplus a \oplus b \oplus b$

وبتطبيق قانوني الحذف من اليمين واليسار للزمرة $< V, \oplus >$ نجد أن $a \oplus b = b \oplus a$ ، إذاً $< V, \oplus >$ زمرة إبدالية .

وبالتالي فإن $< V, \oplus, \times >$ فضاء متجهي على F .

تمرين 2

ليكن $/R$ حقل الأعداد الحقيقية و V مجموعة المتتابعات اللانهائية $< a_n >$ ، $a_n \in /R$ ، حيث المساواة والجمع والضرب في قياس معرفتان حداً حداً أي أن :

$$< a_n > + < b_n > = < a_n + b_n >$$
$$\alpha < a_n > = < \alpha a_n >$$

برهن أن V فضاء متجهي على $/R$ وأن المجموعة :

$U_n = \{ < x_n > |$ متقاربة $\sum x_n^2$ المتسلسلة$\}$ هي فضاء جزئي من V .

الحل

من السهولة التحقق من أن V فضاء متجهي على $/R$ ، نبرهن أن U فضاء جزئي من V . من الواضح إذا أخذنا $x_n = 0$ ، $n \in N$ فإن المتتابعة $< x_n >$ هي أحد عناصر U وعليه فإن $U \neq \phi$.

لتكن $< x_n >, < y_n > \in U$ هذا يعني أن كل من $\sum x_n^2$ ، $\sum y_n^2$ متسلسلة متقاربة . إذاً $\lim\limits_{n\to\infty} \sum\limits_{i=1}^{n} x_i^2 = L$ و $\lim\limits_{n\to\infty} \sum\limits_{i=1}^{n} y_i^2 = M$ لبعض L ، M في $/R$.

والآن
$$(x_i - y_i)^2 = x_i^2 + y_i^2 - 2x_i y_i = 2x_i^2 + 2y_i^2 - (x_i + y_i)^2$$
$$\leq 2x_i^2 + 2y_i^2 \qquad (\text{لأن } (x_i + y_i)^2 \geq 0)$$

والذي يعطينا
$$\sum_{i=1}^{n} (x_i - y_i)^2 \leq 2\sum_{i=1}^{n} x_i^2 + 2\sum_{i=1}^{n} y_i^2$$

بالتالي
$$\lim_{n\to\infty} \sum_{i=1}^{n} (x_i - y_i)^2 \leq 2 \lim_{n\to\infty} \sum_{i=1}^{n} x_i^2 + 2 \lim_{n\to\infty} \sum_{i=1}^{n} y_i^2 = 2L + 2M$$

والذي يؤدي إلى $\sum (x_i - y_i)^2$ متسلسلة متقاربة . نتيجة لهذا نجد أن المتتابعة $< x_n > - < y_2 > = < x_n - y_n > \in U$. وأخيراً لكل $\alpha \in /R$ فإن :

$$\lim_{n\to\infty}\sum_{i=1}^{n}(\alpha x_i)^2 = \alpha^2 L$$

والـــذي يـــؤدي إلى أن $\sum(\alpha x_i)^2$ متسلســـلة متقاربـــة . هـــذا يعـــني أن $\alpha < x_n > = < \alpha x_n > \in U$.

وهكذا فإن U فضاء جزئي من V .

تمرين 3

إذا كان V فضاءً متجهاً على حقل غير منته ، برهن أنه لا يمكن كتابة V على صورة اتحاد عدد منته من فضاءات جزئية فعلية .

الحل

إذا كان ممكناً افرض أن $V = \bigcup_{i=1}^{n} V_i$ وبدون أن نفقد العمومية بإمكاننا أن نفرض أن $V_i \not\subset \bigcup_{\substack{j=1\\ j\neq i}}^{n} V_j$ لكل i . عندئذ يكون $\bigcup_{i=1}^{n-1} V_i \not\subset V_n$ و $V_n \not\subset \bigcup_{i=1}^{n-1} V_i$ ، ومن ثم فإنه يوجد $v \in V_n$ ، $v \notin \bigcup_{i=1}^{n-1} V_i$. ويوجد $w \in \bigcup_{i=1}^{n-1} V_i$ ، $w \notin V_n$.

الآن اعتبر المجموعة $X = \{\lambda v + w \mid \lambda \in F\}$. فليس هناك عنصر في X ينتمي إلى V_n لأن خلاف ذلك يعني أن $w \in V_n$ ، ولكن $V = \bigcup_{i=1}^{n} V_i$ يؤدي إلى أن جميع عناصر X تنتمي إلى $\bigcup_{i=1}^{n-1} V_i$. بما أن F حقل غير منته فإنه بالإمكان إيجاد i_0 ، $1 \le i_0 \le n-1$ ، وعنصرين مختلفين $\alpha, \beta \in F$ بحيث $\alpha v + w \in V_{i_0}$ ، $\beta v + w \in V_{i_0}$ لبعض قيم i_0 ، $0 \le i_0 \le n-1$ ، هذا بدوره يؤدي إلى أن $(\alpha v + w) - (\beta v + w) \in V_{i_0} \subseteq \bigcup_{i=1}^{n-1} V_i$

$$\Rightarrow (\alpha - \beta)v \in \bigcup_{1}^{n-1} V_i$$

$$\Rightarrow (\alpha - \beta^{-1})(\alpha - \beta)v \in \bigcup_{i=1}^{n-1} V_i \qquad (\text{حيث } \alpha \neq \beta)$$

$$\Rightarrow v \in \bigcup_{i=1}^{n-1} V_i$$

وهذا ضد اختيار v . وبالتالي فإن المساواة $V = \bigcup_{1}^{n} V_i$ مستحيلة .

تمرين 4

يقال عن زمرة إبدالية $< V, + >$ أنها قابلة للقسمة إذا كان $nV = V$ لكل عدد صحيح n يختلف عن الصفر ، أي أنه لكل $u \in V$ ، ولكل عدد صحيح $n \neq 0$ يوجد $v \in V$ بحيث يكون $u = nv$. برهن أن $< V, + >$ فضاء متجهي على Q إذا وفقط إذا كان V زمرة قابلة للقسمة وجميع عناصرها الغير صفرية ذو رتبة غير منتهية .

الحل

افرض أن V زمرة قابلة للقسمة وكل عنصر غير صفري في V ذو رتبة غير منتهية . لكل عدد صحيح $q \neq 0$ ، و $u \in V$ يوجد $v \in V$ بحث أن $u = qv$. بالإضافة إذا ذلك إذا كان $u = qv = qv'$ فإن $q(v - v') = 0$. وبما أن V ليس فيه عنصر رتبته منتهية عدا الصفر فإن $v = v'$.

لأي $\frac{p}{q} \in Q$ ، $u \in V$ نعرف $\frac{p}{q} n = pv$ حيث $u = qv$. وحيث أن لكل $u \in V$ ، $0 \neq q \in Z$ يوجد عنصر وحيد v بحيث يكون $u = qv$ فإن التعريف السابق هو تعريف جيد .

إنه لأمر روتيني التحقق من أنه لكل $u, v \in V$ ، $\frac{p}{q}, \frac{r}{s} \in Q$ يكون :

$$\frac{p}{q}(u + v) = \frac{pu}{q} + \frac{pv}{q} , \left(\frac{p}{q} + \frac{r}{s}\right)u = \frac{pu}{q} + \frac{ru}{s}$$

و $1u = u$.

إضـافة إلى ذلـك للعنصـرين $\frac{p}{q}, \frac{r}{s} \in Q$ ، $u \in U$ ، اعتـبر $\frac{p}{q}\left(\frac{r}{s}v\right) = \frac{p}{q}(rv)$ حيـث $u = sv = pw$ حيث $rv = qw$.

مرة أخرى $\left(\frac{p}{q}.\frac{r}{s}\right)u = \left(\frac{pr}{qs}\right)u = prt$ حيث $u = qst$. عندئذ :

$$u = qst \Rightarrow sv = sqt \Rightarrow s(v - qt) = 0 \Rightarrow v - qt = 0$$

(لأن $s \neq 0$ و V لا يحتوي عنصراً غير صفري ذو رتبة منتهية) . ولسبب مشابه فإن :

$$qw = rv \Rightarrow qw = qrt \Rightarrow w = rt$$

وهكذا نحصل على أن

$$\left(\frac{p}{q}.\frac{r}{s}\right)u = prt = pw$$

وكذلك فإن

$$\left(\frac{p}{q}.\frac{r}{s}\right)u = \frac{p}{q}\left(\frac{r}{s}u\right)$$

إذاً V فضاء متجهي على Q .

بالعكس ليكن V فضاءً متجهاً على Q .

لاحظ أنه إذا كان V فضاءً متجهاً على حقل F فإنه لكل $n \in Z$ ، $\lambda \in F$ ، $v \in V$ يكون :

$$n(\lambda v) = (n\lambda)v = \lambda(nv) \qquad \text{(حقق !!)}$$

افرض الآن أن u عنصر في V بحيث $nu = 0$. إذا كان $n \neq 0$ فإن $\frac{1}{n} \in Q$ وحيث أن V فضاء متجهي على Q نحصل على :

$$\left(\frac{1}{n}\right)(nu) = 0 \Rightarrow \left(n\frac{1}{n}\right)u = 0 \Rightarrow u = 0$$

وبالتـالي لـيس في V عنصـر ذو رتبـة منتهيـة عـدا الصـفر بالإضـافة إلى ذلـك لكـل عنصـر $u \in V$ ولكل $n \neq 0$ في Z فإن

$$\frac{1}{n} \in Q \Rightarrow \frac{1}{n}u \in V$$

بوضع $\frac{1}{n}u = v$ نجد أن

$$nv = n\left(\frac{1}{n}u\right) = \left(n\frac{1}{n}\right)u = u$$

إذاً V قابلة للقسمة .

مسائل

1- برهن أن كلاً مما يأتي هو فضاء متجهي على حقل ما K :

(i) مجموعة جميع المصفوفات ذات السعة $m \times n$ والتي عناصرها في K تحت عملية جمع المصفوفات والضرب الاعتيادي للمصفوفات في عنصر من K .

(ii) المجموعة K^∞ مجموعة جميع المتتابعات اللانهائية $x = (x_1, x_2, x_3, \ldots,)$ حيث $x_i \in K$ لكل $i = 1, 2, \ldots$. عملية الجمع والضرب بقياسي لهذه المتتابعات معرفتين كالآتي :

لكل $x = (x_1, x_2, \ldots)$ ، $y = (y_1, y_2, \ldots)$ $x + y = (x_1 + y_1, x_2 + y_2, \ldots)$ ،

ولكل $\lambda \in K$ $\lambda x = (\lambda x_1, \lambda x_2, \ldots)$

2- برهن أن مجموعة جميع كثيرات الحدود في $K[x]$ والتي درجتها $\leq n$ (حيث n عدد صحيح موجب ثابت) هو فضاء جزئي للفضاء المتجهي في مثال 2 .

3- برهن أن مجموعة جميع المتتابعات اللانهائية $(x_1, x_2, \ldots)$ حيث $\sum x_i$ متقاربة هي فضاء جزئي من R^∞ .

4- برهن أن اتحاد فضائين جزئيين W_1 ، W_2 من فضاء متجهي V هو فضاء جزئي إذا وفقط إذا كان إما $W_1 \subseteq W_2$ أو $W_2 \subseteq W_1$.

5- برهن أنه إذا كان F حقلاً يحوي أكثر من k من العناصر ، فإنه لا يمكن التعبير عن V_F كاتحاد k من الفضاءات الجزئية الفعلية .

6- إذا كان N, M, L ثلاث فضاءات جزئية من فضاء متجهي V بحيث $M \subseteq L$ ، برهن أن $L \cap (M + N) = M + (L \cap W)$. اذكر مثالاً لإثبات أنه إذا كان N, M, L فضاءات جزئية من V فليس ضرورياً أن يكون :

$$L \cap (M + N) = L \cap M + L \cap N$$

7- برهن أنه إذا كان L, M, N فضاءات جزئية من فضاء متجهي V فإن $L + [M \cap (L + N)] = (L + M) \cap (L + N)$.

8- هل مجموعة الفضاءات الجزئية لفضاء متجهي V تكون زمرة جزئية تحت العلمية "+" ؟ (الجواب لا) .

9- برهن أنه إذا كان في فضاء متجهي V العلاقة :

$$L \cap (M + N) = L \cap M + L \cap N$$

متحققة لكل الفضاءات الجزئية L, M, N من الفضاء V فإن :

$$L + (M \cap N) = (L + M) \cap (L + N)$$

تكون متحققة أيضاً .

10- اعتبر المجموعات الجزئية V من C^3 والتي تحوي المتجهات (z, z_2, z_3) في أي من الحالات الآتية يكون V فضاءً جزئياً في الفضاء C^3 ؟

أ- z_1 عدد حقيقي .

ب- $z_1 = 0$.

ج- $z_1 + z_2 = 0$.

د- $z_1 + z_2 = 1$.

[إجابة (ب) ، (ج)] .

11- لتكن $P = IR[x]$ اعتبر المجموعات الجزئية V من P والتي تحوي كثيرات الحدود $f(x)$ التي يكون فيها :

(i) $\deg f(x) = 3$.

(ii) $2f(0) = f(1)$.

(iii) $f(t) \geq 0$ لكل $t \in [0, 1]$.

(iv) $f(t) = f(1-t)$ لكل $t \in IR$.

ففي أي من هذه الحالات يكون V فضاءً جزئياً من P_{IR} ؟

[إجابة (ii) و (iv) .]

12- إذا كان V فضاءً متجهاً على حقل F ، برهن أنه لكل عدد صحيح n ، $\lambda \in F$ ، $v \in V$ يكون $n(\lambda v) = \lambda(nv) = (n\lambda)v$.

13- برهن أن مجموعة جزئية غير خالية W من فضاء متجهي V_F يكون فضاءً جزئياً إذا وفقط إذا كان : $\lambda \in F, u, v \in W$ يؤدي إلى أن $\lambda u + v \in W$.

14- أي من هذه المجموعات الآتية تشكل فضاءً جزئياً من الفضاء المتجهي $M_n(F)$ المكون من المصفوفات ذات السعة $n \times n$ على الحقل F .

(a) جميع المصفوفات المثلثية العليا (فوق القطرية من الرتبة n) .

(b) جميع المصفوفات غير المنفردة من الرتبة n .

(c) جميع المصفوفات المتناظرة (المتماثلة) من الرتبة n .

(d) جميع المصفوفات من الرتبة n ، والتي مجموع عناصرها القطرية يساوي الصفر .

[إجابة (a) ، (b) و (d)] .

15- ليكن W_R فضاءً متجهاً و V مجموعة جزئية غير خالية من W_R . يقال أن V مجموعة جزئية محدبة إذا كان $cu + dv \in V$ لكل $u, v \in V$ حيث $c \geq 0,\ d \geq 0$ و $c + d = 1$. أثبت أن تقاطع أي تجمع من المجموعات الجزئية المحدبة هو مجموعة جزئية محدبة .

16- برهن أن الشرط $1.x = x$ لكل $x \in V$ في تعريف الفضاء المتجهي على حقل F يمكن إبداله بالشرط $\lambda x = 0$ إذا وفقط إذا كان $\lambda = 0$ أو $x = 0$ حيث $x \in V, \lambda \in F$.

17- برهن أن مجموعة جميع حلول المعادلة التفاضلية الآتية هي فضاء متجهي :

$$\frac{d^2y}{dt^2} + p\,\frac{dy}{dt} + qy = 0$$

حيث p ، q دوال مثبتة للمتغير t .

18- ليكن V الفضاء المتجهي لجميع الدوال من IR إلى IR (مثال 3) . إذا كان V_e المجموعة الجزئية للدوال الزوجية $(f(-x) = f(x))$ و V_o المجموعة الجزئية للدوال الفردية $(f(-x) = -f(x))$ ، برهن :

1- V_e ، V_O فضاءان جزئيان من V .

2- $V_e + V_O = V$.

3- $V_2 \cap V_O = (0)$.

1- الارتباط الخطي Linear Dependence

لأية مجموعة جزئية X من فضاء متجهي V_F ، عرفنا في البند السابق مفهوم الفضاء الجزئي $< X >$ المولد بالمجموعة X . وعندما تكون X مجموعة منتهية غير خالية ، أثبتنا أن $< X >$ تحوي جميع التراكيب الخطية لعناصر X . في الحقيقة لكل مجموعة جزئية $X(\neq \phi)$ من V_F نستطيع البرهنة على أن $< X >$ تضم جميع التراكيب الخطية لعناصر X (آخذين في كل مرة عدداً منتهياً) .

وهكذا فإن $x \in < X >$ إذا وفقط إذا كان x تركيباً خطياً لعدد منته من عناصر X . في هذه الحالة نقول أن x مرتبطة خطياً على X . لدينا أيضاً التعريف الآتي .

تعريف 11-13

ليكن $x_1, x_2, \ldots, x_n$ عدداً منتهياً من عناصر فضاء متجهي V_F (ليس بالضرورة أن تكون جميعها مختلفة) . يقال عن هذه المتجهات أنها مرتبطة خطياً $(L.D)$ إذا وجدت عناصر $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ أحدها على الأقل لا يساوي الصفر بحيث :

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = 0$$

ويقال عن هذه المتجهات أنها مستقلة خطياً $(L.I)$ إذا كان لكل $\alpha_i \in F$ $(i = 1, 2, \ldots, n)$

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = 0 \Rightarrow \alpha_i = 0$$

المجموعة $X = \{x_1, x_2, \ldots, x_n\}$ التي تضم n من العناصر المختلفة يقال أنها مرتبطة خطياً $(L.D)$ أو مستقلة خطياً $(L.I)$ تبعاً لكون العناصر التي تحويها وعددها n مرتبطة خطياً أو مستقلة خطياً .

وبصورة عامة فإن أية مجموعة جزئية Y من V_F يقال أنها مستقلة خطياً $(L.I)$ إذا كانت جميع المجموعات الجزئية المنتهية وغير الخالية منها مستقلة خطياً وبخلاف ذلك يقال أنها $(L.D)$. وعليه إذا كان $x(\neq 0) \in V$ ، وحيث أن لكل $\alpha \in F$ ،

$\alpha x = 0 \Rightarrow \alpha = 0$ فإننا نستطيع القول أن x مستقلة خطياً أو بمعنى آخر المجموعة الأحادية $\{x\}$ مستقلة خطياً . المجموعة الخالية من المتجهات ϕ هي مجموعة مستقلة خطياً لأنه ليس لها أية مجموعة جزئية منتهية غير خالية ، وبالتالي فهي تحقق الشرط الذي يعرف مجموعة مستقلة خطياً . بما أن لكل $\alpha(\neq 0) \in F$ ، فإن $\alpha 0 = 0$ ، نجد أن 0 هو $L.D$ وبالتالي أية مجموعة من المتجهات تحوي 0 تكون مرتبطة خطياً $(L.D)$.

مثال 11

اعتبر المجموعة $V = \{(\alpha, \beta) : \alpha, \beta \in F\}$ حيث F حقل ما فإن المتجهان $c_1 = (1, 0)$ ، $e_2 = (0, 1)$ في V مستقلة خطياً لأن لكل $\alpha_1, \alpha_2 \in F$:

$$\alpha_1 e_1 + \alpha_2 e_2 = (\alpha_1, 0) + (0, \alpha_2) = (0, 0)$$
$$\Rightarrow (\alpha_1, \alpha_2) = (0, 0) \Rightarrow \alpha_1 = 0, \alpha_2 = 0$$

إضافة إلى ذلك لاحظ أن أي متجه $(\alpha, \beta) \in V$ يمكن التعبير عنه بالصورة $\alpha e_1 + \beta e_2$ أي كتركيب خطي من e_1 و e_2 .

نظرية 11-14

إذا كانت المتجهات $v_1, v_2, \ldots, v_n$ مستقلة خطياً في فضاء متجهي V_F ، فإن كل عنصر في الفضاء الجزئي W المتولد بهذه العناصر يمكن التعبير عنه كتركيب خطي للمتجهات $v_1, v_2, \ldots, v_n$ وبطريقة وحيدة .

البرهان

كل عنصر $w \in W$ يمكن التعبير عنه كتركيب خطي للمتجهات المعطاة (نظرية 11-9) . افرض أن المتجه $w \in W$ يمكن التعبير عنه بطريقتين ولتكن :

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$$
$$w = \beta_1 v_1 + \beta_2 v_2 + \ldots + \beta_n v_n$$

هذا يؤدي إلى أن

$$0 = (\alpha_1 - \beta_1)v_1 + (\alpha_2 - \beta_2)v_2 + \ldots + (\alpha_n - \beta_n)v_n$$

وحيث أن المتجهات v_i ، $i = 1, 2, \ldots, n$ مستقلة خطياً فإن المعادلة الأخيرة تتحقق عندما $\alpha_i = \beta_i = 0$ لكل $i = 1, 2, \ldots, n$ أي أن $\alpha_i = \beta_i$ لكل $1 \le i \le n$. لذا فإن $w = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$ هو التعبير الوحيد للمتجه w كتركيب خطي من المتجهات v_i ، $1 \le i \le n$. □

نظرية 11-15

إذا كان $u_1, u_2, \ldots, u_n$ ، أي n من المتجهات المستقلة خطياً في فضاء متجهي V_F . فإن أي $n+1$ من المتجهات $v_1, v_2, \ldots, v_{n+1}$ التي كل منها تركيب خطي من المتجهات $u_1, u_2, \ldots, u_n$ تكون مرتبطة خطياً .

البرهان

نبرهن النتيجة بالاستنتاج الرياضي على n . إذا كان أي متجه من هذه المتجهات هو المتجه الصفري ، فمن الواضح أن $n+1$ المتجهات المعطاة هي مرتبطة خطياً . نفرض أن أياً من المتجهات v_i ، $1 \le i \le n+1$ ليس المتجه الصفري ، وحيث أن كل من v_1, v_2 تركيب خطي من المتجهات $u_1, u_2, \ldots, u_n$ فإذا كان $n = 1$ فإن $v_1 = \alpha_1 u_1$ ، $v_2 = \alpha_2 u_2$ ، حيث $\alpha_1 \neq 0 \neq \alpha_2$ وهذا يعني أن $v_1 - \alpha_1 \alpha_2^{-1} v_2 = 0$. وبالتالي فإن v_2 و v_1 مرتبطان خطياً .

ولكي نستخدم الاستنتاج الرياضي دعنا نفرض أن النتيجة محققة لكل k من المتجهات المستقلة خطياً حيث $k < n$. والآن يمكننا كتابة :

$$\begin{aligned}
v_1 &= \alpha_{11} u_1 + \alpha_{12} u_2 + \ldots + \alpha_{1n} u_n \\
v_2 &= \alpha_{21} u_1 + \alpha_{22} u_2 + \ldots + \alpha_{2n} u_n \\
&\ldots \qquad \ldots \qquad \ldots \\
v_{n+1} &= \alpha_{n+1,1} u_1 + \alpha_{n+2,2} u_2 + \ldots + \alpha_{n+1,n} u_n
\end{aligned}$$

لبعض قياسيات (عناصر في F) $\alpha_{ij} \in F$. فإذا كان $\alpha_{in} = 0$ لكل $i = 1, 2, \ldots, n+1$ فإن كل v_i هو تركيب خطي من $n-1$ من المتجهات $u_1, u_2, \ldots, u_{n-1}$ وعندئذ فإن فروض

الاستنتاج الرياضي يؤدي إلى أن $v_1, v_2, \dots v_n$ مرتبطة خطياً وبناءً عليه فإن $v_1, v_2, \dots, v_{n+1}$ تكون مرتبطة خطياً أيضاً . وهذا يعني أن واحداً على الأقل من $\alpha_{in} \neq 0$ وليكن وتحديداً $\alpha_{1n} \neq 0$. عندئذ لكل $i = 2, 3, \dots, n+1$ يكون :

$$v_i - \alpha_{in}\alpha_{1n}^{-1}v_1 = (\alpha_{i1} - \alpha_{in}a_{11}\alpha_{1n}^{-1})\,u_1 + (\alpha_{i2} - \alpha_{in}\alpha_{12}\alpha_{1n}^{-1})\,u_2 + \dots + (\alpha_{i,n-1} - \alpha_{in}\alpha_{1,n-1}\alpha_{1n}^{-1})\,u_{n-1}$$

وبناءً على فروض الاستنتاج الرياضي تكون المتجهات $(2 \le i \le n+1)$ $w_i = v_i - \alpha_{in}\alpha_{1n}^{-1}v_1$ مرتبطة خطياً وبالتالي فإنه يوجد $\beta_2, \beta_3, \dots, \beta_{n+1}$ في F ليست جميعها أصفاراً ، بحيث يكون $\beta_2 w_2 + \beta_3 w_3 + \dots \beta_{n+1} w_{n+1} = 0$

أي أن :

$$\beta_2(v_2 - \alpha_{2n}\alpha_{1n}^{-1}v_1) + \beta_3(v_3 - \alpha_{3n}\alpha_{1n}^{-1}v_1) + \dots + \beta_{n+1}(v_{n+1} - \alpha_{n+1,n}\alpha_{1n}^{-1}v_1) = 0$$

أي أن :

$$(-\beta_2\alpha_{2n}\alpha_{1n}^{-1} - \beta_3\alpha_{3n}\alpha_{1n}^{-1} \dots - \beta_{n+1}\alpha_{n+1}, n\alpha_{1n}^{-1})v_1 + \beta_2 v_2 + \dots + \beta_{n+1}v_{n+1} = 0$$

وهذا يثبت أن المتجهات $v_1, v_2, \dots, v_{n+1}$ مرتبطة خطياً . وعلى ذلك فمن مبدأ الاستنتاج الرياضي تكون النتيجة متحققة لجميع n . □

نتيجة 16-11

إذا كانت $\{v_1, v_2, \dots, v_n\}$ مجموعة جزئية مستقلة خطياً من فضاء متجهي V_F ، فإن أية مجموعة جزئية W من V تضم أكثر من n من المتجهات وكل متجه يمكن التعبير عنه كتركيب خطي من $v_1, v_2, \dots, v_n$ تكون مرتبطة خطياً .

البرهان

بما أن W تحوي أكثر من n من العناصر فإنه بالإمكان اختيار $n+1$ من العناصر من W ولتكن u_1, u_2 و u_{n+1} . من النظرية السابقة فإن هذه المتجهات مرتبطة خطياً . أي أن W تحوي مجموعة جزئية مرتبطة خطياً وبالتالي فإن W مرتبطة خطياً . □

تعريف 11-17

يقال لمجموعة جزئية B من فضاء متجهي V_F أنها قاعدة للفضاء V إذا كان :
(1) B مستقلة خطياً ، و (2) B تولد الفضاء المتجهي V .

تعريف 11-18

يقال لفضاء متجهي V_F أنه منته التولد إذا وجدت مجموعة جزئية منتهية من V_F تولد الفضاء V .

مثال 12

لأي حقل F ، اعتبر $F^{(n)}$ الفضاء المتجهي على F والذي يحوي جميع المرتبات النونية بالصيغة $\overbrace{(\alpha_1, \alpha_2, \ldots, \alpha_n)}^{\text{في الموقع } i}$ ، ليكن $e_1 = (1, 0, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0)$

وبصورة عامة $e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ حيث $(i = 1, 2, \ldots n)$. فكما رأينا في مثال 9 تكون المتجهات $e_1, e_2, \ldots, e_n$ مستقلة خطياً وتولد الفضاء $F^{(n)}$ وعلى ذلك فإن $\{e_1, e_2, \ldots, e_n\}$ قاعدة للفضاء $F^{(n)}$ ومن ثم فإن $F^{(n)}$ منته التولد .

قضية 11-19

إذا كانت $x_1, x_2, \ldots, x_n$ متجهات غير صفرية ومرتبطة خطياً في الفضاء V_F ، فإنه يوجد i ، $2 \le i \le n$ بحيث x_i هو تركيب خطي من المتجهات السابقة له $x_1, x_2, \ldots, x_{i-1}$. ويكون الفضاء الجزئي المتولد بالمجموعة $\{x_1, x_2, \ldots, x_n\}$ هو نفس الفضاء المتولد بمجموعة المتجهات $\{x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n\}$.

البرهان

بما أن المتجهات $x_1, x_2, \ldots, x_n$ مرتبطة خطياً فإنه يوجد $\alpha_1, \alpha_2, \ldots, \alpha_n$ في F ليس جميعها صفراً بحيث :

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n = 0 \qquad (1)$$

فإذا كان i أكبر رقم بحيث أن $\alpha_i \neq 0$ فإن العناصر $\alpha_{i+1}, \alpha_{i+2}, \ldots, \alpha_n$ تكون جميعها صفراً. إذا كان $i = 1$ فإن $\alpha_1 x_1 = 0$ وبالتالي $\alpha_1 = 0$ لأن $x_1 \neq 0$ وهكذا فإن $i \geq 2$. ومن ثم فإن المعادلة (1) تعطينا :

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_i x_i = 0 \qquad (2)$$

ومنها

$$\begin{aligned} x_i &= -\alpha_i^{-1}\alpha_1 x_1 - \alpha_i^{-1}\alpha_2 x_2 - \ldots - \alpha_i^{-1}\alpha_{i-1}x_{i-1} \\ &= \beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_{i-1}x_{i-1} \end{aligned}$$

حيث :

$$1 \leq j \leq n-1 \quad \text{لكل} \quad \beta_j = -\alpha_i^{-1}\alpha_j \qquad (3)$$

أي أن x_i هو تركيب خطي من المتجهات $x_1, x_2, \ldots, x_{i-1}$.

ليكن W هو الفضاء الجزئي المتولد من المتجهات $x_1, x_2, \ldots, x_n$ فيمكننا كتابة أي متجه $x \in W$ بالصورة :

$$x = \gamma_1 x_1 + \gamma_2 x_2 + \ldots + \gamma_{i-1}x_{i-1} + \gamma_i x_i + \gamma_{i+1}x_{i+1} + \ldots + \gamma_n x_n$$

لبعض $\gamma_j \in F$ ، $1 \leq j \leq n$.

باستخدام (3) نجد أن :

$$\begin{aligned} x &= \gamma_1 x_1 + \gamma_2 x_2 + \ldots + \gamma_{i-1}x_{i-1} + \gamma_i(\beta_1 x_1 + \beta_2 x_2 + \ldots \\ &\qquad + \beta_{i-1}x_{i-1}) + \gamma_{i+1}x_{i+1} + \ldots + \gamma_n x_n \\ &= (\gamma_1 + \gamma_i\beta_1)x_1 + (\gamma_2 + \gamma_i\beta_2)x_2 + \ldots + (\gamma_{i-1} + \gamma_i\beta_{i-1})x_{i-1} + \\ &\qquad \gamma_{i+1}x_{i+1} + \ldots + \gamma_n x_n \end{aligned}$$

وهذا يبين أن كل $x \in W$ هو تركيب خطي من المتجهات $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$. وبالتالي فإن هذه المتجهات وعددها $(n-1)$ تولد الفضاء W . □

نظرية 11-20

إذا كان V_F فضاءً متجهاً منته التولد . فإن V_F لها قاعدة منتهية . وأن أي قاعدتين للفضاء V_F لهما نفس العدد من المتجهات .

البرهان

بما أن V_F منتهـه التولد فإنه توجد مجموعة جزئية منتهية من المتجهات $B = \{x_1, x_2, \ldots, x_m\}$ تولد V . فإذا كانت B مستقلة خطياً ، كانت هي القاعدة المنتهية المطلوبة . وإذا كانت مرتبطة خطياً فإن لبعض i ، $1 \le i \le m$ توجد مجموعة من المتجهات $B_1 = \{x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m\}$ تولد V أيضاً (قضية 11-19) .

وهكذا فإن B_1 هي مجموعة جزئية من B تحوي $m - 1$ متجهاً والتي تولد V أيضاً . ومرة أخرى إذا كانت B_1 مستقلة خطياً فإننا نكون قد أكملنا البرهان . وإذا كانت مرتبطة خطياً فإنه توجد مجموعة جزئية B_2 من B_1 تحوي $m - 2$ من المتجهات والتي تولد V أيضاً . وبما أن B تحوي فقط m من المتجهات فإن هذه العملية لا يمكن أن تستمر لأكثر من m من المرات ، وهكذا فبعد عدد منته من الخطوات نحصل على مجموعة جزئية مستقلة خطياً B_j من B تولد V . وتكون B_j هي القاعدة المنتهية المطلوبة للفضاء V .

والآن افرض أن B_j تضم n من المتجهات ولتكن B' قاعدة أخرى للفضاء V وتضم عدداً أكثر من n من المتجهات ، فبما أن كل متجه في V وبصورة خاصة كل متجه في B' هو عبارة عن تركيب خطي من n من العناصر الموجودة في B_j فإن B' تكون مرتبطة خطياً (نتيجة 11-16) وهذا تناقض . لذا فإن عدد العناصر في B' وليكن n' لا يمكن أن يتجاوز n $(n' \le n)$ وبتبديل المواقع بين B و B_j نحصل على أن n لا يمكن أن يتجاوز n' $(n \le n')$ أي أن $n = n'$. وهذا يثبت أن كل قاعدة للفضاء V تحوي n من العناصر وهذا يكمل البرهان . □

النظرية السابقة تقودنا إلى التعريف الآتي .

تعريف 11-21

إذا كان V_F فضاء متجهاً له قاعدة منتهية عدد عناصرها n فإن n يسمى بعد الفضاء V ($\text{dimension } V$) . وإذا لم تكن للفضاء V قاعدة منتهية نقول أن V ذو بعد غير منته .

كما لوحظ في نظرية 11-20 أنه إذا كان V_F منته التولد فإن القواعد المختلفة للفضاء V_F لها نفس العدد من المتجهات وليكن n . وعليه فإن بعد الفضاء V_F هو عدد وحيد . إذا كان $V_F = (0)$ فإن المجموعة الخالية ϕ تولد V_F ، وهكذا فإن V_F له بعد مساوي للصفر .

ملاحظة نحن مهتمون فقط بدراسة الفضاءات المتجهة ذات الأبعاد المنتهية . لذا فإن كل فضاء متجهي في هذا الفصل ذو بعد منته إلا إذا ذكر غير ذلك .

اصطلاح سوف يرمز لبعد الفضاء المتجهي بالرمز $\dim V$.

نظرية 11-22

إذا كان V_F فضاءاً متجهاً ذو بعد n ، فإن :

(1) كل $n + 1$ من عناصر V_F تكون مرتبطة خطياً .

(2) إذا كانت المتجهات $z_1, z_2, \ldots, z_n$ تولد V فهي مستقلة خطياً .

البرهان

بما أن بعد الفضاء V هو n $(\dim V = n)$ ، فإن V له قاعدة ، ولتكن $\{x_1, x_2, \ldots, x_n\}$ قاعدة له .

فـإذا كـان $y_1, y_2, \ldots, y_{n+1}$ متجهـات في V عـددها $n+1$ فمـن تعريـف القاعـدة يكون كل y_i ، $1 \le i \le n+1$ ممثلاً بتركيب خطي من المتجهات $x_1, x_2, \ldots, x_n$. واستناداً إلى نظرية 11-15 فإن المتجهات $y_1, y_2, \ldots, y_{n+1}$ هي مرتبطة خطياً وهذا يثبت صحة (1) .

وقد رأينا في برهان نظرية 11-20 أنه إذا وجدت مجموعة جزئية منتهية B من V تولد V فإن B تحوي مجموعة جزئية B' هي قاعدة للفضاء V .

بما أن $B = \{z_1, z_2, \ldots, z_n\}$ يولـد V ، فـإن لهـا مجموعـة جزئيـة B' هـي قاعـدة للفضاء V . وحيث أن $\dim V = n$ فإن B' يجب أن تحوي n من العناصر ، وعليه يكون $B = B'$ ، كمـا أن B نفسـها هـي قاعـدة للفضـاء V وتكـون $z_1, z_2, \ldots, z_n$ مستقلة خطياً وهذا يبرهن (2) . □

نظرية 11-23

إذا كانت $\{u_1, u_2, \ldots, u_k\}$ مجموعة جزئية مستقلة خطياً من فضاء متجهي V_F ذو بعد منته ، فإنه يمكن توسيعها إلى قاعدة للفضاء V ، بمعنى آخر بالإمكان إيجاد متجهات $v_{k+1}, v_{k+2}, \ldots, v_n$ بحيث تكون $u_1, u_2, \ldots, u_k, v_{k+1}, v_{k+2}, \ldots, v_n$ قاعدة للفضاء V .

البرهان

نفـرض $\dim V = n$ عندئـذ تكـون أي $n+1$ مـن المتجهـات في V مرتبطـة خطيـاً (نظرية 11-22) ، أي أن $k \le n$.

لتكن $\{w_1, w_2, \ldots, w_n\}$ قاعدة للفضاء V . نبرهن النتيجة بالاستنتاج الرياضي على k . إذا كـان $k = 1$ ولأن $u_1 \in V$ يكـون لـدينا $u_1 = \alpha_1 w_1 + \alpha_2 w_2 + \ldots + \alpha_n w_n$ لـبعض

$\alpha_i \in F$ ، بما أن $u_1 \neq 0$ فإن $\alpha_i \neq 0$ لبعض i ، إذا كان j أكبر رقم بحيث $\alpha_j \neq 0$

فإن
$$u_1 = \alpha_1 w_1 + \alpha_2 w_2 + \ldots + \alpha_j w_j$$
$$\Rightarrow w_j = \alpha_j^{-1} u_1 - \alpha_j^{-1}\alpha_1 w_1 - \ldots - \alpha_j^{-1}\alpha_{j-1} w_{j-1}$$
$$\Rightarrow w_j \in < u_1, w_1, w_2, \ldots, w_{j-1} >$$
$$\subseteq < u_1, w_1, w_2, \ldots, w_{j-1}, w_{j+1}, \ldots, w_n >$$

بما أن $w_i \in < u_1, w_1, w_2, \ldots, w_{j-1}, w_{j+1}, \ldots, w_n >$ لكل $i \neq j$

فإن $V = < w_1, w_2, \ldots, w_n > \subseteq < u_1, w_1, w_2, \ldots, w_{j-1}, w_{j+1}, \ldots, w_n > \subseteq V$

إذاً $V = < u_1, w_1, w_2, \ldots, w_{j-1}, w_{j+1}, \ldots, w_n >$

وهذا يبرهن أن المتجهات $u_1, w_1, w_2, \ldots, w_{j-1}, w_{j+1}, \ldots, w_n$ وعددها n تولد V . وبما أن $\dim V = n$ ، فإن هذه المتجهات تشكل قاعدة للفضاء V . وعليه النتيجة محققة عندما $k = 1$. ولتطبيق الاستنتاج الرياضي افرض $k > 1$ وأن النتيجة متحققة لأي $k - 1$ من المتجهات المستقلة خطياً . عندئذ بإمكاننا إيجاد متجهات $t_k, t_{k+1}, \ldots, t_n$ بحيث أن $\{u_1, u_2, \ldots, u_{k-1}, t_k, t_{k+1}, \ldots, t_n\}$ تشكل قاعدة للفضاء V . وبما أن $u_k \in V$ فإن :

$$u_k = \beta_1 u_1 + \beta_2 u_2 + \ldots + \beta_{k-1} u_{k-1} + \gamma_k t_k + \ldots + \gamma_n t_n$$ لبعض $B_i, \gamma_j \in F$

إذا كان $\gamma_k = \gamma_{k+1} = \ldots = \gamma_u = 0$ فإن $u_k = \beta_1 u_1 + \beta_2 u_2 + \ldots + \beta_{k-1} u_{k-1}$

والذي يؤدي إلى أن المتجهات $u_1, u_2, \ldots, u_{k-1}, u_k$ مرتبطة خطياً وهذا تناقض .

عليه يوجد $i \geq k$ بحيث $\gamma_i \neq 0$ عندئذ يكون :
$$t_i = -\gamma_i^{-1}\beta_1 u_1 - \ldots - \gamma_i^{-1} u_k - \gamma_i^{-1}\gamma_k t_k - \ldots - \gamma_i^{-1}\gamma_{i-1} t_{i-1} - \gamma_i^{-1}\gamma_{i+1} t_{i+1} - \ldots - \gamma_i^{-1}\gamma_n t_n$$

وبالتالي فإن $t_i \in < u_1, u_2, \ldots, u_k, t_k, t_{k+1}, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n >$

هـذا أيضـاً يبين أن $\{u_1, u_2, \ldots, u_k, t_k, t_{k+1}, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n\}$ قاعـدة للفضـاء V . وحسب الاستنتاج فإن النتيجة صحيحة لجميع $k \leq n$. □

نتيجة 11-24

إذا كان V_F فضاء متجهي ذو بعد n ، فإن أي n من المتجهات المستقلة خطياً من V_F تشكل قاعدة للفضاء V_F .

البرهان

لتكن $x_1, x_2, \ldots, x_n$ أي n من المتجهات المستقلة خطياً في V . النظرية السابقة تمكننا من إضافة بعض المتجهات لنحصل على قاعدة للفضاء V . من ناحية أخرى فإن أية قاعدة للفضاء V تحوي على n من العناصر فقط وبالتالي فإن المتجهات $x_1, x_2, \ldots, x_n$ وعددها n تشكل قاعدة للفضاء V . □

نتيجة 11-25

لأي فضاء جزئي W من فضاء متجهي ذو بعد منته V_F ، فإن $\dim W \le \dim V$ وأن $W = V$ إذا وفقط إذا كان $\dim W = \dim V$.

البرهان

لنفرض أن $\dim V = n$. بما أن V لا تحوي أكثر من n من المتجهات المستقلة خطياً ، فإنه لا توجد مجموعة جزئية مستقلة خطياً من W تحوي أكثر من n عنصراً . لتكن $B = \{y_1, y_2, \ldots, y_m\}$ مجموعة جزئية من W تحوي أكبر عدد من العناصر المستقلة خطياً وليكن m . عندئذ $m \le n$ وأي $m+1$ من المتجهات في W تكون مرتبطة خطياً . وهكذا إذا كان $y(\neq 0) \in W$ ، فإن المتجهات $y_1, y_2, \ldots, y_m, y$ مرتبطة خطياً . وعليه يوجد $\beta_1, \beta_2, \ldots, \beta_m, \beta$ في F ليس جميعها صفراً بحيث $\beta_1 y_1 + \beta_2 y_2 + \ldots + \beta_m y_m + \beta y = 0$.

إذا كـان $\beta = 0$ فـإن الاسـتقلال الخطـي للمتجهـات $y_1, y_2, \dots, y_m$ يـؤدي إلى أن يكون جميع $\beta_1, \beta_2, \dots, \beta_m$ صفراً وهذا تناقض . وهكذا فإن $\beta \neq 0$ وعليه يكون لدينا :

$$y = -\beta^{-1}\beta_1 y_1 - \beta^{-1}\beta_2 y_2 - \dots - \beta^{-1}\beta_m y_m$$

والذي يبين أن كل عنصر في W يمكن التعبير عنه كتركيب خطي من $y_1, y_2, \dots, y_m$ وبالتالي فإن $\{y_1, y_2, \dots, y_m\}$ قاعدة للفضاء W هذا يبرهن الجزء الأول .

الآن إذا كانـت $\{z_1, z_2, \dots, z_n\}$ قاعـدة للفضـاء W تحـوي n مـن المتجهـات ، هـذه المتجهـات تكـون مسـتقلة خطيـاً في V أيضـاً . وبمـا أن أي n مـن المتجهـات المسـتقلة خطيـاً تشـكل قاعـدة للفضـاء V فـإن $\{z_1, z_2, \dots, z_n\}$ تولـد V . وهكـذا يكـون $W = V$. ومـن الواضح أنه إذا كان $W = V$ فإن $\dim W = \dim V$. □

نظرية 26-11

إذا كان U و W فضاءان جزئيان من فضاء متجهي ذو بعد منته V_F ، فإن :

$$\dim(U + W) = \dim U + \dim W - \dim(V \cap W)$$

البرهان

لنفـــرض $\dim U = r$ ، $\dim W = s$ و $\dim(U \cap W) = t$ لـــتكن $\{e_1, e_2, \dots, e_t\}$ قاعـدة للفضـاء $U \cap W$. بمـا أن $U \cap W$ فضـاء جزئي مـن U فإنـه يمكـن توسيع القاعـدة المـذكورة إلى قاعـدة $\{e_1, e_2, \dots, e_t, f_1, f_2, \dots f_{r-t}\}$ للفضـاء U . هـذه القاعـدة تضـم r مـن العناصـر لأن $\dim U = r$ ، بالمثـل توجـد قاعــدة $\{e_1, e_2, \dots, e_t, g_1, g_2, \dots, g_{s-t}\}$ للفضــاء W .

والآن ندعي أن المجموعة :

$$B = \{e_1, e_2, \dots, e_t, f_1, f_2, \dots, f_{r-t}, g_1, g_2, \dots, g_{s-t}\}$$

التي تحوي $r + s - t$ من المتجهات هي قاعدة للفضاء $U + W$ وبالتالي يكون $\dim(U + W) = r + s - t$.

وللبرهنة على صحة الادعاء اعتبر أي $x \in U + W$ ، فإن $x = u + v$ لبعض $u \in U$ ، $v \in W$.

إضافة إلى ذلك فإن :

$$u = \alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_t e_t + \beta_1 f_1 + \beta_2 f_2 + \dots + \beta_{r-t} f_{r-t};$$
$$v = \alpha'_1 e_1 + \alpha'_2 e_2 + \dots + \alpha'_t e_t + \gamma_1 g_1 + \gamma_2 g_2 + \dots + \gamma_{s-t} g_{s-t}$$

لبعض $\alpha_i, \alpha'_j, \beta_k, \gamma_t \in F$ والذي يؤدي إلى أن :

$$x = u + v = (\alpha_1 + \alpha'_1)e_1 + (\alpha_2 + \alpha'_2)e_2 + \dots + (\alpha_t + \alpha'_t)e_t$$
$$+\beta_1 f_1 + \beta_2 f_2 + \dots + \beta_{r-t} f_{r-t} + \gamma_1 g_1 + \gamma_2 g_2 + \dots + \gamma_{s-t} g_{s-t}$$

وهكذا فإن كل متجه x في $U + W$ هو تركيب خطي لمتجهات في B . وعليه فإن B يولد $U + W$. وللبرهنة على أن B مستقلة خطياً نفرض أن :

$$\alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_t e_t + \beta_1 f_1 + \beta_2 f_2 + \dots + \beta_{r-t} f_{r-t}$$
$$+\gamma_1 g_1 + \gamma_2 g_2 + \dots + \gamma_{s-t} g_{s-t} = 0 \qquad \dots (1)$$

لبعض $\alpha_i, \beta_j, \gamma_k \in F$.

هذا يؤدي إلى أن :

$$-(\alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_t e_t + \beta_1 f_1 + \beta_2 f_2 + \dots + \beta_{r-t} f_{r-t}) =$$
$$\gamma_1 g_1 + \gamma_2 g_2 + \dots + \gamma_{s-t} g_{s-t} \in U \cap W$$

ولكن $V \cap W = < e_1, e_2, \dots, e_t >$ ، وهذا يؤدي إلى أن :

$$\gamma_1 g_1 + \gamma_2 g_2 + \dots + \gamma_{s-t} g_{s-t} = \delta_1 e_1 + \delta_2 e_2 + \dots + \delta_t e_t$$

لبعض $\delta_i \in F$.

$$\Rightarrow \delta_1 e_1 + \delta_2 e_2 + \dots + \delta_t e_t - \gamma_1 g_1 - \gamma_2 g_2 - \dots - \gamma_{s-t} g_{s-t} = 0$$

وبما أن $e_1, e_2, \dots, e_t, g_1, g_2, \dots, g_{s-t}$ مستقلة خطياً فإن $\gamma_1 = \gamma_2 = \dots = \gamma_{s-t} = 0$ وبالتالي فإن (1) يؤدي إلى أن :

$$\alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_t e_t + \beta_1 f_1 + \beta_2 f_2 + \ldots + \beta_{r-t} f_{r-t} = 0$$

ولأن $e_1, e_2, \ldots, e_t, f_1, f_2, \ldots, f_{r-t}$ مستقلة خطياً فإن :

$$\alpha_1 = \alpha_2 = \alpha_3 = \ldots = \alpha_t = \beta_1 = \beta_2 = \ldots = \beta_{r-t} = 0$$

وبالتالي فإن جميع المعاملات في الطرف الأيسر من (1) يساوي للصفر . والذي يثبت أن B مستقلة خطياً . أي أن B قاعدة للفضاء $U + W$.

وبذلك توصلنا إلى أن $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$. □

نتيجة 11-27

إذا كان U و W فضاءان جزئيان من فضاء متجهي ذو بعد منته V_F بحيث $U \cap W = \{0\}$ فإن :

$$\dim(U + W) = \dim U + \dim W$$

البرهان

بما أن $U \cap W = (0)$ ، فإن $\dim(U \cap W) = 0$ بالتالي فإن :

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$
$$\Rightarrow \dim(U + W) = \dim U + \dim W . \square$$

تمارين محلولة

تمرين 1

برهن أن المتجهين (ξ_1, ξ_2) ، (η_1, η_2) مرتبطان خطياً في C إذا وفقط إذا كان $\xi_1 \eta_2 = \xi_2 \eta_1$.

الحل

لنفرض أن المتجهين $(\xi_1, \xi_2), (\eta_1, \eta_2)$ مرتبطان خطياً . عندئذ يوجد $\alpha_1, \alpha_2 \in C$ ليس كلاهما صفراً بحيث $\alpha_1(\xi_1, \xi_2) + \alpha_2(\eta_1, \eta_2) = (0, 0)$ دون أن نفقط العمومية ، دعنا نفرض أن $\alpha_1 \neq 0$. هذا يؤدي إلى أن $(\xi_1, \xi_2) = \alpha_1^{-1}\alpha_2(\eta_1, \eta_2)$

ويؤدي إلى أن $\xi_1 = -\alpha_1^{-1}\alpha_2\eta_1$ و $\xi_2 = -\alpha_1^{-1}\alpha_2\eta_2$

$$\Rightarrow \xi_1\eta_2 = -\alpha_1^{-1}\alpha_2\eta_1\eta_2 = (-\alpha_1^{-1}\alpha_2\eta_2)\eta_1 = \xi_2\eta_1$$

وبالعكس افرض أن :

$$\xi_1\eta_2 = \xi_2\eta_1 \qquad (1)$$

إذا كان $\xi_1 = \xi_2 = 0$ فإن $(\xi_1, \xi_2) = (0, 0)$ وعليه فإن (ξ_1, ξ_2) و (η_1, η_2) مرتبطان خطياً .

دعنا نفرض أن $\xi_1 \neq 0$ ، فيكون $\frac{\eta_1}{\xi_1} \in C$. كذلك :

$$\frac{-\eta_1}{\xi_1}(\xi_1, \xi_2) + (\eta_1, \eta_2) = \left(-\eta_1, \frac{-\eta_1\xi_2}{\xi_1}\right) + (\eta_1, \eta_2)$$

$$= (-\eta_1, \eta_2) + (\eta_1, \eta_2) = (0, 0) \qquad \text{(حسب 1)}$$

إذاً $(\eta_1, \eta_2), (\xi_1, \xi_2)$ هما مرتبطان خطياً .

تمرين 2

لتكن $P = IR[x]$ ، ولتكن $f(x), g(x), h(x), k(x) \in P$ بحيث يكون $f(t) = 1$ ، $g(t) = t$ ، $h(t) = t^2$ و $k(t) = 1 + t + t^2$ لكل $t \in IR$. برهن أن $f(x), g(x), h(x)$ مرتبطة خطياً ولكن أي ثلاث منها هي مستقلة خطيا .

الحل

اعتبر العنصر $f(x) + g(x) + h(x) - k(x)$. لكل $t \in IR$ يكون :

$$f(t) + g(t) + h(t) - k(t) = 1 + t + t^2 - (1 + t + t^2) = 0$$

وعليه فإن $f(x) + g(x) + h(x) - k(x)$ هي كثيرة الحدود الصفرية .

(تذكر أن كل كثيرة حدود درجتها n ومعاملاتها أعداد حقيقية لها على الأكثر n جذراً سوف نبرهن هذه النتيجة في وضع أكثر تعميماً في فصل حول الحقول) ، وبالتالي فإن $f(x), g(x), h(x)$ و $k(x)$ مرتبطة خطياً .

والآن نبرهن أي ثلاثة منها مستقلة خطياً ، سوف نأخذ $f(x), g(x), h(x)$ ، $f(x), h(x), k(x)$. وبالمثل يمكن مناقشة الثلاثيتان الباقيتان .

لنفرض $\alpha_1 f(x) + \alpha_2 g(x) + \alpha_3 h(x) = 0$ لبعض $\alpha_1, \alpha_2, \alpha_3 \in IR$ هذا يعطينا :

$$\alpha_1 f(t) + \alpha_2 g(t) + \alpha_3 h(t) = 0 \quad \forall t \in IR$$
$$\Rightarrow \alpha_1 + \alpha_2 t + \alpha_3 t^2 = 0 \qquad \forall t \in IR$$
$$\Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0$$

وعليه فإن $f(x), g(x), h(x)$ مستقلة خطياً .

وأخيراً

$$\beta_1 f(x) + \beta_2 h(x) + \beta_3 k(x) = 0$$
$$\Rightarrow \beta_1 + \beta_2 t^2 + \beta_3(1 + t + t^2) = 0 \quad \forall t \in IR$$

وهكذا حصلنا على $\beta_1 + \beta_3 = 0$ ، $\beta_3 = 0$ ، $\beta_2 + \beta_3 = 0$ وبالتالي فإن $\beta_1 = \beta_2 = \beta_3 = 0$ إذاً $f(x), h(x), k(x)$ هي كذلك مستقلة خطياً .

تمرين 3

تحت أية شروط على القياسي ξ المتجهات الثلاث $(1, 1, 1)$ و $(1, \xi, \xi^2)$ $(1, -\xi, \xi^2)$ تشكل قاعدة للفضاء المتجهي C^3 ؟

الحل

بما أن أية قاعدة للفضاء C^3 تحتوي على ثلاث متجهات فإن ξ تأخذ قيمتين بحيث يكون مربعهما ξ^2 متساويان ، أي أنه علينا إيجاد شرط على قياسي x بحيث تشكل

المتجهات $(1,1,1)$ ، $(1,x,x^2)$ ، $(1,-x,x^2)$ قاعدة للفضاء C^3 بما أن $\dim C^3$ على C يساوي 3 ، فإنه يكفي إيجاد الشرط الذي يجعل المتجهات $(1,1,1)$ ، $(1,x,x^2)$ ، $(1,-x,x^2)$ مستقلة خطياً على C .

هذه المتجهات تكون مستقلة خطياً إذا وفقط إذا كان :

$$\lambda_1(1,1,1)+\lambda_2(1,x,x^2)+\lambda_3(1,-x,x^2)=(0,0,0)$$
$$\Rightarrow \lambda_1=\lambda_2=\lambda_3=0 \quad \forall \lambda_1,\lambda_2,\lambda_3\in C$$

الآن

$$\lambda_1(1,1,1)+\lambda_2(1,x,x^2)+\lambda_3(1,-x,x^2)=(0,0,0)$$

$$\Rightarrow \left.\begin{aligned} \lambda_1+\lambda_2+\lambda_3&=0\\ \lambda_1+\lambda_2 x-\lambda_3 x&=0\\ \lambda_1+\lambda_2 x^2+\lambda_3 x^2&=0\end{aligned}\right\} \qquad (1)$$

وعليه فإن المتجهات المعطاة تكون مستقلة خطياً إذا وفقط إذا كان النظام (1) للمعادلات الخطية ذو حل صفري (تافه) ونعلم أن النظام (1) له الحل التافه إذا وفقط إذا كان :

$$\begin{vmatrix}1&1&1\\1&x&-x\\1&x^2&x^2\end{vmatrix}\neq 0 \Leftrightarrow 2x(x^2-1)\neq 0$$

وهكذا فإن المتجهات $(1,1,1)$ ، $(1,x,x^2)$ ، $(1,-x,x^2)$ تشكل قاعدة للفضاء C^3 إذا وفقط إذا كان $x\notin\{0,1,-1\}$.

إذاً $(1,1,1)$ ، $(1,\xi,\xi^2)$ ، $(1,-\xi,\xi^2)$ تشكل قاعدة للفضاء C^3 إذا وفقط إذا كان $\xi=\pm x$ حيث $x\notin\{0,1,-1\}$.

تمرين 4

افرض أن x و y متجهان و U فضاء جزئي من فضاء متجهي V_F . ليكن W الفضاء الجزئي المولد من U و x . وليكن Y الفضاء الجزئي المولد من U و y . برهن أنه إذا كان $y\in W-U$ فإن $x\in Y$.

الحل

بما أن $y \in W =< U, x >$ ، فإن $y = u + \beta x$ لبعض $u \in U$ و $\beta \in F$.

ولأن $y \notin U$ فإن $\beta \neq 0$. إذاً $\beta^{-1} \in F$ وأن :

$$x = \beta^{-1}y - \beta^{-1}u \in < U, y >= Y$$

تمرين 5

إذا كان x, y, z متجهات في V_F بحيث كان $x + y + z = 0$ ، فإن الفضاء الذي يولده المتجهان x و y هو نفس الفضاء الذي يولده المتجهان y و z .

الحل

ليكن $W =< x, y >$ و $U =< y, z >$. ليكن $w \in W$ ، عندئذ يوجد عنصران $\alpha, \beta \in F$.

$$\begin{aligned} w &= \alpha x + \beta y \\ &= \alpha(-y - z) + \beta y && (x + y + z = 0 \text{ لأن}) \\ &= (\beta - \alpha)y + (-\alpha)z \in < y, z >= U \end{aligned}$$

وهذا يعطينا الاحتواء $W \subseteq U$.

للبرهنة على الاحتواء المعاكس نتبع الآتي :

ليكن $u \in U$ ، عندئذ يوجد $\gamma, \delta \in F$.

$$\begin{aligned} u = \gamma y + \delta z &= \gamma y + \delta(-x - y) \quad (x + y + z = 0 \text{ لأن}) \\ &= (-\delta)x + (r - \delta)y \in < x, y >= W \end{aligned}$$

وبالتالي فإن $U = W$.

تمارين

1- برهن أن المتجهات $(1, 1, 0, 0)$ ، $(0, 1, -1, 0)$ ، $(0, 0, 0, 3)$ في $F^{(4)}$ مستقلة خطياً على F إذا كان F حقلاً مميز يساوي صفر . برهن أن المتجهات نفسها تكون مرتبطة خطياً على F إذا كان مميز F يساوي 3 .

2- برهن أن المتجهات الأربعة $(1, 0, 0)$ ، $(0, 1, 0)$ ، $(0, 0, 1)$ و $(1, 1, 1)$ في C^3 تشكل مجموعة مرتبطة خطياً على C ولكن أي ثلاث متجهات منها تكون مستقلة خطياً .

3- برهن أن $C_{/R}$ هو فضاء متجهي ثنائي البعد .

4- برهن أن الفضاء المتجهي لجميع كثيرات الحدود في $/R[x]$ على $/R$ هو فضاء متجهي ذو بعد غير منته .

5- لتكن S مجموعة جميع كثيرات الحدود في $/R[x]$ والتي درجتها لا تتجاوز n (حيث n عدد صحيح موجب ثابت) . برهن أن بعد الفضاء $S_{/R}$ يساوي n .

6- برهن أنه في فضاء متجهي كل مجموعة جزئية من مجموعة مستقلة خطياً تكون مستقلة خطياً وكل مجموعة تحوي مجموعة مرتبطة خطياً تكون مرتبطة خطياً .

7- ليكن V فضاءً متجهاً على $/R$ ولتكن $T = \{(x, y) \mid x, y \in V\}$. عرف عملية جمع في T على النحو $(x, y) + (z, w) = (x + z, y + w)$ وعليه ضرب قياسي لعدد مركب $\alpha + \beta i$ على النحو :

$$(\alpha + \beta i)(x, y) = (\alpha x - \beta y, \beta x + \alpha y)$$

برهن أن $\dim T$ على C يساوي $\dim V$ على $/R$.

8- لتكن $\{U_1, U_2, \dots, U_t\}$ أي تجمع لفضاءات جزئية من فضاء متجهي V ذو بعد يساوي n بحيث تقاطع أي n من هذه الفضاءات الجزئية هو فضاء جزئي بعد $0 \leq 1$. برهن أن $\dim(U_1 \cap U_2 \cap, \dots, \cap U_t) \geq 1$

9- برهن أن $F[x]$ هو فضاء متجهي ذو بعد غير منته على الحقل F .

[**إرشاد** استخدم الحقيقة أن $T \in I\!R$ عنصر متسام على Q] .

10- إذا اعتبرنا $I\!R$ فضاء متجهاً على Q ، نبرهن أن شرطاً كافياً وضرورياً لكي يكون المتجهان 1 ، ξ مستقلان خطياً في $I\!R$ هو أن العدد الحقيقي ξ بجذر غير نسبي .

11- برهن أنه إذا كان x, y, z متجهات مستقلة خطياً فإن المتجهات $x + y$ ، $y + z$ ، $z + x$ تكون مستقلة خطياً أيضاً مع كون $\text{char}\, F \neq 2$.

12- تحت أية شروط على المقياسي ξ تكون المتجهات $(0, 1, \xi)$ ، $(\xi, 0, 1)$ ، $(\xi, 1, 1 + \xi)$ قاعدة للفضاء C^3 . (إجابة : ليست هناك شروط) .

13- إذا كانت T, S مجموعتان جزئيتان غير خاليتان من فضاء متجهي V فأثبت أن :

i- $S \subseteq T \Rightarrow <S> \subseteq T$.

ii- $<S \cup T> = <S> + <T>$

iii- $S = <\xi>$ إذا وفقط إذا كان S فضاءً جزئياً من V .

iv- $<<S>> = <S>$.

14- برهن أن $B = \{(1, \alpha, \alpha^2), (1, \beta, \beta^2), (1, \gamma, \gamma^2)\}$ هي مجموعة جزئية مستقلة خطياً من R^3 لجميع الأعداد الحقيقية المختلفة α, β, γ . متى تكون β قاعدة ؟

[**إجابة** المجموعة المعطاة تكون قاعدة عندما $\alpha \neq \beta$ ، $\beta \neq \gamma$ ، $\alpha \neq \gamma$]

15- لكل عدد طبيعي n ، إذا كانت الدالة f_n معرفة بالصورة $f_n(x) = e^{nx} \quad \forall x \in I\!R$ فبرهن أن f_1, f_2, f_3 متجهات مستقلة خطياً في $I\!R^R$ (الفضاء المتجهي لجميع الدوال الحقيقية على $I\!R$) .

4- فضاءات القسمة Quotient Spaces

ليكن W فضاءً جزئياً من فضاء متجهي V_F . بما أن W زمرة جزئية من زمرة الجمع $< V, + >$ ، يمكننا أن نعرف زمرة القسمة $V / W = \{x + W \mid x \in V\}$ بحيث يكون لأي عنصرين $x + W, y + W \in V / W$.

$$(x + W) + (y + W) = x + y + W$$

هذه الزمرة كما نعلم إبدالية .

عملية ضرب $x + W$ بالعنصر α كالآتي : لأي $\alpha \in F$ ، $x + W \in V / W$ إذا عرفنا :

$$\alpha(x + W) = \alpha x + W \qquad (1)$$

فإن

$$x + W = y + W$$
$$\Rightarrow x - y \in W \Rightarrow \alpha(x - y) \in W$$
$$\Rightarrow \alpha x - \alpha y \in W \Rightarrow \alpha x + W = \alpha y + W$$

هذا يبين أن عملية الضرب جيدة التعريف .

الآن لأي $\alpha, \beta \in F$ ، $y + W \in V / W$ و $x + W$ نجد أن :

$$(\alpha + \beta)(x + W) = (\alpha + \beta)x + W = \alpha x + \beta x + W$$
$$= (\alpha x + W) + (\beta x + W) = \alpha(x + W) + \beta(x + W)$$

وأن

$$\alpha[(x + W) + (y + W)] = \alpha[(x + y) + W]$$
$$= \alpha(x + y) + W$$
$$= (\alpha x + \alpha y) + W$$
$$= (\alpha x + W) + (\alpha y + W)$$
$$= \alpha(x + W) + \alpha(y + W)$$

$$(\alpha\beta)(x + W) = (\alpha\beta)x + W$$
$$= \alpha(\beta x) + W = \alpha(\beta x + W)$$
$$= \alpha[\beta(x + W)]$$

وأخيراً

$$1(\alpha + W) = 1x + W = x + W$$

هذا يبين أن V / W فضاء متجهي على F .

وعليه نقدم التعريف الآتي :

تعريف 11-28

إذا كان W فضاءً جزئياً من فضاء متجهي V_F . فإن المجموعة $V / W = \{x + W \mid x \in V\}$ تشكل فضاءً متجهاً على F ، حيث أن جمع وضرب المتجهات في قياسيات معرفة على النحو الآتي :

$$(x + W) + (y + W) = (x + y) + W$$
$$\alpha(x + W) = \alpha x + W$$

لكل $x + W, y + W \in V / W$ و $\alpha \in F$.

هذا الفضاء يسمى فضاء القسمة .

نظرية 1-29

إذا كان W فضاءً جزئياً من فضاء متجهي V_F ذو بعد منته فإن :

$$\dim V / W = \dim V - \dim W$$

البرهان

لنفرض أن $\dim V = n$ ، $\dim W = m$. لتكن $\{x_1, x_2, \dots, x_m\}$ قاعدة للفضاء W . المتجهات $x_1, x_2, \dots, x_m$ وعددها m مستقلة خطياً في V وعليه بالإمكان توسيعها إلى قاعدة للفضاء V ولتكن $\{x_1, x_2, \dots, x_m, x_{m+1}, \dots, x_n\}$.

الآن اعتبر $n - m$ من المتجهات الآتية في V / W .

$$x_{m+1} + W, x_{m+2} + W, \dots, x_n + W$$

فبرهن أن هذه المتجهات وعددها $(n - m)$ تشكل قاعدة للفضاء V / W وبذلك يكون $\dim V / W = n - m$.

الآن لأي $x \in V$ فإن $x = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$

يؤدي إلى :

$$x + W = (\alpha_{m+1}x_{m+1} + \dots + \alpha_n x_n) + (\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_m \alpha_m) + W$$
$$= \alpha_{m+1}x_{m+1} + \dots + \alpha_n x_n + W$$

لأن $x_i \in W$ لكل $i = 1, 2, \dots, m$ ويعطينا $\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_m x_m + W = W$

عليه فإن $x + W = \alpha_{m+1}(x_{m+1} + W) + \dots + \alpha_n(x_n + W)$

وهذا يثبت أن المتجهات $x_{m+1} + W, x_{m+2} + W, \dots, x_n + W$ تولد V / W ومطلوب إثبات أن هذه المتجهات مستقلة خطياً . افرض أن :

$$\beta_{m+1}(x_{m+1} + W) + \beta_{m+2}(x_{m+2} + W) + \dots + \beta_n(x_n + W) = \overline{0}$$

لبعض العناصر $\beta_{m+1}, \beta_{m+2}, \dots, \beta_n \in F$.

أي أن $(\beta_{m+1}x_{m+1} + \beta_{m+2}x_{m+2} + \dots + \beta_n x_n) + W = W$

$$\Rightarrow \beta_{m+1}x_{m+1} + \beta_{m+2}x_{m+2} + \dots + \beta_n x_n = \gamma_1 x_1 + \gamma_2 x_2 + \dots + \gamma_m x_m$$

لبعض العناصر $1 \le i \le m$.

$$\Rightarrow \gamma_1 x_1 + \gamma_2 x_2 + \dots + \gamma_m x_m + (-\beta_{m+1})x_{m+1} + (-\beta_{m+2})x_{m+2} + \dots + (-\beta_n)x_n = 0$$
$$\Rightarrow \gamma_1 = \gamma_2 = \dots = \gamma_m = -\beta_{m+1} = -\beta_{m+2} = \dots = -\beta_n = 0$$

(لأن $x_1, x_2, \dots, x_n$ مستقلة خطياً) . هذا يؤدي إلى أن $\beta_{m+1}, \beta_{m+2}, \dots, \beta_n$ جميعها أصفاراً .

هذا يبرهن أن المتجهات $x_{m+1} + W, x_{m+2} + W, \dots, x_n + W$ مستقلة خطياً ، إذاً $\dim(V / W) = n - m = \dim V - \dim W$.

مسائل

1- إذا كان W فضاءً جزئياً من فضاء متجهي V . برهن أنه يوجد تقابل بين الفضاءات الجزئية من V والتي تحوي W والفضاءات الجزئية من V/W .

2- ليكن W فضاءً جزئياً من فضاء متجهي V_F . لكل $a, b \in W$ نعرف $a \equiv b \pmod{W}$ [يسمى تطابق بمعيار W] إذا وفقط إذا كان $a - b \in W$ ولكل $\alpha \in F$ ، $\alpha(a-b) \in W$. برهن أن علاقة التطابق معيار W هي علاقة تكافؤ على V . كذلك برهن أنه لكل $a \in W$ ، فإن $Cl(a) = a + W$.

3- اذكر مثالاً لفضاء متجهي ذو بعد غير منته V_F له فضاء جزئي W بحيث يكون V/W فضاءً متجهاً ذو بعد منته .

5– المجموع المباشر والمتجهات Direct Sum and Complements

تعريف 11-30

إذا كان W, U فضاءان جزئيان من فضاء متجهي V بحيث $V \cap W = (0)$ فإن المجموع $U + W$ يسمى المجموع المباشر للفضائين U و W ويرمز له بالرمز $U \oplus W$.

مثال 13

إذا كان $V = F[x]$ الفضاء المتجهي المشكل من كثيرات جميع الحدود على حقل F فإن $U = \{\alpha_0 + \alpha_1 x \mid \alpha_0, \alpha_1 \in F\}, W = \{\alpha_2 x^2 + \alpha_3 x^3 \mid \alpha_2, \alpha_3 \in F\}$ هما فضاءان جزئيان من V بحيث أن $V \cap W = (0)$. إذاً $U + W = U \oplus W$

مثال 14

اعتبر $V = F^{(4)}$. إذا كان $U = \{(\alpha, \beta, 0, 0) \mid \alpha, \beta \in F\}$ و $W = \{(0, 0, \gamma, \delta) \mid \gamma, \delta \in F\}$. فمن اليسير التحقق من أن المجموعتين الجزئيتين U و W تشكلان فضاءان جزئيان من V . المتجه الصفري للفضاء V هو $(0, 0, 0, 0)$. وإذا كان $z = (\alpha, \beta, 0, 0) = (0, 0, \gamma, \delta)$ لبعض العناصر $\alpha, \beta, \gamma, \delta \in F$ فإن $\alpha = \beta = \gamma = \delta = 0$ وبالتالي فإن $z = 0$ وعليه فإن $U \cap W = (0)$.

إذاً $U + W = U \oplus W$. الآن كل قيمة $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in V$ يمكن التعبير عنها بالصورة $(\alpha_1, \alpha_2, 0, 0) + (0, 0, \alpha_3, \alpha_4)$ حيث $(\alpha_1, \alpha_2, 0, 0) \in U$ و $(0, 0, \alpha_3, \alpha_4) \in W$ هذا يؤدي إلى أن $V = U \oplus W$. الآن يمكننا إعادة صياغة نتيجة 11-27 وكالآتي :

نتيجة 11-27 a

إذا كان U و W فضاءان جزئيان من فضاء متجهي ذو بعد منته V_F بحيث $V + W = U \oplus W$ ، فإن $\dim(U \oplus W) = \dim U + \dim W$.

تعريف 11-31

إذا كان U فضاءً جزئياً من فضاء متجهي V_F ، فإن الفضاء الجزئي المتجهي U' من V_F بحيث $V_F = U \oplus U'$ يسمى متمم U .

وعليه في مثال 14 ، فإن W هو متمم U .

نظرية 11-32

كل فضاء جزئي من فضاء متجهي ذو بعد منته له متمم .

البرهان

ليكن U فضاءً جزئياً من فضاء متجهي ذو بعد منته V_F . وافرض أن $\dim V = n$ ، $\dim U = m$.

بما أن كل مجموعة جزئية مستقلة خطياً من V يمكن توسيعها إلى قاعدة للفضاء V ، فإننا نستطيع إيجاد قاعدة $\{x_1, x_2, \dots, x_n\}$ للفضاء V بحيث تكون $\{x_1, x_2, \dots, x_m\}$ قاعدة للفضاء U . ليكن U' الفضاء الجزئي من V المولد بالمجموعة $\{x_{m+1}, \dots, x_n\}$. اعتبر أي عنصر $x \in V$ فإن

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$$

لبعض العناصر $\alpha_i \in F$ ، أي أن :

$$x = (\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_m x_m) + (\alpha_{m+1} x_{m+1} + \dots + \alpha_n x_n) \in U + U'$$

هذا يؤدي إلى أن :

$$V = U + U' \qquad (1)$$

افرض أن $z \in U \cap U'$ ، بما أن $\{x_1, x_2, \dots, x_m\}$ قاعدة للفضاء U وأن $\{x_{m+1}, \dots, x_n\}$ قاعدة للفضاء U' فإن $z = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_m x_m = \beta_{m+1} x_{m+1} + \dots + \beta_n x_n$

لبعض العناصر $\alpha_i, \beta_j \in F$. بالتالي فإن :

$$\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_m x_m + (-\beta_{m+1})\, x_{m+1} + (-\beta_{m+2})\, x_{m+2} + \dots + (-\beta_n) x_n = 0$$

$$\Rightarrow \alpha_1 = \alpha_2 = \ldots = \alpha_m = -\beta_{m+1} = -\beta_{m+2} = \ldots = -\beta_n = 0$$
$$\Rightarrow z = 0 \Rightarrow U \cap U' = (0)$$

بالتالي (1) يؤدي إلى أن $V = U + U'$ والذي يبين أن U' متمم U . □

نتيجة 11-33

إذا كان U فضاءً جزئياً من فضاء متجهي ذو بعد منته V ، فإن كل متمم للفضاء U يكون له بعد مساو للفرق $\dim V - \dim U$.

البرهان

إذا كان U' متمماً لـ U ، فإن $W = U \oplus U'$. عليه فإن $\dim V = \dim U + \dim U'$ (نتيجة 11-27 a) .

هذا يؤدي إلى أن $\dim U' = \dim V - \dim U$. وبالتالي نكون قد حصلنا على النتيجة . □

النتيجة السابقة تبين أن جميع المتممات لفضاء جزئي ما لها نفس البعد . من جهة أخرى المثال التالي يبين أن المتمم ليس وحيداً .

مثال 15

اعتبر $V = F^{(2)}$. وليكن $U = \{(\alpha, 0) \mid \alpha \in F\}$ ، $U' = \{(0, \beta) \mid \beta \in F\}$ و $W = \{\alpha, \alpha) \mid \alpha \in F\}$. U ، U' و W هي فضاءات جزئية من V وهي مولدة بالمتجهات (0 ,1) ، (1 ,0) و (1 ,1) على الترتيب . عليه فإن بعد كل فضاء منها يساوي واحد . لنأخذ $z \in U \cap U' \Rightarrow z = (\alpha, 0) = (0, \beta)$ لبعض العناصر $\alpha, \beta \in F$ ، هذا يؤدي إلى أن $\alpha = \beta = 0 \Rightarrow z = 0$ ، عليه فإن $U \cap U' = (0)$ وهذا يؤدي إلى أن $U + U' = U \oplus U'$ عندئذ :

$$\dim(U + U') = \dim U + \dim U' = 1 + 1 = 2 \Rightarrow V = U \oplus U'$$

والذي يؤدي إلى أن U' هو متمم U . مرة أخرى :

$$z \in U \cap W \Rightarrow z = (\alpha, 0) = (\beta, \beta)$$

لبعض العناصر $\alpha, \beta \in F$ وهو يؤدي إلى أن :

$$\alpha = \beta = 0 \Rightarrow z = 0 \Rightarrow U \cap W = (0)$$

مرة أخرى توصلنا إلى أن $V = U \oplus W$. عليه فإن W هو متمم U أيضاً ، وبالتالي U' ، W هما متممين مختلفين لـ U . ويتضح من ذلك أنه متمم فضاء جزئي ليس وحيداً .

تمرين محلولة

تمرين 1

تعريف يقال لفضاء متجهي V_F أنه مجموع مباشر (داخلي) لفضاءاته الجزئية $W_1, W_2, \ldots, W_n$ ، ويكتب على الصورة $V = W_1 \oplus W_2 \oplus \ldots \oplus W_n$ إذا كان بالإمكان كتابة كل عنصر $v \in V$ بطريقة واحدة وواحدة فقط بالصورة $\sum_{i=1}^{n} w_i$ حيث $w_i \in W_i$.

أثبت أنه إذا كان $V = W_1 + W_2 + \ldots + W_n$ ، فإن العبارات الآتية متكافئة :

(i) $V = W_1 \oplus W_2 \oplus \ldots \oplus W_n$.

(ii) لكل $1 \le i \le n$ فإن $W_i \bigcap_{\substack{j=1 \\ j \ne i}}^{n} W_j = (0)$.

(iii) لكل $w_i \in W_i$ فإن

$$\sum_{i=1}^{n} w_i = 0 \Rightarrow w_i = 0$$

(iv) إذا كانت المجموعة $B_i = \{b_1^i, \ldots, B_{k_i}^i\}$ قاعدة للفضاء W_i لكل $1 \le i \le n$ ، فإن $\bigcup_{i=1}^{n} B_i$ هو قاعدة للفضاء V . [يقصد بالمجموعة $\bigcup_{i=1}^{n} B_i$ المتجهات :

$$b_1^1, b_2^1, \ldots, b_k^1, b_1^2, \ldots, b_{k_2}^2, \ldots, b_1^n, \ldots, b_{k_n}^n$$

الحل

$(i) \Rightarrow (ii)$

ليكن $x \in W_i \cap \sum_{\substack{j=1 \\ j \neq i}} W_j$. فإن $x = w_i$ ، كذلك :

$$x = w_1 + w_2 + \ldots + w_{i-1} + w_{i+1} + \ldots + w_n$$

حيث $w_i \in W_i$ لجميع $i = 1, 2, \ldots, n$ ومنها نحصل على أن :

$$0 + 0 + \ldots + 0 + w_i + 0 + \ldots + 0 = w_1 + w_2 + \ldots + w_{i-1} + w_{i+1} + \ldots + w_n$$

وبما أنه يمكن كتابة x بطريقة واحدة فقط كمجموع عناصر x_i حيث $x_i \in W_i$ فإن :

$$w_1 = w_2 = \ldots = w_{i-1} = w_i = w_{i+1} = \ldots = w_n = 0$$

هذا يؤدي إلى أن $x = 0$ وبالتالي $W_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{n} W_j = (0)$.

$(iii) \Leftarrow (ii)$

افرض أن $w_1 + w_2 + \ldots + w_n = 0$ حيث $w_i \in W_i$ هذا يؤدي إلى أن :

$$w_i = -(w_1 + w_2 + \ldots + w_{i-1} + w_{i+1} + \ldots + w_n)$$

العنصر إلى اليسار أي w_i ينتمي إلى W_i والعنصر في اليمين ينتمي إلى $\sum_{\substack{j=1 \\ j \neq i}}^{n} W_j$.

حسب (ii) نستنتج أن $w_i = 0$ ، أي أن (iii) متحققة .

$(iv) \Leftarrow (iii)$

ليكن $v \in V$. بما أن $V = \sum_{i=1}^{n} W_i$ ، فإن $V = \sum_{i=1}^{n} w_i$ حيث $w_i \in W_i$.

حسب الفرض B_i قاعدة للفضاء W_i ، وهذا يؤدي إلى أن :

$$w_i = \sum_{j=1}^{k_i} \lambda_j^i b_j^i \quad , \lambda_j^i \in F$$

$$\Rightarrow v = \sum_{i=1}^{n}\sum_{j=1}^{k_i} \lambda_j^i b_j^i$$

والذي يبين أن $\bigcup_{i=1}^{n} B_i$ تولد V .

الآن $\sum_{i=1}^{n}\sum_{j=1}^{k_i} \lambda_j^i b_j^i = 0$ مع كون $\lambda_j^i \in F$

$$\Rightarrow \sum_{i=1}^{n} w_i = 0$$

حيث $w_i = \sum_{j=1}^{k_i} \lambda_j^i b_j^i \in W_i$.

(حسب i)

$$\Rightarrow w_i = 0 \quad \forall\, 1 \le i \le n$$

$$\Rightarrow \lambda_j^i = 0 \quad \forall\, j = 1, 2, \ldots, k \quad \forall\, i = 1, 2, \ldots, n$$

وعليه فإن $\bigcup_{i=1}^{n} B_i$ مجموعة جزئية مستقلة خطياً من V . وبالتالي فإن $\bigcup_{i=1}^{n} B_i$ قاعدة للفضاء V .

$(i) \Leftarrow (iv)$

لنفرض أن $v \in V$ يمكن كتابته بطريقتين على شكل مجموع عناصر كالآتي :

$$V = \sum_{i=1}^{n} w_i = \sum_{i=1}^{n} w_i'$$

حيث $w_i' \in W_i$ و w_i

$$\Rightarrow \sum_{i=1}^{n} (w_i - w_i') = 0$$

$$w_i = \sum_{j=1}^{k_i} \lambda_j^i b_j^i, \qquad w_i' = \sum_{j=1}^{k_i} \mu_j^i b_j^i$$

علماً بأن $\lambda_j^i, \mu_j^i \in F$ حيث لكل $i = 1, 2, \ldots, n$ ، $B_i = \{b_1^i, b_2^i, \ldots, b_{k_i}^i\}$ قاعدة للفضاء W_i . عندئذ

$$v = \sum_{i=1}^{n} w_i = \sum_{i=1}^{n} w_i' \Rightarrow \sum_{i=1}^{n}\left[\sum_{j=1}^{k_i} (\lambda_j^i - \mu_j^i) b_j^i\right] = 0$$

بما أن $\bigcup_{i=1}^{n} B_i$ قاعدة للفضاء V فإن :

$$(\lambda_j^i - \mu_j^i) = 0 \quad \forall\, j = 1, 2, \ldots, k_i, i = 1, 2, \ldots, n$$
$$\Rightarrow \lambda_j^i = \mu_j^i \quad \forall\, j = 1, 2, \ldots, k_i, i = 1, 2, \ldots, n$$
$$\Rightarrow w_i = w_i' \quad \forall i = 1, 2, \ldots, n$$

إذا $V = W_1 \oplus W_2 \oplus \ldots \oplus W_n$.

تمرين 2

ليكن $/R_n$ هو الفضاء المتجهي لجميع المصفوفات ذات السعة $n \times n$ على حقل الأعداد الحقيقية . برهن أنه إذا كانت U مجموعة جميع المصفوفات المتناظرة (المتماثلة) في $/R_n$ و V مجموعة المصفوفات متخالفة التناظر في $/R_n$ فإن V و U فضاءان جزئيان من $/R_n$ بحيث $/R_n = U \oplus V$.

الحل

من الواضح أن O_n المصفوفة الصفرية من السعة $n \times n$ مصفوفة متماثلة ، أي أن U مجموعة غير خالية . ليكن $\alpha, \beta \in /R$ ، $X, Y \in U$ فإن :

$$(\alpha X + \beta Y)^* = \alpha X^* + \beta Y^* = \alpha X + \beta Y$$

لأن X و Y مصفوفتان متماثلتان (لاحظ أن A^* تمثل حدود (transpose) المصفوفة A) .

هذا يعني أن U فضاء جزئي من $/R_n$.

بتطبيق حقيقة أن المصفوفة X تكون متخالفة التناظر إذا وفقط إذا كان $X^* = -X$ ونجد أن V هو أيضاً فضاء جزئي من $/R_n$.

لنفرض الآن أن $A \in /R_n$. عندئذ $A = \frac{1}{2}(A + A^*) + \frac{1}{2}(A - A^*)$ ، حيث $\left[\frac{1}{2}(A + A^*)\right]^* = \frac{1}{2}(A^* + A)$ و :

$$\left[\frac{1}{2}(A - A^*)\right]^* = \frac{1}{2}(A^* - A) = -\frac{1}{2}(A - A^*) \Rightarrow A = X + Y$$

حيـــــث $X = \frac{1}{2}(A + A^*) \in U$ ، $Y = \frac{1}{2}(A - A^*) \in V$ وهــــــذا يـــــؤدي إلى أن $/R_n = U + V$.

الآن إذا كان $X \in U \cap V$ فإن

$$X^* = X, \qquad X^* = -X$$
$$\Rightarrow X = -X \Rightarrow 2X = O_n$$
$$\Rightarrow X = O_n$$

إذاً $U \cap V = \{O_n\}$ وعليـه فـإن $/R_n = U \oplus V$. (نتيجـة لـذلك يمكننـا القـول أن كـل مصـفوفة مربعـة عناصـرها أعـداد حقيقيـة يمكـن التعبـير عنهـا بطريقـة واحـدة وواحـدة فقـط كمجموع مصفوفة متماثلة ومصفوفة متخالفة التناظر) .

تمرين 3

يقـال للفضـاءات الجزئيـة V_1, V_2 و V_3 من فضـاء متجهـي V_F أنها مستقلة إذا كـان $V_i \cap \sum\limits_{\substack{j=1 \\ j \neq i}}^{3} V_j = (0)$ لكل $i = 1, 2, 3$.

بـين أنـه إذا كانـت V_1, V_2, V_3 فضـاءات جزئيـة مسـتقلة فـإن $V_i \cap V_j = (0)$ لكـل $i \neq j$ ، $1, 2, 3$ ومن ثم اذكر مثالاً لبيان أن العكس ليس بالضرورة صحيحاً .

الحل

بما أنه إذا كان $i \neq j$ فإن $V_i \subseteq \sum\limits_{\substack{j=1 \\ j \neq i}}^{3} V_j$.

$$\Rightarrow V_i \cap V_j \subseteq V_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{3} V_j = (0) \Rightarrow V_i \cap V_j = (0)$$

إذاً إذا كانت هناك ثلاث فضاءات جزئية مستقلة ، فإن تقاطع أي فضائين جزئيين مختلفين منها يكون هو (0) . وسنوضح أن العكس ليس بالضرورة صحيحاً .

ليكن $V = IR^3$ وليكن $e_1 = (1, 0, 0)$ ، $e_2 = (0, 1, 0)$ و $e_3 = (0, 0, 1)$.

لنأخـــــذ $V_1 =< e_1 >$ ، $V_2 =< e_2 >$ و $V_3 =< e_1 + e_2 >$. مـــــن الواضــــح أن $V_1 \cap V_2 = (0)$.

الآن :

$$x \in V_1 \cap V_3 \Rightarrow x = \lambda_1 e_2 = \lambda_2(e_1 + e_2) \qquad (\text{لبعض } \lambda_1, \lambda_2 \in IR)$$
$$\Rightarrow (\lambda_1 - \lambda_2)e_1 - \lambda_2 e_2 = 0$$
$$\Rightarrow \lambda_1 = \lambda_2, \lambda_2 = 0 \quad (\text{لأن } \{e_1, e_2\} \text{ مجموعة جزئية مستقلة خطياً من } IR^3)$$
$$\Rightarrow x = 0$$

وهكذا يثبت أن $V_1 \cap V_3 = 0$.

بالمثل يمكن أن نثبت أن $V_2 \cap V_3 = (0)$ ، كذلك $V_3 \subseteq V_1 + V_2$ لأنه :

$$x \in V_3 \Rightarrow x = \alpha_1(e_1 + e_2), \quad \alpha_1 \in IR$$
$$= \alpha_1 e_1 + \alpha_1 e_2 \Rightarrow x \in V_1 + V_2$$

بالتالي فإن $V_3 \cap (V_1 + V_2) = V_3 \neq (0)$.

وهكذا فإن الفضاءات الجزئية V_1, V_2, V_3 ليست مستقلة .

تمارين

1- اعتبر الفضاء المتجهي $V = IR^3$. حدد متممات الفضاءات الجزئية V المولدة بالمجموعات الجزئية الآتية من V .

(a) $\{(1, 0, 0), (0, 1, 0)\}$

(b) $\{(1, -1, 3), (-4, 2, 0), (-3, -1, -15)\}$

(c) $\{(1, 1, 0), (0, 1, 0)\}$

(d) لعددين حقيقيين ثابتين ومختلفين α و β .

$\{(1, \alpha, \alpha^2), (1, \beta, \beta^2)\}$

[**إجابة** لاحظ أن متمم فضاء جزئي معطى ليس وحيداً . فيما يلي نذكر متمماً واحداً لكل من الفضاءات الجزئية المولدة بالمجموعات (a) ، (b) ، (c) و (d) .

(a) $< (0, 0, 1) >$ و (b) $\{0\}$ و (c) $< (0, 0, 1) >$ و (d) $< (0, 0, 1) >$]

2- لتكن B قاعدة للفضاء المتجهي V_F . إذا كانت B_1 أية مجموعة جزئية من B و W الفضاء الجزئي الذي تولده B_1 ، برهن أن الفضاء الجزئي من V المولد بالمجموعة $B - B_1$ هو متمم للفضاء W .

3- أثبت أن المتجهان $(1, 0, 1)$ ، $(2, 1, 4)$ مستقلان خطياً في IR^3 . أوجد قاعدة للفضاء IR^3 تحوي هذان المتجهان . استخدم القاعدة نفسها لإيجاد متمم للفضاء الجزئي $< (1, 0, 1), (2, 1, 4) >$ من IR^3 .

[**إجابة** $\{(1, 0, 1), (2, 1, 4), (0, 0, 1)\}$ ، $< (0, 0, 1) >$]

4- ليكن F حقلاً يحوي q عنصراً وليكن V_F فضاء متجهي ذو بعد n و W فضاءً جزئياً من V_F ذو بعد $m < n$. كم متمما للفضاء W في V ؟

[**إجابة** $q^{m(n-m)}$]

5- ليكن V_F فضاءً متجهاً ذو بعد n . إذا كان V_1 ، V_2 فضاءان جزئيان يعد كل منهما أكبر من $\frac{n}{2}$. برهن أن $V_1 \cap V_2 \neq (0)$.

6- ليكن x, y, z عناصر في فضاء متجهي V'_F . ولتكن L, M, N فضاءات جزئية مولدة بالعناصر x, y, z على الترتيب . برهن أن x, y, z مستقلة خطياً على F إذا وفقط إذا كانت L, M, N مستقلة .

7- ليكن V الفضاء المتجهي لجميع الدوال الحقيقية على $I\!R$. إذا كان : $V_1 = \{f \in V \mid f(-x) = f(x)\}$ و $V_2 = \{f \in V \mid f(-x) = -f(x)\}$ برهن أن V_1, V_2 فضاءان جزئيان من V وأن $V = V_1 \oplus V_2$.

8- ليكن V_1, V_2 فضاءان جزئيان من فضاء متجهي V بحيث أن $V = V_1 + V_2$. فإذا كان W متمماً للفضاء $V_1 \cap V_2$ من V_2 [أي أن $V_2 = (V_1 \cap V_2) \oplus W$] . برهن أن $V = V_1 \oplus W$.

9- ** ليكن V فضاءً متجهاً ذو بعد منته على حقل F . إذا كان $V = V_1 \oplus V_2$ و L أي فضاء جزئي من V . برهن أن :

$$2 \dim L - \dim V \leq \dim[(V_1 \cap L) \oplus (V_2 \cap L)] \leq \dim L$$

10- برهن بإعطاء مثال أنه تحت شروط معينة من الممكن إيجاد ثلاث فضاءات جزئية V_1, V_2, V_3 من فضاء متجهي V_F ذو بعد منتهي V_F بحيث :

$$V = V_1 \oplus V_2 = V_2 \oplus V_3 = V_3 \oplus V_1$$

ما الذي يمكن استنتاجه حول بعد الفضاء V ؟

[**إجابة** $\dim V$ عدد صحيح زوجي]

6- المصفوفات وتغيير القواعد

تعريف 11-34 (قاعدة مرتبة)

ليكن V_F فضاءً متجهاً ذو بعد منته n عندئذ أي مرتب نوني (n- مرتب) $(x_1, x_2, \ldots, x_n)$ لمتجهات في V_F يسمى قاعدة مرتبة للفضاء V_F إذا كانت المجموعة $\{x_1, x_2, \ldots, x_n\}$ هي قاعدة للفضاء V_F ، وعليه ففي قاعدة مرتبة ، ترتيب العناصر يؤخذ في الاعتبار . على سبيل المثال إذا كان $V = F^{(3)}$ ، فإننا نعلم أن $\{e_1, e_2, e_3\}$ حيث $e_1 = (1, 0, 0)$ ، $e_2 = (0, 1, 0)$ ، $e_3 = (0, 0, 1)$ هي قاعدة للفضاء V . عندئذ كل من المرتبات الثلاثية (e_1, e_2, e_3) ، (e_2, e_1, e_3) ، (e_1, e_3, e_2) هي قاعدة مرتبة للفضاء V_F . لاحظ أن المرتبات الثلاثية الثلاث مختلفة . وعليه فهي قواعد مرتبة مختلفة للفضاء المتجهي V_F .

إن مفهوم القاعدة المرتبة مفيد جداً في مناقشة المصفوفات وهذا ما ننوي القيام به في هذا البند .

ليكن $(x_1, x_2, \ldots, x_n)$ قاعدة مرتبة ثابتة لفضاء متجهي V_F ، وليكن $(y_1, y_2, \ldots, y_r)$ أي r - مرتب من متجهات في V_F ، بما أن كل عنصر في V يمكن التعبير عنه بطريقة واحدة فقط كتركيب خطي للمتجهات $x_1, x_2, \ldots, x_n$ يكون :

$$y_i = \sum_{i=1}^{n} \alpha_{ij} x_i , \; j = 1, 2, \ldots, r$$

حيث α_{ij} (يتعين بطريقة وحيدة) هي عناصر في F وعليه نحصل على مصفوفة $n \times r$ على F

$$(\alpha_{ij}) = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1r} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2r} \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nr} \end{bmatrix}$$

تسمى هذه المصفوفة ، بمصفوفة $(y_1, y_2, \dots, y_r)$ بالنسبة إلى $(x_1, x_2, \dots, x_n)$.
تذكر أنه يقال عن مصفوفة (α_{ij}) ذات سعة $n \times n$ على حقل F أنها مصفوفة غير منفردة إذا وجدت مصفوفة (β_{ij}) ذات سعة $n \times n$ على F بحيث أن $(\alpha_{ij})(\beta_{ij}) = I = (\beta_{ij})(\alpha_{ij})$ ، حيث I هي المصفوفة المحايدة على F . برهن الآن ما يلي.

نظرية 11-35

لتكن $(x_1, x_2, \dots, x_n)$ قاعدة مرتبة للفضاء المتجهي V_F و $(y_1, y_2, \dots, y_n)$ أي $n-$ مرتب من عناصر في V_F . عندئذ يكون $(y_1, y_2, \dots, y_n)$ قاعدة مرتبة للفضاء V_F إذا وفقط إذا كانت مصفوفة $(y_1, y_2, \dots, y_n)$ نسبة إلى $(x_1, x_2, \dots, x_n)$ غير منفردة .

البرهان

لتكن (α_{ij}) مصفوفة $(y_1, y_2, \dots, y_n)$ نسب إلى $(x_1, x_2, \dots, x_n)$. استناداً للتعريف فإن :

$$y_j = \sum_{i=1}^{n} \alpha_{ij} x_i, \; j = 1, 2, \dots, n \qquad (1)$$

لتكن $(y_1, y_2, \dots, y_n)$ قاعدة مرتبة للفضاء V_F ولتكن (β_{ij}) مصفوفة $(x_1, x_2, \dots, x_n)$ نسبة إلى $(y_1, y_2, \dots, y_n)$ فيكون :

$$x_i = \sum_{k=1}^{n} \beta_{ki} y_{kj}, \; i = 1, 2, \dots, n \qquad (2)$$

من (1) و (2) نجد أن

$$x_i = \sum_{k=1}^{n} \beta_{ki} \left(\sum_{l=1}^{n} \alpha_{lk} x_l \right)$$

$$= \sum_{l=1}^{n} \left(\sum_{k=1}^{n} \alpha_{lk} \beta_{ki} \right) x_l \qquad (3)$$

من ناحية أخرى فإن $x_i = \sum_{l=1}^{n} \delta_{li} x_i$ حيث $\delta_{li} = 0$ عندما $l \neq i$ و $\delta_{ii} = 1$ (أي عندما $l = i$) .

وهكذا
$$\sum_{l=1}^{n} \delta_{li} x_i = \sum_{l=1}^{n} \left(\sum_{k=1}^{n} (\alpha_{ik} \beta_{ki} \right) x_i$$

منها نستنتج أن $\delta_{li} = \sum_{k=1}^{n} \alpha_{ik} \beta_{ki}$.

وعليه فإن $\delta_{li} = (\alpha_{ij})(\beta_{ij})$. أي أن $I = (\alpha_{ij})(\beta_{ij})$. وبالمثل فإن $I = (\beta_{ij})(\alpha_{ij})$.

إذاً (α_{ij}) مصفوفة غير منفردة .

وبالعكس لتكن (α_{ij}) مصفوفة غير منفردة و $(\beta_{ij}) = (\alpha_{ij})^{-1}$ ، عندئذ نستنتج أنه لأي $i = 1, 2, \ldots, n$ فإن

$$\sum_{j=1}^{n} \beta_{ji} y_j = \sum_{j=1}^{n} \beta_{ji} \left(\sum_{k=1}^{n} \alpha_{kj} x_k \right)$$
$$= \sum_{k=1}^{n} \left(\sum_{j=1}^{n} \alpha_{kj} \beta_{ji} \right) x_k = x_i$$

لأن
$$\sum_{j=1}^{n} \alpha_{kj} \beta_{ji} = \begin{cases} 0 & k \neq i \text{ عندما} \\ 1 & k = i \text{ عندما} \end{cases}$$

إذاً $x_i \in < y_1, y_2, \ldots, y_n >$ لكل i .

وعليه فإن $V = < y_1, y_2, \ldots, y_n >$. وبما أن $\dim V = n$ ، فإن المتجهات $y_1, y_2, \ldots, y_n$ تشكل قاعدة للفضاء المتجهي V ، إذاً $(y_1, y_2, \ldots, y_n)$ قاعدة مرتبة للفضاء V ، وهكذا يكمل البرهان . □

تعريف 11-36

تسمى القاعدة المرتبة $(e_1, e_2, \ldots, e_n)$ للفضاء المتجهي $F^{(n)}$ حيث $e_1 = (1, 0, \ldots, 0)$ ، $e_2 = (0, 1, 0, \ldots, 0)$ ، … ، $e_n = (0, 0, \ldots, 0, 1)$ بالقاعدة القياسية (المعيارية) للفضاء $F^{(n)}$.

مثال 15

اعتبر $F^{(3)}$. لتكن $f_1 = (1, 0, 0)$ ، $f_2 = (1, \alpha, 0)$ ، $f_3 = (1, \alpha, \beta)$ حيث α, β عناصر غير صفرية في F .

يمكن بسهولة رؤية أن هذه المتجهات مستقلة خطياً . وعليه فإن (f_1, f_2, f_3) قاعدة مرتبة للفضاء المتجهي V .

لتكن (e_1, e_2, e_3) القاعدة القياسية للفضاء V . بما أن $e_1 = (1, 0, 0)$ ، $e_2 = (0, 1, 0)$ ، $e_3 = (0, 0, 1)$ نحصل على

$$f_1 = e_1 = 1.e_1 + 0.e_2 + 0.e_3$$
$$f_2 = 1.e_1 + \alpha.e_2 + 0.e_3$$

و

$$f_3 = 1.e_1 + \alpha.e_2 + \beta.e_3$$

لذا فإن مصفوفة (f_1, f_2, f_3) بالنسبة إلى (e_1, e_2, e_3) هي

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & \alpha & \alpha \\ 0 & 0 & \beta \end{pmatrix}$$

بما أن

$$e_1 = f_1 = 1.f_1 + 0.f_2 + 0.f_3$$
$$e_2 = -\alpha^{-1}.f_1 + \alpha^{-1}.f_2 + 0.f_3$$
$$e_3 = 0.f_1 - \beta^{-1}.f_2 + \beta^{-1}.f_3$$

فإن مصفوفة (e_1, e_2, e_3) بالنسبة إلى (f_1, f_2, f_3) هي

$$B = \begin{pmatrix} 1 & -\alpha^{-1} & 0 \\ 0 & \alpha^{-1} & -\beta^{-1} \\ 0 & 0 & \beta^{-1} \end{pmatrix}$$

إذاً $B = A^{-1}$.

نظرية 11-37

ليكن V_F فضاءً متجهاً ذو بعد n . إذا كانت $A = (\alpha_{ij})$ هي مصفوفة القاعدة $(f_1, f_2, \dots, f_n)$ بالنسبة إلى القاعدة $(e_1, e_2, \dots, e_n)$ وأن $B = (\beta_{ij})$ هي مصفوفة القاعدة $(g_1, g_2, \dots, g_n)$ بالنسبة إلى $(f_1, f_2, \dots, f_n)$ ، فإن مصفوفة $(g_1, g_2, \dots, g_n)$ بالنسبة إلى $(e_1, e_2, \dots, e_n)$ هي AB .

البرهان

الآن

$$f_k = \sum_{j=1}^{n} \alpha_{jk} e_j, k = 1, 2, \ldots, n$$

$$g_i = \sum_{k=1}^{n} \beta_{ki} f_k, i = 1, 2, \ldots, n$$

وعليه فإن

$$g_i = \sum_{k=1}^{n} \beta_{ki} \left(\sum_{j=1}^{n} \alpha_{jk} e_j \right)$$

$$= \sum_{j=1}^{n} \left(\sum_{j=1}^{n} \alpha_{jk} \beta_{kj} \right) e_j$$

$$= \sum_{j=1}^{n} \gamma_{ji} e_j \quad ; \quad i = 1, 2, \ldots, n$$

حيـث $\gamma_{ji} = \sum_{k=1}^{n} \alpha_{jk} \beta_{ki}$ وعليـه فـإن $(\gamma_{ij}) = (\alpha_{ij})(\beta_{ij})$ ، إذاً مصـفوفة $(g_1, g_2, \ldots, g_n)$ نسبته إلى $(e_1, e_2, \ldots, e_n)$ هي $(\gamma_{ij}) = (\alpha_{ij})(\beta_{ij}) = AB$

وهذا يثبت النظرية . □

مسائل

1- إذا كان V_F فضاءً متجهاً ذو بعد n و $(e_1, e_2, \ldots, e_n)$ قاعدة مرتبة لـ V_F ، برهن أن الراسم $(f_1, f_2, \ldots, f_n) \leftrightarrow (\alpha_{ij})$
هو تناظر أحادي بين مجموعة جميع القواعد المرتبة للفضاء V_F ومجموعة جميع المصفوفات غير المنفردة ذات السعة $n \times n$ على F ، حيث $(f_1, f_2, \ldots, f_n)$ قاعدة مرتبة للفضاء V_F و (α_{ij}) مصفوفة $(f_1, f_2, \ldots, f_n)$ بالنسبة إلى $(e_1, e_2, \ldots, e_n)$.

2- ليكن $V = IR^3$. أوجد مصفوفة القاعدة المرتبة (f_1, f_2, f_3) نسبة للقاعدة القياسية (e_1, e_2, e_3) للفضاء V_F عندما f_1, f_2, f_3 تكون معطاة كما يلي :

(i) $f_1 = (1, \cos x, \sin x)$ ، $f_2 = (1, 0, 0)$ ، $f_3 = (1, -\sin x, \cos x)$

(ii) $f_1 = (2, 1, 0)$ ، $f_2 = (0, 2, 1)$ ، $f_3 = (0, 1, 2)$.

وفي كل حالة أوجد مصفوفة (e_1, e_2, e_3) بالنسبة إلى (f_1, f_2, f_3) .

[**إجابة** مصفوفتا (f_1, f_2, f_3) نسبة إلى (e_1, e_2, e_3) هما :

$$\text{(i)} \begin{pmatrix} 1 & 1 & 1 \\ \cos x & 0 & -\sin x \\ \sin x & 0 & \cos x \end{pmatrix} \quad \text{(ii)} \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

ومصفوفتا (e_1, e_2, e_3) نسبة إلى (f_1, f_2, f_3) هما :

$$\text{(i)} \begin{pmatrix} 0 & \cos x & \sin x \\ 1 & \sin x - \cos x & -\sin x - \cos x \\ 0 & -\sin x & \cos x \end{pmatrix} \quad \text{(ii)} \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} \\ \frac{1}{6} & -\frac{1}{3} & \frac{2}{3} \end{pmatrix}]$$

3- أوجد العدد الكلي للقواعد المرتبة للفضاء $V = F^{(n)}$ حيث F حقل يحوي q عنصراً .

[**إجابة** $(q^n - 1)(q^n - q)(q^n - q^{n-1})$] .

7– فضاءات الضرب الداخلي (Inner Product Spaces)

إن خواص الفضاءات المتجهة التي نوقشت في البنود السابقة اعتمدت أساساً على جمع المتجهات وضرب متجهات في قياسيات . في هذا البند نقدم بنية أخرى في فضاء متجهي مفترضين وجود دالة ، مثل الضرب الداخلي والمعيار . هذه الدوال تعمم مفاهيم طول المتجه ، التعامد بين متجهين والزاوية بين متجهين . في البداية يبدو هذا العرض غير ملائم وليس له تطبيقات مباشرة . ولكن في الحقيقة أنه يزودنا بحلقة ربط بين التحليل والجبر . فالفضاء المتجهي المزود بـ "معيار" يصبح فضاءً مترياً . وعليه يمكن استخدام مفاهيم النهاية ، المتتابعات والاتصال . مع ذلك فلن نستطيع التوسع في هذه الممكنات جميعها ، وبدلاً من ذلك سوف نركز على المظاهر الجبرية لهذه الدوال . لتوضيح النظرية بأسلوب معقول (كأن نجعله يظهر امتداداً طبيعياً لمفاهيم هندسية مثل الطول ، التعامد والزاوية) علينا أن نضحي ببعض العمومية . لذا فإننا في هذا البند لن نأخذ بعين الاعتبار الفضاءات المتجهة على حقل اختياري ونفضل الاقتصار على أن يكون F هو حقل الأعداد الحقيقية أو المركبة . في الحالة الأولى يسمى V_F فضاء متجهي حقيقي وفي الحالة الثانية يسمى فضاء متجهي مركب .

ملاحظة إذا كان $\alpha \in I\!R$ فإن $|\alpha|$ يرمز للقيمة المطلقة للعدد α أي أن $|\alpha| = \alpha$ إذا كان $\alpha \geq 0$ و $|\alpha| = -\alpha$ عندما $\alpha < 0$. وإذا كان $\alpha = x + iy$ حيث $x, y \in R$ فإن $|\alpha|$ يرمز لمعيار (مقياس) α ، أي أن $|\alpha| = \sqrt{x^2 + y^2}$.

تعريف 11-38

يقال لفضاء متجهي V_F أنه فضاء ضرب داخلي إذا وجدت دالة $f : V \times V \to F$ تحقق البديهيات التالية :

لكل $u, v, w \in V$ ، $\alpha, \beta \in F$.

IP-1 $f(u, v) = \overline{f(v, u)}$ أي المرافق المركب للدالة $f(v, u)$.

IP-2 $f(u, u) \geq 0$ وأن $f(u, u) = 0$ إذا وفقط إذا كان $u = 0$.

IP-3 $f(\alpha u + \beta v, w) = \alpha f(u, w) + \beta f(v, w)$.

الدالة f التي تحقق IP-1 ، IP-2 ، IP-3 ، تسمى ضرب داخلي على V .

ملاحظة

1- حسب IP-1 فإن $f(u, u) = \overline{f(u, u)}$ وعليه فإن $f(u, u)$ عدد حقيقي ، لذا فإن IP-2 له معنى .

2- إذا كان $F = IR$ فإن IP-1 لا يعني سوى أن $f(u, v) = f(v, u)$.

اصطلاح من المعتاد أن يرمز إلى $f(u, v)$ بأحد الرموز التالية :

$$< u \mid v > ; u.v ; (u, v)$$

في هذا الكتاب سوف نستخدم الرمز $< u \mid v >$.

مثال 16

لكل عنصرين $u = (a, b)$ ، $v = (c, d)$ في C^2 ، عرف $< u \mid v >$ يساوي $a\bar{c} + b\bar{d}$.

أي أن $< u \mid v > = a\bar{c} + b\bar{d}$. ندعي أن هذا يمثل ضرب داخلي على C^2 . أي أنه تحقق البديهيات الثلاثة .

IP-1 $\overline{< v \mid u >} = \overline{c\bar{a} + d\bar{b}} = \bar{c}a + \bar{d}b = a\bar{c} + b\bar{d} = < u \mid v >$

IP-2 $< u \mid u > = a\bar{a} + b\bar{b} = | a |^2 + | b |^2 \geq 0$

وأن

$$\begin{aligned} < u \mid u > = 0 &\Leftrightarrow | a |^2 + | b |^2 = 0 \Leftrightarrow | a | = | b | = 0 \\ &\Leftrightarrow a = b = 0 \\ &\Leftrightarrow u = 0 \end{aligned}$$

IP-3 إذا كان $\alpha, \beta \in C$ و $w = (x, y) \in C^2$ فإن :

$$\begin{aligned} < \alpha u + \beta v \mid w > &= (\alpha a + \beta c)\overline{x} + (\alpha b + \beta d)\overline{y} \\ &= \alpha(a\overline{x} + b\overline{y}) + \beta(c\overline{x} + d\overline{y}) \\ &= \alpha < u \mid w > + \beta < v \mid w > \end{aligned}$$

إذاً C^2 فضاء ضرب داخلي ، أي أن ادعائنا صحيح .

ملحوظة الضرب الداخلي المعرف في مثال 16 يشير عادة للضرب الداخلي القياسي .

مثال 17

لكل $u = (a, b) \in /R^2$ ، $v = (c, d)$. عرف :

$$< u \mid v > = ac - bc - ad + 4bd$$

من الواضح أن

$$< v \mid u > = ca - cb - da + 4db = < u \mid v >$$

كذلك :

$$\begin{aligned} < u \mid u > &= a^2 - ab - ab + 4b^2 = a^2 - 2ab + 4b^2 \\ &= (a - b)^2 + 3b^2 \geq 0 \end{aligned}$$

وأن

$$< u \mid u > = 0 \Leftrightarrow (a - b)^2 + 3b^2 = 0 \Leftrightarrow a = b = 0 \Leftrightarrow u = 0$$

وأخيراً إذا كان $w = (e, f) \in /R^2$ و $\alpha, \beta \in /R$ فإن :

$$\begin{aligned} < \alpha u + \beta v \mid w > &= (\alpha a + \beta c)e - (\alpha b + \beta d)e \\ &\quad -(\alpha a + \beta c)f + 4(\alpha b + \beta d)f \\ &= \alpha(ae - be - af + 4bf) + \beta(ce - de + 4df) \\ &= \alpha < u \mid w > + \beta < v \mid w > \end{aligned}$$

إذاً $/R^2$ فضاء ضرب داخلي .

مثال 18

ليكن V الفضاء المتجهي على C لجميع الدوال المتصلة ذات القيم المركبة المعرفة على الفترة $[0, 1]$. إذا كان $f(t), g(t) \in V$ نعرف :

$$< f(t) \mid g(t) > = \int_0^1 f(t)\, \overline{g(t)}\, dt$$

من الواضح أن $$\overline{\int_0^1 g(t)\,\overline{f(t)}\,dt} = \int_0^1 \overline{g(t)}\,f(t)\,dt = \int_0^1 f(t)\,\overline{g(t)}\,dt$$

إذاً $$< f(t) \mid g(t) > = \overline{< g(t), f(t) >}$$

مرة أخرى $$< f(t) \mid f(t) > = \int_0^1 f(t)\,\overline{f(t)}\,dt = \int_0^1 |\ f(t)\ |^2\ dt \geq 0$$

والمساواة تتحقق إذا وفقط إذا كان $f(t) = 0$ ، وأخيراً لكل $\alpha, \beta \in C, h(t) \in V$ فإن :

$$\begin{aligned} < \alpha f(t) + \beta g(t) \mid h(t) > &= \int_0^1 [\alpha f(t) + \beta g(t)]\,\overline{h(t)}\,dt \\ &= \alpha\int_0^1 f(t)\,\overline{h(t)}\,dt + \beta\int_0^1 g(t)\,\overline{h(t)}\,dt \\ &= \alpha < f(t) \mid h(t) > + \beta < g(t) \mid h(t) > \end{aligned}$$

أي أن V فضاء ضرب داخلي .

مثال 19

اعتبر الفضاء المتجهي IR^n لكل $u = (x_1, x_2, \ldots, x_n)$ ، $V = (y_1, y_2, \ldots, y_n)$ في IR^n ، ضع $< u \mid v > = \sum_{i=1}^{n} x_i y_i$.

تعريف 11-39

فضاء الضرب الداخلي الحقيقي المنته البعد يسمى فضاء إقليدي . وفضاء الضرب الداخلي المركب المنته البعد يسمى فضاء وحدوياً . قبل أن نقدم التعريف التالي نود أن نطبع في ذهن القارئ أنه من الآن فصاعداً عندما نتكلم عن جذر تربيعي لعدد غير سالب فإننا نقصد القيمة الموجبة للجذر التربيعي وبناءً على هذا الاتفاق فإن $\sqrt{4} = 2$ وليس -2 .

تعريف 11-40

لأي متجه $v \in V$ فإن معيار v (أو طول v) يعرف بأنه $\sqrt{< v \mid v >}$.

ملاحظة حسب التعريف فإن معيار $v \in V$ هو دائماً عدد حقيقي غير سالب .

اصطلاح سنرمز لمعيار v بالرمز $\| v \|$.

تعريف 11-41

لكل $u, v \in V$ فإن $\| u - v \|$ يسمى المسافة بين v, u .

اصطلاح سوف نستخدم الرمز $d(u, v)$ ليشير للمسافة بين v, u .

نتوقف هنا قليلاً لإثبات خواص معينة للضرب الداخلي والتي هي نتيجة مباشرة للبديهيات IP-1 ، IP-2 ، IP-3 والتعريف 11-40 .

نظرية 11-42

إذا كان V فضاء ضرب داخلي فإنه لجميع المتجهات $u, v, w, x \in V$ ، وعناصر الحقل $\alpha, \beta, \gamma, \delta \in F$ ، فيكون :

(i) $< u \mid \alpha v + \beta w > = \overline{\alpha} < u \mid v > + \overline{\beta} < u \mid w >.$

(ii) $< \alpha u + \beta v \mid \gamma w + \delta x > = \alpha\overline{\gamma} < u \mid w > + \alpha\overline{\delta} < u \mid x > + \beta\overline{\gamma} < v \mid w > + \beta\overline{\delta} < v \mid x >$

(iii) $< 0 \mid v > = < u \mid 0 > = 0$

(iv) $< u \mid v > = 0, \quad \forall u \in V \Rightarrow v = 0, < u \mid v > = 0, \quad \forall v \in V \Rightarrow u = 0$

(v) $\| \alpha u \| = | \alpha | \| u \|$

البرهان

(i) استناداً إلى $IP - 1$ فإن :

$$
\begin{aligned}
< u \mid \alpha v + \beta w > &= \overline{< \alpha v + \beta w \mid u >} \\
&= \overline{\alpha < v \mid u > + \beta < w \mid u >} && \text{(حسب IP-3)} \\
&= \overline{\alpha}\, \overline{< v \mid u >} + \overline{\beta}\, \overline{< w \mid u >} && \text{(حسب خاصية المرافق)} \\
&= \overline{\alpha} < u \mid v > + \overline{\beta} < u, w > && \text{(حسب IP-1)}
\end{aligned}
$$

(ii) (حسب IP-3)

$$< \alpha u + \beta v \mid \gamma w + \delta x > = \alpha < u \mid \gamma \omega + \delta x > + \beta < v \mid \gamma w + \delta x >$$

$$= \alpha \{ \bar{\gamma} < u, w > + \bar{\delta} < u \mid x > \} + \beta \{ \bar{\gamma} < v \mid w > + \bar{\delta} < v \setminus x > \} \qquad \text{(حسب i)}$$

$$= \alpha \bar{\gamma} < u \mid w > + \alpha \bar{\delta} < u \mid x > + \beta \bar{\gamma} < u \mid w > + \beta \bar{\delta} < v \mid x >$$

(iii) $< 0 \mid v > = < 0u + 0w \mid v > = 0 < u \mid v > + 0 < w \mid v > = 0$

بصورة مشابهة :

$$< u \mid 0 > = < u \mid 0v + 0w > = \bar{0} < u \mid v > + \bar{0} < u \mid w > = 0$$

(iv) (حسب IP-2)

$$< u \mid v > = 0 \quad \forall v \in V \Rightarrow < u \mid u > = 0 \Rightarrow u = 0$$

(v) (حسب ii) $\qquad \| \alpha u \|^2 = < \alpha u \mid \alpha u > = \alpha \bar{\alpha} < u, u >$

إذاً $\| \alpha u \| = | \alpha | \| u \|$. □

من الممكن إثبات أن البديهيات IP-1 ، IP-2 ، IP-3 محققة وعليه فإن IR^2 فضاء ضرب داخلي .

ملحوظة من الآن فصاعداً وفيما تبقى من هذا البند فإن V يرمز لفضاء ضرب داخلي .

نظرية 11-43 (متباينة شوارتز)

لكل $u, v \in V$ ، فإن $| < u \mid v > | \leq \| u \| \| v \|$.

البرهان

إذا كان $u = 0$ فإن الطرف الأيسر $| < u, v > | = < 0 \mid v > = 0$

و $\| u \| \| v \| = \| 0 \| \| v \| = 0$

إذاً $< u \mid v > = \| u \| \| v \|$

الآن افـــرض أن $u \neq 0$ ، فـــإن $\| u \| \neq 0$ فـــإذا لم يكـــن $\| u \| \neq 0$ كـــان $\| u \| = 0 \Rightarrow < u \mid u > = 0 \Rightarrow u = 0$ ، وهذا يناقض الفرضية أن $u \neq 0$.

ضع
$$w = v - \frac{< v \mid u >}{\| u \|^2} u$$

بما أن $\| w \|^2 \geq 0$ فإن
$$\left\langle v - \frac{< v \mid u >}{\| u \|^2} u \mid v - \frac{< v \mid u >}{\| u \|^2} u \right\rangle \geq 0$$
$$\Rightarrow < v \mid v > - \frac{\overline{< v \mid u >}}{\| u \|^2} < v \mid u > - \frac{< v \mid u >}{\| u \|^2} < u \mid v >$$
$$+ \frac{< v \mid u > \overline{< v \mid u >}}{\| u \|^2} < u \mid u > \geq 0$$
$$\Rightarrow \| v \|^2 - \frac{|< v \mid u >|^2}{\| u \|^2} - \frac{\overline{< u \mid v >} < u \mid v >}{\| u \|^2}$$
$$+ \frac{|< v \mid u >|^2}{\| u \|^4} \| u \|^2 \geq 0$$
$$\Rightarrow \| v \|^2 - \frac{|< u \mid v >|^2}{\| u \|^2} \geq 0$$
$$\Rightarrow |< u \mid v >|^2 \leq \| u \|^2 \| v \|^2$$
$$\Rightarrow |< u \mid v >| \leq \| u \| \| v \| . \square$$

ملاحظة هذه المتباينة تسمى أيضاً متباينة كوشي شوارتز .

نظرية 11-44

كل فضاء ضرب داخلي هو فضاء متري .

البرهان

ليكن V فضاء ضرب داخلي . لكل $u, v \in V$ ضع $d(u, v) = \| u - v \|$.

بما أن المعيار عدد غير سالب ، فإن $d(u, v) \geq 0$.أضف لذلك أن :
$$d(u, v) = 0 \Leftrightarrow \| u - v \| = 0 \Leftrightarrow < (u - v) \mid (u - v) = 0 \Leftrightarrow u = v$$

لذلك
$$d(u, v) = \| u - v \| = \sqrt{< (u - v) \mid (u - v) >}$$
$$= \sqrt{(-1)(-1)(< (v - u) \mid (v - u) >)}$$

$$= \sqrt{< (v-u) \mid (v-u) >} = \| v - u \| = d(v, u)$$

ندعي أن $\| u + v \| \leq \| u \| + \| v \|$ لكل $u, v \in V$ لإثبات الادعاء فإن :

$$\begin{aligned} \| u + v \|^2 &= < u + v \mid u + v > \\ &= < u \mid u > + < v \mid u > + < u \mid v > + < v \mid v > \\ &= \| u \|^2 + \overline{< u \mid v >} + < u \mid v > + \| v \|^2 \\ &= \| u \|^2 + 2R(< u \mid v >) + \| v \|^2 \end{aligned}$$

حيث $R(\alpha)$ يرمز للجزء الحقيقي للعدد المركب α .

لما كان $R(\alpha) \leq |\alpha|$ فإن $\| u + v \|^2 \leq \| u \|^2 + 2 | < u \mid v > | + \| v \|^2$

(حسب متباينة شوارز) $\leq \| u \|^2 + 2 \| u \| \| v \| + \| v \|^2$

$$\Rightarrow \| u + v \|^2 \leq (\| u \| + \| v \|)^2$$
$$\Rightarrow \| u + v \| \leq \| u \| + \| v \|$$

وهكذا فإن ادعائنا محقق .

وأخيراً لكل $u, v, w \in V$ يكون $d(u, v) + d(v, w) = \| u - v \| + \| v - w \|$

(حسب ادعائنا) $\geq \| u - v + v - w \|$

$$\Rightarrow d(u, v) + d(v, w) \geq \| u - w \| = d(u, w)$$

إذاً V فضاء متري . □

إن لمفهوم التعامد أهمية كبرى في الهندسة ، وفيما يلي نعرض مفهوماً مشابهاً في فضاءات الضرب الداخلي .

تعريف 11-45

ليكن $u, v \in V$. يقال أن u عمودي على v إذا كان $< u \mid v > = 0$.

ملاحظة يتضح من التعريف أنه إذا كان u عمودياً على v فإن v عمودي على u ، لأن

$$< u \mid v > = 0 \Rightarrow \overline{< v \mid u >} = 0 \Rightarrow < v \mid u > = \overline{0} = 0$$

تعريف 11-46

إذا كان W فضاءً جزئياً من V ، فإن المتمم العمودي للفضاء W يرمز له بالرمز W ويعرف بأنه المجموعة $\{u \in V \mid < u \mid w > = 0, \quad \forall\, w \in W\}$

مثال 20

كما رأينا في مثال 16 ، أنه إذا كان $u = (a,b) \in C^2$ ، $v = (c,d)$ ، فإن $< u, v > = a\bar{c} + b\bar{d}$ يمثل ضرباً داخلياً لمتجهات $x = (3,5)$ ، $y = (5i, -3i)$ متعامدان لأن $< x \mid y > = 3(-5i) + 5(3i) = 0$.

مثال 21

في مثال 18 ، المتجهان $\sin \pi t$ ، $\cos \pi t$ متعامدان لأن :

$$\begin{aligned} < \sin \pi \mid \cos \pi t > &= \int_0^1 \sin \pi t \cos \pi t dt \\ &= \frac{1}{2}\int_0^1 \sin 2\pi t\, dt = -\frac{1}{4\pi}\left(\cos 2\pi t\right)_0^1 = 0 \end{aligned}$$

مثال 22

ليكن $V = IR^2$ و $W = \{(a,a) \mid a \in IR\}$. عندئذ يكون W فضاءً جزئياً من V . نزود V بالضرب الداخلي المعرف في مثال 17 أي أن لكل $v = (x', y'), u = (x,y) \in IR^2$ نضع $< u \mid v > = xx' - yx' - xy' + 4yy'$

ندعي أن $W^{\perp} = \{(x,0) \mid x \in IR\}$. بما أن :

$$(p,q) \in W^{\perp} \Rightarrow < (a,a) \mid (p,q) > = 0, \quad \forall \quad a \in IR$$

إذا أخذنا $a \neq 0$ ، فإن

$$(p,q) \in W^{\perp} \Rightarrow ap - ap - aq + 4aq = 0 \Rightarrow aq = 0 \Rightarrow q = 0$$

ولأي $r \in IR$ فإن :

$$< (a, a) \mid (r, 0) > = ar - ar - 0 + 4.0 = 0, \qquad \forall \quad (a, a) \in W$$

إذاً ادعائنا قد تحقق .

قضية 11-47

لأي فضاء جزئي W من V فإن $W^{\perp}$ فضاء جزئي من V يحقق $W \cap W^{\perp} = (0)$.

البرهان

من الواضح أن $0 \in W^{\perp}$ عليه فإن $W^{\perp}$ مجموعة غير خالية . وإذا كان $u, v \in W^{\perp}$ و $\alpha, \beta \in F$ فإن $< u \mid w > = < v \mid w > = 0$ لجميع $w \in W^{\perp}$. ولكل $w \in W$ يكون :

$$< \alpha u + \beta v \mid w > = \alpha < u \mid w > + \beta < v \mid w > = 0 \Rightarrow \alpha u + \beta v \in W^{\perp}$$

وبالتالي فإن $W^{\perp}$ هو فضاء جزئي من V . وأخيراً :

$$x \in W \cap W^{\perp} \Rightarrow x \in W \text{ and } x \in W^{\perp}$$
$$\Rightarrow < x \mid x > = 0 \Rightarrow x = 0 \Rightarrow W \cap W^{\perp} = (0) . \square$$

تعريف 11-48

يقال لمجموعة جزئية x من V أنها مجموعة متعامدة إذا كان لكل $x, y \in X$ فإن $< x \mid y > = 0$ طالما $x \neq y$.

تعريف 11-49

يقال لمجموعة جزئية X من V أنها مجموعة عيارية متعامدة ، إذا كان :

(i) $\| x \| = 1$ لكل $x \in X$.

(ii) $< x \mid y > = 0$ لكل $x, y \in X$ طالما أن $x \neq y$.

مثال 23

ليكن V الفضاء المتجهي على IR لجميع الدوال الحقيقية المتصلة المعرفة على الفترة $[0, 1]$ مع الضرب الداخلي .

$$< f \mid g > = \int_0^1 f(x)g(x)dx, \qquad \forall \quad f, g \in V$$

لكل $n \in N$ ، نعرف $f_n(x) = \sqrt{2} \cos 2\pi nx$ و $g_n(x) = \sqrt{2} \sin 2\pi nx$ افرض أن :

$$X = \{1, f_1, g_1, f_2, g_2, \ldots\}$$

واضح أنه لكل $n \in N$ يكون :

$$< f_n \mid f_n > = \int_0^1 2 \cos^2 \; 2\pi nx \; dx = \int_0^1 (1 + \cos 4\pi nx) dx$$

$$= 1 + \frac{1}{\pi n} (\sin 4\pi nx)_0^1 = 1 \Rightarrow \| f \| = 1$$

بصورة مشابهة لكل $n \in N$ فإن $< g_n \mid g_n > = 1 \Rightarrow \| g_n \| = 1$ ، إضافة إلى ذلك إذا كان $n \neq m$ فإن :

$$\text{(i)} \qquad < f_n \mid g_m > = \int_0^1 2 \cos 2\pi nx \sin 2\pi mx \; dx =$$

$$\int_0^1 \left[\sin 2\pi(n + m)x - \sin 2\pi(n - m)x \right] dx = 0$$

$$\text{(ii)} \qquad < f_n \mid f_m > = \int_0^1 2 \cos 2\pi nx \cos 2\pi mx \; dx =$$

$$\int_0^1 \left[\cos 2\pi(n + m)x + \cos 2\pi(n - m)x \right] dx = 0$$

$$\text{(iii)} \qquad < g_n \mid g_m > = \int_0^1 2 \sin 2\pi nx \sin 2\pi mx \; dx$$

$$\int_0^1 \left[\cos s\pi(m - n)x - \cos 2\pi(n + m)x \right] dx = 0$$

كذلك لكل $n \in N$ فإن

$$< 1 \mid f_n > = \int_0^1 \sqrt{2} \cos 2\pi nx \; dx = 0$$

و

$$< 1 \mid g_n > = \int_0^1 \sqrt{2} \sin 2\pi nx \; dx = 0$$

وعليه فإن X مجموعة جزئية عيارية متعامدة من V .

مثال 24

اعتبر C^2 مع الضرب الداخلي القياسي . إذا أخذنا $e_1 = (0, 1)$ ، $e_2 = (1, 0)$ فإن $\{e_1, e2\}$ مجموعة جزئية عيارية متعامدة من C^2 ، لأن

$$< e_1 \mid e_1 > = 1.\bar{1} + 0.\bar{0} = 1$$

كذلك
$$< e_1, e_2 > = 1.\bar{0} + 0.\bar{1} = 0$$

قضية 11-50

أية مجموعة متعامدة لمتجهات غير صفرية تكون مستقلة خطياً .

البرهان

لتكن X أية مجموعة جزئية متعامدة في فضاء ضرب داخلي V بالصيغة $0 \notin X$. لتكن $v_1, v_2, \ldots, v_k \in X$ و $\alpha_i \in F$ ، بحيث $\sum_{i=1}^{k} \alpha_i v_i = 0$.

لأي $j \in \{1, 2, \ldots, k\}$ فإن $< \sum_{i=1}^{k} \alpha_i v_i \mid v_j > = 0$ (لأن $< v_i \mid v_j > = 0$ عندما $i \neq j$)

$$\Rightarrow \alpha_j < v_j \mid v_j > = 0$$

وبما أن $< v_i, v_j > \neq 0$ لأن $v_j \neq 0$ نستنتج أن $\alpha_j = 0$ ، وبالتالي فإن $v_1, v_2, \ldots, v_k$ مستقلة خطياً على F . نتيجة لذلك فإن X مجموعة جزئية مستقلة خطياً من V . □

نتيجة 11-51

إذا كانت $\{v_j\}$ مجموعة جزئية عيارية متعامدة من V ، فإن المتجهات v_j هذه تكون مستقلة خطياً على F . إضافة إلى ذلك إذا كان $w = \sum_{i=1}^{n} \alpha_i v_i$ فإن $\alpha_i = < w \mid v_i >$ لكل $i \in \{1, 2, \ldots, k\}$.

البرهان

الجزء الأول ينتج من القضية السابقة لإثبات . الجزء الثاني لاحظ أن :

$$< w \mid v_i >=< \sum_{j=1}^{k} \alpha_i v_j \mid v_i >= \sum_{j=1}^{k} \alpha_j < v_j \mid v_i >= \alpha_i$$

لأن $< v_j \mid v_i >= 0$ عندما $i \neq j$ و $< v_i \mid v_i >=\| v_i \|^2= 1$. □

قضية 1-52

إذا كانـت $\{v_1, v_2, \dots, v_k\}$ مجموعـة جزئيـة عياريـة متعامـدة في V فإنه لأي متجه $v \in V$ يكون $v = \sum_{i=1}^{k} < v \mid v_i > v_i$ عمودياً على كل متجه v_i ، أضف إلى ذلك إذا كـــان $y \notin < v_1, v_2, \dots, v_k >$ فإنـــه إذا أخـــذنا $z = y - \sum_{i=1}^{k} < y \mid v_i > v_i$ فـــإن $\| z \| \neq 0$ وإذا أخـذنا $v_{k+1} = \frac{z}{\| z \|}$ فـإن $\{v_1, v_2, \dots, v_{k+1}\}$ ، مجموعـة جزئيـة عياريـة متعامدة من V .

البرهان

لـــيكن $j \in \{1, 2, \dots, k\}$ فيمـــا أن $< v_i \mid v_j >= 0$ عنـــدما $i \neq j$ وأن $< v_i \mid v_i >= 1$ فإن

$$< (v - \sum_{i=1}^{k} < v \mid v_i > v_i) \mid v_j >=< v \mid v_j >= 0$$

وعليه فإن الجزء الأول قد تم إثباته .

الآن افرض أن $y \notin < v_1, v_2, \dots, v_k >$ وأن $\| z \|= 0$ حيث

$$z = y - \sum_{i=1}^{k} < y \mid v_i > vi$$

هذا بدوره يؤدي إلى أن $z = 0$ أو $y = \sum_{i=1}^{k} < y \mid v_i > v_i$.

ومن ذلك فإن y تركيب خطي من $(i = 1, 2, \dots, k)v_i$ ، بعبارة أخرى $y \in < v_1, v_2, \dots, v_k >$ وهذا خلاف الفرض ، وبالتالي فإن $\| z \| \neq 0$. لكي نكمل البرهان علينا أن نبين أن $< v_{k+1} \mid v_i > = 0$ لكل $i = 1, 2, \dots, k$ و $< v_{k+1}, v_{k+1} > = 1$.

حسب الجزء الأول $< z \mid v_i > = 0$ لكل $i = 1, 2, \dots, k$ ولكن

$$< v_{k+1} \mid v_i > = < \frac{z}{\| z \|} \mid v_i > = \frac{1}{\| z \|} < z \mid v_i >$$

وعليه يكون $< v_{k+1} \mid v_i > = 0$ لكل $i = 1, 2, \dots, k$.

وأخيراً $$< v_{k+1} \mid v_{k+1} > = < \frac{z}{\| z \|} \mid \frac{z}{\| z \|} > = \frac{1}{\| z \|^2} < z \mid z > = 1$$

وهكذا فإن القضية قد تم إثباتها . □

والآن نشرح الطريقة المشهورة لبناء قاعدة متعامدة .

(أي مجموعة عيارية متعامدة مولدة) لفضاء ضرب داخلي ذو بعد منته بادئين بقاعدة معطاة . هذه الطريقة تسمى عادة بطريقة جرام شميدت للتعامد .

نظرية 11-53

كل فضاء ضرب داخلي ذو بعد منته له قاعدة عيارية متعامدة .

البرهان

ليكن V فضاء ضرب داخلي ذو بعد n . بما أن كل مجموعة عيارية متعامدة تكون مستقلة خطياً وأن $\dim V = n$ فإننا نحاول إيجاد مجموعة عيارية متعامدة $\{f_1, f_2, \dots, f_n\}$ وهذا يؤدي إلى المطلوب .

الآن لتكن $\{e_1, e_2, \dots, e_n\}$ قاعدة للفضاء V .

نبدأ بوضع $v_1 = e_1$. بما أن $e_1 \neq 0$ ، فإن $\| v_1 \| \neq 0$ ، وبأخذ $f_1 = \frac{v_1}{\| v_1 \|}$

نرى أن $< f_1 \mid f_1 > = 1$.

بما أن $e_2 \notin < f_1 >$ ، حسب القضية 11-52 فإنه يوجد متجه $v_2 = e_2 - < e_2 \mid f_1 > f_1$ وأن $\| v_2 \| \neq 0$ وإذا كان $f_2 = \frac{v_2}{\| v_2 \|}$ فإن $\{f_1, f_2\}$ هي مجموعة جزئية عيارية متعامدة من V بالإضافة إلى أن $\{f_1, f_2\} \subseteq < e_1, e_2 >$. ندعي أن $e_3 \notin < f_1, f_2 >$.

إذا كان الادعاء غير صحيح فبإمكاننا إيجاد $\lambda_1, \lambda_2 \in F$ أحدهما على الأقل يختلف عن الصفر بحيث يكون $e_3 = \lambda_1 f_1 + \lambda_2 f_2$ هذا يؤدي إلى أن :

$$e_3 = \frac{\lambda_1 e_3}{\| v_1 \|} + \frac{\lambda_2 e_2}{\| v_2 \|} - \lambda_2 \frac{< e_1 \mid f_1 >}{\| v_1 \| \| v_2 \|} e_1$$

مرة ثانية وحسب القضية 11-52 يوجد متجه

$$v_3 = e_3 - < e_3 \mid f_1 > f_1 - < e_3 \mid f_2 > f_2$$

وأن $\| v_3 \| \neq 0$ وإذا أخذنا $f_3 = \frac{v_3}{\| v_3 \|}$ فإنه $\{f_1, f_2, f_3\}$ هي مجموعة جزئية عيارية متعامدة من V كذلك فإن $\{f_1, f_2, f_3\} \subseteq < e_1, e_2, e_3 >$.

الآن افرض أن بإمكاننا إنشاء مجموعة عيارية متعامدة :

$$\{f_1, f_2, \ldots, f_i\} \subseteq < e_1, e_2, \ldots, e_r >$$

بنفس الأسلوب السابق يمكن البرهنة على أن $e_{i+1} \notin < f_1, f_2, \ldots, f_n >$.

حسب القضية 11-52 يوجد متجه $v_{i+1} = e_{i+1} - \sum_{k=1}^{i} < e_{i+1} \mid f_k > f_k$ مع كون $\| v_{i+1} \| \neq 0$ و $f_{i+1} = \frac{r_{i+1}}{\| r_{i+1} \|}$ فإن $\{f_1, f_2, \ldots, f_{i+1}\}$ هي مجموعة جزئية عيارية متعامدة من V . بما أن كل مجموعة جزئية عيارية متعامدة من V هي مستقلة خطياً وأن $\dim V = n$ ، فإن هذه العملية تتوقف . عندها نحصل على مجموعة عيارية متعامدة $\{f_1, f_2, \ldots, f_n\}$. هذه تمثل قاعدة للفضاء V لأن $\dim V = n$ وبالتالي توجد قاعدة عيارية متعامدة للفضاء V . □

مثال 25

ليكن V الفضاء المتجهي على $I\!R$ لجميع كثيرات الحدود في $I\!R[x]$ والتي درجتها ≤ 3 . بعد الفضاء V على $I\!R$ يساوي 3 . وأن $\{1, x, x^2\}$ قاعدة للفضاء V . ضع $e_1 = 1$ ، $e_2 = x$ و $e_3 = x^2$ ولكل $f, g \in I\!R[x]$ عرف :

$$< f \mid g > = \int_0^1 f(x)\, g(x)\, dx$$

نطبق طريقة جرام شميدت للتعامد للحصو على قاعدة عيارية متعامدة للفضاء المتجهي V على $I\!R$.

ضع $v_1 = e_1$ و $e_1 = 1$ ضع $f_1 = \frac{e_1}{\| e_1 \|} = \frac{e_1}{\sqrt{\int_0^1 e_1.e_1 dx}} = e_1 = 1$

$$v_2 = e_2 - < e_2 \mid f_1 > f_1 = x - < x \mid 1 >$$

$$= x - \int_0^1 x\, dx = x - \frac{1}{2}$$

فإن
$$f_2 = \frac{v_2}{\| v_2 \|} = \frac{x - \frac{1}{2}}{\sqrt{\int_0^1 \left(x - \frac{1}{2} \right)^2 dx}} = \sqrt{3}(2x - 1)$$

مرة أخرى ضع
$$v_3 = e_3 - < e_3 \mid e_1 > f_1 - < e_3 \mid f_2 > f_2$$

$$= x^2 - \left(\int_0^1 x^2 dx \right) - (6x - 3) \int_0^1 (2x^3 - x^2)\, dx$$

$$= x^2 - x + \frac{1}{6}$$

الآن
$$\| v_3 \|^2 = \int_0^1 \left(x^2 - x + \frac{1}{0} \right)^2 dx = \frac{1}{180} \Rightarrow \| v \| = \frac{1}{6\sqrt{5}}$$

عليه فإن
$$f_3 = \frac{v_3}{\| v_3 \|} = (6x^2 - 6x + 1)\sqrt{5}$$

وبالتالي فإن $\{1, (2x - 1)\sqrt{3}, (6x^2 - 6x + 1)\sqrt{5}\}$ هي قاعدة عيارية متعامدة للفضاء V .

من النظرية التالية نبرهن أنه إذا كان W فضاءً جزئياً من فضاء ضرب داخلي V ذو بعد منته ، فإن $W^{\perp}$ هو فضاء جزئي متمم للفضاء W . وذلك يبرر تسميتنا $W^{\perp}$ بمتمم عمودي للفضاء W .

نظرية 11-54

لكل فضاء جزئي W من فضاء ضرب داخلي ذو بعد منته V يكون $V = W \oplus W^{\perp}$.

البرهان

بما أن W فضاء جزئي من V و V فضاء ضرب داخلي فإن W فضاء ضرب داخلي أيضاً واستناداً إلى نظرية 11-8 توجد قاعدة عيارية متعامدة $\{w_1, w_2, \ldots, w_m\}$ للفضاء W . ليكن $v \in V$ فإن

$$v = \sum < v \mid w_i > w_i + x$$

حيث

$$x = v - \sum_{i=1}^{m} < v \mid w_i > w_i$$

حسب القضية 11-52 فإن $< x \mid w_i > = 0$ لكل $i = 1, 2, \ldots, m$. ولما كان كل عنصر في W يمكن كتابته كتركيب خطي من $w_1, w_2, \ldots, w_m$ فإن $< x \mid w > = 0$ لكل $w \in W$. هذا يعني أن $x \in W^{\perp}$. إذاً $v \in W + W^{\perp}$ وبالتالي $v = W + W^{\perp}$. وأخيراً حسب القضية 11-47 نجد أن $W = W \oplus W^{\perp}$. □

نتيجة 11-55

إذا كان W فضاءً جزئياً في فضاء ضرب داخلي ذو بعد منته . فإن $(W^{\perp})^{\perp} = W$.

البرهان

ليكن $x \in W$ ، لكل $v \in W^\perp$ فإن

$$< x \mid v >= 0 \Rightarrow < v \mid x >= 0 \Rightarrow x \in (W^\perp)^\perp$$

هذا يبين أن $W \subseteq (W^\perp)^\perp$.

حسب نظرية 11-54 فإن $V = W \oplus W^\perp$ كذلك $V = W^\perp \oplus (W^\perp)^\perp$ عليه إذا كان $\dim V = n$ ، $\dim W = m$ فإن $\dim W^\perp = n - m$ و $\dim (W^\perp)^\perp = n - (n - m) = m$ بهذه الطريقة توصلنا إلى أن W فضاء جزئي من $(W^\perp)^\perp$ و $\dim W = (W^\perp)^\perp$ وبالتالي $W = (W^\perp)^\perp$. □

تمارين محلولة

تمرين 1

أوجد إذا كان ممكناً جمع المرتبات الرباعية للأعداد الحقيقية a, b, c, d التي تجعل $< u \mid v >= a\alpha_1^2 + b\beta_2^2 + c\alpha_1\alpha_2 + d\alpha_2\beta_1$ لكل $u = (\alpha_1, \alpha_2) \in IR^2$ ، $v = (\beta_1, \beta_2)$ يعرف ضرب داخلي على IR^2 .

الحل

ليكن $< u \mid v >= a\alpha_1^2 + b\beta_2^2 + c\alpha_1\alpha_2 + d\alpha_2\beta_1$

حيث $v = (\beta_1, \beta_2), u = (\alpha_1, \alpha_2) \in IR^2$

لنأخذ $u = (1, 0)$ ، $v = (0, 0)$ هو المتجه الصفري في IR^2 . فإن

$$< u \mid 0 >= 0 \Rightarrow a = 0$$

وبالتالي فإن لأي متجهين $u = (\alpha_1, \alpha_2)$ ، $v = (\beta_1, \beta_2)$ في IR^2 يكون

$$< u \mid v >= b\beta_2^2 + c\alpha_1\alpha_2 + d\alpha_2\beta_1$$

والآن لنأخـذ $\alpha_1 = \alpha_2 = 0$ ، $\beta_1 = \beta_2 = 1$ أي أن u هـو المتجـه الصـفري في IR^2 و $v = (1,1)$ ، عندئـــذ $0 = b \Leftarrow 0 = < 0 \mid v >$ إذاً $< u \mid v > = (\alpha_1\alpha_2 + d\alpha_2\beta_1$ لكل $v = (\beta_1, \beta_2) \in IR^2$ و $u = (\alpha_1, \alpha_2)$ هذا يؤدي إلى أن

$$< u \mid u > = c\alpha_1\alpha_2 + d\alpha_2\alpha_1 \geq 0$$

أي أن $(c + d)\alpha_1\alpha_2 \geq 0$ لكـــل $\alpha_1, \alpha_2 \in IR$ ، وخصوصـــاً فـــإن $(c + d)\alpha_1^2 \geq 0$ و $(c + d)(-\alpha_1^2) \geq 0$ (بوضع $\alpha_2 = \alpha_1$ و $\alpha_2 = -\alpha_1$ على الترتيب) فإننا نحصل على $(c + d)\alpha_1^2 = 0$ لكل $\alpha_1 \in IR$. نتيجة لذلك فإن $c = -d$. عليه فإن

$$< u \mid v > = c(\alpha_1\alpha_2 - \alpha_2\beta_1)$$

لكل $u = (\alpha_1, \alpha_2), v = (\beta_1, \beta_2) \in IR^2$

وأخيراً
$$< u \mid v > = < v \mid u > \Rightarrow c(\alpha_1\alpha_2 - \alpha_2\beta_1) = c(\beta_1\beta_2 - \beta_2\alpha_1)$$
$$\Rightarrow c\alpha_1(\alpha_2 + \beta_2) = c\beta_1(\alpha_2 + \beta_2) \qquad \forall \quad \alpha_1, \alpha_2, \beta_1, \beta_2 \in IR$$
$$\Rightarrow c\alpha_1 = c\beta_1 \quad \forall \quad \alpha_1, \beta_1 \in IR$$
$$\Rightarrow c = 0$$

إذاً $a = b = c = d = 0$. أي أن المرتـب الرباعـي الوحيـد (a, b, c, d) الـذي يمكـن أن يجعل

$$< u \mid v > = a\alpha_1^2 + b\beta_2^2 + c\alpha_1\alpha_2 + d\alpha_2\beta_1$$

ضـرباً داخلياً هـو $(0, 0, 0, 0)$ حيـث $u = (\alpha_1, \alpha_2), v = (\beta_1, \beta_2) \in IR^2$ ولكـن هـذا لا يجوز إذْ في هـذه الحالة يكون $< u \mid u > = 0$ لمتجهات غير صفرية ، إذاً لا يوجد رباعي مرتب بالصورة المطلوبة .

تمرين 2 (متباينة بسل)

إذا كـان $\{w_1, w_2, \ldots, w_k\}$ مجموعـة جزئيـة عياريـة متعامـدة مـن V فأثبـت أن $\sum_{i=1}^{k} |< w_i \mid v >|^2 \leq \| v \|^2$ لكل $v \in V$.

الحل

ليكن $v \in V$. يمكننا كتابة $v = \sum_{i=1}^{k} < v \mid w_i > w_i + x$ حيث

$$x = v - \sum_{i=1}^{k} < v \mid w_i > w_i$$

حسب القضية 11-52 فإن $< x \mid w_i > = 0 \quad \forall \; i = 1, 2, \dots, n$ بوضع

$$w = \sum_{i=1}^{k} < v \mid w_i > w_i$$

نحصل على $v = w + x$ حيث

$$< w \mid x > = < \sum_{i=1}^{k} < v \mid w_i > w_i \mid x > = \sum_{i=1}^{k} < v \mid w_i > < w_i \mid x > = 0$$

وهكذا فإن

$$\| v \|^2 = < w + x \mid w + x > = < w \mid w > + < x \mid x > = \| w \|^2 + \| x \|^2$$
$$\Rightarrow \| w \|^2 \leq \| v \|^2$$

ولكن

$$\| w \|^2 = < \left(\sum_{i=1}^{k} < v \mid w_i > w_i \right) \mid \left(\sum < v \mid w_i > w_i \right) >$$

$$= \sum_{j=1}^{k} \sum_{i=1}^{k} < v \mid w_i > < \overline{v \mid w_j} > < w_i \mid w_j >$$

$$= \sum_{i=1}^{k} | < v \mid w_i > |^2$$

لأن $(< w_i \mid w_i > = 1$ لكل $i \neq k$ و $0 = < w_i \mid w_j >)$.

$$= \sum_{i=1}^{k} | \overline{< w_i \mid v >} |^2 = \sum_{i=1}^{k} | < w_i \mid v > |^2$$

إذاً

$$\sum_{i=1}^{k} | < w_i \mid v > |^2 \leq \| v \|^2$$

تمرين 3

إذا كان W مجموعة الدوال الحقيقية $y = f(x)$ التي تحقق المعادلة التفاضلية $\frac{d^2 y}{dx^2} + 4y = 0$. برهن أن :

(i) W فضاء جزئي في الفضاء المتجهي V للدوال الحقيقية على $I\!R$.

(ii) بعد W على $I\!R$ يساوي 2 .

وإذا عرفنا $< y \mid z > = \int_0^{\pi} yz\, dz$ لجميع $y, z \in W$ ، أوجد قاعدة عيارية متعامدة للفضاء W .

الحل

(i) ليكن Θ راسماً من $I\!R$ إلى $I\!R$ معرفاً كالآتي $\Theta(x) = 0$ ، لكل $x \in I\!R$ ، من الواضح أن $\Theta \in W$ عليه فإن $W \neq \phi$. لكل $\lambda_1, \lambda_2 \in I\!R$ ، $y_1, y_2 \in W$ فإن

$$\frac{d^2 y_1}{dx^2} + 4y_1 = 0 \quad \text{و} \quad \frac{d^2 y_2}{dx^2} + 4y_2 = 0$$

$$\Rightarrow \frac{d^2}{dx^2}(\lambda_1 y_1 + \lambda_2 y_2) + 4(\lambda_1 y_1 + \lambda_2 y_2)$$
$$= \lambda_1\left(\frac{d^2 y_1}{dx^2} + 4y_1\right) + \lambda_2\left(\frac{d^2 y_2}{dx^2} + 4y_2\right) = 0$$
$$\Rightarrow \lambda_1 y_1 + \lambda_2 y_2 \in W$$

وبالتالي فإن W فضاء جزئي في V .

(ii) حسب نظرية المعادلات التفاضلية كل حل للمعادلة $\frac{d^2 y}{dx^2} + y = 0$ هو بالصورة $c_1 \sin 2x + c_2 \cos 2x$ لبعض $c_1, c_2 \in I\!R$ وعليه فإن $\{\sin 2x, \cos 2x\}$ تولد W ،

إضافة إلى ذلك إذا كان $a \sin 2x + b \cos 2x = 0$ لبعض $a, b \in I\!R$ ، عندئذ

$$\frac{d}{dx}(a \sin 2x + b \cos 2x) = 0 \Rightarrow a \cos 2x - b \sin 2x = 0$$

بما أن $\begin{vmatrix} \sin 2x & \cos 2x \\ \cos 2x & -\sin 2x \end{vmatrix} = -1 \neq 0$

فإن المعادلات الخطية $(\sin 2x)a + (\cos 2x)b = 0$ و $(\cos 2x)a + (-\sin 2x)b = 0$ في a و b لها الحل التافه أي أن $a = b = 0$.

إذاً $a \sin 2x + b \cos 2x = 0 \Rightarrow a = b = 0$

وبالتالي $\{\sin 2x, \cos 2x\}$ هي قاعدة للفضاء W على $I\!R$. وهكذا فإن $\dim W = 2$.

وأخيراً لنأخذ $w_1 = \sin 2x$

$$f_1 = \frac{w_1}{\| w_1 \|} = \frac{\sin 2x}{\sqrt{\int_0^{\pi} \sin^2 2x \, dx}} = \sqrt{\frac{2}{\pi}} \sin 2x$$

ضع

$$\begin{aligned} w2 &= \cos 2x - < \cos 2x \mid f_1 > f_1 \\ &= \cos 2x - \left(\int_0^{\pi} \sqrt{\frac{2}{\pi}} \sin 2x \cos 2x \, dx \right) \sqrt{\frac{2}{\pi}} \sin 2x \\ &= \cos 2x - \frac{2}{\pi} \left(\int_0^{\pi} \sin 2x \cos 2x \, dx \right) \sin 2x \\ &= \cos 2x \end{aligned}$$

عندئذ يكون

$$f_2 = \frac{w_2}{\| w_2 \|} = \frac{\cos x}{\sqrt{\int_0^{\pi} \cos^2 2x \, dx}} = \sqrt{\frac{2}{\pi}} \cos 2x$$

إذاً $\left\{ \sqrt{\frac{2}{\pi}} \cos 2x \text{ و } \sqrt{\frac{2}{\pi}} \sin 2x \right\}$ هي قاعدة عيارية متعامدة للفضاء W على $I\!R$.

تمرين 4

إذا كان x, y متجهين في فضاء إقليدي ، أثبت أنهما متعامدان إذا وفقط إذا كان $\| x + y \|^2 = \| x \|^2 + \| y \|^2$ ثم برهن أن هذه النتيجة ليست بالضرورة صحيحة في الفضاءات الوحدوية .

الحل

$$\begin{aligned} &\| x + y \|^2 = < x + y \mid x + y > = \\ &< x \mid x > + < x \mid y > + < y \mid x > + < y \mid y > = \\ &\qquad \| x \|^2 + 2 < x \mid y > + \| y \|^2 \end{aligned}$$

حيث $< x \mid y > = < \overline{y \mid x} > = < y \mid x >$ لأن $< x \mid y >$ عدد حقيقي .

بما أن x عمود على y إذا وفقط إذا كان $< x \mid y > = 0$ فإن

$$< x \mid y > = 0 \Leftrightarrow 2 < x \mid y > = 0 \Leftrightarrow \| x + y \|^2 = \| x \|^2 + \| y \|^2$$

اعتبر C^2 مع الضرب الداخلي القياسي . ضع $x = (0, i)$ ، $y = (0, 1)$ فإن $< x \mid y > = i \neq 0$ عليه فإن x ليس عمودياً على y .

ولكن
$$\| x + y \|^2 = \| (0, 1 + i) \|^2 = < (0, 1 + i) \mid (0, 1 + i) > = (1 + i)(1 - i) = 2$$

وأن
$$\| x \|^2 = < (0, i) \mid (0, i) > = i(-i) = 1$$

كذلك
$$\| y \|^2 = < (0, 1) \mid (0, 1) > = 1.1 = 1$$

عليه فإن
$$\| x + y \|^2 = \| x \|^2 + \| y \|^2$$

في حين x ليس عمودياً على y .

تمارين

فيما يلي V عبارة عن فضاء ضرب داخلي على F .

1- برهن أنه لكل $u, v \in V$ يكون

$$\| u + v \|^2 + \| u - v \|^2 = 2(\| u \|^2 + \| v \|^2)$$

2- إذا كان V فضاءً وحدوياً برهن أن كل متجهين $x, y \in V$ يكونان متعامدان ، إذا وفقط إذا كان $\| \alpha x + \beta y \|^2 = \| \alpha x \|^2 + \| \beta y \|^2$ لكل $\alpha, \beta \in C$.

3- إذا كان x, y متجهان في فضاء إقليدي بحيث كان $\| x \| = \| y \|$ أثبت أن $x + y$ عمودي على $x - y$.

4- في الفضاء $V = IR^2$ ، أثبت أن متباينة شوارتز تؤدي إلى أن القيمة المطلقة لجيب تمام زاوية لا يتجاوز الواحد .

5- إذا كان W فضاءً جزئياً في V وكان $x \in W$ تحقق

$$< x \mid w > + < w \mid x > \leq < w \mid w >$$

لكل $w \in W$ أثبت أن $< x \mid w > = 0$ لكل $w \in W$.

6- ليكن V الفضاء المتجهي للدوال الحقيقية $y = f(x)$ التي تحقق

$$\frac{d^3 y}{dx^3} - 6 \frac{d^2 y}{dx^2} + 11 \frac{dy}{dx} - 6y = 0$$

أ- برهن أن V فضاء متجهي ثلاثي البعد على IR .

ب- في V عرف $< f, g > = \int_{-\infty}^{0} fg \, dx$.

برهن أن هذا يعرف ضرباً داخلياً على V . ثم أوجد قاعدة عيارية متعامدة للفضاء V على IR .

[الجواب $\left\{ \sqrt{2}e^x, 2(3e^{2x} - 2e^x), (3e^x - 12e^{2x} + 10e^{2x})\sqrt{6} \right\}$ **]** .

7- إذا كان V فضاءً متجهاً ذو بعد منته وكانت $\{w_1, w_2, \ldots, w_n\}$ مجموعة جزئية عيارية متعامدة في V بحيث $\sum_{i=1}^{k} |< w_i \mid v >|^2 = \| v \|^2 \quad \forall \quad v \in V$ ، أثبت أن $\{w_1, w_2, \ldots, w_k\}$ تمثل قاعدة للفضاء V .

8- ليكن W_1 و W_2 فضائين جزئيين من فضاء متجهي V . إذا كان W_1 و W_2 كلاهما فضاء ضرب داخلي ، برهن أن $W_1 + W_2$ هو فضاء ضرب داخلي أيضاً .

[**إرشاد** عرف $< u_1 + +v_1 \mid u_2 + v_2 > = < u_1 \mid u_2 > + < v_1 \mid v_2 >$ لكل $u_1, u_2 \in W_1 \quad ; \quad v_1, v_2 \in W_2$] .

9- إذا كان W_1, W_2 فضاءان جزئيان من V . برهن أن $(W_1 \cap W_2^{\perp}) = W_1^{\perp} + W_2^{\perp}$ و $(W_1 + W_2)^{\perp} = W_1^{\perp} \cap W_2^{\perp}$.

10- إذا كان u, v متجهان في V ، أثبت أن $\| v \| \| u \| = |< v \mid u >|$ إذا وفقط إذا كان u, v مرتبطان خطياً على F .

(هذا يزودنا بشرط ضروري وكافي للمساواة في متباينة ستوارتز) .

12

التحويلات الخطية

Linear Transformations

لدراسة العلاقة بين زمر مختلفة وحلقات مختلفة ، عرضنا في الفصول الأولى مفهومي هومورفزم (تشاكل) زمرة وهومومورفزم (تشاكل) حلقة . بأسلوب مشابه سوف نعرض الآن مفهوم الهومومورفزم (التشاكل) بين الفضاءات المتجهة .

1– تعريف التحويل الخطي

تعريف 12-1

ليكن V_1 و V_2 فضائين متجهين على نفس الحقل F ، يقال لراسم T من V_1 إلى V_2 أنه تحويل خطي أو هومومورفزم فضاء متجهي إذا حقق الخواص الآتية :

1- $T(x + y) = T(x) + T(y)$.

2- $T(\alpha x) = \alpha T(x)$.

لجميع العناصر $\alpha \in F , x, y \in V_1$.

وأحياناً للتأكيد على أن T تحويل خطي من V_1 إلى V_2 مع كون V_1 و V_2 فضائين متجهين على F ، نقول أن T هو F– تحويل خطي إضافة إلى ذلك فإن تعاريف F– أيزمورفزم ، هومومورفزم فوقي (أبيمورفزم) وغيرهما مشابهة لنظائرها في الزمر والحلقات .

مثال 1

لتكن $F[x]$ حلقة جميع كثيرات الحدود على حقل F . يمكننا اعتبار $F[x]$ فضاءً متجهاً على F . لأي :

$f = a_0 + a_1x + \ldots + a_nx^n \in F[x]$ ، نعرف مشتقتها $D(f)$ على النحو الآتي :

$$D(f) = a_1 + 2a_2x + \ldots + na_nx^{n-1}$$

من السهل أن نرى أنه لأي $f, g \in F[x]$ ، $\alpha \in F$ فإن :

$$D(f + g) = D(f) + D(g)$$
$$D(\alpha f) = \alpha D(f)$$

عليه فإن D تحويل خطي من $F[x]$ إلى نفسها . D ليس مونومورفزم لأن $D(2x + 1) = 2 = D(2x)$ ولكن $2x + 1 \neq 2x$.

مثال 2

لأي حقل F اعتبر الراسم $T : F^{(3)} \to F^{(2)}$ المعطى على النحو الآتي :

$$T(\alpha, \beta, \gamma) = (\alpha, \beta) \qquad , \qquad \forall \alpha, \beta, \gamma \in F$$

فإنه لأي $x = (\alpha_1, \beta_1, \gamma_1)\,,\, y = (\alpha_2, \beta_2, \gamma_2) \in F^{(3)}$ ، $\alpha \in F$ يكون :

$$\begin{aligned} T(x + y) &= T(\alpha_1 + \alpha_2, \beta_1 + \beta_2, \gamma_1 + \gamma_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2) \\ &= (\alpha_1, \beta_1) + (\alpha_2, \beta_2) = T(\alpha_1, \beta_1, \gamma_1) + T(\alpha_2, \beta_2, \gamma_2) \end{aligned}$$

و

$$\begin{aligned} T(\alpha x) &= T(\alpha\alpha_1, \alpha\beta_1, \alpha\gamma_1) = (\alpha\alpha_1, \alpha\beta_1) \\ &= \alpha(\alpha_1, \beta_1) = \alpha T(\alpha_1, \beta_1, \gamma_1) = \alpha T(x) \end{aligned}$$

وعليه فإن T تحويل خطي .

مثال 3

ليكن F حقلاً . عرف $T : F^{(2)} \to F^{(3)}$ على النحو الآتي : $T(a, \beta) = (\alpha, \beta, 0)$. من الممكن إثبات أن T تحويل خطي .

اصطلاح سوف نستخدم ت.خ. رمزاً للتحويل الخطي .

ملاحظة 1 سوف نوضح فيما يلي بأمثلة أن الشرطين (1) و (2) من تعريف للتحويل الخطي هما شرطان مستقلان عن بعضهما ، بمعنى أن راسماً ما T من فضاء متجهي U_F إلى فضاء متجهي V_F يمكن أن يحقق الشرط (1) ولا يحقق الشرط (2) أو يحقق الشرط (2) ولا يحقق الشرط (1) .

مثال 4

إذا كان C هو حقل الأعداد المركبة ، فإنه يمكننا اعتباره فضاءً متجهاً على نفسه ، إذا عرفنا $T : C \to C$ على النحو الآتي $T(z) = x$ لأي $z = x + iy$ ، حيث $x, y \in /R$ ، من الواضح أن T يحقق الشرط (1) والآن :

$$T(2 - i) = 2 \ , \ T(5) = 5$$
$$(2 + i)T(2 - i) = (2 + i)\, 2 = 4 + 2i$$

بينما

$$T((2 + i)(2 - i)) = T(4 + 1) = T(5) = 5 \neq (2 + i)T(2 - i)$$

أي أن T لا يحقق الشرط (2) في تعريف 12-1 .

مثال 5

ليكن $T : C \to /R$ ، حيث C هو حقل الأعداد المركبة وهو أيضاً فضاءً متجهي على $/R$ نعرف T على النحو التالي :

$T(z) = \sqrt[3]{x^3 + y^3}, \quad \forall\, z = x + iy \in C$ الجذر التكعيبي الحقيقي للمقدار $x^3 + y^3$ حيث $x, y \in /R$.

عندئذ لأي $\alpha \in R$ فإن $\alpha z = \alpha x + i\alpha y$ يعطينا :

$$T(\alpha z) = \sqrt[3]{\alpha^3 x^3 + \alpha^3 y^3} = \alpha \sqrt[3]{x^3 + y^3} = \alpha T(z)$$

وعليه فإن T يحقق الشرط (2) في تعريف 12-1 ، والآن :

$$T(2 + 3i) = \sqrt[3]{8 + 27} = \sqrt[3]{35}\, , T(3i) = 3\, , T(2) = 2$$

من الواضح أن : $T(2 + 3i) \neq T(2) + T(3i)$

عليه فإن T لا يحقق الشرط (1) .

تعريف 12-2

يقال لفضاء متجهي V_1 أنه أيزومورفيك لفضاء متجهي V_2 ، (كلاهما على نفس الحقل F) ، ويرمز لذلك بالرمز $V_1 \cong V_2$ إذا وجد تحويل خطي أحادي فوقي في V_1 على V_2 .

مثال 6

ليكن V فضاء متجهاً ذو بعد n على الحقل F . ولتكن $\{f_1, f_2, \ldots, f_n\}$ قاعدة للفضاء V ، عرف $T \;:\; V \to F^{(n)}$ كالآتي $T\left(\sum_{i=1}^{n} \alpha_i f_i\right) = (\alpha_1, \alpha_2, \ldots, \alpha_n)$

يترك للقارئ التحقق من أن T أيزومورفزم . أي أن $V \cong F^{(n)}$.

النظرية التالية تمدنا باختبار مناسب تماماً لمعرفة أن الراسم $T \;:\; V_1 \to V_2$ تحويل خطي .

نظرية 12-3

ليكن V_1 و V_2 فضائين متجهين على نفس الحقل F . الراسم $T \;:\; V_1 \to V_2$ هو تحويل خطي (ت.خ) إذا كان وفقط إذا كان :

$$T(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 T(x_1) + \alpha_2 T(x_2)$$

لجميع المتجهات $x_i \in V_i$ ، $\alpha_i \in F$ $(i = 1, 2)$.

البرهان

ليكن $T \;:\; V_1 \to V_2$ تحويلاً خطياً . فمن التعريف يكون :

. $T(\alpha_2 x_2) = \alpha_2 T(x_2)$ و $T(\alpha_1 x_1) = \alpha_1 T(x_1)$

كما أن
$$T(\alpha_1 x_1 + \alpha_2 x_2) = T(\alpha_1 x_1) + T(\alpha_2 x_2)$$
$$= \alpha_1 T(x_1) + \alpha_2 T(x_2)$$

وبالعكس إذا كان $T : V_1 \to V_2$ محققاً لفروض النظرية .

فنعتبر $\alpha \in F \;,\; x, y \in V_1$ وبأخذ $\alpha_1 = 1 = \alpha_2$ ، $x_1 = x, x_2 = y$ ، نجد أن :
$$T(x + y) = T(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 T(x_1) + \alpha_2 T(x_2) = T(x) + T(y)$$

ومرة أخرى بأخذ $\alpha_1 = \alpha \,, \alpha_2 = 0 \,, x_1 = x_2 = x$ نحصل على :
$$T(\alpha x) = T(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 T(x_1) + \alpha_2 T(x_2)$$
$$= \alpha T(x) \qquad (\text{لأن } \alpha_2 T(x_2) = 0)$$

وبالتالي فإن T هو تحويل خطي . □

نظرية 4-12

ليكن $T : V_1 \to V_2$ تحويلاً خطياً . إذا كانت المتجهات $u_1, u_2, \ldots, u_n$ مرتبطة خطيا في V_1 ، فإن $T(u_1), T(u_2) \ldots, T(u_n)$ تكون مرتبطة خطياً في V_2 .

البرهان

بما أن $u_1, u_2, \ldots, u_n$ متجهات مرتبطة خطياً في V_1 فإنه توجد عناصر $\lambda_1, \lambda_2, \ldots, \lambda n$ في الحقل F ، ليس جميعها صفراً تحقق العلاقة :
$$\lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_n u_n = 0$$

ومنها نحصل على :
$$T(0) = 0 = T(\lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_n u_2) = \lambda_1 T(u_1) + \lambda_2 T(u_2 + \ldots + \lambda_u T(u_n)$$

وعليه فإن المتجهات :

$T(u_1) \,, T(u_2) \,, \ldots, T(u_n)$ هي مرتبطة خطيا . □

دعنا نؤكد أن صورة مجموعة متجهات مستقلة خطياً ليست بالضرورة مستقلة خطياً، ونترك للقارئ ضرب مثال يوضح ذلك .

تعريف 5-12 (نواة تحويل خطي)

لأي تحويل خطي $T : V_1 \to V_2$ نواة التحويل T ($\ker T$) يعرف على أنها المجموعة :

$$\text{Ker } T = \{v \in V_1 \mid T(v) = 0\}$$

$\text{Ker } T$ يسمى أيضاً الفضاء الصفري لـ T .

نظرية 6-12

إذا كان $T : V_1 \to V_2$ تحويلا خطياً فإن :

(i) $\ker T$ فضاء جزئي من V_1 .

(ii) لأي فضاء جزئي W في V_1 يكون $T(W)$ فضاء جزئياً من V_2 .

البرهان

(i) بما أن $T(0) = 0$ (برهن ذلك)، $0 \in \ker T$ ، وعليه فإن $\ker T \neq \phi$.

حسب نظرية 6.12 يكون :

$$\begin{aligned} T(\alpha x + \beta y) &= \alpha T(x) + \beta T(y) \\ &= \alpha 0 + \beta 0 = 0 \Rightarrow \alpha x + \beta y \in \ker T \end{aligned}$$

وبالتالي فإن $\ker T$ يكون فضاء جزئياً في الفضاء V (نظرية 6.11) .

(ii) مرة أخرى فإن :

$$\begin{aligned} 0 \in W &\Rightarrow T(0) = 0 \in T(W) \\ &\Rightarrow T(W) \neq \phi \end{aligned}$$

كذلك لكل عنصرين $T(u), T(v) \in T(W)$ حيث $u, v \in W$ ، $\alpha, \beta \in F$ يكون :

$$\alpha T(u) + \beta T(v) = T(\alpha u + \beta v, \in T(u)$$

لأن $\alpha u + \beta v \in W$.

وبالتالي فإن $T(W)$ فضاء جزئي في V_2 . □

ملاحظة 1 من الآن فصاعداً نلفت انتباه القارئ إلى أننا في الغالب نتعامل مع فضاءات متجهة منتهية البعد ، ما لم يذكر خلاف ذلك .

ملاحظة 2 كحالة خاصة للنظرية السابقة ، نجد أن $T(V_1)$ فضاء جزئي من V_2 . عليه فإن $\dim(T(V_1))$ معرف تعريفاً جيداً .

تعريف 12-7

ليكن $T : V_1 \to V_2$ تحويلاً خطياً . فإن مرتبة T $(rank\ T)$ ويرمز لها بالرمز $r(T)$ تعرف بأنها تساوي $\dim(T(V_1))$.

صفرية التحويل T يرمز لها بالرمز $v(T)$ وتعرف بأنها $\dim(\ker T)$.

ملاحظة

$T(V_1)$ يعرف أيضاً بأنه فضاء مرتبة T .

قضية 12-8

لأي تحويل خطي $T : V_1 \to V_2$ ، يكون $r(T) \le \min\{\dim V_1, \dim V_2\}$

البرهان

افرض $\dim V_1 = n$, $\dim V_2 = m$. بما أن $T(V_1)$ فضاء جزئي من V_2 يكون لدينا $\dim T(V_1) \le m$ أي أن $r(T) \le m$.

والآن لأي $n + 1$ من المتجهات $w_1, w_2, \dots, w_{n+1}$ في $T(V_1)$ ولكل $i = 1, 2, \dots, n+1$ ، يمكننا إيجاد $v_i \in V_1$ بحيث يكون $T(v_i) = w_i$. ولما كان بعد V_1

يساوي n فإن المتجهات $v_1, v_2, \ldots, v_{n+1}$ مرتبطة خطياً ، ومن ثم فإن صورها $w_1 = T(v_1), w_2 = T(v_2), \ldots, w_{n+1} = T(v_{n+1})$ مرتبطة خطياً (نظرية 12-4) . وعليه فإن $T(V_1)$ لا يمكن أن يحوي $n+1$ من المتجهات المستقلة خطياً ، أي أن $\dim T(V_1) \leq n$ ، إذن $r(T) \leq n$.

من المناقشات السابقة نستنتج أن $r(T) \leq \min\{m, n\}$. □

نظرية 12-9

(قانون سلفستر للصفرية) . إذا كان $T : V_1 \to V_2$ تحويلاً خطياً فإن :

$$\dim V_1 = r(T)k + v(T)$$

البرهان

افرض أن $v(T) = t, r(T) = s, \dim V_1 = n$ ، فيكون $\dim(\ker T) = t$ بما أن كل مجموعة جزئية مستقلة خطياً من V_1 يمكن توسيعها إلى قاعدة للفضاء V_1 ، فإننا نستطيع إيجاد قاعدة $\{u_1, u_2, \ldots, u_n\}$ للفضاء V_1 بحيث تكون المجموعة $\{u_1, u_2, \ldots, u_t\}$ قاعدة للفضاء $\ker T$ ، وهكذا فإن

$$T(u_i) = 0, \quad \forall\, i = 1, 2, \ldots, t$$

اعتبر أي عنصر $w \in V_1$ ، فيكون $w = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n$ حيث $\alpha_i \in F$ فيكون

$$T(w) = \alpha_1 T(u_1) + \alpha_2 T(u_2) + \ldots + \alpha_2 T(u_n)$$

$$= \sum_{i=t+1}^{n} \alpha_i T(u_i) \qquad (T(u_i) = 0, \qquad \forall\, 1 \leq x \leq t)$$

هذا يبين أن كل عنصر في $T(V_1)$ هو تركيب خطي في $T(u_{t+1}), T(u_{t+2}), \ldots, T(u_n)$ فإذا برهنا أن هذه العناصر هي أيضاً مستقلة خطياً فسوف نحصل على أن $\dim V_1 = n - t$.

دعنا نفترض عكس ذلك أي أنه يوجد $\beta_{t+1}, \beta_{t+2}, \ldots, \beta_n \in F$ ليست جميعها صفراً بحيث يكون

$$\beta_{t+1} T(u_{t+1}) + \beta_{t+2} T(u_{t+2}) + \ldots + \beta_n T(u_n) = 0$$

فيكون

$$T\left(\sum_{i=t+1}^{n}\beta_i u_i\right) = 0 \Rightarrow \sum_{i=t+1}^{n}\beta_i u_i \in \ker T$$

$$\Rightarrow \sum_{i=t+1}^{n}\beta_i u_i = \beta_1 u_1 + \beta_2 u_2 + \ldots + \beta_t u_t \quad (\beta_i \in F \text{ لبعض})$$

$$\Rightarrow \beta_1 u_1 + \beta_2 u_2 + \ldots + \beta_t u_t - \beta_{t+1}u_{t+1} - \beta_{t+2}u_{t+2}\ldots - \beta_n u_n = 0$$

$$\Rightarrow \beta_i = 0 \qquad \forall_i = 1, 2, \ldots, n$$

لأن $u_1, u_2, \ldots, u_n$ مستقلة خطياً وهذا يناقض الفرض . فيكون $\dim(V_1) = n - t$ أي أن $n = t + r(T) = v(T) + r(T)$ أو بمعنى آخر $\dim V_1 = v(T) + r(T)$. □

نظرية 10-12

ليكن $T : V_1 \to V_2$ تحويلاً خطياً . لأي فضاء جزئي H من V_1 فإن $\dim\{T(H)\} \geq \dim H - v(T)$.

البرهان

ليكن T_1 مقصور T على H فيكون T_1 تحويلاً خطياً من H إلى V_2 (برهن ذلك) وعليه يكون :

$$\dim H = r(T_1) + v(T_1) = \dim(T_1(H)) + v(T_1) \qquad (1)$$

والآن :

$$T(H) = T_1(H) \Rightarrow \dim(T(H)) = \dim(T_1(H)) \qquad (2)$$

زد على ذلك ولأن $\ker T_1 = (\ker T) \cap H$ (لماذا ؟) فنحصل على :

$$v(T_1) \leq r(T) \qquad (3)$$

من (1) ، (2) ، (3) نجد أن :

$$\dim[T(H)] = \dim[T_1(H)] = \dim H - v(T_1) \geq \dim H - v(T)$$

هذا يثبت المطلوب . □

تمارين

في التمارين الآتية ، كما في الفصل ، جميع الفضاءات المتجهة U, V, W وغيرها منتهية البعد ومعرفة على نفس الحقل .

-1 برهن أن كلاً من الرواسم الآتية تحويل خطي :

(i) $T : C \to C$ حيث C هو الفضاء المتجهي للأعداد المركبة على R حيث $T(z) = \bar{z}$ لكل $\bar{z}, z \in C$ يرمز إلى مرافق العدد المركب Z .

(ii) ليكن $V = \{(a, b, c) \mid a, b, c \in F\}$ فضاء متجهاً على الحقل F . عرف $T : U \to V$ على النحو الآتي :

$T(a, b, c) = (a, b, c)$ لكل $a, b, c \in F$

(iii) $T : F[x] \to F[x]$ حيث F حقل وأن :

$$T[f(x)] = f(x + 1) - f(x) \qquad \forall\, f(x) \in F[x]$$

-2 برهن أن تحويلاً خطياً $T : U \to V$ يكون أحادياً إذا كان وفقط إذا كان ينقل كل مجموعة جزئية مستقلة خطياً من U إلى مجموعة مستقلة خطياً في V .

-3 لأي تحويل خطي $T : U \to V$ ، أثبت صحة ما يلي :

(i) T تطبيق أحادي إذا كان وفقط إذا كان $v(T) = 0$.

(ii) T تطبيق فوقي إذا وفقط إذا كان $r(T) = \dim V$.

(iii) إذا كان $U = V$ ، فإن T تحويل أحادي إذا وفقط إذا كان T تحويلاً فوقياً .

-4 افرض أن $V_n = \{p(x) \in F[x] \mid \deg p(x) < n\}$. فإذا كان $T : V_n \to V_n$ معرفاً بالصورة $T(p(x)) = p(x + 1)$ برهن أن T أوتومورفزم للفضاء المتجهي V_n .

5- إذا كان U فضاءً جزئياً في فضاء متجهي V ، وعرفنا $T : V \to V / U$ على النحو التالي :

$T(v) = v + U, v \in V$ ، فأثبت أن T تحويل خطي من V على V / U وأن U يمثل نواته .

وإذا كان f تحويلاً خطياً من V على أي فضاء متجهي W ، برهن أن f ينتج أيزومورفزم $\bar{f}$ ، $\bar{f} : V / \ker f \to W$ بحيث يكون $\bar{f}(v + \ker f) = f(v)$ واستنتج أن $V /(\ker f) \cong W$ (تسمى هذه بالنظرية الأساسية لهومومورفزم الفضاءات المتجهة) .

6- ليكن $V_n = \{p(x) \in Q[x] \mid \deg p(x) < n\}$ ،

$$V_{n-1} = \{p(x) \in Q[x] \mid \deg p(x) < n - 1\} \ (n > 1)$$

عرف $T : V_n \to V_{n-1}$ على النحو الآتي $T[p(x)] = \frac{d}{dx} p(x)$

برهن أن T تحويل خطي من V_n على V_{n-1} وأن Q يمثل نواته ، ومن ثم برهن أن $V_n / Q \cong V_{n-1}$.

7- برهن أن $F[x]$ له فضاء جزئين فعليين V (ذو بعد غير منته) بحيث $F[x] \cong V$.

8- ليكن V, U فضاءان جزئيان من فضاء متجهي W . أثبت أن $(U + V) / U \cong V /(V \cap U)$ من ثم استنتج أن :

$$\dim(U + V) = \dim U + \dim V - \dim(U \cap V)$$

(الأيزومورفزم السابق يسمى القانون الثاني للأيزومورفزم) .

9- ليكن V, U فضاءان متجهان لهما نفس البعد n ، بالإضافة إلى أن $\{y_1, y_2, \dots, y_n\}, \{x_1, x_2, \dots, x_n\}$ هما قاعدة لكل من U و V على الترتيب .

برهن أن الراسم $T : U \to V$ بحيث :

$$T\left(\sum \alpha_i x_i\right) = \sum \alpha_i y_i, \quad \forall \sum \alpha_i x_i \in U$$

هو أيزومورفزم ، واستنتج أن أي فضائين متجهين V, U يكون كل منهما أيزومورفيك للآخر إذا وفقط إذا كان لهما نفس البعد .

[**إرشاد** استخدم نظرية 12-9] .

10- اذكر مثالاً لراسم غير خطي $T : U \to V$ ينقل متجهات مرتبطة خطياً في U إلى متجهات مستقلة خطياً في V .

[**إرشاد** Q هو فضاء متجهي على نفسه . عرف $T : Q \to Q$ كالآتي $T(1) = 2$ و $T(x) = x \quad \forall\, x(\neq 1) \in Q$] .

11- إذا كان $V_1, V_2, \ldots, V_n$ فضاءات متجهة على نفس الحقل F وكان $T_i : V_i \to V_{i+1}$ حيث $i = 1, 2, \ldots, n-1$ هي تحويلات خطية بحيث كان :

(i) $\ker T_1 = (0)$.

(ii) $\ker(T_{i+1}) = T_i(V_i)$.

(iii) $T_{n-1}(V_{n-1}) = V_n$

أثبت أن $\sum_{i=1}^{n} (-1)^i (\dim V_i) = 0$

12- إذا كان C فضاء الدوال المتصلة $f : IR \to IR$ ، وعرفنا الراسم $\phi : C \to C$ على النحو :

$$(\phi(f))(x) = \int_0^x f(t)\, dt$$

فأثبت أن ϕ تحويل خطي وأن صورة ϕ $(\mathrm{Im}\,\phi)$ تتألف من كل الدوال التي مشتقاتها متصلة ولها القيمة صفر عند الصفر ، بينما $\ker \phi = \{0\}$.

13- ليكن V الفضاء المتجهي لكثيرات الحدود ذات المعاملات الحقيقية على IR .
عرف $\psi : V \to V$ كالآتي :

$$\psi\left(\sum_{i=0}^{k} a_i x^i\right) = \sum_{i=1}^{k} i a_i x^{i-1}$$

برهن أن ψ تحويل خطي . أثبت كذلك أن $\ker\psi = IR$ و $\operatorname{Im}\psi = V$.

14- ليكن T تحويلاً خطياً من فضاء متجهي V إلى نفسه بحيث أن $\ker T = \operatorname{Im} T$
برهن أن بعد V على F هو عدد زوجي .

2– جبر التحويلات الخطية Algebra of Linear Transformations

ليكن U و V فضاءان متجهان على نفس الحقل F . مجموعة جميع التحويلات الخطية من U إلى V يرمز لها بالرمز $\text{Hom}_f(U,V)$ أو ببساطة $\text{Hom}\,(U,V)$.

تعريف 12-11

لأي $\alpha \in F, T_1, T_2 \in \text{Hom}\,(U,V)$ فإن المجموع $T_1 + T_2$ والضرب في قياسي αT_1 راسمـــان مـــن U إلى V معرفـــان كـــالآتي $(T_1 + T_2)(u) = T_1(u) + T_2(u)$ كـــذلك $(\alpha T_1)\,(u) = \alpha T_1(u)$ لكل $u \in U$.

قضية 12-12

لأي عنصـــرين $T_1, T_2 \in \text{Hom}\,(U,V)$ فـــإن المجمـــوع $T_1 + T_2$ عنصـــر في $\text{Hom}(U,V)$ $(T_1 + T_2 \in \text{Hom}\,(U,V))$.

البرهان

ليكن $x, y \in U$ ، $\alpha, \beta \in F$ بما أن T_1, T_2 تحويلان خطيان ، يكون لدينا :

$$T_1(\alpha x + \beta y) = \alpha T_1(x) + \beta T_1(y)$$
$$T_2(\alpha x + \beta y) = \alpha T_2(x) + \beta T_2(y)$$

وبالتالي فمن تعريف المجموع يكون :

$$\begin{aligned}(T_1 + T_2)\,(\alpha x + \beta y) &= T_1(\alpha x + \beta y) + T_2(\alpha x + \beta y)\\ &= \alpha T_1(x) + \beta T_1(y) + \alpha T_2(x) + \beta T_2(y)\\ &= \alpha\left[(T_1 + T_2)\right](x) + \beta\left[(T_1 + T_2)\,(y)\right] .\ \square\end{aligned}$$

قضية 12-13

إذا كان $\alpha \in F, T \in \text{Hom}\,(U,V)$ ، فإن $\alpha T \in \text{Hom}\,(U,V)$.

البرهان

ليكن $x, y \in U$ و $\beta, \gamma \in F$. فإن $T(\beta x + \gamma y) = \beta T(x) + \gamma T(y)$

هذا يعطينا
$$\begin{aligned}(\alpha T)(\beta x+\gamma y) &= \alpha\left[\beta T(x)\right]+\alpha\left[\gamma T(y)\right]\\ &= (\alpha\beta)T(x)+(\alpha\gamma)T(y)\\ &= (\beta\alpha)T(x)+(\gamma\alpha)T(y)\\ &= \beta\left[(\alpha T)(x)\right]+\gamma\left[(\alpha T)(y)\right]\end{aligned}$$
أي أن αT تحويل خطي وبالتالي فإن $\alpha T \in \text{Hom}(U,V)$. □

قضية 14-12

ليكن U فضاء متجهاً ذو بعد منته و $B=\{x_1,x_2,\dots,x_n\}$ قاعدة له فلأي فضاء متجهي V ، يكون الراسم $f:B\to V$ ممكن التوسيع بطريقة وحيدة إلى تحويل خطي T من U إلى V . إضافة إلى ذلك فإن التحويلان الخطيان T و T' من U إلى V يكونان متساويان إذا وفقط إذا كان $T(x_i)=T'(x_i)$ لكل $1\le i\le n$.

البرهان

بما أن $\{x_1,x_2,\dots,x_n\}$ هي قاعدة للفضاء U ، فإن كل $y\in U$ يمكن التعبير عنه بطريقة واحدة فقط بالصورة $y=\sum_{i=1}^{n}\alpha_i x_i$ حيث $\alpha_i\in F$ ، عرف $T:U\to V$ كالآتي
$$T(y)=\sum_{i=1}^{n}\alpha_i f(x_i),\quad \alpha_i\in F$$
فيكون T تحويلاً خطياً (تحقق من ذلك) .

فإذا ثبتنا أي j من بين $j=1,2,\dots,n$ فإنه بأخذ $\alpha_i=0$ عندما $i\ne j$ و $\alpha_j=1$ نحصل على أن $y=x_i$ ويكون
$$T(y)=\sum_{i=1}^{n}\alpha_i f(x_i)=f(x_j)$$
وعليه فإن T توسيع للراسم f . هذا يثبت الجزء الأول .

ولإثبات الجزء الثاني ، نبين إنه إذا كان الراسمان T',T متفقان على $\{x_1,x_2,\dots,x_n\}$ فإنهما يكونان متساويين ، ولكي نرى ذلك اعتبر $x\in U$ فيكون $x=\sum_{i=1}^{n}\alpha_i x_i$ لبعض $\alpha_i\in F$ ، وبما أن $T(x_i)=T'(x_i)$ لكل i ، فإن :

$$T(x) = \sum_{i=1}^{n} \alpha_i T(x_i) = \sum_{i=1}^{n} \alpha_i T'(x_i) = T'(x)$$

وعليه فإن $T = T'$. □

ملاحظـة إذا كـان V أي فضـاء متجهـي والمجموعـة $\{x_1, x_2, \ldots, x_n\}$ قاعـدة لـه و W أي فضـاء متجهـي آخـر ، فـإن القضـية السـابقة تبـين أنـه إذا أعطينـا أي n مـن المتجهـات $y_1, y_2, \ldots y_n \in W$ (ليسـت بالضـرورة مسـتقلة خطيـاً) ، فإنـه يوجـد تحويـل خطـي $T : V \to W$ بحيث يكون $T(x_i) = y_i$.

نظرية 12-15

إذا كـان U و V فضـاءان متجهـان علـى نفـس الحقـل F ، فـإن $\text{Hom}(U,V)$ يكون فضاءً متجهاً على F .

البرهان

لأي $T_1, T_2 \in \text{Hom}(U,V)$ ، $\alpha \in F$ ، إذا عرفنا :

$$(\alpha T_1)(u) = \alpha T_1(u), (T_1 + T_2)(u) = T_1(u) + T_2(u)$$

لجميع $u \in U$ ، فـإن $T_1 + T_2 \in \text{Hom}(U,V)$ ، $\alpha T_1 \in \text{Hom}(U,V)$ (حسـب القضـيتين 12.12 و 13.12) . ومن ذلك تكون $\text{Hom}(U,V)$ مغلقة تحت عمليتي الجمع والضرب في قياس .

وعلينا أن نتحقق من أن $\text{Hom}(U,V)$ فضاء متجهي . لذا فإننا نفرض :

$$u \in U, \alpha, \beta \in F, T_1, T_2 T_3 \in \text{Hom}(U,V)$$

فيكون :

(1) $(T_1 + T_2)(u) = T_1(u) + T_2(u) = T_2(u) + T_1(u)$.

(لأن الجمع في V إبدالي)

$$\Rightarrow (T_1 + T_2)(u) = (T_2 + T_1)(u), \quad \forall u \in U$$

$$\Rightarrow T_1 + T_2 = T_2 + T_1$$

وعليه فإن عملية الجمع المعرفة إبدالية .

(2) $$[(T_1 + T_2) + T_3](u) = (T_1 + T_2)(u) + T_3(u)$$
$$= [T_1(u) + T_2(u)] + T_3(u)$$
$$= T_1(u) + [T_2(u) + T_3(u)]$$

(لأن عملية الجمع في V تنسيقية و $T_i(u) \in V$) .

$$= [T_1 + (T_2 + T_3)](u)$$

أي أن $(T_1 + T_2) + T_3 = T_1 + (T_2 + T_3)$

(3) عرف $\overline{0} : U \to V$ على النحو الآتي :

$\overline{0}(u) = 0$ (0 المتجه الصفري في V) لكل $u \in U$.

لأي عنصرين $u_1, u_2 \in U$ يكون $\overline{0}(\alpha u_1 + \beta u_2) = 0 = \alpha\,\overline{0}(u_1) + \beta\overline{0}(u_2)$

أي أن $\overline{0} \in \mathrm{Hom}\,(U, V)$

والآن $(T_1 + \overline{0})(u) = T_1(u) + \overline{0}(u) = T_1(u) + 0 = T_1(u)$

هذا يبين أن $T_1 + \overline{0} = T_1$ وبالتالي فإن $\overline{0}$ هو العنصر المحايد الجمعي في $\mathrm{Hom}\,(U, V)$.

(4) عرف $T_1' : U \to V$ بحيث $T_1'(u) = -T_1(u)$ لكل $u \in U$.

لأي $\alpha, \beta \in F, u_1, u_2 \in U$ يكون $T_1'(\alpha u_1 + \beta u_2) = -T_1(\alpha u_1 + \beta u_2)$

$$= -[\alpha T_1(u_1) + \beta T_1(u_2)]$$
$$= \alpha[-T_1(u_1)] + \beta[-T_1(u_2)] = \alpha T_n'(u_1) + \beta T_1'(u_2)$$

وبالتالي فإن T_1' تحويل خطي وعليه $T_1' \in \mathrm{Hom}\,(U, V)$. والآن :

$$(T_1 + T_1')(u) = T_1(u) + T_1'(u) = T_1(u) - T_1(u) = 0 = \overline{0}(u)$$

أي أن $T_1 + T_1' = \overline{0}$ وأن $-T_1 = T_1' \in \mathrm{Hom}\,(U, V)$.

بمعنى أن لكل عنصر في $\mathrm{Hom}\,(U, V)$ نظير جمعي في $\mathrm{Hom}\,(U, V)$ وعلى ذلك $\mathrm{Hom}\,(U, V)$ زمرة أبيلية تحت عملية الجمع .

(5) (i) الآن :

$$[\alpha(T_1 + T_2)](u) = \alpha[T_1 + T_2(u)] = \alpha[T_1(u) + T_2(u)]$$
$$= \alpha T_1(u) + \alpha T_2(u) = (\alpha T_1)(u) + (\alpha T_2)(u)$$
$$= (\alpha T_1 + \alpha T_2)(u)$$

أي أن $\alpha(T_1 + T_2) = \alpha T_1 + \alpha T_2$.

(ii)
$$\begin{aligned}[(\alpha + \beta)T_1](u) &= (\alpha + \beta)T_1(u) = \alpha T_1(u) + \beta T_1(u)\\ &= (\alpha T_1)(u) + (\beta T_1)(u) = (\alpha T_1 + \beta T_1)(u)\end{aligned}$$

وهذا يعني أن $(\alpha + \beta)T_1 = \alpha T_1 + \beta T_1$.

(iii)
$$\begin{aligned}[(\alpha\beta)T_1](u) &= (\alpha\beta)T_1(u) = \alpha[\beta T_1(u)]\\ &= \alpha[(\beta T_1)(u)] = [\alpha(\beta T_1)](u)\end{aligned}$$

والذي يعني أن $(\alpha\beta)T_1 = \alpha(\beta T_1)$.

(iv)
$$(1T_1)(u) = 1T_1(u) = T_1(u)$$

عليه فإن $1T_1 = T_1$.

وهكذا فإن $\mathrm{Hom}\,(U, V)$ فضاء متجهي . □

تعريف 16-12

يقال للحلقة R أنها جبر على حقل F ، إذا كانت الزمرة الجمعية $< R, + >$ للحلقة R هي فضاء متجهي على F ، ولأي $x, y \in R$ ، $\alpha \in F$ يكون :

$$\alpha(xy) = (\alpha x)y = x(\alpha y)$$

نظرية 17-12

لأي فضاء متجهي V_F يكون $\mathrm{Hom}_F(V, V)$ جبراً على F .

البرهان

يأخذ $U = V$ في نظرية 15.12 نستنتج أن $\mathrm{Hom}_F(V, V)$ فضاء متجهي على F . ولأي $T_1, T_2 \in \mathrm{Hom}_F(V, V)$ فإن التركيب $T_1T_2 : V \to V$ معرف كالآتي لكل $\alpha, \beta \in F, v_1, v_2 \in V$.

$$\begin{aligned}T_1T_2(\alpha v_1 + \beta v_2) &= T_1[T_2(\alpha v_1 + \beta v_2)]\\ &= \{\alpha T_1[T_2(v_1)] + \beta T_1[T_2(v_2)]\} \quad (\text{حسب نظرية } 3.1)\\ &= \alpha[T_1T_2(v_1)] + \beta[T_1T_2(v_2)]\end{aligned}$$

أي أن T_1T_2 هو تحويل خطي على V . عليه فإن $T_1T_2 \in \mathrm{Hom}_F(V,V)$.

والآن لكل $T_1, T_2, T_3 \in \mathrm{Hom}_F(V,V)$ ، $v \in V$ ، $\alpha \in F$ يكون :

$$\begin{aligned}[T_1(T_2+T_3)](v) &= T_1[(T_2+T_3)(v)]\\ &= T_1[T_2(v)+T_3(v)]\\ &= T_1T_2(v)+T_1T_3(v)\end{aligned}$$

لذا فإن
$$T_1(T_2+T_3) = T_1T_2 + T_1T_3$$

وبالمثل فإن
$$(T_2+T_3)T_1 = T_2T_1 + T_3T_1$$

وبما أن عملية التركيب هذه تنسيقية بين جميع الرواسم من V إلى V ، هذه الصيغة نفسها تتحقق لجميع عناصر $\mathrm{Hom}_F(V,V)$ وبهذا نصل إلى أن $\mathrm{Hom}_F(V,V)$ حلقة .

وإضافة لذلك فإن :

$$[T_1(\alpha T_2)](v) = T_1[(\alpha T_2)(v)] = T_1[\alpha T_2(v)] = \alpha[T_1\{T_2(V)\}] = [(\alpha T_1)T_2](v)$$

إذاً توصلنا إلى أن
$$T_1(\alpha T_2) = (\alpha T_1)T_2 = \alpha(T_1T_2)$$

واستناداً للتعريف 12-16 يكون $\mathrm{Hom}_F(V,V)$ عبارة عن جبر على F . □

اصطلاح سوف يرمز $\mathrm{Hom}_F(V,V)$ بالرمز $A(V)$ أيضاً .

نظرية 12-18

ليكن V, U فضاءان متجهان على الحقل F لهما البعدان n, m على الترتيب . عندئذ يكون $\mathrm{Hom}\,(V,V)$ فضاءً متجهاً على F ذو بعد mn .

البرهان

لتكن $\{u_1, u_2, \ldots, u_m\}$ و $\{v_1, v_2, \ldots, v_n\}$ قاعدتان للفضائين V, U على الترتيب . بما أن كل راسم من القاعدة $\{u_1, u_2, \ldots, u_m\}$ إلى V يمكن توسيعه إلى تحويل خطي من U إلى V ، فإنه لكل $i = 1,2,\ldots,m$ ، $j = 1,2,\ldots,n$ يمكننا إيجاد تحويل خطي $T_{ji} : U \to V$ بحيث يكون $T_{ji}(u_i) = v_j$ و $T_{ji}(u_k) = 0, \quad \forall\, k \neq i$

إذاً $T_{ij} \in \text{Hom}\,(U,V)$ لكل i, j .

إذا برهنا أن المجموعة $\{T_{ij} \mid i = 1, 2, \dots, m \;,\; j = 1, 2, \dots, n\}$ هي قاعدة للفضاء $\text{Hom}\,(U,V)$ نستنتج من ذلك أن $\dim[\text{Hom}\,(U,V)] = mn$ وهذا يكمل البرهان .

اعتبر أن $T \in \text{Hom}\,(U,V)$. بما أن لكل $T(u_i) \in V, u_i \in U$ و $\{v_1, v_2, \dots, v_n\}$ هي قاعدة للفضاء V فإن :

$$T(u_i) = \sum_{i=1}^{n} \alpha_{ji} V_j \quad (\alpha_{ji} \in F \text{ لبعض}) .$$

والآن $T_{ji}(u_i) = v_j$ و $T_{jk}(u_i) = 0$ لكل $k \neq i$ يعطينا :

$$T(u_i) = \sum_{j=1}^{n} \alpha_{ji} T_{ji}(u_i) = \sum_{j=1}^{n} \left(\sum_{k=1}^{m} \alpha_{jk} T_{jk} \right)(u_i)$$

وهذا يبين أن $T = \sum \alpha_{jk} T_{jk}$.

وبذلك أثبتنا أن كل $T \in \text{Hom}\,(U,V)$ هو تركيب خطي من T_{jk} .

والآن افرض أن لبعض $\beta_{jk} \in F$ كان $\sum_{j=1}^{n} \sum_{k=1}^{m} \beta_{jk} T_{jk} = 0$.

هذا يؤدي إلى أن :

$$\left[\sum_{j=1}^{n} \left(\sum_{k=1}^{m} \beta_{jk} T_{jk} \right) \right](u_i) = 0, \qquad \forall_i = 1, 2, \dots, m$$

$$\Rightarrow \sum_{j=1}^{n} \beta_{jk} \left[\sum_{k=1}^{n} T_{jk}(u_i) \right] = 0, \qquad \forall\, i = 1, 2, \dots, m$$

$$\Rightarrow \sum_{j=1}^{n} \beta_{ji} v_j = 0 \quad \forall\, i = 1, 2, \dots, m$$

$$\Rightarrow \beta_{ji} = 0 \quad \forall\, i = 1, 2, \dots, m,\; j = 1, 2, \dots, n$$

لأن $v_1, v_2, \dots, v_n$ مستقلة خطياً على F عليه فإن العناصر T_{jk} هذه مستقلة خطياً أيضاً ، وبالتالي فإن $\{T_{jk} \mid j = 1, 2, \dots, n, k = 1, 2, \dots, m\}$

هي قاعدة للفضاء $\text{Hom}\,(V,V)$ ، وبذلك نكون قد حصلنا على النتيجة . □

نتيجة 12-19

لأي فضاء متجهي V_F ذو بعد يساوي n ، فإن $A(V)$ جبر على F ذو بعد يساوي n^2 . □

نظرية 12-20

إذا كان $T_1, T_2 \in \text{Hom}\,(U,V)$ ، فإن :

$$r(\alpha T_1) = r(T_1), \quad \forall \alpha (\neq 0) \in F \qquad \text{(i)}$$

$$|\ r(T_1) - r(T_2)\ | \leq r(T_1 + T_2) \leq r(T_1) + r(T_2) \qquad \text{(ii)}$$

البرهان

بما أن $T_1(U)$ فضاء جزئي في V فإن $(\alpha T_1)\,(U) = \alpha T_1(U) \subseteq T_1(U)$

ولنفس السبب فإن $\alpha^{-1} T_1(U) \subseteq T_1(U)$. لذا فإن $\alpha\left[\alpha^{-1} T_1(U)\right] \subseteq \alpha T_1(V)$

أي أن $T_1(U) \subseteq \alpha T_1(U)$. بالتالي فإن $T_1(U) = \alpha T_1(U)$ وهذا يؤدي إلى أن :

$$\dim(U) = \dim\left[(\alpha T_1)\,(U)\right]$$

فيكون $r(T_1) = r(\alpha T_1)$ (تعريف 12-7) .

(ii) لأي $u \in U$ فإن $(T_1 + T_2)\,(u) = T_1(u) + T_2(u)$.

لذا فإن

$$(T_1 + T_2)\,(U) \subseteq T_1(U) + T_2(U)$$

$$\Rightarrow \dim\left[(T_1 + T_2)U\right] \leq \dim\left[T_1(U) + T_2(U)\right] \leq \dim\left[T_1(U)\right] + \dim\left[T_2(U)\right]$$

$$\Rightarrow r(T_1 + T_2) \leq r(T_1) + r(T_2) \qquad (1)$$

وحيث أن $T_1 = (T_1 + T_2) + (-T_2)$ واستناداً للخطوات السابقة يكون :

$$r(T_1) = r\left[(T_1 + T_2) + (-T_1)\right] \leq r(T_1 + T_2) + r(-T_2)$$

بأخذ $\alpha = -1$ من الفقرة (i) نحصل على أن $r(-T_2) = r(T_2)$ ، وعليه فإن :

$$r(T_1) - r(T_2) \leq r(T_1 + T_2) \qquad (2)$$

وبالمثل فإن :

$$r(T_2) - r(T_1) \le r(T_2 + T_1) \qquad (3)$$

من (1) و (2) نستنتج أن $| \, r(T_1) - r(T_2) \, | \le r(T_1 + T_2) \le r(T_1) + r(T_2)$

وهذا يكمل البرهان . □

والأمثلة التالية تبين أن المتباينات الحادة يمكن أن يتحقق في الفرع (ii) من النظرية السابقة .

مثال 6

اعتبر $/R^2 = \{(x, y) : x, y \in /R\}$. لتكن $\{e_1, e_2\}$ قاعدة للفضاء $/R^2$. عرف التحويلات الخطية T_1, T_2 على $/R^2$ كالآتي :

لأي تركيب خطي $\alpha_1 e_1 + \alpha_2 e_2$ حيث $\alpha_1, \alpha_2 \in /R$:

$$T_1(\alpha_1 e_1 + \alpha_2 e_2) = (\alpha_1 + 2\alpha_2)\, e_1 + (3\alpha_1 + 4\alpha_2)\, e_2$$
$$T_2(\alpha_1 e_1 + \alpha_2 e_2) = (\alpha_1 - 2\alpha_2)\, e_1 - (3\alpha_1 + 4\alpha_2)\, e_2$$

فيكون $T_1(e_2) = e_1 + 4e_2$ و $T_1(e_1) = e_1 + 3e_2$.

بإمكاننا أن نرى بسهولة أن $T_1(e_1)$ ، $T_1(e_2)$ مستقلان خطياً ، وهذا يؤدي إلى أن $r(T_1) = 2$. وكذلك $r(T_2) = 2$. أي أن :

$$r(T_1) - r(T_2) = 0 \qquad (1)$$

والآن $(T_1 + T_2)(\alpha e_1 + \alpha e_2) = 2\alpha_1 e_1$ يعطينا $(T_1 + T_2)(/R^2) = < e_1 >$

وهذا هو الفضاء الجزئي ذو البعد 1 المولد بالعنصر e_1 في الفضاء $/R^2$ ، وعلى ذلك فإن :

$$r(T_1 + T_2) = 1 \qquad (2)$$

كما أن :

$$r(T_1) + r(T_2) = 2 + 2 = 4 \qquad (3)$$

من (1) ، (2) و (3) نستنتج مباشرة أن :

$$| r(T_1) - r(T_2) < r(T_1 + T_2) < r(T_1) + r(T_2)$$

نترك للقراء إثبات أنه إذا كان T_1 و T_2 تحويلان خطيان غير صفريان ، فلن يتحقق أبداً أن يكون

$$| r(T_1) - r(T_2) | = r(T_1 + T_2) = r(T_1) + r(T_2)$$

نظرية 12-21

إذا كان $T_1 \in \text{Hom}(V, U)$ ، $T_2 \in \text{Hom}(W, V)$ حيث U, V, W فضاءات متجهة على نفس الحقل F ، فإن :

$$r(T_1) + r(T_2) - n \leq r(T_1T_2) \leq \min\{r(T_1), r(T_2)\}$$

حيث $n = \dim V$.

البرهان

لاحظ أن $T_1T_2 : W \to U$ تحويل خطي (لماذا ؟)

$$\begin{aligned} r(T_1T_2) &= \dim[(T_1T_2)(W)] \\ &= \dim[(T_1)\{T_2(W)\}] \end{aligned}$$

$\leq \min[\dim T_2(W), \dim V]$ (قضية 8.12)

$$\leq \dim T_2(W) = r(T_2) \qquad (1)$$

كذلك $T_1T_2(W) \subseteq T_1(V)$ عليه فإن $\dim[T_1T_2(W)] \leq \dim T_1(V)$

أي أن :

$$r(T_1T_2) \leq r(T_1) \qquad (2)$$

من (1) و (2) نستنتج أن :

$$r(T_1T_2) \leq \min\{r(T_1), r(T_2)\} \qquad (3)$$

بما أن $n = \dim V$ فإن $n = r(T_1) + r(T_1)$ أي أن :

$$v(T_1) = n - r(T_1) \qquad (4)$$

ليكن T_1' مقصور T_1 على $T_2(W)$ فإن $\ker T_1' = (\ker T_1) \cap T_2(W)$ يعطينا :

$$v(T_1') \le v(T_1) \qquad (5)$$

في (4) و (5) نحصل على أن :

$$v(T_1') \le n - r(T_1) \qquad (6)$$

الآن $T_1'[T_2(W)] = T_1[T_2(W)] = T_1T_2(W)$ يعطينا $r(T_1') = r(T_1T_2)$.

بما أن $\dim[T_2(W)] = r(T_1') + v(T_1') = r(T_1T_2) + v(T_1')$ نجد أن :

(حسب 6) $r(T_2) \le r(T_1T_2) + v(T_1') \le r(T_1T_2) + n - r(T_1)$

أي أن :

$$r(T_1) + r(T_2) - n \le r(T_1T_2) \qquad (7)$$

إذاً (3) و (7) تعطيانا :

$$r(T_1) + r(T_2) - n \le r(T_1T_2) \le \min[r(T_1), r(T_2)]. \ \square$$

نتيجة 12-22

إذا كان أحد التحويلين T_2, T_1 أيزومورفزم ، فإن :

$$r(T_1T_2) = \min\{r(T_1), r(T_2)\}$$

البرهان

لكي نكون محددين دعنا نفرض أن التحويل T_1 هو أيزومورفزم ، عندئذ يكون $T_2 = T_1^{-1}(T_1T_2)$ وهذا يعطينا $r(T_2) \le \min[r(T_1T_2), r(T_1^{-1})] \le r(T_1T_2)$ ولكن كما أن $r(T_1T_2) \le r(T_2)$ فإن $r(T_1T_2) = r(T_2)$ ، وبالمثل إذا كان T_2 أيزومورفزم فإن $r(T_1T_2) = r(T_1)$ إذاً النتيجة محققة . $\square$

مثال 7

ليكن V فضاء متجهي على حقل F ذو بعد 5 ، ولتكن المجموعة $\{e_1, e_2, e_3, e_4, e_5\}$ قاعدة للفضاء V_F . عرف $T_1 : V \to V$ ، $T_2 : V \to V$ كالآتي :

لأي $x = \sum_{i=1}^{5} \alpha_i e_i \in V$ فإن $T_1(x) = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3$

و $T_2(x_1 = \alpha_2 e_2 + \alpha_3 e_3 + \alpha_4 e_4$

على الفور نجد أن الفضاء $T_1(V)$ له القاعدة $\{e_1, e_2, e_3\}$ وأن الفضاء $T_2(V)$ له القاعدة $\{e_2, e_3, e_4\}$ ، عليه فإن :

$$r(T_1) = r(T_2) = 3 \qquad (1)$$

والآن $(T_1T_2)(x) = \alpha_2 e_2 + \alpha_3 e_3$

هذا يعطي أن الفضاء $T_1T_2(V)$ له القاعدة $\{e_1, e_3\}$. لذا فإن :

$$r(T_1T_2) \qquad (2)$$

من (1) و (2) على الفور نستنتج أن :

$$r(T_1) + r(T_2) - 5 < r(T_1T_2) < \min\{r(T_1), r(T_2)\}$$

تمارين محلولة

تمرين 1

ليكن V فضاءً متجهاً على حقل F و $W_1, W_2, \ldots, W_n$ فضاءات جزئية في الفضاء V بحيث كان $V = W_1 \oplus W_2 \oplus \ldots \oplus W_n$. لكل $i \in \{1, 2, \ldots, n\}$ عرف $E_i : V \to W_i$ كالآتي :

لأي : $v = \sum_{i=1}^{n} v_i, v_i \in W_i$ ، $E_i(v) = v_i$ بين أنه لكل $i, j \in \{1, 2, \ldots, n\}$ فإن :

(i) E_i تحويل خطي .

(ii) $E_i(x) = x, \quad \forall x \in W_i$.

(iii) $E_jE_i = E_iE_j = 0$ عندما $i \neq j$ و $E_i^2 = E_i$.

(iv) $\sum_{i=1}^{n} E_i = I$ حيث I هو التحويل المحايد على V .

الحل

(i) نبـــين أولاً أن E_i معـــرف تعريفـــاً جيـــداً لكـــل $i \in \{1, 2, \ldots, n\}$. لـــيكن $v = \sum_{i=1}^{n} v_i = \sum_{i=1}^{n} v_i'$ مع كون $v_i, v_i' \in W_i$ ، بما أن V مجموع مباشر للفضاءات $W_1, W_2, \ldots, W_n$ فإننـا نحصـل علـى أن $\forall i = 1, 2, \ldots, n \qquad v_i = v_i',$. إذن $E_i(v) = v_i = v_i'$ هـذا يبرهن أن E_i معرف تعريفاً جيداً . إضافة إلى ذلك افرض $u, v \in V, \alpha, \beta \in F$ فيكون :

$$u = \sum_{i=1}^{n} u_i, v = \sum_{i=1}^{n} v_i \ (1 \le i \le n \text{ ، } u_i, v_i \in V \text{ لبعض})$$

$$\Rightarrow (\alpha u + \beta v) = \sum_{i=1}^{n} (\alpha u_i + \beta v_i)$$

$$\Rightarrow E_i(\alpha u + \beta v) = \alpha u_i + \beta v_i = \alpha E_i(u) + \beta E_i(v)$$

وهذا يبين أن E_i تحويل خطي من V إلى W_i .

(ii) ليكن $x \in W_i$ ، فيكون $x \in V$ وعليه فإن :

$$. \ x = \sum_{i=1}^{n} u_i \ (u_i \in W_i \text{ لبعض})$$

ولمـا كـان V مجمـوع مباشـر للفضـاءات الجزئيـة W_i فإننـا نحصـل علـى أن $u_j = 0, \forall j \ne i$ وأن $u_i = x$. إذاً $E_i(x) = u_i = x$.

(iii) افـــرض أن $i \ne j$ ، لكـــل $v \in V$ ، $E_i(v) = v_i$ ، حيـــث $v = \sum_{i=1}^{n} v_i$ ، $v_i \in W_i$.

الآن :

$$(E_j E_i)(v) = E_j(E_i(v)) = E_j(v_i) = 0 \qquad (i \ne j \text{ لأن})$$

بالمثـل يمكـن بيـان أن $(E_i E_j)(v) = 0$ لكـل $v \in V$ فيكـون $E_i E_j = E_j E_i = 0$ زد علـى ذلك أنه لأي $v \in V$ فإن $E_i^2(v) = E_i(E_i(v)) = E_i(v)$ حيث $v_i \in W_i, v = \sum_{i=1}^{n} v_i$.

باستخدام (ii) أعلاه نحصل على أن $E_i^2(v) = v_i = E_i(v)$. لذا فإن $E_i^2 = E_i$.

(iv) ليكن $v \in V$ فإن $V = \sum_{i=1}^{n} v_i$ حيث $v_i \in W_i$.

$$\Rightarrow \left(\sum_{i=1}^{n} E_i\right)(v) = \sum_{i=1}^{n} E_i(v) = \sum_{i=1}^{n} v_i = v$$

$$\Rightarrow \sum_{i=1}^{n} E_i = I$$

تمرين 2

تعريف 1 يقال لتحويل خطي $T : V \to V$ أنه إسقاط إذا كان $T^2 = T$.

تعريف 2 يقال لمجموعة من الإسقاطات على V أنها متعامدة إذا كان ضرب أي إسقاطين مختلفين فيها مساوياً للصفر .

تعريف 3 يقال لمجموعة من الإسقاطات المتعامدة $E_1, E_2, \ldots, E_n$ على V أنها متكاملة إذا كان $\sum_{i=1}^{n} E_n = I$ حيث I هو التحويل المحايد (الذاتي) على V .

أثبت أنه يوجد تناظر أحادي بين التحليلات المباشرة لفضاء متجهي ومجاميع منتهية من الإسقاطات المتعامدة المتكاملة على ذلك الفضاء المتجهي .

الحل

لكل تحليل مباشر معطى $V = W_1 \oplus W_2 \oplus \ldots \oplus W_4$ ، نحصل على المجموعة $\{E_1, E_2, \ldots, E_n\}$ لإسقاطات متعامدة متكاملة كما برهنا في تمرين 1 .

لتكن $\{E_1, E_2, \ldots, E_n\}$ مجموعة منتهية في الإسقاطات المتعامدة المتكاملة على V .

نفرض أن $v \in V$ فبما أن $\sum_{i=1}^{n} E_i = I$ ، حيث I هو التحويل المحايد على V

فإننا نحصل على $$v = Iv = \left(\sum_{i=1}^{n} E_i\right) v = \sum_{i=1}^{n} E_i(v)$$

عليه فإن $\sum_{i=1}^{n} E_i(V)$ $V \subseteq$ إذن $V = \sum_{i=1}^{n} E_i(V)$.

ضع $W_i = E_i(v)$ لكل $i \in \{1, 2, \dots, n\}$. عندئذ يكون كل W_i فضاء جزئي من V بحيث يكون $V = \sum_{i=1}^{n} W_i$.

والآن ليكن $w_i \in W_i \cap \left(\sum_{j \neq i} W_j\right)$ فإن $w_i = \sum_{j \neq i} w_j$.

حيث $w_k \in W_k$ لكل $k \in \{1, 2, \dots, n\}$. عندئذ يكون $E_i(w_i) = \sum_{i \neq j} E_i(w_i)$ ولكن (لعنصر ما $x \in V$) $w_j \in W_j \Rightarrow w_j = E_j(x)$.

بما أن $E_iE_j = 0$ لكل $i \neq j$ لذلك يكون $E_i(w_i) = \sum_{j \neq i} E_iE_j(x)$.

الآن $w_i \in W_i$ يؤدي إلى أن $w_i \in E_i(y)$ لعنصر ما $y \in V$ هذا يؤدي إلى أن :

$$E_i(w_i) = E_i^2(y) \Rightarrow E_i^2(y) = 0 \Rightarrow E_i(y) = 0 \qquad (E_i^2 = E_i \text{ لأن})$$

هذا بدوره يؤدي إلى أن $w_i = 0$ ، عليه فإن المجموع $\sum_{i=1}^{n} W_i$ مباشر . وبذلك حصلنا على تحليل مباشر للفضاء V .

ليكن P_i هو الإسقاط المرافق للتحليل $W = W_1 \oplus W_2 \oplus \dots \oplus W_n$. عندئذ يكون لكل $v \in V$ ، $v = \sum_{i=1}^{n} v_i$ حيث $v_i \in W$ $(1 \leq i \leq n)$ ، عليه فإن $P_i(v) = v_i$.

والآن $v_i \in W_i \Rightarrow v_i \in E_i(z)$

لبعض $z \in V$ هذا يؤدي إلى أن $E(v_i) = E_i^2(z) = E_i(z) = v_i$

إذاً $p_i(v) = E_i(v)$ لكل $v \in V$ بناء عليه يكون $\forall_i (1 \leq i \leq n)$ $p_i = E_i,$ وبذلك نحصل على المطلوب .

تمرين 3

برهن أنه إذا كان E_1, E_2 إسقاطان بحيث $E_1E_2 = E_2E_1$ ، فإن E_1E_2 و $E_1 + E_2 - E_1E_2$ تكون إسقاطات .

الحل

$$(E_1E_2)^2 = E_1E_2E_1E_2 = E_1E_1E_2E_2 \quad (\text{لأن } E_1E_2 = E_2E_1)$$

$$\Rightarrow E_1^2E_2^2 = E_1E_2$$

وبالتالي فإن التحويل E_1E_2 هو إسقاط .

إضافة إلى ذلك لاحظ أن $(E_1 + E_2)E_1E_2 = E_1^2E_2 + E_2E_1E_1 = 2E_1E_2$

و $E_1E_2(E_1 + E_2) = E_1E_2E_1 + E_1E_2^2 = 2E_1E_2$

أي أن :

$$\begin{aligned}(E_1 + E_2 - E_1E_2)^2 &= (E_1 + E_2)^2 - 2(E_1 + E_2)E_1E_2 + (E_1E_2)^2 \\ &= E_1^2 + E_2^2 + 2E_1E_2 - 4E_1E_2 + E_1E_2 \\ &= E_1 + E_2 - E_1E_2\end{aligned}$$

إذاً $E_1 + E_2 - E_1E_2$ هو إسقاط .

تمارين

في التمارين الآتية جميع الفضاءات المتجهة ذوات أبعاد منتهية إلا إذا ذكر غير ذلك
.

1- لتكن $\{e_1, e_2, \dots, e_n\}$ قاعدة للفضاء V_F و $\lambda_1, \lambda_2, \dots, \lambda_n \in F$ قياسيات مختلفة . إذا كان $T, U \in \text{Hom}\,(V, V)$ بحيث كان $T(e_i) = \lambda_i e_i$ و $TU = UT$ برهن أن $U(e_i) = \mu_i e_i$ لبعض القياسيات $\mu_1, \mu_2, \dots \mu_n$ ، ما الذي يمكن قوله حول U إذا لم تكن λ_i جميعها مختلفة ؟

2- إذا كان U, T تحويلان خطيان في $A(V)$ بحيث كان $UT - TU$ متبادل مع U ، فبرهن أن لكل عدد صحيح موجب k يكون :

$$U^k T - TU^k = kU^{k-1}(UT - TU)$$

3- برهن أن كل جبر على F له محايد يمكن أن يغمر في $A(V)$ لفضاء متجهي V_F . عمم هذه النتيجة إذا كان الجبر بدون محايد .

4- إذا كان $\dim V > 1$ ، برهن أن $A(V)$ غير إبدالية .

5- إذا كان $T(\neq 0) \in A(V)$ ، فبرهن أنه يوجد $S \in A(V)$ بحيث يكون $E = TS \neq 0$ عنصر ذو قوة مماثلة .

6- ليكن $T \in A(V)$ و $V_0 = \{v \in V \mid \exists k \in Z^+, T^k(v) = 0\}$

برهن أن V_0 فضاء جزئي من V وإذا كان $T^m(v) \in V_0$ لكل عدد صحيح موجب m ، فإن $v \in V_0$.

7- إذا كان $T \in A(V)$ بحيث T ينقل كل فضاء جزئي ذو بعد واحد إلى نفسه ، برهن أن $T = \lambda I$ لقياسي $\lambda \in F$ حيث I التحويل المحايد .

[**إرشـــــاد** افـــرض أن $\{e_1, e_2, \dots, e_n\}$ قاعـــدة للفضـــاء V ، فيكـــون $T(e_i) = \lambda_i e_i, \quad \forall\, i = 1, 2, \dots, n$ ومرة أخرى :

$$T < e_1 + e_2 + \dots + e_n > \subseteq < e_1 + e_2 + ..e_n >$$
$$\Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_n]$$

8- اذكر تحويلين خطيين U, T على IR^2 يحققان $UT \neq 0, TU = 0$.

9- اذكر مثالاً لتحويل خطي T على IR^2 بحيث $T^2 = 0$ في حين $T \neq 0$.

10-ليكن W, V فضاءان متجهان على نفس الحقل F وليكن T أيزومورفزم من V على W . بـــرهن أن الراســـم $f : A(V) \to A(W)$ المعـــرف علـــى النحـــو الآتي $f(U) = TUT^{-1}, \quad \forall\, U \in A(V)$ هو أيزومورفزم .

11-إذا كان $T \in A(V)$ ، برهن أن مجموعة جميع التحويلات الخطية U على V التي تحقق $TU = 0$ هي فضاء جزئي من $A(V)$.

12-إذا كـان $T \in A(V)$ يحقق $T^2 - T + I = 0$ حيث I هـو التحويل المحايد على V ، برهن أن T له معكوس .

13-إذا كـان F حقلاً مميز لا يساوي 2 ، برهن أنه إذا كـان E_2, E_1 إسقاطين على فضاء متجهي V على F بحيث كان $E1 + E_2$ إسقاطاً فإن E_2, E_1 يكونان متعامدان .

14- *بـرهن أنـه إذا كـان $E_1, E_2, \dots, E_r$ إسـقاطات علـى فضـاء متجهـي V ، بحيـث كـان $E_1(V) = E_2(V) = \dots = E_r(V)$ و $\alpha_1, \alpha_2, \dots, \alpha_r \in F$ ، $\sum_{i=1}^{r} \alpha_i = 1$ فـإن $\sum_{i=1}^{r} \alpha_i E_i$ هو إسقاط بنفس فضاء رتبة الإسقاط E_i .

15- **لتكن α, β, γ تحويلات خطية من فضاء متجهي V إلى نفسه برهن أن : (متباينة فروبينيس) $r(\alpha\beta) + r(\beta\gamma) \leq r(\beta) + r(\alpha\beta\gamma)$.

16-إذا كان T تحويلاً خطياً من R^3 إلى R^2 وكان U تحويلاً خطياً من R^2 إلى R^3 فبرهن أن التحويل UT ليس له معكوس .

17-إذا كان T تحويلاً خطيا من V إلى V بحيث كان $r(T) = r(T^2)$ ، فأثبت أن $T(V) \cap \ker T = \{0\}$.

3- الفضاءات الثنائية Dual Spaces

تعريف 12-23

إذا كان V فضاءً متجهاً على حقل F فأي تحويل خطي من V إلى F يسمى دالي خطي على V .

تعريف 12-24

الفضاء المتجهي $\text{Hom}_F(V, F)$ المؤلف من جميع الداليات الخطية على V يسمى ثنائي الفضاء V ويرمز له V^* . ويسمى أحياناً الفضاء المرافق .

بما أن بعد F على اعتباره فضاء متجهي على نفسه هو واحد ، فإن نظرية 12-18 تبين أنه لأي فضاء متجهي V_F (ذو بعد منته) يكون :

$$\dim[\text{Hom}_F(V, F)] = \dim V \,.\, \dim F = \dim V$$

أي أن $\dim V^* = \dim V$. سوف نعود ونبرهن هذه العلاقة عند إثباتنا لعلاقة مهمة بين فضاء متجهي وثنائيته .

نظرية 12-25

إذا كان V فضاء متجهي ذو بعد n على حقل F والمجموعة $\{e_1, e_2, \dots, e_n\}$ قاعدة له ، فإن $\{e_1^*, e_2^*, \dots, e_n^*\}$ قاعدة للفضاء V^* حيث $e_i^*(e_j) = 0$ عندما $i \neq j$ و $e_i^*(e_i) = 1$ ، وكذلك $\dim V = \dim V^*$.

البرهان

بما أن كل راسم من $\{e_1, e_2, \dots, e_n\}$ إلى F يمكن توسيعه إلى تحويل خطي على V (قضية 12-14) ، فإن لكل $i = 1, 2, \dots, n$ بإمكاننا تعريف دالي خطي e^* على V بالصورة:

$$e_i^*(e_j) = \begin{cases} 0 & \forall\ j \neq i \\ 1 & i = j \end{cases} \qquad (1)$$

والآن نبرهن أن $B = \{e_1^*, e_2^*, \ldots, e_n^*\}$ قاعدة للفضاء V^* .

ليكن $f \in V^*$. لكل $1 \le i \le n$ افرض $f(e_i) = \alpha_i \in F$. اعتبر :

$$g = \alpha_1 e_1^* + \alpha_2 e_2^* + \ldots + \alpha_n e_n^*$$

لكل $1 \le i \le n$ يكون $g(e_i) = (\alpha_1 e_1^* + \alpha_2 e_2^* + \ldots + \alpha_n e_n^*)(e_i)$

$= \alpha_i e_i^*(e_i) = \alpha_i = f(e_i)$ (لأنه حسب (1) فإن $e_j^*(e_i) = 0$ عندما $j \neq i$) وهكذا فإن f و g ينطبقان على القاعدة $\{e_1, e_2, \ldots, e_n\}$ للفضاء V . وعليه $f = g$ حسب القضية 12-14 ، وهذا يبين أن B يولد V^* . افرض أنه لبعض $\beta_i \in F$ ، $1 \le i \le n$ كان $\sum_{i=1}^{n} \beta_i e_i^* = 0$ فيكون

$$\sum_{i=1}^{n} (\beta_i e_i^*)(e_j) = 0 \Rightarrow \beta_j = 0, \quad \forall\ j = 1, 2, \ldots n$$

لذلك فإن B تكون مستقلة خطياً أيضاً . بالتالي فإن B قاعدة للفضاء V^* . وبما أن B تضم n من العناصر فإن $\dim V^* = \dim V$. وهذا يكمل البرهان . □

تعريف 12-26

ليكن V_F فضاءً متجهي ذو بعد منته وأن $(e_1, e_2, \ldots, e_n)$ قاعدة مرتبة له . فإن القاعدة المرتبة $(e_1^*, e_2^*, \ldots, e_n^*)$ للفضاء V^* بحيث يكون $e_i^*(e_j) = 0$ عندما $i \neq j$ و $e_i^*(e_i) = 1$ يسمى ثنائية القاعدة $V_j(e_1, e_2, \ldots, e_n)$ (أو ببساطة قاعدة ثنائية للفضاء V^*) .

تعريف 12-27

لكل فضاء متجهي V_F ، الثنائي V^{**} للفضاء V^* يسمى الثنائي الثاني للفضاء V .

قضية 12-28

إذا كان V فضاء متجهاً (منتهي البعد) على حقل F ، فإن لكل $v(\neq 0)$ في V يوجد $g \in V^*$ بحيث يكون $g(v) \neq 0$.

البرهان

بما أن $v \neq 0$ فإن $\{v\}$ هي مجموعة جزئية مستقلة خطياً من V ، عليه يمكن توسيعها إلى قاعدة مرتبة للفضاء V ولتكن $(v = v_1, v_2, \dots, v_n)$. لتكن $(v_1^*, v_2^*, \dots, v_n^*)$ هي قاعدة للفضاء V^* الثنائية للقاعدة $(v_1, v_2, \dots, v_n)$ ، فمن التعريف يكون $v_1^*(v_1) = 1 \neq 0$ وبأخذ $g = v_1^*$ نجد أن $g(v) \neq 0$. وهذا يكمل البرهان . □

نظرية 12-29 (قاعدة الثنوية)

إذا كان V_F فضاءً متجهاً ذو بعد منته ، فإنه يوجد أيزومورفزم قانوني من V على V^{**} .

البرهان

عرف $\sigma : V \to V^{**}$ كالآتي :

لأي $v \in V$ ، أولاً عرف $\eta_v : V^* \to F$ كالآتي :

$\eta_v(f) = f(v), \quad \forall f \in V^*$. بما أن لكل $f, g \in V^*$ ، $\alpha, \beta \in F$

$$\begin{aligned} \eta_v(\alpha f + \beta g) &= (\alpha f + \beta g)(v) = (\alpha f)(v) + (\beta g)(v) \\ &= \alpha\,[f(v)] + \beta\,[g(v)] \\ &= \alpha\,[\eta_v(f)] + \beta\,[\eta_v(g)] \end{aligned}$$

فإن η_v دالي خطي على V^* ، أي أن $\eta_v \in V^{**}$.

ضع $\sigma(v) = \eta_v$. الآن لكل $u, v \in V$ ، $\alpha, \beta \in F$ يكون :

$$\sigma(\alpha_u + \beta_v) = \eta_{\alpha_u + \beta_v} \qquad (1)$$

ومرة أخرى لكل $f \in V^*$ فإن $\eta_{\alpha u+\beta v}(f) = f(\alpha u + \beta v) = \alpha f(u) + \beta f(v)$

$$= \alpha\eta_v(f) + \beta\eta_v(f) = (\alpha\eta_u + \beta\eta_v)(f)$$

$$\Rightarrow \eta_{\alpha u+\beta v} = \alpha\eta_u + \beta\eta_v \qquad (2)$$

من (1) و (2) نحصل على $\sigma(\alpha u + \beta v) = \alpha\sigma(u) + \beta\sigma(v)$

وبذلك فإن σ تحويل خطي .

والآن $v \in \ker\sigma \Rightarrow \sigma(v) = 0 \Rightarrow \eta_v(f) = 0, \quad \forall f \in V$

$$\Rightarrow f(v) = 0, \quad \forall f \in V^* \qquad (3)$$

إذا كان $v \neq 0$ فإنه حسب القضية 12-28 يوجد $f \in V^*$ بحيث $f(v) \neq 0$ ، وعليه نستنتج من (3) أن $V = 0$.

وبناء عليه فإن σ مونومورفزم وذلك يبين أن $\dim V = \dim\sigma(V)$ من ناحية أخرى وحسب نظرية 12-25 فإن $\dim V = \dim V^* = \dim V^{**}$ وعليه فإن $\sigma(V)$ فضاء جزئي من V^{**} حيث $\dim\sigma(V) = \dim V^{**}$ وهذا يمكن حدوثه فقط عندما يكون $\sigma(V) = V^{**}$ بالتالي فإن σ فوقي أيضاً . أي أن σ أيزومورفزم من V على V^{**} و σ هو الأيزومورفزم القانوني المطلوب . □

ملاحظة لاحظ أنه في النظرية السابقة $\sigma : V \to V^{**}$ لا يعتمد على أي اختيار خاص لقاعدة الفضاء V وهذا هو سبب تسميته بالأيزومورفزم القانوني .

تعريف 12-30

ليكن V_F فضاءً متجهاً و V^* الفضاء الثنائي له . لأية مجموعة جزئية S من V فإن المجموعة .

$S^{\perp} = \{f \in V^* \mid f(s) = 0, \quad \forall s \in S\}$ تسمى بالمجموعة المتعامدة أو المعدمة للمجموعة S في V^* . لأية مجموعة جزئية T من V^* فإن المجموعة

$T^\perp = \{v \in V \mid f(v) = 0, \quad \forall f \in T\}$ تسمى المجموعة المتعامدة أو المعدمة للتحويل T في V .

قضية 12-31

ليكن V أي فضاء متجهي على الحقل F و V^* الفضاء الثنائي له . إذا كانت S و T مجموعتين جزئيتين من V و V^* على الترتيب ، فإن $S^\perp$ و $T^\perp$ هما فضاءان جزئيان من V^* و V على الترتيب .

البرهان

بما أن $\overline{0}(s) = 0, \quad \forall s \in S$ ، حيث $\overline{0}$ يرمز للدالي الخطي الصفري ، يكون لدينا $\overline{0} \in S^\perp$. عليه فإن $S^\perp \neq \phi$.

الآن لنفرض $f, g \in S^\perp$ ، $\alpha, \beta \in F$ و $s \in S$. بما أن $f(s) = g(s) = 0$ فإن :

$$f(\alpha f + \beta g)(s) = \alpha f(s) + \beta g(s) = 0$$

أي أن $\alpha f + \beta g \in S^\perp$. هذا يبين أن $S^\perp$ فضاء جزئي من V^* .

ومرة أخرى بما أن $f(0) = 0, \quad \forall f \in T$ فإن $0 \in T^\perp$ وعليه $T \neq \phi$.

افرض $u, v \in T^\perp$ ، $\alpha, \beta \in F$ ، $f \in T$. حسب تعريف T^* فإن $f(u) = 0 = f(v)$ وبالتالي فإن :

$$f(\alpha u + \beta v) = \alpha f(u) + \beta f(v) = \alpha 0 + \beta 0 = 0$$

وهكذا فإن $\alpha u + \beta v \in T^\perp$. هذا يبرهن أن $T^\perp$ فضاء جزئي من V . □

القضية التالية هي نتيجة بسيطة للتعريف 12-30 ويترك إثباتها للقراء .

قضية 12-32

ليكن V_F فضاءً متجهاً و V^* فضاءه الثنائي فإن :

(a) لأية مجموعتين جزئيتين S_2, S_1 من V يكون :

$$S_1 \subseteq S_2 \Rightarrow S_2^{\perp} \subseteq S_1^{\perp}$$

(a') لأية مجموعتين جزئيتين T_2, T_1 من V^* يكون :

$$T_1 \subseteq T_2 \Rightarrow T_2^{\perp} \subseteq T_1^{\perp}$$

(b) لأية مجموعة جزئية S من V يكون $S \subseteq S^{\perp\perp}$.

(b') لأية مجموعة جزئية T من V^* يكون $T \subseteq T^{\perp\perp}$. □

نظرية 12-33

ليكن V فضاءً متجهاً ذو بعد منته على حقل F . لأي فضائين جزئيين W و W' من V و V^* على الترتيب يكون

$$\dim W + \dim W^{\perp} = \dim V$$

$$\dim W + \dim(W')^{\perp} = \dim V^*$$

البرهان

ليكن $\dim V = n$ ، $\dim W = r$. بما أن كل مجموعة جزئية مستقلة خطياً من V يمكن توسيعها إلى قاعدة للفضاء V ، يمكننا إيجاد قاعدة مرتبة $(v_1, v_2, \ldots, v_n)$ للفضاء V بحيث $(v_1, v_2, \ldots, v_r)$ تكون قاعدة لـ W . لتكن $(v_1^*, v_2^*, \ldots, v_n^*)$ القاعدة لـ V^* الثنائية للقاعدة $(v_1, v_2, \ldots, v_n)$. استناداً إلى تعريف القاعدة الثنائية ، عندما $1 \le i \le r$ فإن

$$v_j^*(v_i) = 0, \quad \forall j = r+1, r+2, \ldots, n$$

اعتبر أي عنصر $w \in W$ ، $w = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_r v_r$ لبعض العناصر $\alpha_i \in F$ والذي يعطينا

$$v_j^*(w) = \alpha_1 v_j^*(v_1) + \alpha_2 v_j^*(w_2) + \ldots + \alpha_r v_j^*(v_r) = 0, \quad \forall_j \ge r+1$$

إذاً $v_j^* \in W^{\perp}$ لكل $j \ge r+1$ وهكذا فإن الفضاء الجزئي :

$$< v_{r+1}^*, v_{r+2}^*, \ldots, v_n^* > \subseteq w^{\perp} \qquad (1)$$

اعتبر أي عنصر $f \in W^{\perp}$. لما كان $f \in V^*$ فإن :

$$f = \beta_1 v_1^* + \beta_2 v_2^* + \ldots + \beta_n v_n^* \qquad (2)$$

لبعض العناصر $\beta_i \in F$. وحيث أنه لكل $1 \le i \le r$ ، $v_i \in W$ يكون $f(v_i) = 0$.
من (2) نجد أن $f(v_i) = \beta_i$ وعليه فإن $\beta_i = 0$ لكل $1 \le i \le r$. ويكون :

$$f = \beta_{r+1} v_{r+1}^* + \beta_{r+2} v_{r+2}^* + \ldots + \beta_n v_n^*$$

و $f \in < v_{r+1}^*, v_{r+2}^*, \ldots, v_n^* >$.

وهذا يؤدي إلى أن :

$$W^{\perp} \subseteq < v_{r+1}^*, v_{r+2}^*, \ldots, v_n^* > \qquad (3)$$

من (1) و (3) نحصل على :

$$W^{\perp} = < v_{r+1}^*, v_{r+2}^*, \ldots, v_n^* > \qquad (4)$$

في المتساوية الأخيرة يتضح أن $\{v_{r+1}^*, v_{r+2}^*, \ldots, v_n^*\}$ قاعدة للفضاء $W^{\perp}$ تحوي $n - r$ في المتجهات ، وعليه فإن

$$\dim W^{\perp} = n - r = \dim V - \dim W$$

إذاً

$$\dim W + \dim W^{\perp} = \dim V$$

لإثبات الجزء الثاني افرض أن $\dim W' = t$. لدينا $\dim V = \dim V^* = n$ عليه يمكننا إيجاد قاعدة مرتبة $(f_1, f_2, \ldots, f_n)$ للفضاء V^* بحيث تكون $\{f_1, f_2, \ldots, f_t\}$ قاعدة للفضاء W' ويمكن إيجاد قاعدة $(F_1, F_2, \ldots, F_n)$ للفضاء V^{**} ثنائية للقاعدة $(f_1, f_2, \ldots, f_n)$. والآن فإن الراسم $\sigma : V \to V^{**}$ المعطى حسب $[\sigma(v)](f) = f(v)$ لكل $v \in V$ و $f \in V^*$ هو أيزومورفزم (نظرية 12-29) وعليه فيمكننا إيجاد $v_1, v_2, \ldots, v_n$ في V بحيث $\sigma(v_i) = F_i$ لكل $1 \le i \le n$ وعندئذ لكل $i \neq j$ حيث $1 \le i, j \le n$ يكون

$$0 = F_i(f_j) = [\sigma(v_i)](f_i) = f_j(v_i)$$

وعندما $i = j$ فإن $1 = F_j(f_j) = f_j(v_j)$.

وهكذا فإن المجموعة $\{v_1, v_2, \ldots, v_n\}$ هي قاعدة للفضاء V و $(f_1, f_2, \ldots, f_n)$ قاعدة للفضاء V^* ثنائية للقاعدة $(v_1, v_2, \ldots, v_n)$ ، والآن لكل $j \ge t + 1$ ، $1 \le i \le t$ يكون $f_i(v_j) = 0$ مؤدياً إلى $v_j \in (W^{\perp})$.

عليه فإن :

$$< v_{t+1}, v_{t+2}, \ldots, v_n > \subseteq (W')^{\perp} \qquad (5)$$

نفرض أن $v \in (W')^{\perp}$. فحيث أن $v \in V$ ، فإن :

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$$

لبعض العناصر $\alpha_i \in F$ حيث $1 \le i \le n$ ، عندئذ $0 = f_j(v) = \alpha_j$ طالما كان $1 \le j \le t$ هذا يعطي $v = \alpha_{t+1} v_{t+1} + \ldots + \alpha_n v_n \in < v_{t+1}, v_{t+2}, \ldots, v_n >$

ويكون :

$$(W')^{\perp} \subseteq < v_{t+1}, v_{t+2}, \ldots, v_n > \qquad (6)$$

من (5) و (6) نحصل على أن $(W')^{\perp} = < v_{t+1}, v_{t+2}, \ldots, v_n >$

وعليه فإن $\dim (W')^{\perp} = n - t = n - \dim W'$

وهذا يثبت أن $\dim W' + \dim (W')^{\perp} = n = \dim V^*$

وبهذا يكمل البرهان . □

نظرية 12-34

إذا كان T, S فضاءان جزئيان في فضاء متجهي ذو بعد منتهي V_F فإن :

(a) $S^{\perp\perp} = S$

(b) $(S + T)^{\perp} = S^{\perp} \cap T^{\perp}$

(c) $(S \cap T)^{\perp} = S^{\perp} + T^{\perp}$

البرهان

افرض $\dim V = n$ ، $\dim S = r$ ، $\dim T = m$.

(a) حسب القضية 12-32 فإن $S \subseteq T^{\perp\perp}$ ، وحسب النظرية 12-33 فإن

$$\dim S^{\perp} = n - r \text{ و } \dim S^{\perp\perp} = n - \dim S^{\perp} = r = \dim S$$

إذاً S فضاء جزئي من $S^{\perp\perp}$ بحيث $\dim S = \dim S^{\perp\perp}$ ، هذا يبن أن $S = S^{\perp\perp}$.

(b) $f \in (S+T)^{\perp\perp} \Rightarrow f(x)=0, \quad (\forall x \in S+T)$ وبمـــــــــا أن $S \subseteq S+T$

و $T \subseteq S+T$ فإن $f(t)=0$ و $f(s)=0$ لكل $t \in T$ ، $s \in T$

$\Rightarrow f \in S^{\perp}, f \in T^{\perp}$

$\Rightarrow f \in S^{\perp} \cap T^{\perp}$

عليه فإن :

$(S+T)^{\perp} \subseteq S^{\perp} \cap T^{\perp}$ (1)

كذلك فإن $g \in S^{\perp} \cap T^{\perp} \Rightarrow g \in S^{\perp}, g \in T^{\perp}$

$\Rightarrow g(s)=0, g(t)=0, \quad \forall s \in S, t \in T$

$\Rightarrow g(s+t)=0, \quad \forall s \in S, t \in T$

$\Rightarrow g \in (S+T)^{\perp}$ (2)

عليه فإن $S^{\perp} \cap T^{\perp} \subseteq (S+T)^{\perp}$

مـن (1) و (2) نحصـل علـى أن $(S+T)^{\perp} = S^{\perp} \cap T^{\perp}$ بتطبيـق القضـية 12-32 والنظرية 12-33 فإن نفس النتائج كما في a و b يمكن الحصول عليها للفضاءات الجزئية S و T من V^* ، الثنائية للفضاء V .

(c) الآن $T^{\perp}, S^{\perp}$ فضاءان جزئيان في V^* ، فمن (b) يكون :

$(S^{\perp}+T^{\perp})^{\perp} = (S^{\perp})^{\perp} \cap (T^{\perp})^{\perp}$

$= S^{\perp\perp} \cap T^{\perp\perp} = S \cap T$ (حسب a)

وهكذا فإن $(S \cap T)^{\perp} = (S^{\perp}+T^{\perp})^{\perp\perp} = S^{\perp}+T^{\perp}$

هذا يثبت c وبهذا يكمل البرهان . □

النظرية التالية تحقق ثنائية بين الفضاءات الجزئية من الفضاء متجهي V والفضاءات الجزئية من الفضاء V^* . وهذه النظرية هي نتيجة مباشرة للقضية 12-32 ، ونظرية 12-34 .

نظرية 12-35

إذا كان V_F فضاءً متجهاً ذو بعد منته ، فإن الراسم $W \leftrightarrow W^{\perp}$ حيث W فضاء جزئي من V هو تقابل أحادي بين الفضاءات الجزئية من V والفضاءات الجزئية من V^* بحيث :

(a) $W^{\perp\perp} = W$

(b) $W_1 \subseteq W_2$ إذا وفقط إذا كان $W_2^{\perp} \subseteq W_1^{\perp}$

(c) $(W_1 + W_2)^{\perp} = W_1^{\perp} \cap W_2^{\perp}$

(d) $W_1^{\perp} + W_2^{\perp} = (W_1 \cap W_2)$

مسائل

1- افرض $V = F^{(3)}$ إذا كان $e_1 = (1, 0, 0)$ ، $e_2 = (0, 1, 0)$ ، $e_3 = (0, 0, 1)$ عين القاعدة (e_1^*, e_2^*, e_3^*) للفضاء V^* الثنائية للقاعدة المرتبة (e_1, e_2, e_3) للفضاء V وإذا كان $f_1 = (1, 1, 2)$ ، $f_2 = (0, 2, 1)$ ، $f_3(0, 0, 5)$ وكان F حقلاً مميز لا يقبل القسمة على 2 و 5 فأثبت أن $\{f_1, f_2, f_3\}$ قاعدة للفضاء V ، وأوجد القاعدة الثنائية $\{f_1^*, f_2^*, f_3^*\}$ وعبر عن كل f_i^* كتركيب خطي في e_1^*, e_2^*, e_3^* .

2- ليكن W فضاءً جزئياً من فضاء متجهي ذو بعد منته V_F لكل $f \in V^*$ ضع $f^* = f \mid W$ (مقصور f على W) . برهن أن $f^* \in W^*$ وأن $f \to f^*$ هو تحويل خطي من V^* على W^* نواته $W^{\perp}$.

3- اكتب بالتفصيل برهان نظرية 12-35 .

4- *ليكن كل من W, V فضاء متجهي ذو بعد منته على نفس الحقل F و $A : V \to W$ تحويل خطي .

عرف $A^* : W^* \to V^*$ على النحو الآتي :

$$A^*(f) = fA, \quad \forall f \in W$$

بين أن A^* تحويل خطي (يسمى مدور A) . وإذا كان U فضاءً متجهاً آخر على F و $B : W \to V$ تحويل خطي ، فأثبت أن $(BA)^* = A^*B^*$ وكذلك :

(i) $\ker A^* = [A(V)]$ و $v(A^*) = v(A)$

وإذا كان $A' : W^* \to V^*$ عرف $(A')^* = V \to W$ كالآتي لأي $x \in V$ ، ضع $(A')^*(x) = y$ إذا وفقط إذا كان $(A'f)(x) = f(y), \quad \forall f \in W^*$.

(ii) باستخدام حقيقة أنه بين V و V^{**} أيزومورفزم قانوني برهن أن $(A')^*$ تحويل خطي .

(iii) لأي تحويل خطي $A : V \to W$ أثبت أن $A = A^{**}$ واستنتج أن $A \to A^*$ هو تحويل خطي أحادي وفوقي من $\mathrm{Hom}\,(V, W)$ على $\mathrm{Hom}\,(W^*, V^*)$.

5- إذا كان f, g عنصران في V^* بحيث $f(v) = 0$ يؤدي إلى أن $g(v) = 0$ ، برهن أن $g = \lambda f$ لبعض $\lambda \in F$.

6- إذا كان $V = A \oplus B$ ، برهن أن $V^* = A^{\perp} \oplus B^{\perp}$ ثم استنتج أن $V^* / A^{\perp} \cong B^{\perp}$.

[إرشاد : استخدم نظرية 12-34] .

4- المصفوفات والتحويلات الخطية

ليكن كل من V, U فضاءً متجهاً ذو بعد منته على نفس الحقل F و $T : U \to V$ تحويل خطي . افرض أن $(u_1, u_2, \dots, u_n)$ و $(v_1, v_2, \dots, v_m)$ قاعدتين مرتبتين مثبتتين للفضائين U و V على الترتيب . دعنا نتذكر أن تحويلاً خطياً من U إلى V يتحدد بتأثيره على قاعدة الفضاء U وفي المقابل أي راسم من قاعدة للفضاء U إلى V يمكن توسيعه بطريقة وحيدة إلى تحويل خطي من U إلى V ولما كان لكل $1 \le i \le n$ ، $T(u_i) \in V$ ، فإنه يمكننا التعبير عن $T(u_i)$ بطريقة وحيدة بالصورة :

$$T(u_i) = \sum_{j=1}^{m} \alpha_{ji} v_j, \quad \alpha_{ji} \in F$$

فعندئذ نحصل على المصفوفة الآتية من السعة $m \times n$

$$\begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \cdots & \alpha_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \cdots & \alpha_{mn} \end{bmatrix} = (\alpha_{ji}) \qquad (1)$$

كمصفوفة $(Tu_1, Tu_2, \dots, Tu_n)$ نسبة إلى $(v_1, v_2, \dots, v_m)$. وفي المقابل إذا أعطينا المصفوفة (1) فإننا نستطيع تعريف راسم f من $\{u_1, u_2, \dots, u_n\}$ إلى V بحيث يكون $f(u_i) = \sum_{j=1}^{m} \alpha_{ji} v_j$. هذا الراسم يمكن توسيعه بطريقة وحيدة إلى تحويل خطي (ت.خ) $T' : U \to V$.

من الواضح أن مصفوفة $(T'u_1, Tu_2, \dots, T'u_n)$ نسبةً إلى $(v_1, v_2, \dots, v_n)$ هي نفس المصفوفة (1) المصفوفة (α_{ji}) تسمى مصفوفة التحويل الخطي T بالنسبة للقاعدتين المرتبتين $(u_1, u_2, \dots, n_n)$ و $(v_1, v_2, \dots, v_m)$.

بالإضافة إلى ذلك إذا كان $U = V$ وأخذنا $u_i = v_i$ لكل $1 \le i \le n$ فإن المصفوفة (α_{ij}) تسمى مصفوفة T نسبة إلى $(u_1, u_2, \ldots, u_n)$.

قضية 12-36

ليكن V_F, U_F فضاءان متجهان ببعدين n ، m على الترتيب . فإن $\text{Hom}\,(U, V)$ أيزومورفي للفضاء المتجهي لجميع المصفوفات من السعة $m \times n$ على F .

البرهان

لتكن $(u_1, u_2, \ldots, u_n)$ و $(v_1, v_2, \ldots, v_m)$ قاعدتان مرتبتان لكل من V, U على الترتيب . لأي $T \in \text{Hom}\,(U, V)$ ، يكون $T(u_i) = \sum_{j=1}^{m} \alpha_{ji} v_i$ لعناصر وحيدة $\alpha_{ji} \in F$ ، (كما أكدنا في الفصل السابق على أنه لا يوجد فرق بين فضاء متجهي يساري وفضاء متجهي يميني على حقل) . نستطيع أن نكتب :

$$T(u_i) = \sum_{j=1}^{m} v_j \alpha_{ji}\,, \qquad \alpha_{ji} \in F \qquad (1)$$

لذلك فإن (α_{ji}) مصفوفة من السعة $m \times n$. إذا كان $M_{m,n}(F)$ يرمز للفضاء المتجهي لجميع المصفوفات من السعة $m \times n$ على F . عرف :

$$\sigma(T) = (\alpha_{ji}) \qquad (2)$$

ليكن $T, T' \in \text{Hom}\,(U, V)$ ، $\alpha \in F$. ولكل $1 \le i \le n$ افرض $T'(u_i) = \sum_{j=1}^{m} v_j \beta_{ji}$ ، $T(u_i) = \sum_{j=1}^{m} v_j \alpha_{ji}$ لبعض $\beta_{ji} \in F$ ، α_{ji} ، فإن :

$$(T + T')\,(u_i) = T(u_i) + T'(u_i) = \sum_{j=1}^{n} v_j (\alpha_{ji} + \beta_{ji})$$

كذلك
$$(\alpha T)\,(u_i) = \alpha \sum v_j \alpha_{ji} = \sum \alpha (v_j \alpha_{ji}) = \sum v_j (\alpha \alpha_{ji})$$

ومن ثم فإن
$$\sigma(T + T') = (\alpha_{ji} + \beta_{ji}) = \sigma(T) + \sigma(T')$$
$$\sigma(\alpha T) = (\alpha\alpha_{ji}) = \alpha(\alpha_{ji}) = \alpha\sigma(T)$$

إذاً σ هو تحويل خطي .

الآن
$$\sigma(T) = \sigma(T') \Rightarrow (\alpha_{ji}) = (\beta_{ji}) \Rightarrow \alpha_{ji} = \beta_{ji}, \quad \forall_{i,j}$$
$$\Rightarrow T(u_i) = \sum_{j=1}^{m} v_j\alpha_{ji} = \sum_{j=1}^{m} v_j\beta_{ji} = T'(u_i)$$

لكل $1 \le i \le n$. عليه فإن T', T متوافقان على قاعدة للفضاء U . بالتالي فإن $T = T'$ (قضية 12-14) .

وهكذا فإن σ راسم أحادي . الملاحظة قبل القضية تبين أنه إذا أعطيت مصفوفة $(\alpha_{ji}) \in M_{m,n}(F)$ فإنه يوجد تحويل خطي T بحيث يكون $\sigma(T) = \alpha_{ji}$. إذاً σ راسم فوقي . وهذا يكمل البرهان . □

نتيجة 12-37

الفضاء $A(U)$ أيزومورفي مع $M_n(F)$ حلقة المصفوفات من السعة $n \times n$ على الحقل F .

البرهان

في القضية 12-36 وبأخذ $U = V$ ، $u_i = v_i$ لكل $1 \le i \le n$ ونحصل على أنه يوجد أيزومورفزم فضاء متجهي $\sigma : A(U) \to M_n(F)$ بحيث يكون $\sigma(T) = (\alpha_{ji})$ إذا وفقط إذا كان $T(u_i) = \sum_{j=1}^{n} u_j\alpha_{ji}$ لكل $T \in A(U)$.

ليكن T' عنصراً آخر في $A(U)$ و $T'(u_i) = \sum_{j=1}^{n} u_i\beta_{ji}$.

فيكون
$$TT'(u_i) = T\left(\sum_{j=1}^{n} u_j\beta_{ji}\right) = \sum_{j=1}^{n} T(u_j)\,\beta_{ji}$$
$$= \sum_{j=1}^{n}\left(\sum_{k=1}^{n} u_k\alpha_{kj}\beta_{jk}\right) = \sum_{k=1}^{n} u_k\gamma_{ki}$$

حيث $\gamma_{ki} = \sum_{j=1}^{n} \alpha_{kj}\beta_{jk}$.

وهكذا فإن $\sigma(TT') = (\gamma_{ki}) = \sigma(T)\sigma(T')$.

إذاً σ يحافظ على عملية الضرب وبالتالي فإن $A(U) \cong M_n(T)$. □

نظرية 12-38

ليكن $T \in \operatorname{Hom}(U, V)$. ولتكن $(u_1, u_2, \ldots, u_n)$ ، $(v_1, v_2, \ldots, v_m)$ قاعدتين مرتبتين لكل من V, U على الترتيب و (α_{ij}) مصفوفة T نسبة لهاتين القاعدتين فإذا كان $(u'_1, u'_2, \ldots, u'_n)$ ، $(v'_1, v'_2, \ldots, v'_n)$ قاعدتين أخريين للفضائين V, U على الترتيب مع كون P و Q مصفوفتيهما نسبة للقاعدتين $(u_1, u_2, \ldots, u_n)$ و $(v_1, v_2, \ldots, v_m)$ على الترتيب ، فإن مصفوفة T نسبة لهاتين القاعدتين تكون معطاة كالآتي $(\alpha'_{ij}) = Q^{-1}(\alpha_{ij})P$

البرهان

بما أن $P = (p_{ij})$ هي مصفوفة $(u'_1, u'_2, \ldots, u'_n)$ نسبة إلى $(u_1, u_2, \ldots, u_n)$ فإن :
$$u'_i = \sum_{j=1}^{n} u_j p_{ji} \qquad (1)$$

بالمثل إذا كان $Q^{-1} = (q'_{ij})$ فإن :
$$v_i = \sum_{j=1}^{m} v'_j q'_{ji}, \quad 1 \le i \le m \qquad (2)$$

بالإضافة إلى أن :
$$T(u_i) = \sum_{j=1}^{m} v_j\alpha_{ji}, \quad 1 \le i \le n \qquad (3)$$

وبالتالي فإنه من (1) يكون

$$T(u_i') = T\left(\sum_{j=1}^{n} u_j p_{ji}\right) = \sum_{j=1}^{n} T(u_j) p_{ji}$$

[حسب (3)]

$$= \sum_{j=1}^{n}\left(\sum_{k=1}^{m} v_k \alpha_{kj}\right) p_{ji}$$

[حسب (2)]

$$= \sum_{j=1}^{n}\left[\sum_{k=1}^{m}\left(\sum_{t=1}^{m} v_t' q_{tk}'\right)\alpha_{kj}\right] p_{ji}$$

$$= \sum_{t=1}^{m} v_t' \alpha_{ti}'$$

حيث

$$\alpha_{ti}' = \sum_{k=1}^{m}\sum_{j=1}^{n} q_{tk}' \alpha_{kj} p_{ji}$$

لذا فإن (α_{ti}') مصفوفة T نسبة للقاعدتين $(u_1', u_2', \dots, u_n')$ و $(v_1', v_2', \dots, v_m')$ هي $Q^{-1}(\alpha_{nj})\,P$. □

نتيجة 12-39

إذا كانت $A = (\alpha_{ij})$ مصفوفة من السعة $m \times n$ على حقل F ، فإنه توجد مصفوفتان غير منفردتين Q و P بحيث $QAP = diag\,\{1, 1, \dots, 1, 0, 0, \dots, 0\}$

البرهان

ليكن U_F ، V_F فضائين متجهين ببعدين n و m على الترتيب . حسب القضية 12-36 يوجد $T \in \mathrm{Hom}\,(U, V)$ بحيث (α_{ij}) هي مصفوفة U نسبته للقاعدتين المثبتتين $(u_1, u_2, \dots, u_n)$ و $(v_1, v_2, \dots, v_m)$ للفضائين U و V على الترتيب .

نفرض أن $\rho = r(T)$ فإنه يمكننا إيجاد قاعدة $(u_1', u_2', \dots, u_n')$ للفضاء U بحيث يكون $\ker T = < u_{\rho+1}', u_{\rho+2}', \dots, u_n' >$ (نظرية 12-9) فتكون المتجهات $T(u_1'), T(u_2'), \dots, T(u_\rho')$ مستقلة خطياً من V . وعليه توجد قاعدة $(v_1', v_2', \dots, v_m')$ للفضاء V بحيث يكون :

$$v_i' = T(u_i') \quad \text{لكل} \quad 1 \le i \le \rho$$

والآن كل $1 \le i \le \rho$ فإن $T(u_i') = v_i'$ ولكل $i \ge \rho + 1$ فإن $T(u_i') = 0$. وهكذا فإن مصفوفة T بالنسبة للقاعدتين $(u_1', u_2', \dots, u_n')$ و $(v_1', v_2', \dots, v_m')$ هي $diag\left\{\overbrace{1, 1, \dots, 1}^{\rho}, 0, 0, \dots, 0\right\}$ وعلى أية حال فإنه حسب النظرية السابقة يكون $(Q')^{-1}AP' = diag\left\{\overbrace{1, 1, \dots, 1}^{\rho}, 0, 0, \dots, 0\right\}$ ، حيث P' و Q' هما مصفوفتي $(u_1', u_2', \dots, u_n')$ و $(v_1', v_2', \dots, v_m')$ نسبةً إلى $(u_1, u_2, \dots, u_n)$ و $(v_1, v_2, \dots, v_m)$ على الترتيب . وبأخذ $Q = (Q')^{-1}$ و $P = P'$ نحصل على المطلوب . □

نتيجة 12-40

إذا كان $T \in \text{Hom}\,(U, V)$ له $A = (\alpha_{ij}), A' = (\alpha_{ij}')$ كمصفوفتين نسبة للقاعدتين $(u_1, u_2, \dots, u_n)$ و $(u_1', u_2', \dots, u_n')$ للفضاء U ، فإن $A' = P^{-1}AP$ حيث P هي مصفوفة $(u_1', u_2', \dots, u_n')$ نسبة إلى $(u_1, u_2, \dots, u_n)$.

البرهان

بأخذ $U = V$ ، $u_i = v_i$ ، $u_i' = v_i'$ لكل $1 \le i \le n$ ، في النظرية السابقة ، نحصل على أن $P = Q^{-1}$ و $A' = P^{-1}AP$. □

النتيجتان السابقتان تحثنا على تقديم التعاريف الآتية :

تعريف 12-41

يقال عن المصفوفة A من السعة $m \times n$ على F أنها مكافئة للمصفوفة A' من السعة $m \times n$ إذا كان $A' = QAP$ لبعض مصفوفتين غير منفردتين Q, P على F .

تعريف 12-42

يقال عن مصفوفة A من السعة $n \times n$ على حقل F أنها مشابهة للمصفوفة A' من السعة $n \times n$ على F إذا كان $A' = P^{-1}AP$ لمصفوفة غير منفردة P على F .

لذا فإن نتيجة 12-39 تبين أن كل مصفوفة $m \times n$ على حقل F تكون مكافئة لمصفوفة $diag\,\{1, 1, \ldots, 1, 0, 0, \ldots, 0\}$.

تعريف 12-43

لتكن $A = (\alpha_{ij})$ أية مصفوفة على F . لها n عمود بمعنى $A_j = (a_{1j}, a_{2j}, \ldots, a_{nj})$ ، $(j = 1, 2, \ldots, n)$. يمكننا اعتبار كل واحد من هذه الأعمدة عضواً في $F^{(m)}$. فإذا كان W هو الفضاء الجزئي من $F^{(m)}$ المولد بهذه الأعمدة ، فإننا نقول أن W هو فضاء عمود A . وبُعد الفضاء W يسمى مرتبة عمود A . علينا أن نسوق تعريفاً مشابهاً لفضاء صف A ومرتبة صف A .

نظرية 12-44

ليكن $T : U_F \to V_F$ تحويلاً خطياً ، فإذا كانت $A = (\alpha_{ij})$ مصفوفة T نسبة لقاعدتي $(u_1, u_2, \ldots, u_n)$ و $(v_1, v_2, \ldots, v_m)$ للفضائين U و V على الترتيب . فإن مرتبة عمود A يساوي $r(T)$.

البرهان

لكل $1 \le i \le n$ فإن :

$$T(u_i) = \sum_{j=1}^{m} v_j \alpha_{ji} \qquad (1)$$

نفرض أن مرتبة عمود A تساوي s .

فنستطيع إيجاد $i_1, i_2, \ldots, i_s$ بحيث تكون الأعمدة ذات الترقيم $i_1, i_2, \ldots i_s$ للمصفوفة A مستقلة خطياً وجميع الأعمدة الأخرى يمكن التعبير عنها كتركيب خطي من هذه الأعمدة .

نفرض أن
$$T(u_{i1})\beta_1 + T(u_{i2})\beta_2 + \ldots + T(u_{is})\beta_s = 0$$

لبعض $\beta_1, \beta_2, \ldots, \beta_s \in F$ فمن (1) نحصل على
$$\sum_{j=1}^{m} v_j \left(\sum_{k=1}^{s} \alpha_{ji_k} \beta_k \right) = 0$$
$$\Rightarrow \sum_{k=1}^{s} \alpha_{ji_k} \beta_k = 0 \ , \ 1 \le j \le m$$

وبما أن الأعمدة مستقلة خطياً $\beta_k = 0$ لكل k ، وهكذا تكون المتجهات $T(u_{i1}), T(u_{i2}), \ldots, T(u_{is})$ مستقلة خطياً أيضاً .

اعتبر أي $T(u_i)$. بما أن كل عمود للمصفوفة A هو تركيب خطي لـ s من الأعمدة المستقلة خطياً سالفة الذكر فإنه بإمكاننا إيجاد $\alpha_1, \alpha_2, \ldots, \alpha_s \in F$ بحيث يكون :

$$\alpha_{ij} = \sum_{k=1}^{s} \alpha_{ij_k} \alpha_k, \ 1 \le j \le n \qquad (2)$$

من (1) و (2) نحصل على أن
$$T(u_i) = \sum_{j=1}^{m} v_j \alpha_{ji} = \sum_{j=1}^{m} v_j \left(\sum_{k=1}^{s} \alpha_{ji_k} \alpha_k \right)$$
$$= \sum_{k=1}^{s} \left(\sum_{j=1}^{m} v_j \alpha_j i_k \right) \alpha_k$$
$$= \sum_{k=1}^{s} T(u_{ik})\, \alpha_k$$

والآن يكون الفضاء $T(U)$ مولداً بالمتجهات $T(u_1), T(u_2), \ldots, T(u_n)$ وأن $T(u_{ik})$ ، $(k = 1, 2, \ldots, s)$ مستقلة خطياً وجميع $T(u_i)$ الأخرى يمكن التعبير عنها كتركيب خطي في هذه المتجهات وعددها s . وبالتالي فإن $\{T(u_{i_1}), T(u_{i_2}), \ldots, T(u_{i_s})\}$ قاعدة للفضاء $T(U)$. وهكذا فإن مرتبة عمود $A = s = \dim T(U) = r(T)$ وهذا يثبت النظرية . □

بما أن مرتبة تحويل خطي لا تعتمد على اختيار قواعد الفضاءات المتجهة المعطاة وكل مصفوفة $A = (\alpha_{ij})$ من السعة $m \times n$ يقابلها تحويل خطي مصفوفته هي A لفضاء متجهي مناسب ، فإننا نحصل على الآتي :

نتيجة 12-45

المصفوفتين A, B من السعة $m \times n$ على حقل F لهما نفس مرتبة العمود إذا وفقط إذا كانتا متكافئتين .

البرهان يعتمد على نتيجة 12-39 ونظرية 12-44 وتترك التفاصيل للقارئ . □

مسائل

1- لتكن U_F و V_F فضاءان متجهان مع $(u_1, u_2, \dots, u_n)$ و $(v_1, v_2, \dots, v_m)$ قاعدتان مرتبتان مقابلتان لهما . ليكن $T : U \to V$ تحويل خطي و $A = (\alpha_{ij})$ هي مصفوفة T نسبته للقاعدتين أعلاه . إذا كان $(u_1^*, u_2^*, \dots, u_n^*)$ و $(v_1^*, v_2^*, \dots, v_m^*)$ القاعدتان الثنائيتان للفضاءان V^*, U^* على الترتيب . برهن ما يلي :

(a) $(v_k^*T)(u_i) = \alpha_{kj} = \left(\sum \alpha_{kj} u_j^*\right)(u_i)$ لكل $1 \le i \le n$

(b) $v_k^*T = \sum \alpha_{kj} u_j^*$

(c) $T^*(v_k^*) = \sum \alpha_{kj} u_j^*$ (انظر المسألة 4 ، بند 3)

(d) مصفوفة T^* نسبة للقاعدتين أعلاه هي A' المدور أو المنقول لـ A

(e) مرتبة عمود $A' = r(T) = r(T^*) =$ مرتبة عمود A

(f) مرتبة صف $A =$ مرتبة عمود A

(g) مرتبة صف $A =$ مرتبة عمود A'

2- ليكن V فضاءً متجهاً بعده 2 على حقل F . برهن على أن كل عنصر في $A(V)$ يحقق متعددة حدود من الدرجة 2 على F . برهن كذلك أن لكل $S, T \in A(V)$ فيكون $(ST - TS)^2$ متبادلاً مع جميع عناصر $A(V)$.

3- ليكن $U = F^{(3)}$ وافرض أن $\begin{pmatrix} 1 & 1 & 2 \\ -1 & 2 & 1 \\ 0 & 1 & 3 \end{pmatrix}$ هي مصفوفة $T \in A(V)$ نسبة للقاعدة (e_1, e_2, e_3) حيث $e_1 = (1, 0, 0)$ ، $e_2 = (0, 1, 0)$ ، $e_3 = (0, 0, 1)$.

أوجد مصفوفة T نسبة إلى القاعدة (f_1, f_2, f_3) علماً بأن $f_1 = (1, 1, 1)$ ، $f_2 = (0, 1, 1)$ و $f_3 = (0, 0, 1)$.

[الجواب $\begin{pmatrix} 4 & 3 & 2 \\ -2 & 0 & -1 \\ 2 & 1 & 2 \end{pmatrix}$] .

4- ليكن V هو الفضاء المتجهي المكون من جميع كثيرات الحدود على F والتي درجتها أقل من أو تساوي 3 . من $A(V)$ عرف T كالآتي :

$$T(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3) = \alpha_0 + \alpha_1(x+1) + a_2(x+1)^2 + \alpha_3(x+1)^3$$

احسب مصفوفة T نسبة للقاعدتين :

(a) $(1, x, x^2, x^3)$ ، (b) $(1+x, 1+x^2, 1+x^3)$.

وإذا كانت المصفوفة في الفقرة (a) هي A وفي الفقرة (b) هي B ، أوجد مصفوفة C بحيث $B = CAC^{-1}$.

[الجواب

(a) $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 1 & -1 & -3 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$] .

13

الحقـــــول

Fields

عند مناقشتنا لنظرية الحلقات عرفنا الحقل على أنه حلقة إبدالية بعنصر محايد 1 لا يساوي 0 بحيث كل عنصر غير صفري فيها هو وحده ، ومن المؤكد أن القارئ قد لاحظ روعة نظرية الفضاءات المتجهة على حقل . إن لمفهوم الحقل موقعاً رئيسياً في الجبر إذ أنه ذو تطبيقات واسعة في الجبر الخطي ونظرية المعادلات المتعلقة بدراسة جذور كثيرات الحدود ، ولسنا هنا معنيون بمناقشة كافة جوانب نظرية الحلقات ولكننا مهتمون بالدرجة الأولى بتطور ذلك الجانب من نظرية الحقول الذي له تطبيقات مباشرة على نظرية المعادلات .

1– الحقول الجزئية والحقول الأولية

تعريف 13-1 (الحقل الجزئي)

يقال لمجموعة جزئية غير خالية S من حقل F أنها حقل جزئي للحقل F ، إذا كان :

(i) $a \in S$ ، $b \in S$ يؤدي إلى أن $a + b \in S$ و $a . b \in S$.

(ii) S حقل تحت عمليتي الجمع والضرب المستحدثتين .

ملاحظة إذا كان S حقلاً جزئياً من F لا يساوي F ، فسوف نقول أن S حقل جزئي فعلي من الحقل F . وإذا كان S حقلاً جزئياً من الحقل F ، فإن S تشكل زمرة جزئية من F تحت عملية الجمع وأن مجموعة جميع العناصر غير الصفرية من S تشكل زمرة جزئية

لزمرة الضرب من F . وبالتالي فإنه لأي عنصرين $a, b \in S$ فإن $a - b \in S$ ، وإذا كان $b \neq 0$ فإن $b^{-1} \in S$ و $ab^{-1} \in S$. بما أن العنصر المحايد لزمرة ما ينتمي إلى كل زمرة جزئية منها ، فإن الصفر والعنصر المحايد للحقل F كلاهما ينتمي إلى S وهكذا فإن S تحوي على الأقل عنصرين ، هما $1, 0$.

وكما في الزمر الجزئية والحلقات الجزئية فإنه يمكننا أن نثبت الآتي لحقل جزئي .

نظرية 13-2

أية مجموعة جزئية S من حقل F تحوي على الأقل عنصرين هي حقل جزئي من F إذا وفقط إذا كان :

(i) $a \in S, b \in S$ يؤدي إلى أن $a - b \in S$

(ii) $a \in S, b \in S$ و $b \neq 0$ يؤدي إلى أن $ab^{-1} \in S$

نظرية 13-3

تقاطع أية عائلة غير خالية لحقول جزئية من الحقل F هو حقل جزئي من الحقل F .

البرهان

لتكن $\{S_i\}_{i \in I}$ عائلة غير خالية لحقول جزئية من الحقل F و $S = \bigcap_{i \in I} S_i$. بما أن كل حقل جزئي من F يحوي 0 و 1 ، فإن $0, 1 \in S_i$ لكل i . وعليه فإن $0, 1 \in S$. أي أن S تحوي عنصرين على الأقل .

ليكن $a, b \in S$. فإن $a \in S_i$ و $b \in S_i$ لكل i ، وحسب **نظرية 13-2** فإن $a - b \in S_i$ لكل i .

إذا كان $b \neq 0$ فإن $ab^{-1} \in S_i, \quad \forall i \in I$ وهذا يؤدي إلى $ab^{-1} \in \bigcap_{i \in I} S_i = S$

وهكذا فإن S حقل جزئي من الحقل F . وهذا يكمل البرهان . □

إذا كان P هو تقاطع جميع الحقول الجزئية من الحقل F ، فإن P حقل جزئي من F وكل حقل جزئي من F يحوي P . وعليه لا يوجد حقل جزئي من F محتوى فعلياً في P . أي أنه لا يوجد حقل جزئي فعلي للحقل P . هذا يقودنا إلى تعريف الحقل الأولي .

تعريف 4-13

يقال للحقل P أنه حقل أولي إذا كان لا يحوي حقولاً جزئية فعلية .

مثال 1

ليكن p أي عدد صحيح أولي ، فإن $< p >$ مثالي أعظمي للحلقة Z وأن $Z / < p >$ عبارة عن حقل يحوي p من العناصر . فإذا كان S أي حقل جزئي من $Z / < p >$ فإنه يحوي عنصرين على الأقل ، وعندئذ وكما في الزمرة التي رتبتها عدد أولي ليس لها زمرة جزئية فعلية فإن $S = Z / < p >$. وهذا يثبت أن $Z / < p >$ حقل أولي .

مثال 2

ليكن X حقلاً جزئياً من حقل الأعداد النسبية Q ، فإن $1 \in X$. افرض أن $\frac{m}{n} \in Q$ ، حيث $m, n \in Z$ و $n \neq 0$.

الآن $m = m1 \in X$ و $n = n1 \in X$ ، ولكن $n \neq 0$ ، عليه فإن $n = n1 \neq 0$ هو عنصر في X أي أن $\frac{m}{n} \in X$. بالتالي فإن $Q = X$ وبذلك يكون Q حقل أولي .

النظرية التالية تبين أن Q و $Z / < p >$ لكل عدد أولي p هما أساساً الحقلان الأوليان الوحيدان .

نظرية 13-5

أي حقل أولي يكون إما أيزومورفياً إلى حقل الأعداد النسبية أو إلى حقل الأعداد الصحيحة بمعيار عدد أولي ما .

البرهان

ليكن P حقل أولي و e العنصر المحايد للحقل P . نعرف $f : Z \to P$ على النحو الآتي :

$f(n) = ne, \quad \forall\, n \in Z$. f عبارة عن هومومورفزم حلقية و $\ker f$ هو مثالي للحلقة Z ، إذن يوجد عدد صحيح غير سالب q بحيث $\ker f = < q >$. وتظهر الحالات الآتية :

حالة I $q = 0$ ، في هذه الحالة فإن f عبارة عن مونومورفزم وأن $Z \cong f(Z) \subseteq P$. الآن P يحوي حقل القواسم Q' للساحة التامة $f(Z)$ (**نظرية 25-8**) . وحيث أن P حقل أولي ، فإن $P = Q'$. على أية حال فإن Q هو حقل قواسم الحلقة Z . ولكننا نعلم أنه إذا كانت أي ساحتين تامتين بينهما أيزومورفزم فإنه يوجد أيزومورفزم بين حقلي قواسمهما ، فإن $Q \cong Q'$ أي أن $P \cong Q$.

حالة II $q \neq 0$ ، لذا يكون $q > 0$. إذا كان $q = 1$ ، نحصل على $1e = 0$ أي أن $e = 0$ وهذا تناقض ، وعليه فإن $q > 1$. ندعي أن q عدداً أولياً . وخلافاً لذلك نفرض أن $q = ab$ حيث a, b عددين صحيحين كلاهما أكبر من الواحد . عندئذ يكون $0 = qe = (ab)\, e = (ae)\,(be)$. وبالتالي فإن :

$ae = 0$ أو $be = 0$. وهكذا فإن $a \in < q >$ أو $b \in < q >$ ، هذا يعطينا $q \mid a$ أو $q \mid b$. وهذا يناقض حقيقة أن كلاً من b, a أقل من q . عليه فإن q أولي وبالتالي

يكون $Z / < q >$ حقلاً وحسب النظرية الأساسية للهومومورفزم فإن $Z / \ker f \cong f(Z)$ أي أن $Z / < q > \cong f(Z)$.

وهكذا فإن $f(Z)$ حقل جزئي من الحقل F . وبما أن P حقل أولي ، فإن $f(Z) = P$. وهذا بدوره يؤدي إلى أن $Z / < q > \cong P$ ، وهكذا نحصل على النتيجة .

ملاحظة في إثبات **حالة I** من النظرية السابقة فإن الأيزومورفزم $Q \cong P$ معطى بالراسم $x = \frac{n}{m} \to \frac{ne}{me}$ ، لكل $x = \frac{n}{m} \in Q$.

وفي **حالة II** الأيزومورفزم $Z / < q > \cong P$ معطى بالراسم $\bar{n} \to ne$ ، لكل $\bar{n} = n + < q > \in Z / < q >$. □

تعريف 6-13

التقاطع P لجميع الحقول الجزئية من حقل F يسمى الحقل الجزئي الأولي في الحقل F .

تعريف 7-13

لتكن D ساحة تامة بعنصر محايد e حيث $e \neq 0$. يقال أن D ذات مميز صفر إذا كان $ne \neq 0$ لكل عدد صحيح موجب n . ويقال أن D ذات مميز منته إذا كان $ne = 0$ لبعض عدد صحيح موجب n . وإذا كان s أصغر عدد صحيح موجب بحيث $se = 0$ نقول أن مميز D يساوي s . على سبيل المثال مميز Q هو صفر ولكل عدد أولي موجب P فإن مميز الحلقة $Z / < P >$ يساوي P .

نظرية 8-13

إذا كان D ساحة تامة بعنصر محايد فإن مميز D يكون إما صفراً أو عدداً أولياً .

البرهان

ليكن D بمميز منته p ، بما أن $1e = e \neq 0$ فإن $p > 1$. نفترض أن $p = ab$ لعددين صحيحين $a, b > 1$ فيكون $1 < a, b < p$. بالإضافة إلى ذلك فإن $(ae)(be) = pe = 0$ يؤدي إلى إما أن $ae = 0$ أو $be = 0$ ، وهذا يناقض حقيقة أن p هو أصغر عدد صحيح موجب له الخاصية $pe = 0$. وبذلك فإن p عدد أولي . وهذا يبرهن النظرية . □

تمارين محلولة

تمرين 1

برهن أن الهومومورفزمان الوحيدان من $I\!R$ إلى $I\!R$ هما الهومومورفزم الصفري أو الهومومورفزم المحايد .

الحل

ليكن $f : I\!R \to I\!R$ هومومورفزم . بما أن $\ker f$ مثالي في $I\!R$ وأن $I\!R$ حقل، فإن :

$$\ker f = \{0\} \text{ أو } \ker f = I\!R$$

إذا كان $\ker f = I\!R$ ، فإن $f(x) = 0, \quad \forall x \in I\!R$ أي أن f هو الهومومورفزم الصفري .

في الحالة عندما $\ker f = \{0\}$ فإن f دالة أحادية (1-1) . بما أن $\ker f \neq I\!R$ ، يوجد $r \in I\!R$ بحيث $r \notin \ker f$ أي أن $f(r) \neq 0$.

ولكن
$$f(r) = f(r1) = f(r)\,f(1)$$
$$\Rightarrow f(r)\{1 - f(1)\} = 0 \Rightarrow f(1) = 1$$

ليكن m عدداً صحيحاً > 0 . فإن :

$$f(m) = f(1 + 1 + 1 + \ldots \quad m \text{ من المرات})$$
$$= f(1) + f(1) + \ldots \quad m \text{ من المرات}$$
$$= 1 + 1 + 1 + \ldots \quad m \text{ من المرات}$$
$$= m$$

عندما يكون $m = 0$ ولكون f هومومورفزم فإن :

$f(m) = f(0) = 0$ أي أن $f(m) = m$.

وإذا كان m عدداً صحيحاً سالباً ، فإنه بوضع $m = -n$ حيث $n > 0$ يكون :

$$f(m) = f(-n) = -f(n) \qquad (\text{لأن } f \text{ هومومورفزم})$$
$$= -n \qquad (\text{لأن } n \text{ عدد صحيح موجب})$$
$$= m$$

الآن ليكن r عدداً نسبياً فإن $r = \dfrac{P}{q}$ حيث $q > 0, P, q \in Z$.

$$\therefore \quad qr = P$$
$$\Rightarrow f(qr) = f(P) = P \quad (\text{كما برهنا سابقاً})$$
$$\Rightarrow f(r + r + \ldots \quad q \text{ من المرات}) = P$$
$$\Rightarrow f(r) + f(r) + \ldots \quad q \text{ من المرات} = P$$
$$\Rightarrow qf(r) = P \Rightarrow f(r) = \frac{P}{q} = r$$

والآن ليكن $\alpha \geq 0$. فإنه يوجد عدد حقيقي $\in \geq 0$ بحيث $\alpha = \in^2$. وبما أن f هومومورفزم فإن

$$f(\alpha) = f(\in^2) = [f(\in)]^2$$
$$\Rightarrow f(\alpha) \geq 0 \qquad (\text{لأن } f(\in) \in R)$$

إضافة إلى ذلك فإن
$$\alpha \geq \beta \Rightarrow \alpha - \beta \geq 0 \Rightarrow f(\alpha - \beta) \geq 0$$

$$\Rightarrow f(\alpha) - f(\beta) \geq 0 \Rightarrow f(\alpha) \geq f(\beta)$$

ليكن $\alpha < \beta$ بحيث $f(\alpha) = f(\beta)$ ، وحيث أن f أحادي فإن $\alpha = \beta$ وهذا تناقض .

عليه فإن $\alpha < \beta$ يؤدي إلى أن $f(\alpha) > f(\beta)$.

افرض أن $\in > 0$ ، عندئذ يوجد عدد نسبي s بحيث $0 < s < \in$.

ضع $\delta = s$ ، فإن $| x - a | < \delta = s$ يعني أن $-s < x - a < s$

$$\Rightarrow \quad -f(s) < f(x-a) < f(s)$$

$$\Rightarrow \quad -f(s) < f(x) - f(a) < f(s)$$

$$\Rightarrow \quad | f(x) - f(a) | < f(s)$$

$$\Rightarrow \quad | f(x) - f(a) | < s$$ (لأن $f(s) = s$ حيث s عدد نسبي)

$$\Rightarrow \quad | f(x) - f(a) | < \in$$

وعليه فإن $f(x)$ دالة حقيقية متصلة .

وأخيراً إذا كان x عدداً حقيقياً ، فإنه توجد متتابعة كوشي من الأعداد النسبية $\left\{\frac{P_n}{q_n}\right\}$ تكون متقاربة إلى x أي أن $x = \lim\limits_{n\to\infty}\left\{\frac{P_n}{q_n}\right\}$. بما أن f دالة متصلة فإن :

$$f(x) = \lim f\left(\frac{P_n}{q_n}\right) = \lim_{n\to\infty}\frac{P_n}{q_n} = x$$

وبالتالي f هو الهومومورفزم المحايد .

تمرين 2

برهن أن الهومومورفزمات المتصلة الوحيدة من C إلى C هو الهومومورفزم الصفري أو الهومومورفزم المرافق أو الهومومورفزم المحايد .

الحل

بمـا أن C حقـل ، فإنـه وكمـا في التمـرين 1 نحصـل علـى أنـه إذا كـان f لـيس الهومومورفزم الصفري فإن :

$f(r) = r$ لكل عدد نسبي r .

ليكن x أي عدد حقيقي .

توجد متتابعة كوشي من الأعداد النسبية $\left\{\frac{P_n}{q_n}\right\}$ بحيث $x = \lim_{n\to\infty}\left\{\frac{Pn}{q_n}\right\}$ حيث أن f متصل

فحسب الفرض يكون $f(x) = \lim_{n\to\infty} f\left\{\left(\frac{P_n}{q_n}\right)\right\} = \lim_{n\to\infty}\frac{P_n}{q_n} = x$

نعتبر $i = \sqrt{-1}, i^2 = -1 \Rightarrow f(i^2) = f(-1) = -1$

$$\Rightarrow [f(i)]^2 = -1$$

يؤدي إلى أن $f(i) = i$ أو $f(i) = -i$.

في الحالة الأولى عندما $f(i) = i$ فلكل $z = \alpha + i\beta \in C$ $(\alpha, \beta \in IR)$ يكون :

$$\begin{aligned} f(z) &= f(\alpha + i\beta) = f(\alpha) + f(i)f(\beta) \\ &= \alpha + i\beta = z \end{aligned}$$

إذاً f هو الهومومورفزم المحايد .

في الحالة الثانية عندما $f(i) = -i$ لأي $z = \alpha + i\beta \in C$ $(\alpha, \beta \in IR)$ يكون :

$$\begin{aligned} f(z) &= f(\alpha + i\beta) = f(\alpha) + f(i)f(\beta) \\ &= \alpha - i\beta \end{aligned}$$

وبالتالي فإن f هو الهومومورفزم المرافق .

مسائل

1- برهن أن المجموعات الآتية هي حقول جزئية من الحقل IR :

(i) $\{a + b\sqrt{2} \mid a, b \in Q\}$

(ii) $\left\{a + \sqrt[3]{5}\, b + \left(\sqrt[3]{5}\right)^2 c \mid a, b, c \in Q\right\}$

(iii) $\{a + \sqrt{2}\, b + \sqrt{3}\, c + \sqrt{6}\, d \mid a, b, c, d \in Q\}$

2- برهن أن مميز الحقل يكون مساوياً لمميز حقوله الجزئية .

3- برهن أن مميز حقل F يكون صفراً أو عدداً أولياً P حسبما يكون حقله الجزئي الأولي أيزومورفي إلى Q أو $Z / < P >$.

4- برهن صحة أو خطأ أنه إذا كان D هو PID وكان P عنصراً غير قابلاً للتحليل في D فإن مميز $D / < P >$ منته .

[إرشاد : اعتبر الحقل $\frac{Q[x]}{< x >}$] .

5- برهن أنه إذا وجد عنصر غير صفري $a \in F$ (F حقل) ، $na = 0$ لبعض عدد صحيح n فإن $nb = 0$ بجميع $b \in F$. واستنتج أنه إذا وجد لعنصر غير صفري x عدداً صحيحاً موجباً n بحيث $nx = 0$ ، فإن مميز F يكون عدداً منتهياً .

2- توسيع الحقول

تعريف 13-9

حقل موسع للحقل F عبارة عن زوج (K, σ) حيث K حقل و σ مونومورفزم من F إلى K .

فإذا كان E حقلاً و F حقلاً جزئياً من F ، فإن راسم الإدخال $i : F \to E$ المعرف حسب $i(x) = x$ لكل $x \in F$ هو مونومورفزم . وبالتالي فإن (E, i) هو حقل موسع للحقل F . في هذه الحالة عندما يكون مثلاً i الراسم التافه فلن نشير إلى i وببساطة نقول أن E حقل موسع للحقل F . في الحالة العامة لحقل توسيع (K, σ) فإن K يحوي حقلاً جزئياً $\sigma(E)$ أيزومورفياً إلى F . كما أكدنا في البداية فإنه باستطاعتنا أن نعتبر أي نظامين جبريين بينهما أيزومورفزم شيئاً واحداً .

فإننا هنا نعتبر أن F و $\sigma(F)$ لا فرق بينهما ومن ثم نعامل F كأنه حقل جزئي من K ، وببساطة سوف نقول أن K هو حقل توسيع للحقل F . من الآن فصاعداً فإن F يمثل حقلاً و K حقل توسيع للحقل F .

بما أنه لأي $\alpha \in F$ ، $x \in K$ يكون $\alpha x \in K$ فإننا نحصل على عملية خارجية $F \times K \to K$ معطاة $(\alpha, x) \to \alpha x$.

مباشرة يمكننا أن نجد أن زمرة الجمع $< K, + >$ عبارة عن فضاء متجهي على F نسبة للعملية الخارجية في K بالنسبة إلى F المعرفة سابقاً ، وعليه فإن للحقل K قاعدة وبعد على F .

تعريف 13-10

بعد K باعتباره فضاءً متجهاً على F يسمى درجة K .

اصطلاح : $[K : F]$ سوف يرمز لدرجة K على F .

مثال 3

$Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$ هي حقل موسع للحقل Q . المجموعة الجزئية $\{1, \sqrt{2}\}$ تمثل قاعدة للفضاء $Q[\sqrt{2}]$ على Q . وبالتالي $[Q[\sqrt{2}] : Q] = 2$.

مثال 4

اعتبر x غير محدد على الحقل F . ليكن K حقل القواسم للحقل $F[x]$. عندئذ وكما نعلم لكل $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n \in F$ ، يكون :

$$\alpha_0 1 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n = 0$$

يؤدي إلى أن $\alpha_i = 0, \quad \forall i$ ، ومنها نستنتج أن $\{1, x, x^2, \ldots, x^n, \ldots\}$ هي مجموعة جزئية غير منتهية من K وهي مستقلة خطياً على F . وبالتالي فإن $[K : F]$ غير منتهية .

تعريف 13-11

يقال أن K توسيعاً منتهياً أو غير منته للحقل F حسبما تكون درجة K على F منتهية أو غير منتهية .

وهكذا في مثال 3 ، $Q[\sqrt{2}]$ هو توسيع منته للحقل Q وفي مثال 4 ، K هو توسيع غير منته للحقل F . النظرية التالية حول درجة توسيع لها أهمية كبيرة .

نظرية 13-12

إذا كان K توسيعاً منتهياً للحقل F و L توسيعاً منتهياً للحقل K ، فإن L يكون توسيعاً منتهياً للحقل F و $[L : F] = [L : K][K : F]$.

البرهان

نفرض أن $[K : F] = n$ و $[L : K] = m$. عندئذ بإمكاننا إيجاد قاعدة $\{x_1, x_2, \ldots, x_n\}$ لـ K على F وقاعدة $\{y_1, y_2, \ldots, y_m\}$ لـ L على K . نعتبر العناصر

$x_i y_j, i = 1, 2, \ldots, n, \ j = 1, 2, \ldots, m$. إذا استطعنا أن نبين أن mn من عناصر L المذكورة تكون مستقلة خطياً على F وأنها تولد L باعتباره فضاء متجهي على F فإن ذلك يبين أن $[L : F] = mn = [L : K][K : F]$ وتكون النظرية قد برهنت . ومن ناحية الاستقلال الخطي افرض $\sum_{i,j} \alpha_{ij} x_i y_j = 0$. لبعض $\alpha_{ij} \in F$. ومنها نحصل على $\sum_{j=1}^{m} \left(\sum_{i=1}^{n} \alpha_{ij} x_i \right) y_j = 0$. وبما أن $y_1, y_2, \ldots, y_m$ مستقلة خطياً على K و $\sum \alpha_{ij} x_i \in K$ لكل j فإن $\sum_{i=1}^{n} \alpha_{ij} x_i = 0, \ \ \forall j = 1, 2, \ldots, n$. ولأن $x_1, x_2, \ldots, x_n$ مستقلة خطياً على F فإن $\alpha_{ij} = 0, \ \forall ij$. أي أن العناصر $x_i y_j$ مستقلة خطياً على F .

اعتبر أي عنصر x في L . فحيث أن $\{y_1, y_2, \ldots, y_m\}$ قاعدة لـ L على K فإن $x = \sum_{j=1}^{m} a_j y_j$ لبعض $a_j \in K$ ، $j = 1, 2, \ldots, m$ ، ومرة أخرى بما أن $\{x_1, x_2, \ldots, x_n\}$ قاعدة للفضاء K على F فإنه لكل j يكون $a_j = \sum_{i=1}^{n} \alpha_{ij} x_i$ لبعض $\alpha_{ij} \in F$. وبالتالي فإن :

$$x = \sum_{j=1}^{m} \sum_{i=1}^{n} \alpha_{ij} x_i y_j \quad \text{حيث} \quad \alpha_{ij} \in F \quad \text{لكل} \quad i, j \ .$$

أي أن العناصر $x_i y_j$ حيث $i = 1, 2, \ldots, n$ ، $j = 1, 2, \ldots, m$ وعددها mn تمثل قاعدة للفضاء L على F وبذلك نحصل على النتيجة . □

تعريف 13-13

لتكن S مجموعة جزئية في الحقل K . يقال أن الحقل الجزئي K' من K مولد بالمجموعة S إذا كان :

(i) $S \subseteq K'$.

(ii) لكل حقل جزئي L من K ، $S \subseteq L$ يؤدي إلى أن $K' \subseteq L$.

اصطلاح يرمز للحقل الجزئي المولد بمجموعة جزئية S بالرمز $< S >$.

أساساً الحقل الجزئي المولد بالمجموعة S عبارة عن تقاطع جميع الحقول الجزئية من K والتي تحوي S . الآن إذا كان K حقل توسيع للحقل F و S أية مجموعة جزئية من K ، فإن الحقل الجزئي من K المولد بالمجموعة $F \cup S$ يقال أنه الحقل الجزئي من K المولد بالمجموعة S على F وهذا الحقل الجزئي يرمز له $F(S)$.

من ناحية ثانية إذا كانت S مجموعة منتهية وعناصرها $a_1, a_2, \dots, a_n$ ، عندئذ نكتب $F(S) = F(a_1, a_2, \dots, a_n)$.

تعريف 13-14

يقال للحقل K بأنه منته التولد على F إذا وجد عدد منته من العناصر $a_1, a_2, \dots, a_n$ في K بحيث $K = F(a_1, a_2, \dots, a_n)$.

حالة خاصة : إذا كان K مولد بعنصر واحد على F ، فإن K يسمى توسيع بسيط . عليه فإن $Q[\sqrt{2}] = Q(\sqrt{2})$ هو حقل توسيع بسيط لـ Q . اعتبر أي عنصر $a \in K$ وليكن $F(a)$ هو الحقل الجزئي في K المولد بـ a على F . عندئذ لكل $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n \in F$ ، فإن $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \dots + \alpha_n a^n \in F(a)$. هذا يعني أن $F[a] \subseteq F(a)$. وبالتالي فإن حقل القواسم T لـ $F[a]$ محتوى أيضاً في $F(a)$. من ناحية أخرى $F \subseteq T$ و $a \in T$ ، وعليه $F(a) \subseteq T$ ونحصل على $T = F(a)$ ، بمعنى آخر $F(a)$ هو حقل القواسم للحلقة الجزئية من K المولدة من $F \cup \{a\}$. هذه المناقشة يمكن أن توسع لكل مجموعة S وبإمكاننا القول أن $F(S)$ هو حقل القواسم لـ $F[S]$ ، الحلقة الجزئية من K المولدة من $F \cup S$.

دعنا نشير إلى أنه لأي $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ في $F[x]$ ولأي $a \in K$ ، $f(a)$ يرمز للعنصر $\alpha_0 + \alpha_1 a + \ldots + \alpha_n a^n$ ، وبالإمكان أيضاً التحقق من أن الراسم $f(x) \to f(a)$ هو هومومورفزم حلقة من $F[a]$ إلى K .

تعريف 13-15

يقال لعنصر a في K أنه جذر أو صفر لكثيرة حدود $P(x) \in F[x]$ إذا كان $P(a) = 0$. في هذه الحالة نقول أيضاً أن $P(x)$ متحقق بالعنصر a .

تعريف 13-16

يقال لعنصر a في K أنه عنصر جبري على F إذا كان a جذراً لكثيرة حدود غير صفرية $f(x) \in F(x)$. يقال أن K توسيع جبري للحقل F إذا كان كل عنصر في K جبرياً على F .

إذا كانت $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ حيث $\alpha_0 \neq 0$ ، فإن $f(a) = \alpha_0 + \alpha_1 a + \ldots + \alpha_n a^n$. وإذا كان $f(a) = 0$ فإن $n \neq 0$ وهكذا فإن $n > 0$ وأن $\deg f(x) > 0$ بمعنى آخر أن $f(x)$ هي كثيرة حدود غير ثابتة .

تعريف 13-17

يقال لكثيرة حدود غير صفرية $f(x)$ في $F[x]$ أنها كثيرة حدود واحدية على F إذا كان معامل أعلى قوة لـ x في $f(x)$ مساوياً للواحد ، العنصر المحايد للحقل F.

نظرية 13-18

إذا كان $a \in K$ عنصراً جبرياً على F ، فإنه توجد كثيرة حدود واحدية واحدة فقط $P(x)$ ذات درجة موجبة على F بحيث :

(i) $P(a) = 0$ ، (ii) إذا كان لأي $f(x) \in F[x]$ ، $f(a) = 0$ فإن $P(x)$ يقسم $f(x)$.

البرهان

حيث أن a جبري على K ، a جذر لبعض كثيرة حدود غير صفرية على F . لتكن $t(x)$ كثيرة حدود غير صفرية على F والأقل درجة بحيث $t(a) = 0$ نفرض أن درجة $t(x)$ يساوي n . فإن $n > 0$ وأن :

$$t(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n$$

مع $\alpha_n \neq 0, \alpha_i \in F$ نأخذ :

$$P(x) = x^n + \alpha_n^{-1}\alpha_{n-1}x^{n-1} + \alpha_n^{-1}\alpha_{n-2}x^{n-2} + \ldots + \alpha_n^{-1}\alpha_0 = \alpha_n^{-1}t(x)$$

ونجد أن $P(a) = 0$ مع كون $\deg P(x) = n = \deg t(x)$. هذا يبين أن $P(x)$ كثيرة حدود واحدية على F بحيث أن $P(x)$ هي الأقل درجة من بين جميع كثيرات الحدود الغير صفرية على F والتي هي محققة بالعنصر a .

لتكن $f(x)$ أية كثيرة حدود بحيث $f(a) = 0$ ، حسب خوارزمية القسمة بإمكاننا إيجاد كثيرتي حدود $r(x), g(x)$ في $F[x]$ ، بحيث :

$$f(x) = P(x)\, q(x) + r(x)$$

و $r(x) = 0$ أو $\deg r(x) < \deg P(x)$.

الآن $0 = f(a) = P(a)\, q(a) + r(a) = r(a)$.

وبالتالي $r(x) = 0$ ، لأنه لا توجد كثيرة حدود غير صفرية ودرجتها أقل من $\deg P(x)$ متحققة بالعنصر a . وعليه فإن $f(x) = P(x)\, q(x)$ و $P(x)$ يقسم $f(x)$.

افرض الآن أن $P_i(x) = x^m + \beta_{m-1}x^{m-1} + \ldots + \beta_0$ كثيرة حدود واحدية أخرى بحيث $P_1(a) = 0$ ولأية كثيرة حدود $f(x)$ في $F[x]$ ، $f(a) = 0$ يؤدي إلى أن $P_1(x)$ يقسم $f(x)$. عندئذ وكحالة خاصة فإن $P_1(x) \mid P(x)$ وعليه $P(x) = l(x)P_1(x)$ لبعض

$l(x) \in F[x]$. عندئذ الأصغرية لدرجة $P(x)$ تبين أن $l(x)$ هي كثيرة حدود ثابتة غير صفرية . لتكن $l(x) = c$ ، $\deg P(x) = n$. عندئذ بمقارنة معامل x^n في $p(x)$ و $cP_1(x)$ نحصل على أن $c = 1$ والذي يعطينا $p(x) = p_1(x)$. أي أن $p(x)$ وحيد . هذا يكمل البرهان . □

تعريف 13-19

إذا كان a عنصراً في K جبرياً على F ، فإن كثيرة الحدود الواحدية الأقل درجة على F والمتحققة بالعنصر a تسمى متعددة الحدود الأصغرية لـ a على F .

إذا كانت درجة كثيرة الحدود الأصغرية للعنصر a هو n ، عندئذ يقال أن a عنصر جبري على F درجته n .

مثال 5

نؤكد أن $x^2 - 3$ هي كثيرة الحدود الأصغرية لـ $\sqrt{3}$ على Q . من الواضح أن $x^2 - 3$ كثيرة حدود واحدية وأنها متحققة بـ $\sqrt{3}$. لكون $\sqrt{3}$ عدد غير نسبي فإنه لا يحقق أية كثيرة حدود درجتها تساوي واحد على Q . وعليه فإن تأكيدنا صحيح .

مثال 6

$x^3 - 2$ هي كثيرة الحدود الأصغرية لـ $\sqrt[3]{2}$ على Q ، $x^3 - 2$ هي كثيرة حدود واحدية متحققة بـ $\sqrt[3]{2}$. حسب اختبار أيزنستن $x^3 - 2$ غير قابلة للتحليل على Q وعليه لا توجد كثيرة حدود على Q درجتها أقل من 3 متحققة بـ $\sqrt[3]{2}$ (نظرية 13-18) . وهكذا فإن $x^3 - 2$ هي كثيرة الحدود الأصغرية لـ $\sqrt[3]{2}$ على Q .

نظرية 13-18 تبين أن كثيرة الحدود الأصغرية لـ $a \in K$ على F وحيدة . تذكر تعريف عنصر غير قابل للتحليل على ساحة تامة D بعنصر محايد . ندعي أن كثيرة الحدود الأصغرية $P(x)$ لعنصر جبري a في K على F هو عنصر غير قابل للتحليل . لاحظ أولاً أن $\deg p(x) > 0$ وعليه فإن $P(x)$ ليست بوحدة .

ليكن $p(x) = q(x)\, s(x)$ لبعض كثيرتي حدود غير صفريتين $p(x)$ ، $s(x)$ في $F[x]$. عندئذ $p(a) = q(a)\, s(a) = 0$ يعطينا $q(a) = 0$ أو $s(a) = 0$. عليه $p(x) \mid q(x)$ أو $p(x) \mid s(x)$ ، بما أن $p(x) \mid q(x)$ أو $p(x) \mid s(x)$ ، $p(x)$ إما مترافقة مع $q(x)$ أو مترافقة مع $s(x)$. هذا يبين أن $p(x)$ عنصر غير قابل للتحليل . تذكر أيضاً أنه في ساحة تامة D والتي هي PID إذا كان p عنصر غير قابل للتحليل في D فإن لأي $a \in D$ إما $p \mid a$ أو أن HCF (العامل المشترك الأكبر) لـ a و p هو 1 . أي أن $p\lambda + a\mu = 1$ لبعض $\lambda, \mu \in D$. كحالة خاصة لأية $f(x) \in F[x]$ أما $p(x) \mid f(x)$ أو توجد كثيرتي حدود $A(x), B(x)$ في $F[x]$ بحيث $p(x)\, A(x) + f(x)\, B(x) = 1$.

والآن نبرهن الآتي :

نظرية 13-20

العنصر a في K يكون جبرياً على F إذا وفقط إذا كان $[F(a) : F]$ عدداً منتهياً.

البرهان

ليكن $[F(a) : F] = n$ حيث n عدد صحيح موجب . عندئذ أي $n + 1$ في عناصر $F(a)$ تكون مرتبطة خطياً على F ، بالأخص $1, a, a^2, \ldots, a^n$ مرتبطة خطياً على F . وعليه يوجد $\alpha_0, \alpha_1, \ldots \alpha_n \in F$ ليس جميعها صفراً ، بحيث :

$$\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n = 0$$

هذا يبرهن أن a عنصر جبري على F .

بالعكس ليكن a عنصراً جبرياً على F و $p(x)$ كثيرة الحدود الأصغرية للعنصر a على F . ليكن $n = \deg p(x)$. اعتبر أي عنصر غير صفري $f(a) = \alpha_0 + \alpha_1 a + \ldots + \alpha_n a^n$ في $F[a]$ ، عندئذ $p(x)$ لا يقسم $f(x)$. وبالتالي توجد $A(x)$ و $B(x)$ بحيث $p(x)\,A(x) + f(x)\,B(x) = 1$ (انظر الملاحظات السابقة لهذه النظرية).

هذا يعطي $1 = p(a)\,A(a) + f(a)\,B(a) = f(a)\,B(a)$ (لأن $p(0) = 0$) . وعليه $[f(a)]^{-1} = B(a) \in F[a]$. وبالتالي فإن $F[a]$ حقل .

من ناحية أخرى $F(a)$ هو حقل قواسم $F[a]$. نحصل على $F(a) = F[a]$. الآن اعتبر العناصر $1, a, a^2, \ldots, a^{n-1}$ في $F(a)$ ، إذا وجدت عناصر $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1} \in F$ ليس جميعها صفراً بحيث :

$$\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_{n-1} a^{n-1} = 0$$

فإن a تحقق كثيرة حدود ذات درجة $< n =$ درجة كثيرة الحدود الأصغرية . هذا تناقض . وبذلك فإن $1, a, a^2, \ldots, a^{n-1}$ مستقلة خطياً على F .

اعتبر $f(a) = \beta_0 + \beta_1 a + \beta_2 a^2 + \ldots + \beta_m a^m \in F[a] = f(a)$ حيث $f(x) = \beta_0 + \beta_1 x + \ldots + \beta_m x^m$. حسب خوارزمية القسمة توجد كثيرتي حدو $q(x)$ ، $r(x)$ بحيث

$$f(x) = q(x)\,p(x) + r(x)$$

حيث $r(x) = 0$ أو $\deg r(x) < \deg p(x)$

وبما أن $p(a) = 0$ فإن $f(a) = q(a)\,p(a) + r(a) = r(a)$ ولأن $r(x) = 0$ أو $\deg r(x) < \deg p(x)$ يكون : $r(x) = \delta_0 + \delta_1 a + \ldots + \delta_{n-1} a^{n-1}$ لبعض $\delta_i \in F$ ، وعليه فإن $f(a) = r(a) = \delta_0 + \delta_1 a + \ldots + \delta_{n-1} a^{n-1}$ والذي يبين أن $f(a)$ تركيب خطي

من العناصر $1, a, \ldots, a^{n-1}$ ، أي أن $\{1, a, a^2, \ldots, a^{n-1}\}$ قاعدة للحقل $F(a)$ على F .
بالتالي فإن $[F(a) : F] = n$ ، وهو منته . □

نظرية 13-21

كل توسيع منته لحقل هو توسيع جبري .

البرهان

ليكن K توسيعاً منتهياً للحقل F و $[K : F]$. لأي $a \in K$ فإن $F(a)$ حقل جزئي من K . ولكن $[F(a) : F] \mid n$ ، عليه فإن $[F(a) : F]$ عدد منته ، أي أن a عنصر جبري على F (نظرية 13-20) . بالتالي فإن K توسيع جبري للحقل F . □

ملاحظة 1 عكس النظرية السابقة ليس صحيحاً . في هذا السياق انظر مثال 15 .

ملاحظة 2 ليكن F_1 حقل بحيث $F \subseteq F_1 \subseteq K$. افرض أن العنصر $a \in K$ جبري على F . حيث أن كل كثيرة حدود على F هي كثيرة حدود على F_1 ، فإن a عنصر جبري على F_1 أيضاً . أي أنه إذا كانت $p(x)$ كثيرة الحدود الأصغرية للعنصر a على F و $p_1(x)$ كثيرة الحدود الأصغرية للعنصر a على F_1 ولأن $p(x) \in F_1[x]$ نحصل على $p_1(x) \mid p(x)$ في $F_1[x]$ ومنها نستنتج أن $\deg p_1(x) \leq \deg p(x)$. من جهة أخرى نعلم أن $[F(a) : F] = \deg p(x)$ و $[F_1(a) : F_1] = \deg p_1(x)$ ولذلك فإن $[F_1(a) : F_1] \leq [F(a) : F]$.

والآن نبرهن النظرية المهمة الآتية .

نظرية 13-22

إذا كان L توسيعاً جبرياً للحقل K ، و K توسيع جبري للحقل F ، فإن L توسيع جبري للحقل F .

البرهان

ليكن a عنصراً في L . بما أن L توسيع جبري للحقل K ، يوجد بعض $\alpha_i \in K$ $(i = 1, 2, \dots, n)$ و $1 \le n$ بحيث :

$$a^n + \alpha_1 a^{n-1} + \alpha_2 a^{n-2} + \dots + \alpha_n = 0$$

لنأخذ $F_0 = F$ و $F_i = F_{i-1}(\alpha_i)$ لكل $1 \le i \le n$.

بما أن كل α_i عنصر جبري على F ، و $F \subseteq F_{i-1} \subseteq K$ فإن α_i جبري على F_{i-1} أيضاً وأن $[F_i : F_{i-1}] \le [F(\alpha_i) : F]$ (ملاحظة 2 السابقة) .

هذا يؤدي إلى أن $[F_i : F_{i-1}]$ منته .

العلاقة $[F_n : F] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}]\dots[F_1 : F]$ تبين أن $[F_n : F]$ منته . الآن $\alpha_i \in F_n$ لكل $i = 1, 2, \dots, n$ ، وكذلك a عنصر جبري على F_i لأنه يحقق كثيرة حدود غير صفرية بمعاملات في F_n . إذاً $[F_n(a) : F_n]$ عدد منته . فإن $[F_n(a) : F] = [F_n(a) : F_n][F_n : F]$ يؤدي إلى أن $[F_n(a) : F]$ عدد منته . عليه $F_n(a)$ توسيع جبري للحقل F (نظرية 13-21) . وبالتالي a عنصر جبري على F لأن $a \in F_n(a)$ ، وبذلك L توسيع جبري للحقل F . □

نظرية 13-23

المجموعة S التي تضم عناصر K الجبرية على F هي حقل جزئي من K تحوي F ولا يوجد عنصر a في K جبري على S ولا ينتمي إلى S .

البرهان

بما أن كل $\alpha \in F$ يحقق كثيرة الحدود $x - \alpha$ على F ، عليه فإن $\alpha \in S$ وهكذا فإن $F \subseteq S$. اعتبر $a, b \in S$ فإن كل من $[F(a) : F]$ و $[F(b) : F]$ عدد منته ، وحيث أن b عنصر جبري على F ، فإن b جبري على $F(a)$. وبالتالي $[F(a, b) : F(a)]$ عدد منته . هذا يؤدي إلى أن $[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F]$ منته . وعليه فإن $F(a, b)$ توسيع جبري للحقل F . الآن $a - b \in F(a, b)$ ، عليه $a - b$ جبري على F و $a - b \in S$. بطريقة مشابهة إذا كان $b \neq 0$ فإن $ab^{-1} \in S$. وهكذا فإن S حقل جزئي من K يحوي F وهذا يكمل الإثبات الجزء الأول من النظرية . في المناقشة السابقة إذا أخذنا S بدلاً من F فإن S_1 ، مجموعة جميع عناصر K الجبرية على S تكون حقلاً جزئياً من K يحوي S . وعليه فإن S_1 توسيع جبري للحقل S و S جبري للحقل F . وهكذا فإن S_1 توسيع جبري للحقل F (نظرية 13-22) إذاً $S \subseteq S_1$ وعليه $S = S_1$. إذا كان $a \in K$ أي عنصر جبري على S فإنه حسب تعريف S_1 فإن $a \in S_1$ وبالتالي $a \in S$ لأن $S = S_1$ بالتالي لا يوجد عنصر في K يكون جبرياً على S ولا ينتمي إلى S .

نتيجة 13-23

إذا كان a, b أي عنصرين في K جبريين على F فإن :

(i) $a + b$ ، ab هما جبريان على F .

(ii) إذا كان $b \neq 0$ فإن ab^{-1} جبري على F .

البرهان

يتبع من الحقيقة $a - b$ ، ab^{-1} عنصران في S و S توسيع جبري للحقل F . □

بإمكاننا تفسير النظرية السابقة بالقول أن S أكبر توسيع جبري ممكن لـ F في K ، وأن S مغلق جبرياً بالنسبة إلى K ، بمعنى أنه لا يوجد توسيع جبري فعلي للحقل S في K . هذا يجعلنا أن نسمي S بالانغلاق الجبري لـ F نسبة إلى K . كحالة خاصة عندما يكون K نفسه توسيع جبري للحقل F فإن $S = K$.

دعنا ننظر بإمعان للحقل $F(a)$. عندما يكون $a \in K$ جبرياً على F . لقد أثبتنا في البداية (نظرية 13-18) أنه إذا كانت $p(x)$ كثيرة الحدود الأصغرية لـ a على F فلأي $F[x] \ni f(x)$ فإن $f(a) = 0$ إذا وفقط إذا كانت $f(x) \in < p(x) >$. الآن الراسم $\sigma : F[x] \to F[a]$ المعرف كالآتي $\sigma[g(x)] = g(a)$ لكل $g(x) \in F[x]$ هو هومومورفزم فوقي . من الواضح أن $g(x) \in \ker \sigma$ إذا وفقط إذا كان $g(a) = 0$. وبذلك $\ker \sigma = < p(x) >$. وهكذا وحسب النظرية الأساسية للهومومورفزم ، نحصل على $\frac{F[x]}{< p(x) >} \cong F[a]$. من ناحية أخرى $F[a] = F(a)$ (كما برهنا خلال إثبات نظرية 20-13) . أي أن $\frac{F[x]}{< p(x) >} \cong F(a)$ وبذلك حصلنا على النتيجة الآتية .

نظرية 13-24

إذا كان أي عنصر a في K جبرياً على F وكانت $p(x)$ كثيرة الحدود الأصغرية للعنصر a على F فإن $\frac{F[x]}{< p(x) >} \cong F(a)$. □

ملاحظة

في الأيزومورفزم $\eta : \frac{F[x]}{< p(x) >} \to F(a)$ نجد أن :

$\eta\left[\overline{g(x)}\right] = g(a) \quad \forall\, g(x) \in F[x]$. عليه وبالأخص لكل $\alpha \in F$ $\eta(\overline{\alpha}) = \alpha$ [لأنه إذا كان $g(x) = \alpha$ فإن $g(a) = \alpha$] .

نظرية 13-25

إذا كـان أي عنصرين a و b في K يحققـان نفـس كثيرة الحـدود الأصـغرية $p(x)$ علـى F ، فإنـه يوجـد أيزومـورفزم σ مـن $F(a)$ علـى $F(b)$ بحيـث $\sigma(\alpha) = \alpha$ لجميـع $\alpha \in F$ وأن $\sigma(a) = b$ ، بمعنى آخر σ يبقي عناصر F ثابتاً وينقل a على b .

البرهان

حسـب نظريـة 13-24 يوجـد أيزومـورفزم η_1 مـن $\dfrac{F[x]}{< p(x) >}$ علـى $F(a)$ و η_2 مـن $\dfrac{F[x]}{< p(x) >}$ علـى $F(b)$ بحيـث لكـل $f(x) \in F[x]$ فـإن $\eta_1\left[\overline{f(x)}\right] = f(a)$ و $\eta_2\left[\overline{f(x)}\right] = f(b)$ فإن $\sigma = \eta_2\eta_1^{-1}$ هو أيزومورفزم من $F(a)$ على $F(b)$ بحيث :

$$\sigma(\alpha) = \eta_2\eta_1^{-1}(\alpha = \eta_2(\overline{\alpha}) = \alpha \quad \text{لكل} \quad \alpha \in F$$

و $\sigma(a) = \eta_2\eta_1^{-1}(a) = \eta_2(\overline{x}) = b$.

قضية 13-26 (نظرية العامل)

أي عنصر $a \in K$ هو جذر لكثيرة حدود $f(x)$ على F ذات درجة موجبة إذا وفقط إذا كان $(x - a) \mid f(x)$ في $K[x]$.

البرهان

بمـا أن $f(x) \in K[x]$ ، فـإن $x - a \in K[x]$ ، حسـب خوارزميـة القسـمة توجـد كثيرتي حـدود وحيـدتان $q(x), r(x) \in F[x]$ بحيـث $f(x) = (x - a)\,q(x) + r(x)$ وأنـه إمـا $r(x) = 0$ أو $\deg r(x), < \deg(x - a) = 1$. بالتالي فإن $r(x) = c$ لبعض $c \in K$ ونحصل على أن :

$$f(x) = (x - a)\,q(x) + c \qquad (1)$$

ليكن a جذراً لكثيرة الحدود $f(x)$. فإن $f(a) = 0$ وبتعويض a بدلاً من x في (1) نحصل على
$$0 = f(a) = (a - a)\, q(a) + c$$
أي أن $c = 0$. عليه فإن $f(x) = (x - a)\, q(x)$ أن $(x - a) \mid f(x)$.

وبالعكس إذا كان $(x - a) \mid f(x)$ في $K[x]$ فإن $f(x) = (x - a)\, g(x)$ لبعض $g(x) \in K[x]$. إذاً $f(a) = (a - a)\, g(a) = 0$ وأن a جذر لكثيرة الحدود $f(x)$. □

تعريف 13-27

إذا كان العنصر $a \in K$ جذراً لكثيرة حدود غير صفرية $f(x)$ على حقل جزئي F في الحقل K ، فإنه يقال عن a أنه جذر بتكرار m إذا كان $(x - a)^m \mid f(x)$ ولكن $(x - a)^{m+1} \nmid f(x)$ في $K[x]$. إذاً إذا كان a جذراً بتكرار m في K ، فإن $f(x) = (x - a)^m q(x)$ لبعض $q(x) \in K[x]$. إذا كان a جذراً لكثيرة الحدود $q(x)$ ، عندئذ وحسب القضية 13-26 فإن $(x - a) \mid q(x)$ وهذا بدوره يؤدي إلى $(x - a)^{m+1} \mid f(x)$. هذا يناقض فرضية أن a جذر تكراره m في K أي أن $q(a) \neq 0$.

السؤالين التاليين حول الجذور لهما صلة بالموضوع .

1- إذا كانت $f(x) \in F[x]$ كثيرة حدود ذات درجة موجبة ، فكم جذراً يمكن أن يكون لها في F ؟

2- هل يوجد حقل توسيع للحقل F بحيث يكون لكثيرة الحدود $f(x)$ أكبر عدد ممكن من الجذور ؟ وما هو هذا العدد الأكبر ؟

السؤال (1) إجابته بالنظرية التالية :

نظرية 13-28

كثيرة حدود درجتها $n \geq 1$ على الحقل F لا يمكن أن يكون لها أكثر من n جذراً في أي حقل توسيع للحقل F .

البرهان

لتكن $f(x)$ كثيرة حدود درجتها $n \geq 1$ في $F[x]$. نطبق الاستنتاج على n . ليكن $n = 1$ فإن $f(x) = \alpha x + \beta$ لبعض $\alpha, \beta \in F$ و $\alpha \neq 0$. إذاً $-\beta\alpha^{-1}$ هو الجذر الوحيد لكثيرة الحدود $f(x)$ في أي حقل توسيع للحقل F . وبذلك فإن النتيجة متحققة عندما $n = 1$. لتطبيق الاستنتاج الرياضي ، نفرض أن $n > 1$ والنتيجة متحققة لجميع كثيرات الحدود ذات درجة موجبة $< n$ على أي حقل . ليكن K حقل توسيع للحقل F . إذا كان K لا يحوي أي جذر لكثيرة الحدود $f(x)$ فإن النتيجة متحققة . افرض أن $a \in K$ جذر لكثيرة الحدود $f(x)$ ، بتكرار $m \geq 1$ في K فإن $f(x) = (x-a)^m f_1(x)$ لبعض $f_1(x) \in K[x]$.

الآن $\deg f_1(x) = n - m < n$ وبذلك لا يمكن أن يكون لكثيرة الحدود $f_1(x)$ أكثر من $n - m$ جذراً في K . بالتالي فإنه لا يمكن أن يكون لكثيرة الحدود $f(x)$ أكثر من $n = (n-m) + m$ جذراً في K . $\square$

بعد إجابتنا على السؤال الأول ، نركز اهتمامنا للسؤال الثاني . دعنا نتذكر أنه إذا كان $a \in K$ أي عنصر جبري على F ، فإن كثيرة الحدود الأصغرية $p(x)$ للعنصر a على F غير قابلة للتحليل وأن $\deg p(x) \geq 2$ طالما $a \notin F$.

نأخذ أولاً عكس النظرية السابقة .

نظرية 13-29 (كرونيكر)

إذا كانت $p(x)$ كثيرة حدود غير قابلة للتحليل على F ، عندئذ يوجد توسيع E للحقل F بحيث $[E : F] = \deg p(x)$ وأن $p(x)$ له جذر في E .

البرهان

لما كانت $p(x)$ غير قابلة للتحليل ، $V =< p(x) >$ مثالي أعظمي للحلقة $F[x]$. فإن $\frac{F[x]}{V}$ حقل . لنأخذ $E = \frac{F[x]}{V}$ ونعرف الراسم $\sigma : F \to E$ كالآتي :

$$\sigma(\alpha) = \overline{\alpha} = \alpha + V \in E, \quad \forall \alpha \in F$$

σ عبارة عن هومومورفزم حلقة . وحيث أن درجة كل كثيرة حدود غير صفرية في $V = < p(x) >$ أكبر من أو يساوي 1 ، فإن $\overline{0} \neq \overline{\alpha}$ عندما $\alpha \neq 0$.

أي أن σ مونومورفزم وبالتالي (E, σ) توسيع للحقل F . حسب اتفاقنا فإننا لا نميز بين F وصورته $\sigma(F)$ في E وكل α في F مع $\overline{\alpha}$ في E . ليكن :

$$p(x) = \alpha_0 + \alpha_1 x + ... + \alpha_n x^n, \alpha_n \neq 0, \alpha_i \in F$$

فإن $\overline{0} = \overline{p(x)} = \alpha_0 + a_1\overline{x} + \alpha_2(\overline{x})^2 + ..\alpha_n(\overline{x})^n$ هذا يبين أن $\overline{x}$ جذر لكثيرة الحدود $p(x)$. وعليه فإن E يحوي جذراً لكثيرة الحدود $p(x)$ ، وهذا مباشرة يؤدي إلى أن $[E : F] \geq \deg p(x) = n$.

الآن لأية $f(x) \in F[x]$ يمكننا كتابة $f(x) = p(x)\, q(x) + r(x)$ لبعض $q(x), r(x) \in F[x]$ مع $r(x) = 0$ أو $\deg r(x) < \deg p(x)$ نحصل على $\overline{f(x)} = \overline{r(x)}$ لأن $\overline{p(x)} = \overline{0}$. لما كان $r(x) = 0$ أو $\deg r(x) < \deg p(x)$ يمكننا كتابة $r(x) = \beta_0 + \beta_1 x + ... + \beta_{n-1}x^{n-1}$ لبعض $\beta_i \in F$ و $i = 0, 1, ..., n-1$ وعليه :

$$\overline{f(x)} = \overline{r(x)} = \beta_0 + \beta_1\overline{x} + ... + \beta_{n-1}(\overline{x})^{n-1}$$

هذا يبين أن كل عنصر من E تركيب خطي من $\bar{I}, \overline{x}, (\overline{x})^2, ..., (\overline{x})^{n-1}$.

وعليه فإن $[E : F] \leq n$ وكما برهنا سابقاً فإن $[E : F] \geq n$ وبالتالي نحصل على $[E : F] = n$. □

الآن نحن على استعداد لإعطاء إجابة كاملة للسؤال 2 .

نظرية 13-30

إذا كانت $f(x)$ أية كثيرة حدود درجتها $n \geq 1$ على الحقل F ، عندئذ يوجد حقل توسيع E للحقل F وأن $f(x)$ لها n جذراً في E و $[E : F] \leq n!$.

البرهان

البرهان يعتمد على الاستنتاج على درجة كثيرة الحدود $f(x)$. ليكن $\deg f(x) = 1$ فإن $f(x)$ هي بالصيغة $\alpha x + \beta$ لبعض $\alpha, \beta \in F$ مع كون $\alpha \neq 0$ وجذره الوحيد هو $-\beta\alpha^{-1}$ والذي ينتمي إلى F . هنا نأخذ $E = F$ وعليه نجد أن النتيجة صحيحة عندما $\deg f(x) = 1$. لتطبيق الاستنتاج افرض أن النتيجة صحيحة لأية كثيرة حدود درجتها $< n$ على أي حقل . لنفرض $p(x)$ عامل غير قابل للتحليل لكثيرة الحدود $f(x)$ ولتكن درجتها m . عندئذ $m \leq n$ ويوجد حقل توسيع E' للحقل F بحيث $p(x)$ لها جذراً ، وليكن a في E' و $[E' : F] = m$ (نظرية 13-29) . فإن a جذر كثيرة الحدود $f(x)$ أيضاً ، و $f(x) = (x - a) f_1(x)$ لبعض $f_1(x) \in E'(x)$ [لماذا ؟] . الآن $\deg f_1(x) = 1 < n$. وبالتالي باستخدام فروض الاستنتاج يوجد حقل توسيع E للحقل E' بحيث $f_1(x)$ لها $n - 1$ جذراً في E و $[E : E'] \leq (n - 1)!$ وأيضاً $a \in E$. حيث أن الجذور الـ n لكثيرة الحدود $f(x)$ هي a و $n - 1$ من جذور $f_1(x)$ نستنتج أن جميع جذور $f(x)$ وعددها n تقع في E . كذلك :

$$[E : F] = [E : E'][E' : F] \leq (n - 1)!\, n = n!$$

ملاحظة في النظرية السابقة إذا كانت $a_1, a_2, \dots, a_n$ هي جذور $f(x)$ في K وعددها n ، فإن $F(a_1, a_2, \dots, a_n)$ هو حقل جزئي من E يحوي F بحيث لا يوجد أي حقل جزئي فعلي K للحقل $F(a_1, a_2, \dots, a_n)$ يحوي F وجميع جذور $f(x)$. إضافة إلى ذلك باستخدام الاستنتاج يمكن الإثبات ببساطة أن :

$$f(x) = \alpha(x - a_1)(x - a_2)\dots(x - a_n)$$

لبعض $\alpha(\neq 0) \in F$. عليه فإن :

$f(x) = (\alpha x - \alpha a_1)(x - a_2)\dots(x - a_n)$ عبارة عن ضرب n من العوامل الخطية .

تعريف 13-31

لتكن $f(x)$ أية كثيرة حدود درجتها $n \geq 1$ على الحقل F . فإن حقل التوسيع E للحقل F يسمى حقل انفلاق كثيرة الحدود $f(x)$ إذا كان :

a- $f(x)$ قابلاً للتحليل إلى n من العوامل الخطية على E .

b- لا يوجد أي حقل جزئي فعلي E' من E يحوي F بحيث أن $f(x)$ يمكن تحليله إلى n من العوامل الخطية على E' .

بصورة مكافئة يمكن القول أن E هو حقل انفلاق لكثيرة الحدود $f(x)$ إذا كان E يحوي جذور $f(x)$ و $E = F(a_1, a_2, \ldots, a_n)$ ، الحقل المولد بـ F و n من الجذور $a_1, a_2, \ldots, a_n$ لـ $f(x)$ في E . النظرية السابقة تبين وجود حقل انفلاق وهذه النظرية لا تبين شيئاً عن وجود علاقة بين أي حقلي انفلاق لنفس كثيرة الحدود من عدم وجودها . هذا ما سوف نتناوله الآن .

تذكر أنه إذا كانت R ، R' أي حلقتين بحيث يوجد أيزومورفزم σ من R على R' ، فإنه بالإمكان توسيع σ إلى أيزومورفزم τ من $R[x]$ على $R'[t]$ حيث t, x هما غير محددين بحيث $\tau(x) = t$ إذا كان A أي مثالي للحلقة $R[x]$ فإن $\tau(A)$ مثالي للحلقة $R[t]$ وبإمكاننا تعريف أيزومورفزم $\eta : \dfrac{R[x]}{A} \to \dfrac{R'[t]}{\tau(A)}$ كالآتي :

$\eta[f(x) + A] = \tau[f(x)] + \tau(A)$ لكل $f(x) \in R[x]$. الآن لكل :

$$f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n \in R[x]$$

فإن

$$\tau([f(x)]) = \sigma(\alpha_0) + \sigma(\alpha_1)\, t + \ldots + \sigma(\alpha_n)\, t^n$$

كحالة خاصة نأخذ حقلين F', F ونأخذ أيزومورفزم σ من F على F' و τ الأيزومورفزم الموسع المناظر من $F[x]$ على $F'[t]$. للملائمة لكل $\alpha \in F$ نرمز α' لصورته $\sigma(\alpha)$ ولكل $f(x) \in F[x]$ نرمز $f'(t)$ لصورته $\tau[f(x)]$.

لتكن $p(x)$ أية كثرة حدود غير قابلة للتحليل على F . افرض $p'(t) = r'(t)\, s'(t)$ لبعض كثيرتي حدود $r'(t), s'(t)$ موجبتي الدرجة في $F'(t)$. بما أن τ أيزومورفزم نحصل على أن $r(x), s(x) \in F[x]$ بحيث $r'(t), s'(t)$ هي الصورة المناظرة لـ $r(x), s(x)$ تحت τ . لاحظ أن τ يحافظ على الدرجات وعليه $s(x), r(x)$ كثيرتي حدود ذات درجة موجبة بحيث

$$\tau[p(x)] = \tau[r(x)]\,\tau[s(x)] = \tau[r(x)\, s(x)]$$

وبالتالي $p(x) = r(x)\, s(x)$ و $p(x)$ قابلة للتحليل ، هذا يتعارض مع الفرض أن $p(x)$ غير قابلة للتحليل . وهكذا فإن $p'(t)$ غير قابلة للتحليل . وكما بينا سابقاً فإنه يوجد أيزومورفزم

$$\eta : \frac{F[x]}{< p(x) >} \to \frac{F'[t]}{< p'(t) >}$$

بحيث $\eta[f(x) + < p(x) >] = f'(t) + < p'(t) >$ لكل $f(x) \in F[x]$ والآن نبرهن الآتي .

نظرية 13-32

لتكن $p(x)$ كثيرة حدود غير قابلة للتحليل في $F[x]$ و $p'(t)$ كثيرة الحدود المناظرة في $F'[t]$. افرض أن u و v هما جذري كثيرتي الحدود $p(x)$ و $p'(t)$ على الترتيب في بعض حقلي توسيع E و E' للحقلين F', F على الترتيب ، عندئذ يوجد أيزومورفزم μ من $F(u)$ على $F'(v)$ بحيث $\mu(\alpha) = \alpha'$ لكل $\alpha \in F$ و $\mu(u) = v$.

البرهان

$p'(t)$ غير قابلة للتحليل (حسب الملاحظات التي تسبق هذه النظرية) .

الآن يوجد أيزومورفزم

$$\sigma_1 : \frac{F[x]}{< p(x) >} \to F(u)$$

وأيزومورفزم

$$\sigma_2 : \frac{F'[t]}{< p'(t) >} \to F'(v)$$

بحيث $\sigma_1(f(x) + < p(x) >) = f(u)$ و $\sigma_2(f'(t) + < p'(t) > = f'(v)$. (حسب نظرية 13-24 والملاحظة) إضافة إلى ذلك فإن الراسم

$$\eta : \frac{F[x]}{< p(x) >} \to \frac{F'[t]}{< p'(t) >}$$

المعرف بالصورة $\eta[f(x) + < p(x) >] = f'(t) + < p'(t) >$ هو أيزومورفزم .

لاحظ أن $\sigma_1(x + < p(x) >) = u$ و $\sigma_2(t + < p'(t) >) = v$. الآن $\mu = \sigma_2\eta\sigma_1^{-1}$ هو أيزومورفزم من $F(u)$ على $F'(v)$.

لأي $\alpha \in F$ يكون

$$
\begin{aligned}
\mu(\alpha) &= (\sigma_2\eta\sigma_1^{-1})(\alpha) \\
&= \sigma_2\eta[\alpha + < p(x) >] \\
&= \sigma_2[\alpha' + < p'(t) >] = \alpha' \\
\mu(u) &= (\sigma_2\eta\sigma_1^{-1})(u) = \sigma_2\eta[x + < p(x) >] \\
&= \sigma_2[t + < p'(t) >] = v . \ \square
\end{aligned}
$$

نتيجة 13-33

ليكن $F \subseteq K$ أي حقلان . إذا كان $\alpha, \beta \in K$ لهما نفس كثيرة الحدود الأصغرية $p(x)$ على F ، عندئذ يوجد أيزومورفزم μ من $F(\alpha)$ على $F(\beta)$ بحيث $\mu(\alpha) = \beta$ و $\mu(a) = a$ لكل $a \in F$.

البرهان

في النظرية أعلاه نأخذ $F = F'$ و σ الراسم الذاتي (المحايد) فنحصل على النتيجة . $\square$

تعريف 13-34

يقال لعنصرين a, b في K أنهما مترافقان على حقل جزئي F من K إذا كانا جبريان على F ولهما نفس كثيرة الحدود الأصغرية على F .

مثال 7

$\sqrt{3}$ و $-\sqrt{3}$ عنصران من $I\!R$ مترافقان على Q لأن $x^2 - 3$ هي كثيرة الحدود الأصغرية على Q لكل من $\sqrt{3}$ و $-\sqrt{3}$.

مثال 8

$\sqrt[3]{2}$ ، $\sqrt[3]{2\omega}$ ، $\sqrt[3]{2\omega^2}$ حيث $\omega^2 + \omega + 1 = 0$ هي عناصر في C مترافقة على Q . العناصر الثلاثة لها نفس كثيرة الحدود الأصغرية $x^3 - 2$ على Q .

نظرية 13-35

ليكن $F \overset{\sigma}{\cong} F'$ ولتكن $f(x)$ أية كثيرة حدود درجتها ≥ 1 على F و $f'(t)$ كثيرة الحدود المناظرة على F' . إذا كان E', E حقلي انفلاق $f(x)$ و $f'(t)$ على F و F' على الترتيب ، فإنه يوجد أيزومورفزم ψ من E على E' بحيث $\psi(\alpha) = \alpha'$ لكل $\alpha \in F$.

البرهان

ليكن $\deg f(x) = n$. لاحظ أن درجة $[E : F]$ منته . نستخدم الاستنتاج على $[E : F]$. افرض $[E : F] = 1$ عندئذ $E = F$ وجميع الجذور $a_1, a_2, \ldots, a_n$ لـ $f(x)$ وعددها n تقع في F ، بالإضافة إلى $f(x) = \alpha(x - a_1)(x - a_2)$ لبعض $\alpha(\neq 0) \in F$. فإن $f'(t) = \alpha'(t - a_1')(t - a_2')\ldots(t - a_n')$ فنحصل على أن $a_1', a_2', \ldots, a_n'$ تقع كلها في F' . وعليه $E' = F'$.

عندئذ بإمكاننا أخذ ψ بأن يكون الأيزومورفزم σ من F على F' . عليه فإن النتيجة متحققة عندما $[E : F] = 1$. لتطبيق الاستنتاج افرض $[E : F] > 1$ ونفرض أن النتيجة صحيحة لجميع حقول الانفلاق E على أي حقل F درجته $< [E : F]$. بما أن $[E : F] > 1$ فإنه على الأقل أحد جذور $f(x)$ وليكن u لا يقع في F . إذا كان $p(x)$ كثيرة الحدود الأصغرية للعنصر u على F فإن $\deg g(x) > 1$. لتكن $p'(t)$ كثيرة الحدود المناظرة على F' . كثيرة الحدود $p'(t)$ غير قابلة للتحليل . وحيث أن $p(x) \mid f(x)$ نحصل

على أن $f(x) = p(x)\,q(x)$ لبعض $q(x) \in F[x]$ وبالتالي فإن $f'(t) = p'(t)\,q'(t)$. ليكن v جذراً لـ $p'(t)$ في E' . يوجد أيزومورفزم $\theta : F(u) \to F'(v)$ بحيث $\theta(\alpha) = \sigma(\alpha) = \alpha', \quad \forall \alpha \in F$ و $\theta(u) = v$ (نظرية 13-32) .

الآن $f(x) = (x - u) f_1(x)$ و $f'(t) = (t - v) g_1(t)$ لبعض $f_1(x) \in F(u)[x]$ و $g_1(t) \in F'(v)[t]$. إذا كان θ_1 يرمز للأيزومورفزم من $F(u)[x]$ على $F'(v)[t]$ بحيث أن θ_1 توسيعاً للأيزومورفزم θ و $\theta_1(x) = t$ فإن :

$$f'(t) = \theta_1[f(x)] = \theta_1[(x - u) f_1(x)] = (t - v)\,\theta_1[f_1(x)]$$

وهذا يعطينا $\theta_1[f_1(x)] = g_1(t)$ لأن $f'(t) = (t - v)\,g_1(t)$.

إضافة إلى ذلك لكون E يحوي كل جذور $f(x)$ وعددها n فإن E يحوي كل جذور $f_1(x)$ وعددها $n - 1$. إذا كان E_1 حقل انفلاق $f_1(x)$ على $F(u)$ محتوى في E ، فإنه إضافة إلى احتوائه كل جذور $f_1(x)$ ، E_1 يحوي u أيضاً . بالتالي E_1 يحوي جميع جذور $f(x)$. وعليه حسب تعريف حقل الانفلاق نحصل على أن $E \subseteq E_1$. وهكذا فإن $E = E_1$. وعليه E هو حقل انفلاق $f_1(x)$ على $F(u)$. بصورة مشابهة فإن E' حقل انفلاق $g_1(t)$ على $F'(v)$.

الآن $[E : F] = [E : F(u)][F(u) : F]$ و $[F(u) : F] = \deg f(x) > 1$. والذي يعطينا $[E : F(u)] < [E : F]$. عندئذ وحسب فروض الاستنتاج الرياضي يوجد أيزومورفزم ψ من E على E' وهو توسيع للأيزومورفزم $\theta : F(u) \to F'(v)$ من جهة أخرى θ توسيع لـ σ وبالتالي نجد أن $\psi(\alpha) = \theta(\alpha) = \alpha', \quad \forall \alpha \in F$ وهذا يثبت النظرية . □

إذا أخذنا $F = F'$ وكانت σ الدالة الذاتية نستنتج الآتي :

نتيجة 13-36

إذا كان E' و E حقلي انفلاق لنفس كثيرة الحدود $f(x)$ ذات درجة ≤ 1 على حقل F ، عندئذ يوجد أيزومورفزم ψ من E على E' بحيث $\psi(\alpha) = \alpha$ لكل $\alpha \in F$. □

ليكن a عنصراً جبرياً في K على الحقل F و $p(x)$ كثيرة الحدود الأصغرية العنصرية على F . لكل عنصر غير صفري $f(a) \in F(a)$ حيث $f(x)$ كثيرة حدود على F . بيّنا (نظرية 13-20) أن معكوس $f(a)$ هو بعض كثيرة حدود $g(a) \in F(a)$ ونوضح ذلك في المثال الآتي .

مثال 9

اعتبر الحقل $Q(\sqrt{2})$. حيث أن $3 + \sqrt{2} \in Q(\sqrt{2})$ ، فإن $\frac{1}{3+\sqrt{2}} = \frac{3-\sqrt{2}}{7} = \frac{3}{7} - \frac{1}{7}\sqrt{2}$ هي كثيرة حدود في $\sqrt{2}$ على Q .

مثال 10

اعتبر $1 - \sqrt[3]{2} + \sqrt[3]{4} \in Q[\sqrt[3]{2}] = Q(\sqrt[3]{2})$. لتكن $p(x) = x^3 - 2$ ، $f(x) = x^2 - x + 1$ ، $p(x)$ هي كثيرة الحدود الأصغرية لـ $\sqrt[3]{2}$. لإيجاد معكوس $f(\sqrt[3]{2})$ نجد كثيرتي حدود ، $h(x), g(x)$ بحيث $f(x)\,g(x) + p(x)\,h(x) = 1$. كثيرتي الحدود $h(x)$ ، $g(x)$ يمكن إيجادها بطريقة خوارزمية القسمة . الآن $\deg f(x) < \deg g(x)$ ، بقسمة $p(x)$ على $f(x)$ نحصل على :

$$x^3 - 2 = (x+1)(x^2 - x + 1) - 3$$

عليه فإن

$$(x^3 - 2)\left(-\frac{1}{3}\right) + (x+1)\left(\frac{x^2}{3} - \frac{x}{3} + \frac{1}{3}\right) = 1$$

وبتعويض $x = \sqrt[3]{2}$ نحصل على

$$\frac{(\sqrt[3]{2}+1)}{3}\left(\sqrt[3]{4} - \sqrt[3]{2} + 1\right) = 1$$

أي أن $\frac{\sqrt[3]{2}}{3} + \frac{1}{3} = \left(\sqrt[3]{4} - \sqrt[3]{2} + 1\right)^{-1}$ هي كثيرة حدود في $\sqrt[3]{2}$ على Q .

الآن ندرج كثيرتي حدود أحاديتين مختلفتين وغير قابلتين للتحليل لهما نفس حقل الانفلاق .

مثال 11

اعتبر كثيرتي الحدود $x^2 + x + 1$ ، $x^2 + 3$ على Q وهما من الدرجة الثانية وليس لهما جذور نسبية . وبالتالي فهما غير قابلتان للتحليل (لاحظ بصورة عامة إذا كانت $f(x)$ كثيرة حدود درجتها $3 >$ على حقل F ليس لها جذر في F ، فإنه لا يمكن القول بأن $f(x)$ غير قابلة للتحليل) . جذرا $x^2 + 3$ هما $\pm\sqrt{-3}$ ، أي أن $Q\left(\sqrt{-3}\right)$ هو حقل انفلاق $x^2 + 3$.

إذا كان $\omega = \frac{-1 + \sqrt{-3}}{2}$ فإن ω ، ω^2 هما جذري $x^2 + x + 1$ ، وبالتالي فإن $F(\omega)$ هو حقل انفلاق $x^2 + x + 1$ (لماذا ؟) .

والآن $\sqrt{-3} = 2\omega + 1 \in Q(\omega)$ يعطي $Q\left(\sqrt{-3}\right) \subseteq Q(\omega)$.

مرة أخرى $\omega = \frac{1}{2} + \frac{\sqrt{-3}}{2} \in Q\left(\sqrt{-3}\right)$ يعطينا $Q(\omega) \subseteq Q\left(\sqrt{-3}\right)$ وبالتالي فإن $Q(\omega) = Q\left(\sqrt{-3}\right)$.

وهكذا فإن $x^2 + 3$ ، $x^2 + x + 1$ لهما نفس حقل الانفلاق . لاحظ هنا أن $[Q(\omega) : Q] = \deg(x^2 + x + 1) = 2$.

مثال 12

اعتبر كثيرة الحدود $x^3 - 2$ على Q . جذورها في C هي $\alpha = \sqrt[3]{2}$ ، $\omega\alpha$ ، $\omega^2\alpha$ حيث ω هو الجذر التكعيبي التخيلي للواحد الصحيح . ولا واحد من هذه الجذور هو عدد نسبي ، عليه فإن $x^3 - 2$ غير قابلة للتحليل على Q . وهكذا إذا كان E حقل انفلاق كثيرة الحدود $x^3 - 2$ على Q فإن $[E : Q] \le 3! = 6$. الآن

$[Q(\alpha):Q]=3$ ، $[Q(\omega):Q]=2$ لأن $Q(\omega)$ ، $Q(\alpha)$ كلاهما حقل جزئي في E ، نحصل على أن $[E:Q] \mid 3$ و $[E:Q] \mid 2$ ، وبالتالي $[E:Q] \mid 6$. أي أن $[E:Q]=6=3!$.

مثال 13

اعتبر كثيرة الحدود x^3-3x+1 على Q . كثيرة الحدود هذه ليس لها جذراً نسبياً ، عليه فهي غير قابلة للتحليل على Q . جذورها في R هي $-2\cos\frac{\pi}{9}$ ، $2\cos\frac{2\pi}{9}$ ، $2\cos\frac{4\pi}{9}$. ليكن $\alpha=-2\cos\frac{\pi}{9}$. اعتبر $E \subseteq Q(\alpha)$ ، حيث E حقل انفلاق x^3-2x+1 .

الآن

$$2\cos\frac{2\pi}{9} = 4\cos^2\frac{\pi}{9}-2 = \alpha^2-2 \in Q(\alpha)$$

$$2\cos\frac{4\pi}{9} = 4\cos^2\frac{2\pi}{9}-2 = (\alpha^2-2)^2-2 \in Q(\alpha)$$

وعليه فإن جميع جذور x^3-3x+1 تقع في $Q(\alpha)$. وهكذا فإن $E \subseteq Q(\alpha)$. إذاً $E=Q(\alpha)$ بالإضافة إلى ذلك فإن $[E:Q]=[Q(\alpha):Q]$ وهذا يساوي درجة كثيرة الحدود الأصغرية لـ α على Q ويساوي $\deg(x^3-3x+1)$ وهو 3 .

في هذه الحالة $[E:Q]=3<3!$.

مثال 14

اعتبر كثيرة الحدود x^4-1 على Q . جذورها هي $1,-1,i,-1$ حيث $i=\sqrt{-1}$. أي أن حقل انفلاق x^4-1 على Q هو $Q(i)$ وأن $[Q(i):Q]=2$.

مثال 15

تعريف : يقال للعدد المركب α أنه عدد جبري إذا كان جبرياً على Q ، حقل الأعداد النسبية . حيث أن الأعداد الجبرية تكون حقلاً (نظرية 13-23) ، افرض أن A يمثل

حقل الأعداد الجبرية . حسب التعريف ، A هو توسيع جبري للحقل Q . ندعي أن A ليس توسيعاً منتهيا لـ Q . إذا كان كذلك ، افرض أن $[A : Q] = n$.

اعتبر كثيرة الحدود $x^{n+1} - 3$ على Q . حسب اختبار أيزنستن كثيرة الحدود هذه غير قابلة للتحليل على Q . ليكن α جذراً كثيرة الحدود $x^{n+1} - 3$ فإن α جبري على Q وعليه $\alpha \in A$. لما كانت $x^{n+1} - 3$ غير قابلة للتحليل على Q فإن $[Q(\alpha) : Q] = n + 1$ ، ولكن $\alpha \in A$ يؤدي إلى أن $Q(\alpha) \subseteq A$ وهذا غير معقول لأن $Q(\alpha)$ فضاء جزئي من A على Q وأن $[A : Q] = n$. بالتالي فإن الفرض خاطئ . عليه فإن A عبارة عن توسيع غير منته على Q .

المثال السابق يبين أن ليس بالضروري أن يكون توسيع جبري ما توسيعاً منتهياً . في حين كل توسيع منته هو توسيع جبري (نظرية 13-21) .

والآن نناقش العلاقة بين جذور ومعاملات كثيرة الحدود .

نظرية 13-37

إذا كانت $f(x) = \alpha_0 + \alpha_1 x + ... + \alpha_n x^n \in F[x]$ كثيرة حدود درجتها $n \geq 1$ ، جذورها $a_1, a_2, ..., a_n$ تقع في حقل توسيع ما E للحقل F ، فإن :

$$s_1 = \sum_i a_i = -\frac{\alpha_{n-1}}{\alpha_n}, \; s_2 = \sum_{i>j} a_i a_j = \frac{\alpha_{n-2}}{\alpha_n}, \; s_3 = \sum_{i>j>k} a_i a_j a_k = \frac{\alpha_{n-3}}{\alpha_n}$$

وهكذا ... وإن $s_n = a_1 \, a_2 \, ... a_n = (-1)^n \dfrac{\alpha_0}{\alpha_n}$.

البرهان

بما أن $\deg f(x) = n$ ، $\alpha_n \neq 0$ ، عليه $\alpha_n^{-1} = \dfrac{1}{\alpha_n} \in F$ إضافة إلى ذلك لكون $a_1, a_2, ..., a_n$ هي كل جذور $f(x)$ فإن $f(x) = \alpha_2 (x - a_1)(x - a_2) ... (x - a_n)$

هذا يعطينا $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-2}x^{n-2} + \alpha_{n-1}x^{n-1} + \alpha_n x^n$

$$= \alpha_n\left[x^n - s_1 x^{n-1} + s_2 x^{n-2} + \ldots + (-1)^n s_n\right]$$

حيث $s_1 = \sum_i a_i$ ، $s_2 = \sum_{i>j} a_i a_j$ ، $s_3 = \sum_{i>j>k} a_i a_j a_k$ وهكذا إلى أن نصل $s_n = a_1 a_2 \ldots a_n$.

والآن وحيث أن x عنصر متسامي على F فبمقارنة معاملات القوى المتساوية لـ x نحصل على أن $-\alpha_n s_1 = \alpha_{n-1}$ ، $\alpha_n s_2 = \alpha_{n-2}$ و $\alpha_n s_3 = \alpha_{n-3}$ وهكذا إلى أن نصل أخيراً إلى أن $(-1)^n \alpha_n s_n = \alpha_0$.

بما أن α_n وحدة في F نحصل على أن : $s_1 = \frac{-\alpha_{n-1}}{\alpha_n}$ ، $s_2 = \frac{\alpha_{n-2}}{\alpha_2}$ ، $s_3 = \frac{-\alpha_{n-2}}{\alpha_n}$ ... $s_n = (-1)^n \frac{\alpha_0}{\alpha_n}$.

تمارين محلولة

ملاحظة : في جميع هذه التمارين المحلولة K يمثل حقل توسيع لـ F .

تمرين 1

$a, b \in K$ عنصران جبريان على F درجتهما n و m على الترتيب حيث n, m عددان أوليان نسبياً ، برهن أن $F(a, b)$ درجته mn على F .

الحل

لدينا $[F(a) : F] = m$ و $[F(b) : F] = n$. لتكن :

$x^m + \alpha_1 x^{m-1} + \ldots + \alpha_m$ كثيرة الحدود الأصغرية للعنصر a على F .

هذه هي أيضاً كثيرة حدود على $F(b)$. وبالتالي فإن a يحقق كثيرة حدود درجتها m على $F(b)$.

بالتالي فإن $[F(b)(a) : F(b)] \leq m$ أي أن $[F(a,b) : F(b)] \leq m$ ، الآن :

$$[F(a,b) : F] = [F(a,b) : F(b)][F(b) : F] \leq mn \qquad (1)$$

مرة أخرى $[F(a,b) : F] = [F(a,b) : F(a)][F(a) : F] \Rightarrow m \mid [F(a,b)F]$

وبالمثل يكون $[F(a,b) : F] = [F(a,b) : F(b)][F(b) : F] \Rightarrow n \mid [F(a,b) : F]$

لما كان $(m,n) = 1$ نحصل على أن $mn \mid [F(a,b) : F]$ وعليه :

$$mn \leq [F(a,b) : F] \qquad (2)$$

من (1) و (2) نحصل على النتيجة المطلوبة .

تمرين 2

برهن أنه إذا كان $a \in K$ عنصراً جبرياً على F ودرجته عدد فردي ، فإن $F(a) = F(a^2)$.

الحل

من الواضح $a^2 \in F(a) \Rightarrow F(a^2) \subseteq F(a)$

لتكن $p(x) = x^{2n+1} + \alpha_0 x^{2n} + \dots + \alpha_{2n}$ كثيرة الحدود الأصغرية لـ a على F فإن :

$$a^{2n+1} + \alpha_0 a^{2n} + \dots + \alpha_{2n} = 0$$

$$\Rightarrow a(a^{2n} + \alpha_1 a^{2n-1} + \dots + \alpha_{2n-1}) + (\alpha_0 a^{2n} + \alpha_2 a^{2n-2} + \dots + \alpha_{2n}) = 0$$

الآن وحيث أن $[F(a) : F] = 2n+1$ فإن $a^{2n} + \alpha_1 a^{2n-2} + \dots + \alpha_{2n-1} \neq 0$ لذا فإن :

$$a = -(a^{2n} + \alpha_1 a^{2n-2} + \dots + \alpha_{2n-1})^{-1}(\alpha_0 a^{2n} + \alpha_1 a^{2n-2} + \dots + \alpha_{2n}) \in F(a^2)$$

وهكذا نرى أن $F(a) \subseteq F(a^2)$. بالتالي فإن $F(a) = F(a^2)$.

تمرين 3

أوجد درجة حقل انفلاق $x^5 - 3x^3 + x^2 - 3$ على Q .

الحل

الآن $x^5 - 3x^3 + x^2 - 3 = (x^2 - 3)(x^3 + 1)$ يبين أن جذور كثيرة الحدود المعطاة في C هي $\pm\sqrt{3}$ ، -1 ، $\frac{1 \pm i\sqrt{3}}{2}$ ، وعليه فإن حقل انفلاق $x^5 - 3x^3 + x^2 - 3$ على Q هو $K = Q\left(\pm\sqrt{3}, -1, \frac{1 \pm i\sqrt{3}}{2}\right)$.

ندعي أن $K = Q\left(\sqrt{3}, i\right)$ الآن $\frac{1 \pm i\sqrt{3}}{2} \in K$.

$$\Rightarrow \left(\frac{1 + i\sqrt{3}}{2}\right) - \left(\frac{1 - i\sqrt{3}}{2}\right) = i\sqrt{3} \in K$$

كذلك $\sqrt{3} \in K$ وعليه $i \in K$. وهكذا فإن $Q\left(\sqrt{3}, i\right) \subseteq K$. مرة ثانية $\sqrt{3} \in Q\left(\sqrt{3}, i\right) \Rightarrow \pm i\sqrt{3} \in Q\left(\sqrt{3}, i\right)$. وكنتيجة لذلك فإن $\frac{1 \pm i\sqrt{3}}{2} \in Q\left(\sqrt{3}, i\right)$. وعليه فإن $K \subseteq Q\left(\sqrt{3}, i\right)$. وهكذا فإن ادعائنا تحقق .

الآن
$$[K : Q] = \left[K : Q\left(\sqrt{i}\right)\right]\left[Q(i) : Q\right] \leq 2.2 = 4$$

لأن كثيرة الحدود الأصغرية لـ i على Q هي $x^2 + 1$. كذلك :

$[K : Q] = \left[K : Q\left(\sqrt{3}\right)\right] \times \left[Q\left(\sqrt{3}\right) : Q\right]$ يبين أن 2 عامل لـ $[K : Q]$. وعليه فإنه إما $[K : Q] = 2$ أو يساوي 4 في حالة $[K : Q] = 2$ نحصل على أن $\left[K : Q\sqrt{3}\right] = 1$ وهذا يعني أن $K = Q\left(\sqrt{3}\right)$ وهو غير معقول لأن $i \in K$ ولكن $i \notin Q\left(\sqrt{3}\right)$. وعليه فإن $[K : Q] = 4$.

تمرين 4

أوجد حقل انفلاق لكثيرة الحدود $x^p - 1$ على Q حيث p عدد أولي .

الحل

جذور $x^p - 1$ في C هي $1, e^{\frac{2\pi i}{p}}, e^{\frac{4\pi i}{p}}, \ldots, e^{\frac{2(p-1)\pi i}{p}}$. إذا كان $\xi = e^{\frac{2\pi i}{p}}$ فإن حقل الانفلاق $x^p - 1$ على Q هي :

$K = Q(1, \xi, \xi^2, \dots, \xi^{p-1}) = Q(\xi)$ (برهن) .

الآن ξ جذر لكثيرة الحدود $1 + \dots + x^{p-2} + x^{p-1} = \dfrac{x^p - 1}{x - 1}$.

ولكن هذه هي كثيرة الحدود الأصغرية لـ ξ على Q (انظر مثال 30 ، الفصل العاشر) وعليه $[Q(\xi) : Q] = p - 1$ أو بمعنى آخر $[K : Q] = p - 1$.

تمرين 5

يقال لحقل F أنه مغلق جبرياً إذا كانت كل كثيرة حدود غير ثابتة في $F[x]$ تنفلق كلياً (بمعنى أن جميع جذورها) في F . برهن أن الحقل المغلق جبرياً لا يمكن أن يكون منتهياً .

الحل

افرض F حقل منته مغلق جبرياً . ليكن $F = \{a_1, a_2, \dots a_n\}$. اعتبر كثيرة الحدود $f(x) = 1 + \prod_{i=1}^{n} (x - a_i) \in F[x]$. يجب أن تكون كل جذورها في F لأن F مغلق جبرياً . ولكن أي واحد من a_i ليس جذراً لـ $f(x)$. وعليه نحصل على تناقض ، أي أنه لا يمكن أن يكون F منتهياً .

تمرين 6

ليكن F حقلاً بمميز يختلف عن 2 وليكن $\alpha, \beta \in F$ عنصران بحيث $x^2 - \beta, x^2 - \alpha$ غير قابلتان للتحليل على F . إذا كان K حقل انفلاق $f(x) = (x^2 - \alpha)(x^2 - \beta)$ على F ، عندئذ برهن أن $[K : F]$ يساوي إما 2 أو 4 حسبما $x^2 - \alpha^{\beta}$ قابل للتحليل أو غير قابلة للتحليل على F .

الحل

جذور $f(x)$ في أي حقل توسيع للحقل F هي $\pm\sqrt{\alpha}$ ، $\pm\sqrt{\beta}$. وعليه $K = F\left(\pm\sqrt{\alpha}, \pm\sqrt{\beta}\right) = F\left(\sqrt{\alpha}, \sqrt{\beta}\right)$.

الآن $\left[F\left(\sqrt{\alpha}, \sqrt{\beta}\right) : F\left(\sqrt{\alpha}\right)\right] \leq 2$. في حالة $x^2 - \alpha\beta$ قابلة $\left[F\left(\sqrt{\beta}\right) : F\right] = 2 \Rightarrow$ للتحليل على F يكون لدينا $\sqrt{\alpha\beta} \in F$ وهذا بدوره يؤدي إلى أن $\sqrt{\alpha\beta} \in F(\alpha)$. ولكن $\sqrt{\alpha} \in F\left(\sqrt{\alpha}\right)$ عليه $\sqrt{\beta} \in F\left(\sqrt{\alpha}\right)$. كنتيجة لذلك $\left[F\left(\sqrt{\alpha}, \sqrt{\beta}\right) : F\left(\sqrt{\alpha}\right)\right] = 1$ وهكذا فإن

$$[K : F] = \left[F\left(\sqrt{\alpha}, \sqrt{\beta}\right) : F\left(\sqrt{\alpha}\right)\right]\left[F\left(\sqrt{\alpha}\right) : F\right] = 2$$

افرض الآن أن $x^2 - \alpha^n$ غير قابلة للتحليل على F .

لأن $\sqrt{\alpha\beta}$ جذر لـ $x^2 - \alpha\beta$ على $F\left(\sqrt{\alpha}\right)$ ، نحصل على :

$\left[F\left(\sqrt{\alpha\beta}, \sqrt{\alpha}\right) : F\left(\sqrt{\alpha}\right)\right] \leq 2$. إذا كان $\left[F\left(\sqrt{\alpha\beta}, \sqrt{\alpha}\right) : F\left(\sqrt{\alpha}\right)\right] = 1$ نحصل على $\sqrt{\alpha\beta} \in F\left(\sqrt{\alpha}\right)$.

$$\Rightarrow \sqrt{\alpha\beta} = a + b\sqrt{\alpha}, a, b \in F \Rightarrow \alpha\beta = a^2 + \alpha b^2 + 2ab\sqrt{\alpha}$$
$$\Rightarrow 2ab\sqrt{\alpha} = \alpha\beta - a^2 - \alpha b^2 \in F \Rightarrow \sqrt{\alpha} \in F$$

(لأن $b \neq 0, a \neq 0$ و $Char\ F \neq 2$)

(لاحظ أن $a = 0 \Rightarrow \sqrt{\beta} = b \in F$ وهو يؤدي إلى أن $x^2 - \beta$ قابلة للتحليل على F . في حين إذا كان $b = 0$ نحصل على أن $\sqrt{\alpha\beta} = a$ والذي يبين أن $x^2 - \alpha\beta$ قابلة للتحليل على F!) .

هذا بدوره يؤدي إلى أن $x^2 - \alpha$ قابلة للتحليل على F ، وهذا تعارض . بالتالي فإن $\left[F\left(\sqrt{\alpha\beta}, \sqrt{\alpha}\right) : F\left(\sqrt{\alpha}\right)\right] = 2$. ولكن $F\left(\sqrt{\alpha\beta}, \sqrt{\alpha}\right) \subseteq F\left(\sqrt{\alpha}, \sqrt{\beta}\right)$ عليه $\left[F\left(\sqrt{\alpha}, \sqrt{\beta}\right) : F\left(\sqrt{\alpha}\right)\right] \geq 2$. أي أن $\left[F\left(\sqrt{\alpha}, \sqrt{\beta}\right) : F\left(\sqrt{\alpha}\right)\right] = 2$ نتيجة لذلك نجد أن $[K : F] = 4$.

تمرين 7

برهن أن $\sqrt[3]{5} + \sqrt{2}$ جبري على Q ذو درجة 6 .

الحل

ضع $\alpha = \sqrt{2} + \sqrt[3]{5}$. هذا يؤدي إلى :

$$\alpha - \sqrt{2} = \sqrt[3]{5} \Rightarrow \left(\alpha - \sqrt{2}\right)^3 = 5 \Rightarrow \alpha^3 + 6\alpha - 3 = (3\alpha^2 + 2)\sqrt{2}$$
$$\Rightarrow (\alpha^3 + 6\alpha - 5)^2 = 2(3\alpha^2 + 2)^2$$

والذي يؤدي إلى أن α جبري على Q ذو درجة أقل أو يساوي 6 . لكي نبرهن الجزء الثاني ندعي أن $Q\left(\sqrt{2} + \sqrt[3]{5}\right) = Q\left(\sqrt{2}, \sqrt[3]{5}\right)$. عندئذ وحسب ما استنتج من تمرين 1 نحصل على الجزء الثاني . الآن :

$$\sqrt{2}, \sqrt[3]{5} \in Q\left(\sqrt{2}, \sqrt[3]{5}\right) \Rightarrow \sqrt{2} + \sqrt[3]{5} \in Q\left(\sqrt{2}, \sqrt[3]{5}\right)$$
$$\Rightarrow Q\left(\sqrt{2} + \sqrt[3]{5}\right) \subseteq Q\left(\sqrt{2}, \sqrt[3]{5}\right) \qquad (1)$$

إضافة إلى ذلك
$$\sqrt{2} + \sqrt[3]{5} \in Q\left(\sqrt{2} + \sqrt[3]{5}\right) \Rightarrow \left(\sqrt{2} + \sqrt[3]{5}\right)^2 \in Q\left(\sqrt{2} + \sqrt[3]{5}\right)$$

أي أن
$$2 + 2\sqrt{2}\sqrt[3]{5} + \sqrt[3]{25} \in Q\left(\sqrt{2} + \sqrt[3]{5}\right) \Rightarrow$$
$$\sqrt[3]{5}\left(\sqrt{2} + \sqrt{2} + \sqrt[3]{5}\right) \in Q\left(\sqrt{2} + \sqrt[3]{5}\right) \Rightarrow 5\left[\sqrt{2} + \left(\sqrt{2} + \sqrt[3]{5}\right)\right]^3 \in$$
$$\left(\sqrt{2} + \sqrt[3]{5}\right)$$

لدينا الآن
$$5\left(\sqrt{2} + \alpha\right)^3 \in Q(\alpha) \Rightarrow \left(\sqrt{2} + \alpha\right)^3 \in Q(\alpha)$$
$$\Rightarrow 2\sqrt{2} + 6\alpha + 3\sqrt{2}\alpha^2 + \alpha^3 \in Q(\alpha)$$
$$\Rightarrow \sqrt{2}(2 + 3\alpha^2) \in Q(\alpha)$$

لأن $6\alpha + \alpha^3 \in Q(\alpha)$ وعليه $\sqrt{2} \in Q(\alpha)$.

هذا يبين أن $\sqrt[3]{5} = \alpha - \sqrt{2} \in Q(\alpha)$. وهكذا فإن :

$$\sqrt{2}, \sqrt[3]{5} \in Q(\alpha) \Rightarrow Q\left(\sqrt{2}, \sqrt[3]{5}\right) \subseteq Q\left(\sqrt{2} + \sqrt[3]{5}\right) \qquad (2)$$

(1) و (2) يؤديان إلى أن $Q\left(\sqrt{2} + \sqrt[3]{5}\right) = Q\left(\sqrt{2}, \sqrt[3]{5}\right)$.

مسائل

ملاحظة : في المسائل الآتية F يمثل حقل و K حقل توسيع لـ F ، إلا إذا ذكر خلاف ذلك .

1- إذا كان $[K : F]$ برهن أن $K = F$.

2- ما الفرق بين " K توسيع منته للحقل F " و " K منته التولد" . اذكر مثال توضيح إجابتك .

[**إرشاد** إذا كان x متاسمي (غير جبري) على F فإن $K = F(x)$ هو منته التولد على F ولكنه ليس توسيعاً منتهيا] .

3- لأي عنصرين a, b في K ، برهن أن $F(a, b) = F(b, a)$.

4- برهن أن كثيرة حدود تكعيبية على حقل F غير قابلة للتحليل إذا وفقط إذا كانت لا تملك جذراً في F .

[**إرشاد** إذا كانت $ax^3 + bx^2 + cx + d$ قابلة للتحليل فإن :

$$ax^3 + bx^2 + cx + xd = a(x + \alpha)(x^2 + \beta x + \gamma)$$

لبعض $\alpha, \beta, \gamma \in F$] .

5- لتكن $x^2 + ax + b$ كثيرة حدود تربيعية على F . برهن إذا كان α جذراً لها في أي حقل توسيع للحقل F ، فإن $\beta = -(a + \alpha)$ هو أيضاً جذر لكثيرة الحدود التربيعية وأن حقل الانفلاق لكثيرة الحدود التربيعية هذه على F هو $F(\alpha)$.

6- أوجد قاعدة ودرجة $Q(\sqrt{2}, \sqrt{3})$ على Q .

[الجواب $\{1, \sqrt{2}, \sqrt{3}\sqrt{6}\}$,4] .

7- برهن أن $F(\sqrt{2} + \sqrt{3}) = F(\sqrt{2}, \sqrt{3})$.

8- إذا كان F حقلاً جزئياً لساحة تامة D بحيث كل عنصر من D هو جبري على F برهن أن D حقل . استنتج أنه إذا كان K أي توسيع جبري للحقل F ، فإن أية ساحة تامة جزئية من K تحوي F عبارة عن حقل جزئي من K .

9- لأي حقلين جزئيين N, M للحقل F عرف :

$MN = \left\{\sum x_i y_i \mid x_i \in M, y_i \in N\right\}$ برهن الآتي :

(i) MN حلقة جزئية من K .

(ii) إذا كان K توسيعاً جبرياً للحقل F و N, M يحويان F ، فإن MN حقل جزئي من K يحوي F بحيث $MN = < M \cup N >$. في هذه الحالة إذا كان كل من M و N منتهي البعد على F استنتج أنه إذا كان $[MN : F] = [M : F][N : F]$ فإن $M \cap N = F$. برهن أن العكس صحيح إذا كان واحد من $[M : F]$ و $[N : F]$ يساوي 2 . اذكر مثال للبرهنة على أن العكس ليس صحيحاً دائماً .

[إرشاد : خذ $M = Q(\sqrt[3]{2})$ ، $N = Q(\omega\sqrt[3]{2})$ ، $F = Q$ حيث ω هو الجذر التكعيبي التخيلي للواحد الصحيح] .

10- في $Q(\sqrt{2})$ عبر عن العناصر الآتية ككثيرات حدود في $\sqrt{2}$

(i) $\frac{1}{2+\sqrt{2}}$ (ii) $\frac{3+\sqrt{2}}{5+\sqrt{8}}$ (iii) $\frac{1}{(3+\sqrt{2})}$

[الإجابة (i) $1-\frac{1}{2}\sqrt{2}$ (ii) $\frac{11}{17}-\frac{1}{17}\sqrt{2}$ (iii) $\frac{11}{49}-\frac{6}{49}\sqrt{2}$.

11- في $Q(\sqrt[3]{2})$ عبر عن العناصر الآتية ككثيرات حدود في $\sqrt[3]{2}$:

(i) $\frac{3}{1+\sqrt[3]{2}-\sqrt[3]{4}}$ (ii) $\left(1+\sqrt[3]{2}+6\sqrt[3]{4}\right)^{-1}$ (iii) $\frac{1}{2-\sqrt[3]{4}}$.

[الإجابة (i) $\frac{9}{5}+\frac{3}{5}\sqrt[3]{2}+\frac{6}{5}\sqrt[3]{4}$ (ii) $\frac{-11}{831}+\frac{71}{831}-\frac{5}{831}\sqrt[3]{4}$
(iii) $1+\frac{1}{2}\sqrt[3]{2}+\frac{1}{2}\sqrt[3]{4}$] .

12- لتكن x^3+ax^2+bx+c أية كثيرة حدود تكعيبية غير قابلة للتحليل على Q وليكن E حقل انفلاقها . برهن أن جميع جذور الحدود التكعيبية هي أعداد حقيقية حينما يكون $[E:Q]=3$.

13- برهن أن حقل انفلاق x^6-1 على Q هو نفس حقل الانفلاق لـ x^4+x^2+1 على Q وأن $[E:Q]=2$.

14- أوجد حقول الانفلاق ودرجاتها لكثيرات الحدود الآتية على Q .

(i) x^4+1 (ii) x^6+1 (iii) x^4-2 (iv) x^5-1 .

[الإجابة (i) $4, Q(\sqrt{2}, i)$ (ii) $4, Q(\sqrt{3}, i)$ (iii) $8, Q\left(2^{\frac{1}{4}}, i\right)$
(iv) $4, Q\left(e^{\frac{2\pi i}{3}}\right)$] .

15- أوجد شروط ضرورية وكافية لكي تكون كثيرة حدود تكعيبية على Q لها حقل انفلاق درجته 3 .

[إرشاد : ليكن $D=-4a^3-27b^2$ ، فإن درجة حقل الانفلاق هي 3 إذا وفقط إذا كان D مربعاً كاملاً] .

16- لتكن $f(x)$ كثيرة حدود على F و σ أوتومورفزم لحقل $F\subseteq K$ بحيث σ يبقي كل عنصر في F ثابتاً . برهن أنه لأي جذر α لـ $f(x)$ في K فإن $\sigma(\alpha)$ أيضاً جذر لـ $f(x)$.

17- ليكن m أي عدد صحيح موجب وليس مربعاً كاملاً بين أن الراسم :

. $Q(\sqrt{m})$ هو أتومورفزم لـ $\alpha + \beta\sqrt{m} \to \alpha - \beta\sqrt{m}, \alpha, \beta \in Q$
عندئذ أو بخلافه برهن أن لكل عددين نسبيين α, β مع $\beta \neq 0$ إذا كانت $p(x)$ كثيرة الحدود الأصغرية لـ $\alpha + \beta\sqrt{m}$ على Q فإن $p(x)$ هي أيضاً كثيرة الحدود الأصغرية لـ $\alpha - \beta\sqrt{m}$ على Q .

18- باستخدام المسألة 16 ، أثبت إذا كان العدد المركب $a + ib$ جذر لكثيرة حدود $f(x)$ على IR حقل الأعداد الحقيقية ، فإن $a - ib$ أيضاً جذر لـ $f(x)$.

[إرشاد : $z \to \bar{z}, z \in C$ عبارة عن أتومورفزم لـ $R(i)$ يبقي عناصر IR ثابتاً] .

19- ليكن F حقلاً و D حلقة قاسمية بحيث F محتواة في مركز D . اذكر مثال يبين أن كثيرة حدود $f(x)$ ذات درجة $n > 1$ على F قد يكون لها أكثر من n جذراً في D .

[إرشاد : لتكن D الحلقة القاسمية للرباعيات الحقيقية . برهن $x^2 + 1$ لها عدداً غير منتهياً من الجذور في D] .

20- ليكن $v, u \in K$ جبريان على F درجتهما n, m على الترتيب . بين أن درجة u على $K(v)$ هي m إذا وفقط إذا كانت درجة v على $K(u)$ تساوي n ، وأن العبارتين صحيحتين إذا كان n, m أوليان نسبياً .

21- نقول أن حقل ما هو جبري مطلقاً إذا كان جبرياً على حقله الجزئي الأولي . بين أن الحقل الجبري المطلق بمميز منته لا يملك ساحة تامة جزئية ليس حقلاً .

22- ليكن $F_1 \supseteq F_2 \supseteq \ldots \supseteq F_n$ سلسلة منتهية من الحقول بحيث أن كل $[F_i : F_{i+1}]$ منته ، عندئذ بين أن :

$$[F_1 : F_n] = \prod_{i=1}^{n-1} [F_i : F_{i+1}]$$

23- تعريف . يقال لعدد مركب أنه عدد صحيح جبري إذا كان يحقق كثيرة حدود واحدية في $Z[x]$. العدد المركب i عدد جبري صحيح لأنه يحقق $x^2 + 1$.

أثبت الآتي :

(i) إذا كان عدد نسبي ما جبرياً صحيحاً فإنه يجب أن يكون عدداً صحيحاً .

(ii) إذا كان α عدداً جبرياً عندئذ يوجد عدد صحيح موجب n بحيث $n\alpha$ عدد جبري صحيح .

(iii) الأعداد الصحيحة الجبرية تكون حلقة جزئية من C .

24- برهن أن لكل عدد صحيح m ، كل من $\cos m^0$ ، $\sin m^0$ عدد جبري .

[إرشاد : $\left(e^{\frac{\pi m i}{180}}\right)^{180} = \pm 1$] .

3– التوسيعات القابلة للفصل وغير القابلة للفصل

ليكن F حقلاً و $F(x)$ كثيرة حدود غير ثابتة على F . في البند السابق عرضنا مفهوم التكرارية (التعددية) لجذر كثيرة حدود $f(x)$ في أي حقل توسيع ويقال لجذر a لكثيرة الحدود $f(x)$ أنه جذر مكرر لـ $f(x)$ إذا كان تكرار a أكبر أو يساوي 2 . في هذا البند سنناقش وجود جذور مكررة لكثيرات الحدود . لأجل ذلك نعرف مفهوم المشتقة .

تعريف 13-38

إذا كانت $f(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_n x^n$ كثيرة حدود في $F[x]$ ، فإن مشتقة $f(x)$ والتي نرمز لها $f'(x)$ معرفة على أنها $f'(x) = \alpha_1 + 2\alpha_2 x + \dots + n\alpha_n x^{n-1}$. عليه بالأخص إذا كانت $f(x) = \alpha_0$ فإن $f'(x) = 0$ بمعنى آخر مشتقة أية كثيرة حدود ثابتة تساوي الصفر إضافة إلى ذلك فواضح من التعريف أنه إذا كانت $f(x)$ كثيرة حدود من الدرجة n عندئذ إما $f'(x) = 0$ أو درجة كثيرة الحدود $f'(x)$ تكون على الأكثر $n-1$. لتوضيح هذا افرض أن F حقل مميز p وأن $g(x) = x^p$ عندئذ $g'(x) = px^{p-1} = 0$ لأن مميز $F[x]$ يساوي p أيضاً من جهة أخرى إذا أخذنا F بحيث يكون مميزه صفراً و $\deg f(x) = n \geq 1$ عندئذ $\alpha_n \neq 0$ يعطينا $n\alpha_n \neq 0$. عليه فإن $\deg f'(x) = n-1$.

القضية الآتية هي نتيجة مباشرة من تعريف المشتقة .

قضية 13-39

لتكن $f(x), g(x) \in F[x]$ ، $\alpha \in F$ عندئذ :

(i) $[f(x) + g(x)]' = f'(x) + g'(x)$

(ii) $[\alpha f(x)]' = \alpha f'(x)$

(iii) $[f(x)\, g(x)]' = f'(x)\, g(x) + f(x)\, g'(x)$. □

قضية 13-40

لتكن $f(x) \in F[x]$ كثيرة حدود غير ثابتة . فإن العنصر α في حقل توسيع K للحقل F هو جذر مكرر لـ $f(x)$ إذا وفقط إذا كان α جذراً مشتركاً لـ $f(x)$ و $f'(x)$.

البرهان

ليكن α جذراً لـ $f(x)$ بتكرار m . فإن $f(x) = (x - a)^m g(x)$ ، $g(x) \in K[x]$ و $g(\alpha) \neq 0$. منها نحصل على أن :

$$f'(x) = m(x - \alpha)^{m-1} g(x) + (x - \alpha)^m g'(x)$$

ليكن α جذراً مكرراً لكثيرة الحدود $f(x)$ فإن $2 \leq m$ ، عليه :

$$f'(\alpha) = m(\alpha - \alpha)^{m-1} g(\alpha) + (\alpha - \alpha)^m g'(\alpha) = 0$$

(لأن $m - 1 > 0$) .

هذا يعني أن α جذر مشترك لـ $f(x)$ و $f'(x)$. لاحظ إذا لم يكن α جذراً مكرراً فإن $m = 1$ و $f'(x) = g(x) + (x - \alpha)g'(x)$. في هذه الحالة $f'(\alpha) = g(\alpha) \neq 0$ ، وهذا يبرهن القضية . □

قضية 13-41

إذا كانت $f(x)$ كثيرة حدود غير قابلة للتحليل على الحقل F ، فإن $f(x)$ لها جذر مكرر في بعض حقل توسيع [تحديداً حقل انفلاق $f(x)$ على F] إذا وفقط إذا كانت $f(x) = 0$.

البرهان

افرض أن $f(x)$ لها جذر مكرر في حقل توسيع K للحقل F وليكن a . حسب قضية 13-40 فإن a جذر لكثيرة الحدود $f'(x)$ أيضاً . بما أن $f(x)$ غير قابلة للتحليل على F ويتحقق بالعنصر a ، فإنه لأية كثيرة حدود غير صفرية $g(x)$ فإن $g(a) = 0$ يؤدي إلى أن $f(x)$ تقسم $g(x)$. وبالأخص فإن $f(x) \mid f'(x)$. إذا كان $f'(x) \neq 0$ فكما نعلم فإن $\deg f'(x) < \deg f(x)$. وبالتالي فإن $f(x)$ لا يمكن أن تقسم $f'(x)$. إذاً $f'(x) = 0$.

وبالعكس افرض أن $f'(x) = 0$. ليكن K حقل انفلاق $f(x)$ على F وليكن $a \in K$ جذراً مكرراً لكثيرة الحدود $f(x)$. فإن $f(a) = 0 = f'(a)$ وحسب القضية 41-13 فإن a جذر مكرر لكثيرة الحدود $f(x)$. أي أن $f(x)$ لها جذر مكرر في K . □

نتيجة 13-42

لا توجد كثيرة حدود غير قابلة للتحليل على حقل بمميز صفر بحيث يكون لها جذر مكرر في أي حقل توسيع .

البرهان

ليكن F حقلاً بمميز 0 و $f(x)$ كثيرة حدود غير قابلة للتحليل على F . افرض أن $\deg f(x) = n \geq 1$. عندئذ يكون $\deg f'(x) = n - 1 \geq 0$ (الملاحظة بعد تعريف 13-38) وعليه فإن $f'(x) \neq 0$ ، وحسب النظرية السابقة لا يمكن أن يكون لكثيرة الحدود $f(x)$ جذراً مكرراً في أي حقل توسيع . □

مثال 16

ليكن $F = Z_2(t)$ حيث t غير محدد على Z_2 حقل الأعداد الصحيحة معيار 2 . اعتبر كثيرة الحدود $f(x) = x^2 - t$ على F . ليكن K حقل انفلاق $f(x)$ و a_1, a_2 أي جذرين لكثيرة الحدود $f(x)$ في K .

فإن $x^2 - t = (x - a_1)(x - a_2)$. بمقارنة المعاملات نحصل على أن $a_1 = -a_2$. من جهة أخرى مميز F يساوي 2 يعطينا $-a_2 = a_2$. عليه فإن $a_1 = a_2$ وأن $f(x) = (x - a_2)^2$ موضحة بذلك أن a جذر مكرر لـ $f(x)$. من الممكن أن تكون $f(x)$ غير قابلة للتحليل على F (انظر سؤال 6 . نهاية هذا البند) . إضافة إلى ذلك $f'(x) = 2x = 0$.

تعريف 13-43

يقال لكثيرة حدود غير قابلة للتحليل $f(x) \in F[x]n$ ذات درجة أنها قابلة للفصل إذا كان لها n من الجذور المختلفة في حقل انفلاقها . بخلاف ذلك يقال أنها غير قابلة للفصل . بصورة عامة يقال لكثيرة حدود غير ثابتة $g(x) \in F[x]$ أنها قابلة للفصل إذا كانت جميع عوامل $g(x)$ الغير قابلة للتحليل على F هي قابلة للفصل بخلاف ذلك يقال أن $g(x)$ غير قابلة للفصل .

في القضية 13-41 فإن كثيرة الحدود غير القابلة للتحليل $f(x)$ تكون قابلة للفصل إذا وفقط إذا كانت $f'(x) \neq 0$ والنتيجة 13-42 تبين أن كل كثيرة حدود غير صفرية على حقل بمميز صفر تكون قابلة للفصل . مثال 16 هو لكثيرة حدود غير قابلة للتحليل وغير قابلة للفصل . اعتبر $f(x) = (x - 1)(x^2 + x + 1)$ على Q لها جذر مكرر وهو 1 . من جهة أخرى العوامل الغير قابلة للتحليل هي $(x - 1)$ ، $(x^2 + x + 1)$ وكل منها قابلة للفصل وعليه حسب التعريف فإن $f(x)$ قابلة للفصل .

قضية 13-44

كثيرة حدود $f(x)$ على حقل F بمميز $p > 0$ غير قابلة للفصل إذا وفقط إذا كان $f(x) \in F[x^p]$ بمعنى آخر $f(x)$ هي كثيرة حدود في x^p .

البرهان

لتكن $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_n x^n$ مع كون $\alpha_n \neq 0$ ، فإن $f'(x) = \alpha_1 + 2\alpha_2 x + ... + n\alpha_n x^{n-1}$. الآن $f(x)$ غير قابلة للفصل إذا وفقط إذا كان $f'(x) = 0$ ولكن

$$f'(x) = 0 \Leftrightarrow \alpha_1 = 2\alpha_2 = ... = n\alpha_n = 0$$

لأي $1 \leq k \leq n, k$ فإن

$$k\alpha_k = 0 \Leftrightarrow p \mid k \quad \text{or} \quad \alpha_k = 0$$

وعليه حينما يكون $f'(x) = 0$ نجد أنه إذا كان لأي $\alpha_k \neq 0, k$ فإن $p \mid k$ أي أن $h = k_1 p$ لبعض $k_1 \geq 1$. ذلك يعني في $f(x)$ إذا كان أي حد $a_k x^k$ فيه $\alpha_k \neq 0$ فإنه من الشكل $\alpha_{k_1 p} x^{pk_1} = \alpha_{k_1 p}(x^p)^{k_1}$. عليه فإن $f(x) = \beta_0 + \beta_1 x^p + \beta_2 x^{2p} + ... + \beta_m x^{mp}$ لبعض عدد صحيح موجب m . وهكذا فإن $f(x) \in F[x^p]$ والنتيجة متحققة . □

تعريف 13-45

إذا كان a عنصراً في حقل توسيع K للحقل F جبري على F ، عندئذ يقال أن a عنصر قابل للفصل (غير قابل للفصل) على F ، إذا كانت كثيرة الحدود الأصغرية لـ a على F قابلاً للفصل (غير قابلاً للفصل) .

يقال لتوسيع جبري K لحقل F أنه توسيع قابل للفصل إذا كان كل عنصر في K قابلاً للفصل على F . بخلافه يقال أن K توسيع غير قابل للفصل .

كما لاحظنا سابقاً كل كثيرة حدود على حقل بمميز صفر هي قابلة للفصل ، نجد أن كل توسيع جبري لحقل بمميز صفر هو توسيع قابل للفصل .

من جهة أخرى إذا أخذنا $F = Z_2(x)$ و K حقل الانفلاق لـ $x^2 - t$ (مثال 16) فإن K توسيع منته للحقل F لأن $[K : F]$ ولكن K توسيع غير قابل للفصل لأن $x^2 - t$ لها جذراً مكرراً في K . لاحظ أن F غير منتهية بمميز منته .

سوف نوضح أن كل توسيع جبري لحقل منته هو توسيع قابل للفصل لذا سوف نوضح أولاً النتيجة الآتية .

قضية 13-46

لتكن D أية ساحة تامة بمميز عدد أولي p . فإن الراسم $\sigma : D \to D$ المعطى حسب $\sigma(a) = a^p$ هو مونومورفزم من D إلى D .

البرهان

لأي عنصرين $a, b \in D$ فإن :

$$(a+b)^p = a^p + C_1^p a^{p-1} b + C_2^p a^{p-2} b^2 + \dots + C_p^p b^p$$

لكل r بحيث $1 \le r \le p-1$ فإن $p \mid C_r^p$ وعليه فإن $C_r^p a^{p-r} b^r = 0$ لجميع $r = 1, 2, \dots, p-1$ ، وبذلك فإن $(a+b)^p = a^p + b^p$ وأن الإبدالية للضرب تبين أن $(ab)^p = a^p b^p$ عليه فإن

$$\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$$

$$\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\,\sigma(b)$$

وهكذا فإن σ أندومورفزم . إضافة إلى ذلك فإن :

$$a \in \ker \sigma \Rightarrow \sigma(a) = 0 \Rightarrow a^p = 0 \Rightarrow a = 0$$

عليه فإن $\ker \sigma = \{0\}$ وأن σ هو مونومورفزم . □

نتيجة 13-47

إذا كان F حقلاً منتهياً بمميز عدد أولي p فإن $a \to a^p$ هو أنومورفزم للحقل F .

البرهان

وجدنا في القضية السابقة أن الراسم $\sigma : F \to F$ المعطى حسب $\sigma(a) = a^p, \ \forall a \in F$ هو مونومورفزم ، وعليه فإن عدد العناصر الموجودة في $\sigma(F)$

يساوي عدد العناصر الموجودة في F . من ناحية ثانية F حقل منته وأن $\sigma(F) \subseteq F$ فإننا نحصل على $\sigma(F) = F$ وهكذا فإن σ أوتومورفزم . □

نظرية 13-48

أي توسيع جبري لحقل منته F هو توسيع قابل للفصل .

البرهان

لتكن $f(x)$ أية كثيرة حدود غير قابلة للتحليل على F . افرض أن $f(x)$ غير قابلة للفصل على F ، لذلك فإن $f(x) \in F[x^p]$ (قضية 13-44) ، $f(x) = \beta_0 + \beta_1 x^p + \beta_2 x^{2p} + \ldots + \beta_m x^{mp}$ لبعض $\beta_i \in F\ (0 \le i \le m)$. لما كان $\alpha \to \alpha^p, \alpha \in F$ هو أوتومورفزم لـ F ، فبإمكاننا إيجاد $\alpha_i \in F$ بحيث $\beta_i = \alpha_i^p$ لكل i وبالتالي فإن

$$f(x) = \alpha_0^p + \alpha_1^p x^p + \alpha_2^p x^{2p} + \ldots + \alpha_m^p x^{mp}$$

$= (\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_m x^m)^p$ (القضية 13-46) .

هذا يؤدي إلى أن $f(x)$ غير قابلة للتحليل . وهذا تعارض لذلك فإن $f(x)$ قابلة للفصل . عليه وبالأخص إذا كان K أي توسيع جبري للحقل F ، فإن كثيرة الحدود الأصغرية لكل عنصر في K على F هي قابلة للفصل . وعليه حسب التعريف فإن K توسيع قابل للفصل للحقل F . □

دعنا نتذكر أن حقل توسيع K للحقل F يقال أنه توسيع بسيط للحقل F إذا كان $K = F(a)$ لبعض $a \in K$ و a معروف بأنه عنصر بدائي لـ K على F . إحدى النظريات التي لها أهمية كبيرة في نظرية الحقل هي نظرية لاجرانج للعنصر البدائي والتي تنص على أن كل توسيع منته قابل للفصل هو توسيع بسيط . إثبات هذه النظرية يتطلب بعض النتائج العميقة ولا نذكرها هنا . ومع ذلك نبرهن حالة خاصة لهذه النظرية .

نظرية 13-49

إذا كان F حقلاً بمميز صفر و a, b عنصران في بعض حقل توسيع للحقل F جبريان على F ، فإن $F(a,b) = f(c)$ لبعض $c \in F(a,b)$.

البرهان

لتكن $f(x), g(x)$ كثيرتي الحدود الأصغرية لـ a, b على F على الترتيب ولتكن m, n درجتهما على الترتيب . افرض أن K حقل انفلاق $f(x)\, g(x)$ على F . عندئذ $a, b \in K$. من الواضح كل جذر لـ $f(x)$ هو جذر لـ $f(x)\, g(x)$ ، عليه K يحوي حقل انفلاق $f(x)$.

الحالة مشابهة بالنسبة إلى $g(x)$. بما أن K حقل توسيع قابل للفصل للحقل F (نتيجة 13-42) . $f(x)$ لها m جذراً مختلفاً . $a_1 = a, a_2, \ldots, a_m$ في K و $g(x)$ لها n جذراً مختلفاً $b_1 = b, b_2, \ldots, b_n$ في K . $2 \le i \le m$ ، $2 \le j \le n$ نعرف $\lambda_{ij} = \dfrac{a_i - a}{b - b_j} \in K$.

هذه الـ λ_{ij} هي منتهية في العدد . بما أن مميز F يساوي الصفر فإن F يحوي عدداً غير منتهياً من العناصر . من الواضح أنه بإمكاننا إيجاد $\alpha (\neq 0)$ بحيث $\alpha \neq \lambda_{ij}$ لكل $i, j \ge 2$.

فإن $\alpha(b - b_i) \neq a_i - a, \quad \forall\, i, j \ge 2$ أي أن $a_i + \alpha b_i \neq a + \alpha b$ لكل $i, j \ge 2$ ، نضع $c = a + \alpha b \in F(a,b)$ ، عليه $F(c) \subseteq F(a,b)$. نبين أن $F(c) = F(a,b)$.

بما أن $c \in F(c)$ وكل معامل في $f(x)$ ينتمي إلى F فهو ينتمي إلى K أيضاً منها نحصل على أن كثيرة الحدود $h(x) = f(c - \alpha x) \in K[x]$. إضافة إلى ذلك

$\deg h(x) = \deg f(x) = m$ (لماذا ؟) . الآن $h(b) = f(c - \alpha b) = f(a) = 0$ افرض أنه عندما $j \geq 2$ فإن $h(b_j) = 0$ ، عندئذ $f(c - \alpha b_j) = 0$ وعليه $c - \alpha b_j = a_i$ لبعض i لأن $a_1, a_2, \ldots, a_n$ هي الجذور الوحيدة لـ $f(x)$. إذا كان $i = 1$ فإن $a_i = a$ وهذا يعطينا $c = \alpha b_j + a$ أي أن $\alpha b_j + a = \alpha b + a$ والذي يؤدي إلى $b_j = b$. هذا تناقض . عليه فإن $i \geq 2$ في تلك الحالة سوف نحصل على $\alpha b + a = \alpha b_j + a_i$ وهذا أيضاً لا يجوز ، وعليه $h(b_j) \neq 0$. أي أنه عندما $j \geq 2$ فإن $x - b_j$ لا يقسم $h(x)$. الآن $x - b$ عامل لـ $h(x)$ على K . بما أن b أيضاً جذر لـ $g(x)$ في K ، فإن $x - b$ هو عامل مشترك لـ $h(x), g(x)$ ندعي أن $x - b$ هو HCF (العامل المشترك الأكبر) لـ $h(x), g(x)$ لما كانت $f(x)$ لا تملك أي جذر مكرر ، $(x - b)^2 \nmid g(x)$. بما أن $g(x) = (x - b)(x - b_2)\ldots(x - b_n)$ و $(x - b_j)$ لا يقسم $h(x)$ لكل $j \geq 2$ فإن $x - b$ هو HCF لـ $h(x), g(x)$. الآن $h(x) \in F(c)[x]$ لأن $c \in F(c)$ و $\alpha \in E$. كذلك فإن $g(x) \in F(x)[x]$. لتكن $g_1(x)$ كثيرة الحدود الأصغرية لـ b على $F(c)$. فإن $g_1(x) \mid h(x), g_1(x) \mid g(x)$ على $F(c)$ وبالتالي على K أيضاً لأن $F(c) \subseteq K$.

عليه $(x - b) \mid g_1(x)$ على K لأن $x - b$ هو HCF لـ $h(x), g(x)$ على K .

من جهة أخرى $g_1(x)$ هي كثيرة حدود واحدية ذات درجة موجبة ، وعليه يكون لدينا $x - b = g_1(x) \in F(c)[x]$. هذا يؤدي إلى أن $b \in F(c)$. وبالتالي فإن :

$$a = c - ab \in F(c)$$

أي أن $F(a, b) \subseteq F(c)$. وبالتالي $F(c) = F(a, b)$. □

نظرية 13-50

كل حقل توسيع منته لحقل بمميز صفر هو توسيع بسيط .

البرهان

ليكن K حقل توسيع منته للحقل F . عندئذ يوجد عدد منته من العناصر $a_1, a_2, \ldots, a_n$ في K بحيث $K = F(a_1, a_2, \ldots, a_n)$.

نبرهن بالاستنتاج الرياضي على n . إذا كان $n = 1$ ، في هذه الحالة فإن K هو توسيع بسيط . افرض $n > 1$ والنظرية صحيحة لجميع التوسيعات المنتهية للحقل F والمولدة بأقل من n عنصراً . ليكن $K_1 = F(a_1, a_2, \dots, a_{n-1})$. حسب فروض الاستنتاج يوجد $b \in K_1$ بحيث $K_1 = F(a_1, a_2, \dots, a_{n-1})$.

إذاً $K = F(b, a_n)$ (لماذا ؟) . النظرية 13-41 تعطينا $K = F(c)$ لبعض $c \in F(b, a)$ والذي يثبت النظرية . □

تعريف 13-51 (حقل جالوا)

الحقل الذي يحوي عدداً منتهياً من العناصر يسمى حقل جالوا .

مثال 17

اعتبر الحلقة Z_p حلقة الأعداد الصحيحة معيار p ، حيث p عدد أولي . Z_p يحوي p من العناصر وهي $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{p-1}$. تذكر أن $Z_p - \{0\}$ هي زمرة تحت عملية الضرب (انظر مثال 7 ، ملاحظة 2 ، بند 1 ، الفصل الثاني) . وعليه كل عنصر غير صفري في Z_p له معكوس ضربي . بالتالي فإن Z_p حقل يحوي p عنصراً .

مثال 18

حقل الانفلاق K لـ $x^2 + x + \overline{1}$ على Z_2 يحوي $\overline{0}, \overline{1}, \alpha$ و $\overline{1} + \alpha$ حيث $\alpha^2 + \alpha + \overline{1} = 0$. K عبارة عن حقل جالوا يحوي أربعة عناصر .

مثال 19

ليكن K حقل انفلاق $x^2 + \overline{1}$ على Z_3 . K يحوي 9 عناصر هي $\overline{0}, \overline{1}, \overline{2}, \alpha, \overline{2}\alpha, \overline{1} + \alpha, \overline{1} + \overline{2}\alpha, \overline{2} + \alpha, \overline{2} + \overline{2}\alpha$ حيث $\alpha^2 + 1 = 0$. فإن K حقل جالوا يحوي 9 عناصر .

نظرية 13-52

ليكن F حقلاً يحوي q عنصراً . فإن :

(i) $char\ F$ يساوي p لبعض عدد أولي p .

(ii) $q = p^n$ لبعض $n \in N$.

البرهان

ليكن e العنصر المحايد (الضربي) لـ F . بما أن F يحوي q عنصراً ، العناصر $e, 2e, 3e, \ldots, (q+1)e$ لا يمكن أن تكون مختلفة . لذا يوجد عددان صحيحان l, k بحيث $1 \le l < k \le q+1$ بحيث $ke = le$ أي أن $(k-l)\,e = 0$. ليكن p أصغر عدد صحيح موجب بحيث $pe = 0$. ندعي أن p عدد أولي . افرض أن $p = rs$ مع كون $p > r > 1$ و $p > s > 1$ عندئذ وحيث أننا نعمل في حقل فإن :

$$pe = 0 \Rightarrow pe^2 = 0 \Rightarrow rse^2 = 0 \Rightarrow (re)\,(se) = 0$$

يؤدي إلى $re = 0$ أو $se = 0$ ، ولكن كل من النتائج أعلاه خلاف اختيار p ، بالتالي فإن p عدد أولي . وهذا يثبت أن $char\ F = p$.

للجزء الثاني نستخدم النظرية 13-5 . لما كان الحقل الجزئي الأولي P للحقل F أيزومورفي مع $Z / < p >$ فإنه يحوي p من العناصر . بما أن F حقل منته ، $[F : P] = n$ لبعض $n \in N$. لتكن $\{a_1, a_2, \ldots, a_n\}$ قاعدة لـ F على P . كل عنصر في F يمكن كتابته بطريقة واحدة فقط بالصورة $\sum_{i=1}^{n} \lambda_i a_i$ $\lambda_i \in P,$. بما أن كل λ_i يمكن اختياره في P من الطرق . فإن المجموع الكلي لعناصر F هي p^n وعليه $q = p^n$. □

نظرية 13-52 تنص على أن عدد العناصر في حقل منته يجب أن يكون قوة لعدد أولي ما . لذا لا يوجد حقل يحوي 6 ، 10 أو 12 من العناصر . في الاتجاه الآخر سوف

نبين أنه إذا أعطينا عدداً أولياً p وعدداً صحيحاً موجباً n ، فإنه يوجد حقل يحوي p^n عنصراً . نظرية لـ مور (E.H. Moore) تضمن وجود حقل كهذا .

لنبرهن أولاً القضية الآتية .

قضية 13-53

إذا كان F حقلاً يحوي q عنصراً ، فإن F هو حقل انفلاق $x^q - x$ على حقله الجزئي الأولي .

البرهان

بما أن العناصر الغير صفرية لحقل تشكل زمرة تحت عملية الضرب ، $G = F - \{0\}$ زمرة رتبتها $q - 1$ تحت الضرب . لكل $a \in G$ يكون $a^{q-1} = 1 \Rightarrow a^q = a$.

بوضوح $0^q = 0$. عليه لكل $b \in F$ ، $b^q = b$. نتيجة لذلك فإن كل عنصر في F هو جذر لكثيرة الحدود $x^q - x$. إذا كان P الحقل الجزئي الأولي للحقل F ، فإن $x^q - x \in P[x]$ لا يمكن أن يكون لها أكثر من q جذراً في أي حقل توسيع لـ P (نظرية 13-28) عليه جميع جذور $x^q - x$ تقع في F . وهكذا فإن F هو حقل انفلاق $x^q - x$ على P . □

نظرية 13-54 (مور E.H. Moore)

لكل عدد أولي P ولكل $n \in N$ ، يوجد حقل يحوي P^n عنصراً .

البرهان

اعتبر $f(x) = x^{P^n} - x$. من الواضح $f(x) \in Z_p[x]$. ليكن K حقل انفلاق $f(x)$ على Z_p . ندعي أن K حقل يحوي p^n عنصراً .

الآن $x^{p^n} - x = \sum_{i=1}^{p^n} (x - a_i), a_i \in K$. الراسم $\sigma : K \to K$ المعطى بـ $\sigma(y) = y^{p^n}, \quad \forall y \in K$ عبارة عن مونومورفزم (انظر قضية 13-46 والمسألة 7) . نتيجة لذلك فإن $\sigma(K), (\cong K)$ عبارة عن حقل جزئي من K . الآن لكل i $(1 \le i \le p^n)$ ، $a_i^{P^n} = a_i = \sigma(a_i) \Rightarrow a_i \in \sigma(K)$. وهكذا فإن كل جذر لـ $f(x)$ ينتمي إلى $\sigma(K)$ و $\sigma(K)$ يحوي الحقل الجزئي الأولي Z_p للحقل K (برهن !) . وعليه $\sigma(K)$ يحوي حقل انفلاق $f(x)$ على Z_p . هذا يسبب أن يكون $\sigma(K) = K$.

لاحظ أن كل عنصر في $\sigma(K)$ هو جذر لـ $f(x)$ و عليه $K = \{a_1, a_2, \ldots, a_p^2\}$ ندعي أن جميع الـ a_i هذه مختلفة الآن $f'(x) = p^n x^{p^{n-1}} - 1 = -1$ لأن $char\ K = p$ لذا فإن $f(x)$ ليس لها أي جذور مكررة (قضية 13-41) ، أي أن ادعائنا قد تحقق . بالتالي فإن K يحوي p^n عنصراً . $\square$

النظرية التالية تبين أن لكل عدد أولي p ولكل $n \in N$ يوجد حقل وحيد (ضمن حدود الأيزومورفزم) يحوي p^n عنصراً .

نظرية 13-55

الحقول المنتهية والتي تحوي نفس العدد من العناصر تكون أيزومورفية .

البرهان

ليكن K_1, K_2 حقلين كل منهما يحوي q عنصراً . حسب نظرية 13-52 ، $q = p^n$ لبعض $n \in N$ لعدد أولي p إضافة إلى ذلك مميز كل من K_1 ، K_2 يساوي p . ليكن P_1, P_2 الحقلان الجزئيان الأوليان من K_1 ، K_2 على التوالي . وحيث أن $P_1 \cong Z / < p >$ ، $P_2 \cong Z / < p >$ فإن $P_1 \cong P_2$. الآن حسب قضية 13-53 K_1 هو

حقل انفلاق $x^q - x$ على P_1 و K_2 هو حقل انفلاق $y^q - y$ على P_2 ، وحسب نظرية 13-35 فإن $K_1 \cong K_2$. □

اصطلاح : يرمز لحقل منته يحوي q عنصراً بالرمز $GF(q)$.

أخيراً نعطي وصفاً مهما للحقول المنتهية .

نظرية 13-56

يكون حقل ما منتهياً إذا وفقط إذا كانت زمرته الضربية دائرية .

البرهان

ليكن F حقل يحوي q عنصراً . فإن $G = F - \{0\}$ زمرة أبيلية رتبتها $q - 1$. ليكن n دليل G . من تعريف الدليل فإن $n \leq q - 1$ و $x^n = 1$ لكل $x \in G$. وحسب نظرية 13-28 فإن $x^n - 1$ لها على الأكثر n جذراً في G وعليه فإن $q - 1 \leq n$. إذاً $n = q - 1$ وبالتالي يوجد عنصر $a \in G$ بحيث $o(a) = q - 1$ أي أن G زمرة دائرية .

بالعكس افرض أن $G = F - \{0\}$ زمرة دائرية مولدة بالعنصر a . إذا كان $a = 1$ فإننا أثبتنا ما هو مطلوب لأنه عندئذ $o(G) = 1 \Rightarrow o(F) = 2$. دعنا نناقش الآن الحالة $a \neq 1$ ، افرض أن $Char\ F = 0$ ، $-1 \in G$ و $-1 \neq 1$ يؤدي إلى أن $-1 = a^n$ لبعض $n (\neq 0) \in Z$ هذا يؤدي إلى أن :

$$(-1)^2 = a^{2n} \Rightarrow a^{2n} = 1 \quad \text{حيث } n \neq 0$$

والذي يبين أن G زمرة منتهية . هذا يؤدي بدوره إلى أن F حقل منته وهذا غير معقول لأن أي حقل بمميز صفر لا يمكن أن يكون حقلاً منتهياً . لذلك $Char\ F \neq 0$. بالتالي فإن $Char\ F = p$ حيث p عدد أولي . الحقل الجزئي الأولي P للحقل F لكونه

أيزومورفي مع الحقل Z_p فإنه يحوي p من العناصر . بما أن $a-1 \neq 0$ فإن $a-1 \in G$. فيكون $a-1 = a^n$ لبعض $n \in Z$. وهكذا فإن a يحقق بعض كثيرة حدود في $P[x]$ أي أن a عنصر جبري على P . وبالتالي فإن $[P(a) : P] = r$ لبعض $r \in N$ ولأن P يحوي p عنصراً فإن $P(a)$ يحوي p^r عنصراً .

الآن $0 \in P(a)$ وكل عنصر غير صفري في F هو قوة للعنصر a فإنه ينتمي إلى $P(a)$ أيضاً لذلك فإن $F \subseteq P(a)$. ولكن $P(a) \subseteq F$ إذاً $F = P(a)$ يحوي p^r عنصراً . □

تمارين محلولة

تمرين 1

يقال لحقل F أنه حقل تام إذا كانت جميع التوسيعات المنتهية لـ F هي توسيعات قابلة للفصل .

برهن أن التوسيع الجبري لحقل تام هو توسيع قابل للفصل .

الحل

ليكن a عنصراً في K ، حقل توسيع جبري للحقل K . بما أن a جبري على F ، $[F(a) : F] = n$ لبعض $n \in N$. هذا يؤدي إلى أن $F(a)$ توسيع منته للحقل F . حسب الفروض F حقل تام ، عليه $F(a)$ توسيع قابل للفصل . كنتيجة لذلك فإن a قابل للفصل على F . أي أن K توسيع قابل للفصل للحقل F .

تمرين 2

ليكن F حقلاً بمميز $p(\neq 0)$ و a عنصراً في بعض حقل توسيع للحقل F . برهن أن a عنصر قابل للفصل على F إذا وفقط إذا كان $F(a^p) = F(a)$.

الحل

ليكن K حقل توسيع للحقل F و $a \in K$ عنصر قابل للفصل على F . كثيرة الحدود الأصغرية $f(x) = \alpha_0 + \alpha_1 x + \ldots + a_{n-1}x^{n-1} + x^n$ لـ a على F هي قابلة للفصل. لتكن $g(x) = \alpha_0^p + \alpha_1^p x + \ldots + \alpha_{n-1}^p x^{n-1} + x^n$. في هذه الحالة يكون a^p جذراً لـ $g(x)$ لأن

$$g(a^p) = \alpha_0^p + \alpha_1^p a^p + \ldots + \alpha_{n-1}^p a^{(n-1)p} + a^{pn}$$
$$= (\alpha_0 + \alpha_1 a + \ldots + \alpha_{n-1}a^{n-1} + a^n)^p = [f(a)]^p = 0$$

كذلك $g(x)$ غير قابلة للتحليل على F . في الحقيقة إذا كان $h(x)$ عاملاً لـ $g(x)$ في $F[x]$ فإن $h(x^p)$ عامل لـ $g(x^p)$ في $F[x]$. ولكن $g(x^p) = [f(x)]^p$ و $f(x)$ غير قابلة للتحليل على F هذا يؤدي إلى أن $h(x^p) = [f(x)]^k$ لبعض $0 \le k \le p$. بأخذ مشتقة الطرفين نحصل على أن $k[f(x)]^{k-1} f'(x) = 0$. كون $f(x)$ قابلة للفصل يؤدي إلى أنه إما $k = 0$ أو $k = p$.

واستناداً إلى ذلك فإن $h(x^p) = 1$ أو $h(x^p) = [f(x)]^p$.

في الحالة الأولى $h(x) = 1$ وفي الحالة الأخيرة $h(x^p) = g(x^p) \Rightarrow h(x) = g(x)$ وعليه $g(x)$ هي كثرة الحدود الأصغرية لـ a^p على F أي أن :

$[F(a^p) : F] = n = [F(a) : F]$ وبالتالي $F(a^p) = F(a)$.

بالعكس ، ليكن $F(a^p) = F(a)$ وافرض أن a غير قابلة للفصل على F . كثيرة الحدود الأصغرية $f(x)$ لـ a على F غير قابلة للفصل . هذا يبين أن $f(x) = g(x^p)$ وعليه a^p جذر لـ $g(x)$. من الواضح أن درجة $g(x)$ يساوي (مثلاً) $\frac{n}{p} = m$. وهكذا ولأن $1 < p$ فإن

$$[F(a^p) : F] \le m < n$$

بما أن حسب الفرض

$$[F(a) : F] = [F(a) : F(a^p)][F(a^p) : F] \le m$$

نحصل على $n \le m$. هذا غير معقول ، إذاً فإن a عنصر قابل للفصل .

تمرين 3

إذا كان a عنصراً في K ، (حقل توسيع للحقل F) قابل للفصل على حقل F والذي مميزه $(p \neq 0)$. فإن $F(a)$ توسيع قابل للفصل للحقل F .

الحل

ليكن $b \in F(a)$ وحيث أن a جبرياً على F ، فإن $[F(a) : F]$ منته .

ليـــــــــــــــكن : $[F(b) : F] = m$ ، $[F(a) : F(b)] = n$ ، $\left[F(a) : F(b^p)\right] = q$ و $\left[F(b^p) : F\right] = s$.

الآن
$$nm = [F(a) : F(b)][F(b) : F] = [F(a) : F] = \left[F(a) : F(b^p)\right]$$
$$\left[F(b^p) : F\right] = qs$$

مرة أخرى $F(b^p)$ حقل جزئي من $F(b)$ يؤدي إلى أن $q \leq n \Leftarrow s \leq m$.

لتكن $f(x) = \alpha_0 + \alpha_1 x + ... + x^n$ كثيرة الحدود الأصغرية لـ a على $F(b)$. لما كانت $\{1, b, ..., b^{m-1}\}$ قاعدة لـ $F(b)$ على F ، فإن لكل i ، $0 \leq i \leq n-1$ ، $\alpha_i = \lambda_{i,0} + \lambda_{i,1} b + ... + \lambda_{i,m-1} b^{m-1}$ حيث $\lambda_{i,j} \in F$ لكل $0 \leq j \leq n-1$ إضافة إلى ذلك $f(a) = 0$ يؤدي إلى أن a^p جذر لكثيرة الحدود :

$$g(x) = \alpha_0^p + \alpha_1^p x + ... + x^n$$

لكل i ، $0 \leq i \leq n-1$ فإن

$$\alpha_i^p = (\lambda_{i,0} + \lambda_{i,1} b + ... + \lambda_{i,m-1} b^{m-1})^p$$
$$= \lambda_{i,0}^p + \lambda_{i,1}^p b^p + ... + \lambda_{i,m-1}^p b^{(m-1)p} \in F(b^p)$$

وهكذا $g(x) \in F(b^p)[x]$ متحققة بـ a^p . كنتيجة لذلك :

$\left[F(a^p, b^p) : F(b^p)\right] \leq n$. ولكن a عنصر قابل للفصل على F والذي يؤدي إلى أن $F(a^p) = F(a)$ (تمرين 2) . وعليه $\left[F(a) : F(b^p)\right] \leq n$ بمعنى آخر $q \leq n$. [لاحظ أن $F(a^p) = F(a)$ و $b^p \in F(a)$ يؤدي إلى أن $F(a^p, b^p) = F(a^p)$] .

بالتالي فإن $q = n$ و $F(b) = F(b^p)$ يؤدي إلى أن b قابل للفصل على F .
وهكذا $F(a)$ توسيع قابل للفصل للحقل F .

تمرين 4

ليكن K حقل توسيع للحقل F ، $a, b \in K$ عنصران قابلان للفصل على F .
أثبت أن $F(a, b)$ توسيع قابل للفصل للحقل F .

الحل

عندما يكون F حقلاً منتهياً فإن $F(a, b)$ توسيع قابل للفصل حسب نظرية 13-48 . وفي حالة $Char\ F = 0$ ، يوجد $c \in F(a, b)$ بحيث $F(a, b) = F(c)$. $Char\ F = 0$ يؤدي إلى أن كثيرة الحدود لـ c غير القابلة للتحليل على F قابلة للفصل . وعليه c عنصر قابل للفصل على F . ويكون $F(a, b)$ هو عنصر قابل للفصل على F .

الحالة الوحيدة الباقية هي للحقل الغير منتهي بمميز $p(\neq 0)$. بمتابعة المناقشة المعطاة في إثبات نظرية 13-49 ، يمكننا بسهولة أن نجد أن $F(a, b)$ توسيع بسيط لـ F أي أن $F(a, b) = F(c)$ حيث $c = a + \lambda b, \lambda \in F$.

الآن افرض أن $[F(c) : F] = m$. بإمكاننا كتابة :

$$b = \beta_0 + \beta_1 c + \dots + \beta_{m-1} c^{m-1} , a = \alpha_0 + \alpha_1 c + \dots + \alpha_{m-1} c^{m-1}$$

مع كون $\alpha_i, \beta_i \in F$ ، $i = 0$ و $1, \dots$ و $m - 1$.

من الواضح أن $a^p = \alpha_0^p + \alpha_1 c^p + \dots + \alpha_{m-1}^{p-1} c^{(m-1)p} \in F[c^p]$ وبصورة مشابهة $b^p \in F(c^p)$.

بما أن a, b قابلان للفصل على F ، نحصل على $F(a) = F(a^p) \subseteq F(c^p)$ و $F(b) = F(b^p) \subseteq F(c^p) \Rightarrow a, b \in F(c^p)$ هذا يؤدي إلى أن $c = a + \lambda b \in F(c^p)$

أي أن $F(c) \subseteq F(c^p)$. من الواضح أن $F(c^p) \subseteq F(c)$ وعليه $F(c) = F(c^p)$ يؤدي إلى أن c قابل للفصل على F . من النتيجة في تمرين 3 نحصل على $F(a,b)$ توسيع قابل للفصل للحقل F .

تمرين 5 (نظرية ستينتز)

إذا كان K توسيعاً منتهياً للحقل F فإن K توسيع بسيط للحقل F إذا وفقط إذا كان عدد الحقول الجزئية في K والذي يحوي F منته .

الحل

افرض K توسيع بسيط للحقل F . عندئذ $K = F(c)$ لبعض $c \in K$. لتكن $f(x)$ كثيرة الحدود الأصغرية لـ c على F و L حقل جزئي من K يحوي F . لكون c عنصراً جبرياً على L ، لتكن :

$$g(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1}x^{n-1} + x^n$$

كثيرة الحدود الأصغرية لـ c على L . وحيث أن $f(x) \in F[x] \Rightarrow f(x) \in L[x]$ نحصل على $g(x)$ تقسم $f(x)$ في $L[x]$ ، وبالتالي في $K[x]$. ضع $L_0 = F(\alpha_0, \ldots, \alpha_{n-1})$. عليه $g(x) \in L_0[x]$ بالإضافة إلى ذلك $L_0 \subseteq L$ يبين أن g غير قابلة للتحليل على L_0 . أي أن $g(x)$ هي كثيرة الحدود الأصغرية لـ c على L_0 . لاحظ الآن أن $K = F(c) \subseteq L(c) \Rightarrow K = L(c)$ وعليه فإن $[K : L] = n$. مناقشة مشابهة بين أن $K = L_0(c)$ ولكون $g(x)$ كثيرة الحدود الأصغرية لـ c على L_0 نحصل على $[K : L_0] = n$. وهكذا فإن $L = L_0$. عليه فإن الحقول الجزئية الوحيدة في K والتي تحوي F هي بالصيغة $F(\beta_0, \beta_1, \ldots, \beta_{n-1})$ حيث $\beta_0 + \beta_1 x + \ldots + \beta_{s-1}x^{s-1}x^s$ هو عامل لـ $f(x)$ في $K[x]$. ولأن عدد العوامل الواحدية لـ $f(x)$ في $K[x]$ منته نحصل على أن عدد الحقول الجزئية من K والتي تحوي F يكون منتهياً .

افرض الآن أن عدد الحقول الجزئية من K والتي تحوي F منته . عندما يكون F حقلاً منتهياً ، ولأن K توسيع منته لـ F فإن K حقل منته . وبالتالي فإن $K - \{0\}$ زمرة دائرية تحت الضرب . ليكن $K - \{0\} = < c >$ عندئذ $K = F(c)$ توسيع بسيط للحقل F . عليه دعنا نفرض أن F حقل غير منته . بما أن لكل $a \in F$ ، $F(a)$ حقل جزئي من K يحوي F وأن عدد الحقول الجزئية من K والتي تحوي F منته ، بإمكاننا اختيار $b \in F$ بحيث $[F(b) : F] = n$ وأن n أكبر عدد من بين جميع الأعداد الصحيحة $[F(a) : F]$ حيث $a \in K$. ندعي أن $K = F(b)$. إذا كان ادعائنا غير صحيح بإمكاننا إيجاد $c \in K$ بحيث $c \notin F(b)$. حسب الفرض مجموعة الحقول $F(cd + b)$ حيث $d \in F$ هي مجموعة منتهية ، لأن F حقل غير منته ، يوجد $r, s \in F$ ، $r \neq s$ بحيث $F(cr + b) = F(cs + b)$. افرض أن $Z = cr + b$. عندئذ :

$$F(z) = F(cs + b) \Rightarrow cr + b, cs + b \in F(z) \Rightarrow c(r - s) =$$
$$(cr + b) - (cs + b) \in F(z) \Rightarrow c \in F(z) \text{ (لأن } r - s \neq 0)$$

إضافة إلى ذلك $b = (cr + b) - cr \in F(z) \Rightarrow F(b) \subseteq F(z)$ ولكن $c \in F(z)$ و $c \notin F(b)$ وبالتالي $F(b) \neq F(z)$ بمعنى آخر $[F(z) : F(b)] > 1$ وهذا بدوره يعطي $[F(z) : F] = [F(z) : F(b)][F(b) : F] > n$ هو تناقض مع اختيار n . لذا فإن $K = F(b)$ توسيع بسيط للحقل F .

مسائل

1- اكتب بالتفصيل برهان القضية 11-39 .

2- ليكن F حقلاً بمميز عدد أولي $p > 0$ اعتبر $f(x) = x^p - x$ ، بين أن :

(i) $f'(x) = -1$.

(ii) $f(x)$ و $f'(x)$ ليس لهما جذراً مشتركاً .

(iii) جميع جذور $f(x)$ في حقل انفلاقها على F مختلفة .

[**إرشاد** لأجل (ii) لاحظ أنه ليس لـ $f'(x)$ جذر و (iii) ينتج من (ii)] .

3- إذا كان K حقل توسيع للحقل Z_p ، برهن أن Z_p هو الحقل الجزئي الأولي لـ K .

4- برهن أن كل حقل توسيع منته لحقل منته هو توسيع بسيط (حالة خاصة أخرى لنظرية العناصر البدائية) .

5- لتكن $f(x) \in F[x]$ كثيرة حدود غير قابلة للتحليل . برهن أن HCF ، العامل المشترك الأكبر لـ $f(x)$ و $f'(x)$ هو 1 إذا وفقط إذا كان $f'(x) \neq 0$.

[**إرشاد** استخدم القضية 13-41] .

6- برهن أنه لا توجد دالة كسرية $\frac{f(t)}{g(t)}$ ، $f(t), g(t) \in F(t)$ ، $g(t) \neq 0$ بحيث ، $t = \left[\frac{f(t)}{g(t)}\right]^2$ حيث t غير محدد على F . استنتج أن $x^2 - t$ غير قابلة للتحليل على $Z_2(t)$.

7- إذا كان F حقلاً بمميز p ، برهن أن لجميع $a, b \in F$ ولجميع الأعداد الصحيحة الغير سالبة n فإن :

(i) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

(ii) $(a-b)^{p^n} = a^{p^n} - b^{p^n}$.

[**إرشاد** استخدم الاستنتاج على n] .

8- ليكن F حقلاً منتهياً و n أي عدد صحيح موجب . برهن أنه توجد على الأقل كثيرة حدود واحدة درجتها n غير قابلة للتحليل على F .

[**إرشاد** ليكن K حقل الانفلاق لكثيرة الحدود $x^{q^n} - x$ على F حيث q هو رتبة F ، فإن $[K : F] = n$ ، يعطينا $K = F(c)$ لبعض $c \in K$. عندئذ كثيرة الحدود الأصغرية للعنصر c على F هي كثيرة الحدود المطلوبة] .

9- برهن أن أي حقل مميز صفر أو أي حقل منته هو حقل تام .

10- لكل ثلاث حقول $F \in L \in K$ ، برهن أنه إذا كان K قابل للفصل على F فإن K قابل للفصل على L .

11- إذا كان K توسيعاً للحقل F ، برهن أن مجموعة عناصر K القابلة للفصل على F تشكل حقلاً جزئياً من K .

12- أوجد عنصراً بدائياً في كل من الحقول الآتية على Q :

(i) $Q(\sqrt{2}, \sqrt{3})$.

(ii) $Q(i, \sqrt{2})$.

(iii) $Q(\sqrt{2}, \sqrt[3]{5})$.

(iv) $Q(\sqrt{-3}, \sqrt{2})$.

(v) $Q(\omega, \sqrt{2})$ حيث ω الجذر التكعيبي التخيلي للواجد الصحيح .

(vi) $Q(\omega, \sqrt[3]{2})$.

13- ليكن F حقلاً بمميز $p > 0$ و $a \in F$ عنصراً بحيث لا يوجد $b \in F$ يحقق $b^p = a$ (أي أن $\sqrt[p]{a} \notin F$) عندئذ بين أن $x^p - a$ غير قابلة للتحليل وغير قابلة للفصل على F .

14- استنتج من سؤال 13 أن حقلاً بمميز $p > 0$ يكون تاماً إذا وفقط إذا كان الراسم $a \to a^p, a \in F$ أتومورفزم للحقل F .

15- استنتج من سؤال 13 أنه لأي حقل F بمميز $p(\neq 0)$ ، إذا كان π متسامياً على F فإن $F(\pi)$ ليس حقلاً تاماً .

16- ليكن F حقلاً بمميز $p > 0$ وكانت $f(x)$ كثيرة حدود غير ثابتة على F ، برهن الآتي :

(i) يوجد عدد صحيح $n \geq 0$ و $g(x) \in F[x]$ بحيث $f(x) = g(x^{p^n})$ و $g'(x) \neq 0$.

(ii) إذا كانت $f(x)$ غير قابلة للتحليل ، فإن $g(x)$ غير قابلة للتحليل .

(iii) إذا كانت $f(x)$ غير قابلة للتحليل ، فإن $g(x)$ قابلة للفصل .

(iv) إذا كانت $f(x)$ غير قابلة للتحليل فإن كل جذر لمتعددة الحدود $f(x)$ يكون تكراره p^n في حقل انفلاق $f(x)$.

(v) إذا كان العنصر a في حقل توسيع K للحقل F جبرياً على F فإنه يوجد عدد صحيح غير سالب n بحيث يكون a^{p^n} قابلاً للفصل على F .

17- إذا كانت f دالة من الحقل F إلى F بحيث $f(x) = x^{-1}$ عندما $x \neq 0$ ، و $f(0) = 0$ ، عندئذ برهن أن f أوتومورفزم إذا وفقط إذا كان F يحوي إما 2 أو 3 أو 4 عنصراً .

18- ليكن F حقلاً منتهياً بمميز يختلف عن 2 . وليكن a عنصراً غير صفري في F . بين أن a مربع عنصر في F إذا وفقط إذا كان $a^{\frac{q-1}{2}} = 1$ وأن a ليس مربعاً لأي عنصر في F إذا وفقط إذا كان $a^{\frac{q-1}{2}} = -1$ حيث $o(F) = q$.

19- ليكن Z_2 حقل الأعداد الصحيحة معيار 2 و x, y عنصران متساميان على Z_2 اعتبر $Z_2(x, y)$ حقل القواسم لـ $Z_2[x, y]$ ليكن F الحقل الجزئي $Z_2(x^2, y)$ للحقل $K = Z_2(x, y)$. بين أن :

(i) $\{1, x, y, xy\}$ قاعدة لـ K على F و (ii) كل عنصر في K يحقق كثيرة حدود على F ذات درجة على الأكثر 2 . استنتج أن K ليس توسيعاً بسيطاً للحقل F .

20- برهن أن كل توسيع منفصل منته لأي حقل هو توسيع بسيط .

21- ليكن K توسيعاً للحقل F و $a, b \in K$ عنصران جبريان على F . إذا كان واحد من a أو b منفصلاً على F برهن أن $F(a, b)$ توسيع بسيط للحقل F .

14

نظرية جالوا
GALOIS THEORY

نظرية جالوا هي إحدى النظريات الأكثر تميزاً في الجبر المجرد ، وهذه النظرية عبارة عن تركيبة ممتازة من نظرية الزمر ونظرية التوسيعات الجبرية للحقل . ولها عدة تطبيقات في نظرية المعادلات والهندسة . في الكتب التمهيدية في الجبر المجرد مثل الكتاب الذي بين أيدينا ليس بالإمكان مناقشة تفاصيل نظرية جالوا بالكامل . وبإمكان القراء المهتمين أن يجدوا تفسيرات قيمة في بعض الكتب المدرجة في المراجع . على أية حال سوف ندرس المفاهيم الأساسية ونعطي بعض التطبيقات البسيطة .

1– المونومورفزمات واستقلاليتها الخطية

لتكن S أية مجموعة و K أي حقل . ضع $M(S, K)$ رمزاً لمجموعة جميع الرواسم من S إلى K . لكل $\varphi_1, \varphi_2 \in M(S, K)$ و $a \in K$ إذا عرفنا :

$$(\varphi_1 + \varphi_2)(s) = \varphi_1(s) + \varphi_2(s)$$
$$(a\varphi_1)(s) = a\varphi_1(s), \quad \forall s \in S$$

فإن $\varphi_1 + \varphi_2 \in M(S, K)$ و $a\varphi_1 \in M(S, K)$. تحت عمليتي الجمع والضرب هاتين فإن $M(S, K)$ تصبح فضاءً متجهاً على K . المتجه الصفري في $M(S, K)$ هو الراسم $\overline{0} : S \to K$ المعرف على النحو الآتي : $\overline{0}(s) = 0$ لكل $s \in S$ عليه يمكننا القول أن العناصر $\varphi_1, \varphi_2, \ldots, \varphi_n \in M(S, K)$ مستقلة خطياً على K ، إذا كان لأي $a_1, a_2, \ldots, a_n \in K$

$$a_1\varphi_1 + a_2\varphi_2 + \ldots + a_n\varphi_n = \overline{0}$$

يؤدي إلى أن $a_i = 0$ لكل $i = 1, 2, \ldots, n$ أي أن :

$a_1\varphi_1(s) + a_2\varphi_2(s) + \ldots + a_n\varphi_n(s) = 0$ لجميع $s \in S$ يؤدي إلى أن $a_i = 0$ لكل $i = 1, 2, \ldots, n$.

بصورة خاصة اعتبر الحقل E والفضاء المتجهي $M(E, K)$.

ليكن $\sigma_1, \sigma_2, \ldots, \sigma_n$ أي n في المونومورفزمات المختلفة من E إلى K . من الواضح $\sigma_i \in M(E, K)$ لكل $i = 1, 2, \ldots, n$. عليه بإمكاننا التحدث عن استقلالها أو ارتباطها الخطي على K .

نظرية 14-1

ليكن E و K حقلين . إذا كان $\sigma_1, \sigma_2, \ldots, \sigma_n$ أي n من المونومورفزمات المختلفة من E إلى K فإنها تكون مستقلة خطياً على K .

البرهان

نبرهن النظرية بالاستنتاج الرياضي على n . الآن لأي $a_1 \in K$ فإن $a_1\sigma_1 = \overline{0} \Rightarrow a_1\sigma_1(x) = 0$ لجميع $x \in E$. هذا يؤدي إلى أن $a_1 = 0$ لأن $\sigma_1(x) \neq 0$ لجميع $E \ni (x \neq 0)$ عليه فإن النتيجة تتحقق عندما $n = 1$. دعنا نفرض أن النتيجة محققة لأية مجموعة من المونومورفزمات من E إلى K والتي عدد عناصرها أقل من n .

نفرض بعضاً من $a_i \in K$ ، $i = 1, 2, \ldots, n$ غير صفري وأن :

$$a_1\sigma_1 + a_2\sigma_2 + \ldots + a_n\sigma_n = \overline{0} \qquad (1)$$

فروض الاستنتاج تؤدي إلى أن جميع a_i تختلف عن الصفر .

بما أن $a_n \neq 0$ ، فبقسمة (1) على a_n نحصل على :

$$b_1\sigma_1 + b_2\sigma_2 + \ldots + b_{n-1}\sigma_{n-1} + \sigma_n = \overline{0} \qquad (2)$$

حيث $b_i = a_i a_n^{-1}, \quad \forall\, i = 1, 2, 3, \ldots, n-1$

بما أن σ_1 و σ_n مختلفان فإنه يوجد $x_1 \in E$ بحيث $\sigma_1(x_1) \neq \sigma_n(x_n)$ من الواضح $x_1 \neq 0$. لكل $x \in E$ لدينا من (2) :

$$b_1\sigma_1(x_1x) + b_2\sigma_2(x_1x) + \ldots + \sigma_n(x_1x) = 0$$

أي أن :

$$b_1\sigma_1(x_1)\sigma_1(x) + b_2\sigma_2(x_1)\sigma_2(x) + \ldots + \sigma_n(x_1)\sigma_n(x) = 0 \qquad (3)$$

عليه :

$$b_1\,\frac{\sigma_1(x_1)}{\sigma_n(x_1)}\,\sigma_1(x) + b_2\,\frac{\sigma_2(x_1)}{\sigma_n(x_1)}\,\sigma_2(x) + \ldots + \sigma_n(x) = 0 \quad \forall\, x \in E \qquad (4)$$

من (2) يكون :

$$b_1\sigma_1(x) + b_2\sigma_2(x) + \ldots + \sigma_n(x) = 0, \quad \forall\, x \in E \qquad (5)$$

بطرح (5) من (4) نحصل على :

$$b_1\left[\frac{\sigma_1(x_1)}{\sigma_n(x_1)} - 1\right]\sigma_1(x) + b_2\left[\frac{\sigma_2(x_1)}{\sigma_n(x_1)} - 1\right]\sigma_2(x) + \ldots + b_{n-1}\left[\frac{\sigma_{n-1}(x_1)}{\sigma_n(x_1)} - 1\right]\sigma_{n-1}(x) = 0, \quad \forall\, x \in E$$

وحيث أن $b_1\left[\frac{\sigma_1(x_1)}{\sigma_n(x_1)} - 1\right] \neq 0$ فإن المعادلة الأخيرة تؤدي إلى أن $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ مرتبطة خطياً على K وهذا يناقض فروض الاستنتاج .

إذاً $\sigma_1, \sigma_2, \ldots, \sigma_n$ مستقلة خطياً على K وهذا يثبت النظرية . □

بأخذ $E = K$ فإننا نحصل على النتيجة التالية .

نتيجة 14-2

أي مجموعة من أوتومورفزمات K تكون مستقلة خطياً على K . □

قضية 14-3

مجموعة جميع الأوتومورفزمات لحقل ما تشكل زمرة تحت عملية تركيب الرواسم .

البرهان

لتكن $Aut\,(K)$ مجموعة جميع أوتومورفزمات الحقل K ، بما أن الراسم المحايد I على K هو أوتومورفزم للحقل K فإن $I \in Aut\,(K)$.

(i) **الانغلاق** : ليكن $\sigma_1, \sigma_2 \in Aut\,(K)$ فإن كل من σ_1, σ_2 هو راسم أحادي وفوقي . عليه فإن $\sigma_1\sigma_2$ هو أيضاً راسم أحادي وفوقي ، إضافة إلى ذلك لأي $x, y \in K$ فإن :

$$\begin{aligned}
\sigma_1\sigma_2(x+y) &= \sigma_1[\sigma_2(x+y)] + \sigma_1[\sigma_2(x)+\sigma_2(y)] \\
&= \sigma_1[\sigma_2(x)] + \sigma_1[\sigma_2(y)] = \sigma_1\sigma_2(x) + \sigma_1\sigma_2(y) \\
\sigma_1\sigma_2(xy) &= \sigma_1[\sigma_2(xy)] = \sigma_1[\sigma_2(x)\sigma_2(y)] \\
&= \{\sigma_1[\sigma_2(x)]\}\{\sigma_1[\sigma_2(y)]\} = [\sigma_1\sigma_2(x)][\sigma_1\sigma_2(y)]
\end{aligned}$$

هذا يبين أن $\sigma_1\sigma_2$ أوتومورفزم للحقل F . أي أن $\sigma_1\sigma_2 \in Aut\,(K)$.

(ii) **التنسيقية** : تستنتج من كون عملية تركيب الرواسم عملية تنسيقية بصورة عامة .

(iii) **وجود المحايد** : الراسم المحايد I على K هو المحايد في $Aut\,(K)$.

(iv) **وجود المعكوس** : اعتبر أي $\sigma \in Aut\,(K)$. بما أن σ راسم أحادي وفوقي فإن σ^{-1} (معكوس الراسم σ) له وجود حيث لكل $x \in K$ ، $\sigma^{-1}(x) = y$ إذا وفقط إذا كان $\sigma(y) = x$. اعتبر الآن أن $x_1, x_2 \in K$ وليكن $\sigma^{-1}(x_1) = y_1$ ، $\sigma^{-1}(x_2) = y_2$ ، فإن $\sigma(y_1) = x_1$ ، $\sigma(y_2) = x_2$. عليه فإن :

$$\sigma(y_1 + y_2) = \sigma(y_1) + \sigma(y_2) = x_1 + x_2$$

و

$$\sigma(y_1y_2) = \sigma(y_1)\sigma(y_2) = x_1x_2$$

وهكذا فإن

$$\sigma^{-1}(x_1 + x_2) = y_1 + y_2 = \sigma^{-1}(x_1) + \sigma^{-1}(x_2)$$

و

$$\sigma^{-1}(x_1x_2) = y_1y_2 = \sigma^{-1}(x_1)\,\sigma^{-1}(x_2)$$

بالتالي فإن σ^{-1} هو أوتومورفزم للحقل K أي أن $\sigma^{-1} \in Aut(K)$ وهذا يثبت أن $Aut(K)$ زمرة . □

تعريف 14-4

ليكن F حقلاً و K أي حقل توسيع للحقل F . عندئذ يقال للأوتومورفزم σ للحقل K أنه F أوتومورفزم إذا كان $\sigma(x) = x$ لكل $x \in F$ (أي أن σ يبقي كل عنصر في F ثابتاً) .

من الواضح أن I الأوتومورفزم المحايد للحقل K هو F أوتومورفزم) . ليكن σ_1, σ_2 كلاهما F– أوتومورفزم للحقل K فإن $\sigma_1\sigma_2^{-1} \in Aut\,(K)$ لأن $Aut\,(K)$ زمرة . كذلك لكل $x \in F$ فإن $\sigma_2(x) = x, \sigma_1(x) = x$ وهذا يؤدي إلى أن $\sigma_1(x) = x$ و $\sigma_2^{-1}(x) = x$ ويؤدي كذلك إلى أن $\sigma_1\sigma_2^{-1}(x) = \sigma_1(\sigma_2^{-1}(x)) = \sigma_1(x) = x$ عليه فإن $\sigma_1^{-1}\sigma_2$ هو أيضاً F– أوتومورفزم للحقل K . وهكذا فإن مجموعة F– أوتومورفزمات الحقل F عبارة عن زمرة جزئية من جميع أوتومورفزمات K .

اصطلاح : سوف يرمز لزمرة جميع F– أوتومورفزمات الحقل K بالرمز $G(K, F)$ وتسمى هذه الزمرة زمرة جالوا للحقل K على F .

قضية 14-5

ليكن K أي حقل توسيع للحقل F و $a \in K$ عنصراً جبرياً على F . فإن لكل F– أوتومورفزم σ للحقل K فإن $\sigma(a)$ هو مرافق للعنصر a على F .

البرهان

لتكن $f(x) = x^n + \alpha_{n-1}x^{n-1} + \alpha_{n-2}\alpha^{n-2} + \ldots + \alpha_0$ كثيرة حدود الأصغرية للعنصر a على F . فإن $a^n + \alpha_{n-1}a^{n-1} + \alpha_{n-2}a^{n-2} + \ldots + \alpha_0 = 0$

عليه
$$\begin{aligned} 0 &= \sigma(0) = \sigma(a^n + \alpha_{n-1}a^{n-1} + \alpha_{n-2}a^{n-2} + \dots + \alpha_0) \\ &= [\sigma(a)]^n + \sigma(\alpha_{n-1})[\sigma(a)]^{n-1} + \sigma(\alpha_{n-2})[\sigma(a)]^{n-2} + \dots + \sigma(\alpha_0) \\ &= [\sigma(a)]^n + \alpha_{n-1}[\sigma(a)]^{n-1} + \alpha_{n-2}[\sigma(a)]^{n-2} + \dots + \alpha_0 \end{aligned}$$

لأن $\sigma(\alpha_i) = \alpha_i$ لكل $i = 1, 2, \dots, n-1$.

هذا يبن أن $\sigma(a)$ هو أيضاً جذر لكثيرة الحدود $f(x)$. عليه فإن $\sigma(a)$ مرافق للعنصر a على F . □

ملاحظة : ليكن $K = F(a_1, a_2, \dots, a_n)$ أي توسيع جبري منته حيث $\{a_1, a_2, \dots, a_n\}$ قاعدة للفضاء K . فإنه يمكن التعبير عن كل $x \in K$ بالصورة :

$$x = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$$

فإذا فرضنا أن σ هو F– أوتومورفزم للحقل K فإن :

$$\begin{aligned} \sigma(x) &= \sigma(\alpha_1)\sigma(a_1) + \sigma(\alpha_2)\sigma(a_2) + \dots + \sigma(\alpha_n)\sigma(a_n) \\ &= \alpha_1\sigma(a_1) + \alpha_2\sigma(a_2) + \dots + \alpha_n\sigma(a_n) \end{aligned}$$

عليه إذا كانت العناصر $\sigma(a_1)$ ، $\sigma(a_2)$ ، ... ، $\sigma(a_n)$ معلومة فإن $\sigma(x)$ يكون معلوماً . أي أن σ يتحدد بصورة تامة ، بصور عناصر القاعدة لـ K . وبصورة أكثر تعميماً إذا كان K منتهي التولد على F و $a_1, a_2, \dots, a_n$. مجموعة تولد K على F ، فإن σ يتعين بواسطة العناصر $\sigma(a_1), \sigma(a_2), \dots, \sigma(a_n)$.

قضية 6-14

لتكن G زمرة من أوتومورفزمات الحقل K فإن المجموعة $F_0 = \{x \in K \mid \sigma(x) = x, \ \ \forall \sigma \in G\}$ هي حقل جزئي من K .

البرهان

بما أن $\sigma(0) = 0$ ، $\sigma(1) = 1$ لكل $\sigma \in G$ ، فإن $0, 1 \in F_0$. ليكن $x, y \in F_0$. فإن لكل $\sigma \in G$ يكون $\sigma(x) = x$ ، $\sigma(y) = y$ ويكون $\sigma(x - y) = \sigma(x) - \sigma(y) = x - y$.

وعندما $y \neq 0$ فإن $\sigma(xy^{-1}) = \sigma(x)\sigma(y^{-1}) = xy^{-1}$ ومن ثم فإن $x - y \in F_0$ ،
وعندما $y \neq 0$ فإن $xy^{-1} \in F_0$. وهكذا فإن F_0 حقل جزئي من K . □

تعريف 7-14

لتكن G زمرة من أوتومورفزمات الحقل K . الحقل الجزئي F_0 من K الذي يحوي جميع العناصر $x \in K$ بحيث $\sigma(x) = x$ لكل $\sigma \in G$ يسمى بالحقل المثبت تحت G .
سوف يرمز للحقل المثبت تحت G بالرمز $\Gamma(G)$ أو K_G .

ملاحظة 1 ليكن P الحقل الجزئي الأولي للحقل K . نعلم أن P محتوى في كل حقل جزئي من K . بوجه خاص إذا كان F_0 هو الحقل المثبت تحت G ، فإن $P \subseteq F_0$ ويكون $\sigma(x) = x$ لكل $x \in P$ ولكل $\sigma \in G$. لذا فإن كل أوتومورفزم للحقل K هو P– أوتومورفزم .

ملاحظة 2 كل عنصر في G يمكن اعتباره F_0– أوتومورفزم للحقل K حيث $F_0 = \Gamma(G)$.

ملاحظة 3 إذا كان K حقل توسيع للحقل F و G زمرة عناصرها F– أوتومورفزمات للحقل K ، فإن $F_0 \supseteq F$ ، الحقل المثبت تحت G .

قبل أن نواصل نتوقف قليلاً لإعطاء بعض الأمثلة على المفاهيم التي عرضناها قبل ذلك .

مثال 1

ليكن $K = Q(\sqrt{2})$ ، كثيرة الحدود الأصغرية للعنصر $\sqrt{2}$ على Q هي $x^2 - 2$ وأن $\{1, \sqrt{2}\}$ تمثل قاعدة لـ K على Q . فيكون أي عنصر $x \in K$ هو على الصورة $x = a + b\sqrt{2}$ ، $a, b \in Q$. ليكن σ أي أوتومورفزم للحقل K فإن $\sigma(a) = a$ لكل

$a \in Q$. إضافة إلى ذلك فإن $\sigma(\sqrt{2})$ هو مرافق $\sqrt{2}$ على Q . ولما كان $\pm\sqrt{2}$ هما الجذران الوحيدان لكثيرة الحدود $x^2 - 2$ فإننا نحصل على $\sigma(\sqrt{2}) = \sqrt{2}$ أو $\sigma(\sqrt{2}) = -\sqrt{2}$.

حالة 1 عندما $\sigma(\sqrt{2}) = \sqrt{2}$ فإن :

$\sigma(x) = \sigma(a) + \sigma(b)\sigma(\sqrt{2}) = a + b\sqrt{2} = x$ لكل $x \in K$ ، هذا يعطينا $\sigma = I$ ، الراسم المحايد على K .

حالة 2 إذا كان $\sigma(\sqrt{2}) = -\sqrt{2}$ فإن $\sigma(x) = a - b\sqrt{2}$ ، إذاً $Aut\,(K)$ تحوي عنصرين فقط هما I والأوتومورفزم η بحيث $\eta(x) = a - b\sqrt{2}$ لكل $x = a + b\sqrt{2} \in K$. فإذا فرضنا أن x ينتمي إلى الحقل المثبت F_0 تحت $Aut\,(K)$ فإن $\eta(x) = x$. أي أن $a - b\sqrt{2} = a + b\sqrt{2}$ عليه $b = 0$ ويكون $x = a \in Q$ ، وهكذا فإن $F_0 \subseteq Q$. من ناحية ثانية $Q \subseteq F_0$ لأن Q حقل أولي . عليه فإن Q هو الحقل المثبت تحت $Aut\,(K)$.

مثال 2

ضع $K = Q(\sqrt[3]{2})$. كثيرة الحدود الأصغرية للعنصر $\sqrt[3]{2}$ على Q هي $x^3 - 2$ ، ولها جذر حقيقي واحد فقط وهو $\sqrt[3]{2}$. K هو حقل من أعداد حقيقية ، عليه $\sqrt[3]{2}$ هو الجذر الوحيد لكثيرة الحدود $x^3 - 2$ في K . إذا كان σ أي أوتومورفزم للحقل K ، فإن $\sigma(\sqrt[3]{2}) \in K$ هو جذر لكثيرة الحدود $x^3 - 2$. عليه $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. ليكن x عنصراً في K . يمكن التعبير عن x بالصورة $\alpha + (\sqrt[3]{2})\beta + (\sqrt[3]{2})^2\gamma$ حيث $\alpha, \beta, \gamma \in Q$. عليه :

$$\sigma(x) = \sigma(\alpha) + \sigma(\sqrt[3]{2})\sigma(\beta) + [\sigma(\sqrt[3]{2})]^2\sigma(\gamma) = \alpha + \sqrt[3]{2}\beta + (\sqrt[3]{2})^2\gamma = x$$

هذا يعني أن $\sigma = I$ ، عليه فإن $Aut\,(K) = \{I\}$.

في هذه الحالة الحقل المثبت تحت $Aut\,(K)$ هو نفسه K .

مثال 3

ليكن L أي حقل بمميز 2 و t أي عنصر غير محدد على L . ليكن $F = L(t)$ و K حقل انفلاق كثيرة الحدود $x^2 - t$ على F . فإذا كان $a \in K$ جذراً لكثيرة الحدود $x^2 - t$ ، فإن $t = a^2$ و $x^2 - t = x^2 - a^2 = (x - a)^2$ ، هذا يبين أن a هو المرافق الوحيد للعنصر a على F . عليه لكل $\sigma \in G(K, F)$ ، $\sigma(a) = a$ (قضية 14-5) لنأخذ $x \in K$ فيكون $x = \alpha + a\beta$ لبعض $\alpha, \beta \in F$ لأن $K = F(a)$. عليه $\sigma(x) = \sigma(\alpha) + \sigma(a)\,\sigma(\beta) = \alpha + a\beta = x$. بالتالي $\sigma = I$ و $Aut\ K = \{I\}$. في هذه الحالة الحقل المثبت تحت $G(K, F)$ هو K نفسه .

نظرية 14-8 (آرتين)

لتكن G زمرة جزئية منتهية لأوتومورفزمات الحقل K ، F_0 الحقل المثبت تحت G . عندئذ درجة K على F_0 يساوي رتبة الزمرة G .

البرهان

ليكن $o(G) = n$ فسوف نبين أنه :

(i) إذا كان $[K : F_0]$ منته وليكن m مثلاً ، فإن $n \leq m$.

(ii) $[K : F_0]$ منته ، وليكن m ، فإن $m \leq n$.

(i) افرض $m < n$ ، وأن $\sigma_1 = I, \sigma_2, \ldots, \sigma_n$ عناصر في G .

لتكن $\{x_1, x_2, \ldots, x_n\}$ قاعدة لـ K على F_0 . اعتبر النظام الآتي لعدد m من المعادلات الخطية المتجانسة .

$$\sigma_1(x_j)u_1 + \sigma_2(x_j)u_2 + \ldots + \sigma_n(x_j)u_n = 0, \forall\ j = 1, 2, \ldots, m \qquad (1)$$

لما كان عدد المعادلات أقل من عدد المتغيرات فإن المعادلة (1) لها حل غير تافه ، مثلاً $(y_1, y_2, \ldots, y_n)$ ، ومن ثم تكون :

$$\sigma_1(x_j)y_1 + \sigma_2(x_j)y_2 + \ldots + \sigma_n(x_j)y_n = 0, \forall\ j = 1, 2, \ldots m \qquad (2)$$

اعتبر أي عنصر $x \in K$ ، فإن $x = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_m x_m$ لبعض $\alpha_i \in F_0$ لكون $\{x_1, x_2, \ldots, x_m\}$ قاعدة لـ K على F_0 . في (2) بضرب المعادلة التي رقمها j في α_j ، وجمع المعادلات الناتجة واستخدام حقيقة أن $\sigma_i(\alpha_j) = \alpha_j$ لكل i, j نحصل على :

$$y_1\sigma_1(x) + y_2\sigma_2(x) + \ldots + y_n\sigma_n(x) = 0, \quad \forall\, x \in K$$

عليه فإن $y_1\sigma_1 + y_2\sigma_2 + \ldots + y_n\sigma_n = \overline{0}$ مع كون واحدة على الأقل من $y_j \neq 0$. هذا مستحيل (نظرية 14-1) . عليه $m \not< n$ وهكذا فإن $m \geq n$.

(ii) افرض وجود $n+1$ من العناصر المستقلة خطياً في K على F_0 ولتكن $x_1, x_2, \ldots, x_{n+1}$. اعتبر النظام المتكون و n من المعادلات الخطية المتجانسة في $n+1$ من المجاهيل .

$$\sigma_j(x_1)u_1 + \sigma_j(x_2)u_2 + \ldots + \sigma_j(x_{n+1}) = 0, \forall\, j = 1, 2, \ldots, n \qquad (3)$$

بما أن عدد المتغيرات أكبر من عدد المعادلات ، فإن المعادلات (3) المتجانسة هذه يكون لها حل غير تافه ، $(z_1, z_2, \ldots, z_{n+1})$ مثلاً بأقل عدد من المركبات غير الصفرية وليكن r . يمكننا إعادة ترقيمهم . وافرض أن $z_n = 0$ لكل $j \geq r+1$.

عندئذ (3) تعطي :

$$\sigma_j(x_1)z_1 + \sigma_j(x_2)z_2 + \ldots + \sigma_j(x_r)z_r = 0, \forall\, j = 1, 2, \ldots, n \qquad (4)$$

بقسمة المعادلات على z_r وبوضع $z_i' = \frac{z_i}{z_r}$ لكل i ، نحصل على :

$$\sigma_j(x_1)z_1' + \sigma_j(x_2)z_2' + \ldots + \sigma_j(x_{r-1})z_{r-1}' + \sigma_j(x_r) = 0 \quad \forall\, j \qquad (5)$$

الآن عندما $j = 1$ ، $\sigma_j = I$ ، فإن $\sigma_1(x_i) = x_i$ لكل i . من (5) نحصل على :

$$x_1z_1' + x_2z_2' + \ldots + x_{r-1}z_{r-1}' + x_r = 0 \qquad (6)$$

إذا كانت العناصر $z_1', z_2', \ldots, z_{r-1}'$ جميعها تنتمي إلى F_0 فإن (6) تعطي أن $x_1, x_2, \ldots, x_r$ مرتبطة خطياً على F_0 . وهذا غير ممكن . وبالتالي فإن واحدة على الأقل منها ولتكن z_1' لا تنتمي إلى F_0 . وزيادة على ذلك لاحظ أن $r \neq 1$ لأن غير ذلك يجعل $z' = 0$. لما كان

$z_1' \notin F_0$ ، يوجد بعض $\sigma_i \in G$ بحيث $\sigma_i(z_1') \neq z_1'$. بتأثير σ_i على (5) نحصل على

$$\sigma_i\left[\sigma_j(x_1)z_1'\right] + \sigma_i\left[\sigma_j(x_2)z_2'\right] + \ldots + \sigma_i\left[\sigma_j(x_{r-1})z_{r-1}'\right] + \sigma_i\sigma_j(x_r) = 0, \quad \forall\ j = 1, 2, \ldots, n$$

أي أن

$$\sigma_i\sigma_j(x_1)\sigma_i(z_1') + \sigma_i\sigma_j(x_2)\sigma_i(z_2')j + \ldots + (\sigma_i\sigma_j)\,(x_{r-1})\sigma_i(z_{r-1}') + \sigma_i\sigma_j(x_r) = 0 \quad \forall\ j = 1, 2, \ldots, n$$

من ناحية أخرى $\sigma_i(G) = G$ ، عليه كل $\sigma_k \in G$ هو بالصيغة $\sigma_i\sigma_j$ ، نحصل على

$$\sigma_j(x_1)\sigma_i(z_1') + \sigma_j(x_2)\sigma_i(z_2') + \ldots + \sigma_j(x_{r-1})\sigma_i(z_{r-1}') + \sigma_j(x_r) = 0, \quad \forall\ j = 1, 2, \ldots, n \tag{7}$$

بطرح (7) من (5) نحصل على :

$$\sigma_j(x_1)\left[z_1' - \sigma_i(z_1')\right] + \sigma_j(x_2)\left[z_2' - \sigma_i(z_2')\right] + \ldots + \sigma_j(x_{r-1})\left[z_{r-1}' - \sigma_i(z_{r-1}')\right] = 0, \quad \forall\ j = 1, 2, \ldots, n \tag{8}$$

الآن نضع $t_k = z_k' - \sigma_i(z_k')$ لكل $k = 1, 2, \ldots, r-1$ و $t_k = 0$ لكل $k = r, r+1, \ldots, n+1$ عندئذ (8) تعطي :

$$\sigma_j(x_1)t_1 + \sigma_j(x_2)t_2 + \ldots + \sigma_j(x_{r-1})t_{r-1} + \sigma_j(x_r)t_r + \ldots + \sigma_j(x_{n+1})t_{n+1} = 0, \quad \forall\ j = 1, 2, \ldots, n \tag{9}$$

كذلك فإن $t_1 \neq 0$ لأن $z_1' \neq \sigma_i(z_1')$ عليه يكون $(t_1, t_2, \ldots, t_{r-1}, 0, 0, \ldots, 0)$ حلاً غير تافه لنظام المعادلات (3) وله أقل من r من المركبات غير الصفرية . لكن حسب اختيارنا فإن $(z_1 z_2, \ldots, z_r, 0, 0, \ldots, 0)$ حل غير تافه للنظام (3) له أقل عدد من المركبات التي تختلف عن الصفر وعددها r . إذاً حصلنا على تناقض . وهذا يبين أن $m \leq n$ وبالتالي فإن $m = n$ أي أن $[K : F_0] = o(G)$. وهذا يكمل البرهان . □

ملاحظة 1 لتكن G أية زمرة (ليست بالضرورة منتهية) من أوتومورفزمات الحقل K بحيث $[K : F_0] = m$ منته حيث F_0 يمثل الحقل المثبت تحت G . في الجزء الأول من إثبات

النظرية السابقة لم نكن بحاجة لفرض أن G زمرة منتهية ، في الواقع حصلنا على أن G لا يمكن أن تحوي أكثر من m من العناصر .

ملاحظة 2 ليكن K توسيعاً منتهياً للحقل F و G زمرة جميع F أوتومورفزمات الحقل K . عندئذ يكون الحقل المثبت F_0 تحت G حاوياً F . ويكون $[K : F_0] \leq [K : F]$ ومنها $o(G) \leq [K : F]$.

تعريف 9-14

يقال لتوسيع منته K للحقل F أنه توسيع جالوا للحقل F ، إذا كان F هو الحقل الجزئي المثبت للحقل F تحت الزمرة $G(K, F)$ لجميع F- أوتومورفزمات الحقل K .

نتيجة 10-14

ليكن $K = F(\alpha)$ توسيعاً بسيطاً منتهياً قابلاً للفصل للحقل F عندئذ يكون K حقل انفلاق لكثيرة الحدود الأصغرية للعنصر α على F إذا وفقط إذا كان F هو الحقل المثبت تحت زمرة جميع F- أوتومورفزمات الحقل K .

البرهان

لتكن $f(x)$ كثيرة الحدود الأصغرية للعنصر α على F نفرض أن $\deg f(x) = m$ فإن $[K : F] = m$. لتكن $\alpha_1 = \alpha, \alpha_2, \alpha_3, \dots \alpha_r$ المرافقات المختلفة للعنصر α في K . عندئذ $K = F(\alpha_i)$ لكل $i = 1, 2, \dots r$. لكل i يوجد F- أوتومورفزم σ_i للحقل K بحيث $\sigma_i(\alpha_1) = \alpha_i$. بما أن α_1 يولد K على F فكل σ_i يتحدد بطريقة واحدة فقط . إضافة لذلك لأي F- أوتومورفزم σ للحقل K ، ولأن $\sigma(\alpha_1)$ مرافق للعنصر α_1 (قضية 5-14) . فإن $\sigma(\alpha_1) = \alpha_i$ لبعض α_i . من هذا ينتج أن $\sigma = \sigma_i$. وبالتالي فإن الزمرة $G(K, F)$ تكون من $\sigma_1, \sigma_2, \dots, \sigma_r$. ليكن F_0 الحقل المثبت تحت $G(K, F)$. عندئذ

حسب النظرية السابقة $[K : F_0] = o[G(K, F)] = r$. عليه $F = F_0$ إذا وفقط إذا كان $r = m$ لذلك فإن F هو الحقل المثبت تحت G إذا وفقط إذا كانت جميع جذور $f(x)$ وعددها m تنتمي إلى K بمعنى إذا وفقط إذا كان K هو حقل انفلاق $f(x)$ على F .

مثال 4

اعتبر أي عدد أولي p . لتكن $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ ، عندئذ :

$$f(x+1) = x^{p-1} + pC_1 x^{p-2} + pC_2 x^{p-3} + \ldots + pC_{p-2} x + p$$

بما أن p يقسم معاملات $x^{p-2}, x^{p-3}, \ldots, x$ والحد الثابت p ، p^2 لا يقسم الحد الثابت و p لا يقسم 1 وهو معامل x^{p-1} ، فحسب معيار آيزنستن $f(x+1)$ غير قابلة للتحليل على Q ، عليه فإن $f(x)$ غير قابلة للتحليل .

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + x + 1)$$

عليه لأي جذر مركب α لـ $x^p - 1$ إذا كان $\alpha \neq 1$ ، فإن α جذر لكثيرة الحدود $x^{p-1} + x^{p-2} + \ldots + x + 1$.

اعتبر $\alpha_i = e^{\frac{2\pi i}{p}}, i = 1, 2, \ldots, p-1$. فإن أي من α_i لا يساوي 1 وجميعها مختلفة . عليه $\alpha_1, \alpha_2, \ldots, \alpha_{p-1}$ هي $p-1$ من الجذور المختلفة لـ $f(x)$ على Q ويكون $K = Q(\alpha_1, \alpha_2, \ldots, \alpha_{p-1})$ هو حقل انفلاق كثيرة الحدود الأصغرية $f(x)$ لـ α_1 على Q .

وهكذا فإن الحقل المثبت للزمرة G لكل الـ Q– أوتومورفزمات للحقل K هو Q .

من ناحية أخرى Q عبارة عن حقل جزئي أولي ، عليه كل أوتومورفزم للحقل K هو Q– أوتومورفزم . إذاً Q هو الحقل المثبت تحت زمرة جميع الأوتومورفزمات للحقل K . وهذا يعني أن K توسيع جالوا للحقل Q .

مثال 5

اعتبر $K = Q\left(\sqrt{-3}, \sqrt[3]{2}\right)$. K هو حقل انفلاق $x^3 - 2$ على Q . لتكن G زمرة جميع أوتومورفزمات الحقل K . في الواقع G هي زمرة جميع Q– أوتومورفزمات الحقل

K . بما أن $[K : Q] = 6$ فإن $o(G) \le 6$ (حسب ملاحظة 2 بعد النظرية 14-8) . افرض أن $x^3 - 2$ غير قابلة للتحليل على $F = Q\left(\sqrt{-3}\right)$ فإن على الأقل أحد جذور كثيرة الحدود $x^3 - 2$ وليكن β ينتمي إلى $Q\left(\sqrt{-3}\right)$. فيكون $Q(\beta) \subseteq Q\left(\sqrt{-3}\right)$.

وهكذا فإن $\left[Q\left(\sqrt{-3}\right) : Q\right] \mid [Q(\beta) : Q]$. من ناحية ثانية $[Q(\beta) : Q] = 3$ و $\left[Q\left(-\sqrt{3}\right) : Q\right] = 2$ ومنها نحصل على أن 3 يقسم 2 وهذا لا يجوز . بذلك حصلنا على تناقض .

بالتالي فإن $x^3 - 2$ غير قابلة للتحليل على F . الآن $K = Q\left(\sqrt{-3}, \sqrt[3]{2}\right) = F\left(\sqrt[3]{2}\right)$ هو توسيع بسيط للحقل F ولأنه يحوي جميع جذور $x^3 - 2$ فإن K هو حقل انفلاق كثيرة الحدود الأصغرية $x^3 - 2$ للعنصر $\sqrt[3]{2}$ على F . وهكذا فإن الزمرة G_1 لجميع F- أوتومورفزمات الحقل K هي زمرة بحيث F هو الحقل الثابت تحت G_1 . عليه فإن $o\,(G_1) = [K : F] = 3$. على أية حالة G_1 زمرة جزئية للزمرة G ، بالتالي $3 \mid o\,(G)$. مرة أخرى $x^2 + 3$ غير قابلة للتحليل على $F_1 = Q\left(\sqrt[3]{2}\right)$ و K هو حقل انفلاق $x^2 + 3$ على F_1 ، مع $[K : F_1] = 2$. من ذلك نحصل أيضاً على أن $2 \mid o\,(G)$. وهكذا فإن $6 \mid o\,(G)$. هذا يبين أن $6 \le o\,(G)$. عليه $o\,(G) = 6$ وهذا يبرهن أن $[K : Q] = o\,(G)$ وبالتالي Q هو الحقل المثبت تحت G و K توسيع جالوا للحقل Q .

مثال 5-a

اعتبر كثيرة الحدود $x^4 - x^2 + 1$ على Q :

$$x^4 - x^2 + 1 = (x^2 + \sqrt{3}x + 1)\,(x^2 - \sqrt{3}x + 1) \Rightarrow x = \frac{\pm\sqrt{3} + i}{2}$$

حقل الانفلاق K لكثيرة الحدود $x^4 - x^2 + 1$ على Q هو الحقل $Q\left(\frac{\pm\sqrt{3} \pm i}{2}\right) = Q\left(\sqrt{3}, i\right)$. وأن $[K : Q] = 4$. سوف نحدد زمرة جالوا للحقل K على

Q . لما كانت $x^4 - x^2 + 1$ غير قابلة للتحليل على Q (برهن !) ، يوجد $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in G(K, Q)$.

بحيث $\sigma_1\left(\frac{\sqrt{3}+i}{2}\right) = \frac{\sqrt{3}+i}{2}$ ، $\sigma_2\left(\frac{\sqrt{3}+i}{2}\right) = \frac{\sqrt{3}-i}{2}$ ، $\sigma_3\left(\frac{\sqrt{3}+i}{2}\right) = \frac{-\sqrt{3}-i}{2}$ ، $\sigma_4\left(\frac{\sqrt{3}+i}{2}\right) = \frac{-\sqrt{3}+i}{2}$.

إضافة إلى ذلك لأي $\sigma \in G(K, Q)$ يكون $\sigma\left(\frac{\sqrt{3}+i}{2}\right)$ جذراً لكثيرة الحدود $x^4 - x^2 + 1$

لذا فإن $G(K, Q) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$. الآن :

$$\sigma_1\left(\frac{\sqrt{3}+i}{2}\right) = \frac{\sqrt{3}+i}{2} \Rightarrow \sigma_1\left(\frac{\sqrt{3}-i}{2}\right) = \sigma_1\left(\frac{2}{\sqrt{3}+i}\right)$$

$$= \left(\frac{\sqrt{3}+i}{2}\right)^{-1} = \frac{2}{\sqrt{3}+i} = \frac{\sqrt{3}-i}{2},$$

$$\sigma_1\left(\frac{-\sqrt{3}-i}{2}\right) = -\sigma_1\left(\frac{\sqrt{3}+i}{2}\right) = \frac{-\sqrt{3}-i}{2}$$

و

$$\sigma_1\left(\frac{-\sqrt{3}+i}{2}\right) = \frac{-\sqrt{3}+i}{2}$$

هذا يبين أن

$$\sigma_1\left(\sqrt{3}\right) = \sigma_1\left(\frac{\sqrt{3}+i}{2} + \frac{\sqrt{3}-i}{2}\right) = \frac{\sqrt{3}+i}{2} + \frac{\sqrt{3}-i}{2} = \sqrt{3}$$

$$\sigma_1(i) = \sigma_1\left(\frac{\sqrt{3}+i}{2} - \frac{\sqrt{3}-i}{2}\right) = \frac{\sqrt{3}+i}{2} - \frac{\sqrt{3}-i}{2} = i$$

و $\sigma_1\left(\sqrt{3}i\right) = \sigma_1\left(\sqrt{3}\right)\sigma_1(i) = \sqrt{3}i$ ، ولكن $\{1, \sqrt{3}, i, \sqrt{3}i\}$ هي قاعدة للحقل K على Q . بالتالي $\sigma_1 = I$ هو الأوتومورفزم المحايد للحقل K . على نفس المنوال يمكن التحقق من أن $\sigma_2\left(\sqrt{3}\right) = \sqrt{3}$ ، $\sigma_2(i) = -i$ ، $\sigma_2\left(\sqrt{3}i\right) = -\sqrt{3}i$ ، $\sigma_3\left(\sqrt{3}\right) = -\sqrt{3}$ ، $\sigma_3(i) = -i$ ، $\sigma_3\left(\sqrt{3}i\right) = \sqrt{3}i$ و $\sigma_4\left(\sqrt{3}\right) = -\sqrt{3}$ ، $\sigma_4(i) = i$ ، $\sigma_4\left(\sqrt{3}i\right) = -\sqrt{3}i$.

الآن $G(K, Q)$ هي زمرة رتبتها تسمى 4 وهذا يعني إما أنها زمرة دائرية رتبتها 4 أو أيزومورفية لزمرة كلاين الرباعية .

الآن $\sigma_2^2\left(\sqrt{3}\right) = \sigma_2\left(\sqrt{3}\right) = \sqrt{3}$ ، $\sigma_2^2(i) = \sigma_2(-i) = -\sigma_2(i) = i$ وأن :

$$\sigma_2^2\left(\sqrt{3}i\right) = \sigma_2\left(-\sqrt{3}i\right) = -\sigma_2\left(\sqrt{3}i\right) = \sqrt{3}i$$

هذا يؤدي إلى أن $\sigma_2^2 = I$.

مرة أخرى $\sigma_3^2\left(\sqrt{3}\right) = \sigma_3\left(-\sqrt{3}\right) = \sqrt{3}$ ، $\sigma_3^2(i) = \sigma_3(-i) = -\sigma_3(i) = i$ و $\sigma_3^2\left(\sqrt{3}i\right) = \sigma_3\left(\sqrt{3}i\right) = \sqrt{3}i$.

هذا يبين أن $\sigma_3^2 = I$. وبطريقة مشابهة يمكننا التحقق من أن $\sigma_4^2 = I$. عليه فإن $G(K, Q)$ لا يحوي عنصراً رتبته 4 . هذا بدوره يؤدي إلى أن $G(K, Q)$ أيزومورفية لزمرة كلاين الرباعية . عليه فإن زمرة جالوا للحقل K على Q أيزومورفية مع زمرة كلاين الرباعية.

مسائل

1- حقق جميع بديهيات فضاء متجهي في $M(S, K)$. إذا كانت S مجموعة منتهية تحوي n من العناصر . برهن أن $M(S, K)$ ذو بعد n على K .
[**إرشاد** لكل $s \in S$. عرف $f_s : S \to K$ هكذا $f_s(s) = 1$ و $f_s(t) = 0$ لكل $t \neq s$. برهن أن هذه العناصر f_s حيث $s \in S$ تشكل قاعدة للفضاء $M(S, K)$ على K] .

2- ليكن K حقل انفلاق لكثيرة الحدود $f(x)$ على الحقل F وليكن W مجموعة جميع جذور $f(x)$ في K . لكل $\tau \in G(K, F)$ ليكن τ_1 مقصور τ على W برهن أن τ_1 هو تبديل للمجموعة W . إضافة إلى ذلك لكل $\tau, \eta \in G(K, F)$. $\tau_1 = \eta_1$ إذا وفقط إذا كان $\tau = \eta$. ومن ثم استنتج أن $G(K, F)$ زمرة تباديل للمجموعة W .

3- ليكن $K = F(a)$ توسيعاً جبرياً بسيطاً درجته n لحقل ما F بمميز صفر . برهن أن عدد مرافقات a في K على F يقسم $[K : F]$.
[**إرشاد** إذا كان F_0 هو الحقل المثبت تحت $G(K, F)$ ، فإن $[K : F_0]$ هو عدد مرافقات a في K على F] .

4- ليكن $K = F(a_1, a_2, \ldots, a_n)$ توسيعاً جبرياً منتهياً للحقل F . برهن أن كل عنصر في K هو تركيب خطي على F من أحاديات بالصيغة $a_1^{i_1} a_2^{i_2} \ldots a_n^{i_n}$ حيث $i_j \geq 0$ لكل $j = 1, 2, \ldots, n$. ومن ثم استنتج أنه إذا كان كل من σ ، η هو F- أوتومورفزم للحقل K فإنهما متساويان إذا وفقط إذا كانا يتفقان على a_i لكل i أي $\sigma(a_i) = \eta(a_i)$ لكل i .

-5 برهن أن الأوتومورفزم المحايد هو الأوتومورفزم الوحيد لحقل يحوي p عنصراً حيث p عدد أولي .

-6 برهن أن زمرة جالوا لـ K ، حقل انفلاق كثيرة الحدود $x^n - 1$ على Q هي زمرة إبدالية .

-7 أثبت أنه في مثال 5 ، زمرة جالوا أيزومورفية إلى S_3 .

-8 أوجد زمرة جالوا لحقل انفلاق كل من كثيرات الحدود التالية على Q :

(i) $x^4 - 2$ (ii) $x^4 - x^2 - 6$ (iii) $x^3 - 3$

(iv) $x^4 + 5x^2 + 6$ (v) $x^4 + 1$ (vi) $x^3 - x - 1$

(vii) $(x^2 - 3x + 1)^2(x^3 - 2)$ (viii) $x^4 + x^3 + x^2 + x + 1$

[**الإجابة** (i) الزمرة الدايهيدرالية ودرجتها 8 ، (ii) زمرة كلاين الرباعية ، (iii) S_3 (iv) زمرة كلاين الرباعية ، (v) زمرة كلاين الرباعية ، (vi) S_3 ، (vii) $S_3 \times Z_2$ ، (viii) Z_4] .

-9 أوجد زمرة جالوا كثيرة الحدود $x^6 - 2$ على $Q(\sqrt{3})$. [**الإجابة** Z_6] .

-10 بين أن زمرة جالوا لكثيرة الحدود $(x^2 - 2)(x^3 - 3)$ على Q أيزومورفية مع $S_3 \times Z_2$.

2– التوسيعات العادية والنظرية الأساسية لنظرية جالوا

تعريف 14-11

يقال لتوسيع جبري K للحقل F أنه توسيع عادي للحقل F إذا كانت كل كثيرة حدود غير قابلة للتحليل $f(x)$ على F لها جذر في K تتحلل إلى عوامل خطية على K .

بعبارة أخرى نقول أن التوسيع الجبري K للحقل F هو توسيع عادي للحقل F إذا أعطينا $\beta \in K$ وكانت $f(x)$ هي كثيرة حدوده الأصغرية ودرجتها n على F ، فإن حقل انفلاق كثيرة الحدود $f(x)$ على F محتوى في K .

اعتبر أي حقل توسيع K درجته 2 للحقل F . لتكن $f(x)$ أية كثيرة حدود غير قابلة للتحليل على F ولها جذر وليكن α في K فإن $F(\alpha) \subseteq K$. عليه $[F(\alpha) : F] \leq 2$. من ناحية أخرى فإن $[F(\alpha) : F] = \deg f(x)$. بالتالي إما $\deg f(x) = 1$ أو $\deg f(x) = 2$. إذا كان $\deg f(x) = 1$ فإن $f(x)$ هي بالصورة $ax + b$ حيث $a, b \in F$ و $a \neq 0$. فيكون الجذر الوحيد لكثيرة الحدود $f(x)$ هو $\frac{-b}{a}$ والذي ينتمي إلى F . وعليه فإن F هو حقل انفلاق $f(x)$ محتوى في K . إذا كان $\deg f(x) = 2$ ، فإن $f(x)$ بالصورة $ax^2 + bx + 1$ حيث $a, b, c \in F$ و $a \neq 0$. في تلك الحالة إذا كان α جذراً لكثيرة الحدود $f(x)$ في K فإن $f(x) = a(x - \alpha)\left(x + \alpha + \frac{b}{a}\right)$ حيث $\alpha \in K$ ، $-\left(\alpha + \frac{b}{a}\right) \in K$ عليه فإن $f(x)$ تتحلل بصورة تامة على K . هذا يبين K توسيع عادي للحقل F .

والآن نعطي نظرية تزودنا بطريقة ممتازة لإنشاء عدد كبير من التوسيعات العادية .

نظرية 14-12

ليكن K توسيعاً جبرياً منتهياً للحقل F . فإن K توسيع عادي للحقل F إذا وفقط إذا كان K هو حقل انفلاق على F لبعض كثيرة حدود غير صفرية على F .

البرهان

افرض أن $K = F(a_1, a_2, \dots, a_n)$ توسيعاً جبرياً منتهياً للحقل F وأن K توسيعاً عادياً للحقل F .

لكل a_i افرض أن $f_i(x)$ هي كثيرة الحدود الأصغرية للعنصر a_i على F . فإن $f_i(x)$ تنفلق تماماً على K . افرض $f(x) = f_1(x)\dots f_n(x)$. الآن $f(x)$ تنفلق تماماً كذلك على K . عليه K يحوي حقل انفلاق $f(x)$. وحيث أن $a_1, a_2, \dots, a_n$ هي جذور لكثيرة الحدود $f(x)$ و K مولد بهذه الجذور على F فإننا نستنتج أن K كذلك محتوى في حقل انفلاق $f(x)$ على F وعلى ذلك فإن K هو حقل انفلاق $f(x)$ على F .

وبالعكس ليكن K حقل انفلاق كثيرة حدود $f(x)(\neq 0)$ على F . بفرض $a_1, a_2, \dots, a_n$ هي جذور كثيرة الحدود $f(x)$ في K فإن $K = F(a_1, a_2, \dots a_n)$ لتكن $p(x)$ أي كثيرة حدود غير قابلة للتحليل على F لها جذر β في K . $p(x)$ هي كثيرة حدود على K أيضاً ولكنها قد تكون قابلة للتحليل . ليكن L حقل انفلاق $p(x)$ على K . إذا أثبتنا أن $L = K$ فسوف ينتج أن جميع جذور $p(x)$ تقع في K أي أن $p(x)$ تنفلق تماماً على K .

افرض نقيضاً لذلك أنه يوجد جذر β' لكثيرة الحدود $p(x)$ في L بحيث $\beta' \notin K$. بما أن β و β' مرافقان على F ، يوجد F- أيزومورفزم σ من $F(\beta)$ فوقي على $F(\beta')$ بحيث $\sigma(\beta) = \beta'$. الآن $F \subseteq F(\beta) \subseteq K$ يعطي أن K هو أيضاً حقل انفلاق $f(x)$ على $F(\beta)$. إضافة لذلك فإن $K(\beta') = F(a_1, a_2, \dots, a_n, \beta') = F(\beta')(a_1, a_2, \dots, a_n)$ يعطي أن $K(\beta')$ هو حقل انفلاق

$f(x)$ علـــى $F(\beta')$. لـــذا يوجـــد أيزومـــورفزم τ مـــن K فـــوقي علـــى $K(\beta)$ بحيـــث $\sigma(x) = \tau(x), \quad \forall\, x \in F(\beta)$ (نظرية 13-25) .

τ هو أيضاً F- أيزومورفزم لأن σ كذلك . لتكن :

$f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_n x^n$ ، $\alpha_n \neq 0$ و $\alpha_i \in F$ لكـــــــــل $i = 0, 1, 2, \dots, n$. بما أن $a_1, a_2, \dots, a_n$ هي جذور $f(x)$ فإن :

$$f(x) = \alpha_n (x - a_1)(x - a_2) \dots (x - a_n) \qquad (1)$$

عندئذ يمكن توسيع τ إلى τ' ، الأيزومورفزم من $K[x]$ وفوقي على $K(\beta')[x]$. الآن :

$$\begin{aligned} \tau'[f(x)] &= \tau'(\alpha_0) + \tau'(\alpha_1)x + \tau'(\alpha_2)x^2 + \dots + \tau'(\alpha_n)x^n \\ &= \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_n x^n \end{aligned}$$

لأن $\tau'(\alpha_i) = \tau(\alpha_i) = \sigma(\alpha_i) = \alpha_i$ لجميـــع قـــيم i ، هـــذا يعطـــي أن $\tau'[f(x)] = f(x)$.

كذلك :
$$\tau'[f(x)] = \alpha_n [x - \tau(\alpha_1)][x - \tau(\alpha_2)] \dots [x - \tau(\alpha_n)]$$

لذا فإن :

$$f(x) = \alpha_n [x - \tau(\alpha_1))][x - \tau(\alpha_2)] \dots [x - \tau(\alpha_n)] \qquad (2)$$

من (1) و (2) نحصل على أن $\tau(a_1), \tau(a_2), \dots, \tau(a_n)$ هي مثل $a_1, a_2, \dots, a_n$ مع احتمالية أنها مرتبة بترتيب مختلف . ويكون $F(a_1, a_2, \dots, a_n) = F(\tau(a_1), \tau(a_2), \dots, \tau(a_n))$

على أية حال
$$\begin{aligned} K(\beta') = \tau(K) &= \tau[F(a_1, a_2, \dots, a_n] \\ &= F(\tau(a_2), \tau(a_2), \dots, \tau(a_n)) \\ &= F(a_1, a_2, \dots, a_n) = K \end{aligned}$$

وبالتالي $\beta' \in K$ وهذا تناقض . عليه فإن $p(x)$ تنغلق تماماً على K . لذا فإن K هو توسيع عادي للحقل F . هكذا يكمل البرهان . □

فيما يلي بعض النتائج للنظرية السابقة .

نتيجة 14-13

ليكن K توسيعاً عادياً منتهياً للحقل F . إذا كان E أي حقل جزئي من K يحوي F ، فإن K هو توسيع عادي للحقل E أيضاً .

البرهان

بما أن K توسيع عادي منته للحقل F ، توجد كثيرة حدود $f(x)$ على F بحيث أن K هو حقل انفلاق $f(x)$ على F . عندئذ K هو حقل انفلاق $f(x)$ على E . عليه حسب النظرية السابقة فإن K توسيع عادي للحقل E . □

نتيجة 14-14

ليكن K توسيع عادي منته للحقل F . إذا كان α_1, α_2 أي عنصرين في K مترافقان على F ، فإنه يوجد $F-$ أوتومورفزم σ للحقل K بحيث $\sigma(\alpha_1) = \alpha_2$.

البرهان

ليكن K حقل انفلاق كثيرة الحدود $f(x)$ على F . بما أن α_1, α_2 مترافقان على F ، يوجد $F-$ أيزومورفزم τ من $F(\alpha_1)$ فوقي على $F(\alpha_2)$ بحيث $\tau(\alpha_1) = \alpha_2$. الآن K حقل انفلاق $f(x)$ على $F(\alpha_1)$ وكذلك على $F(\alpha_2)$. عليه يوجد أوتومورفزم σ للحقل K وهو توسيع لـ τ أي أن $\sigma(x) = \tau(x)$ لكل $x \in K$. عندئذ :

$\sigma(\alpha_1) = \tau(\alpha_1) = \alpha_2$ ولكل $\alpha \in F$ فإن $\sigma(\alpha) = \tau(\alpha) = \alpha$.

وبالتالي فإن σ هو $F-$ أوتومورفزم للحقل K بحيث $\sigma(\alpha_1) = \alpha_2$. □

ملاحظة اعتبر ثلاثة حقول $F \subseteq K \subseteq L$ ، بحيث K توسيع عادي منته للحقل F و L توسيع عادي منته للحقل K . هل بإمكاننا القول أن L توسيع عادي للحقل F ؟ . الجواب بصورة عامة هو لا ، كما يبين في المثال الآتي .

مثال 6

ليكن $F = Q$ ، $K = Q(\sqrt{2})$ ، $L = Q(\sqrt[4]{2})$ بما أن $[K : F] = 2$ فإن K توسيع عادي للحقل F . $x^2 - \sqrt{2}$ هي كثيرة حدود على K بحيث $x^2 - \sqrt{2} = (x - \sqrt[4]{2})(x + \sqrt[4]{2})$ على L وهو حاصل ضرب عاملين خطيين جذورها تولد L على K .

عليه فإن L هو حقل انفلاق $x^2 - \sqrt{2}$ على Q . ومن ثم فإن L هو توسيع عادي للحقل K . من ناحية أخرى فإن $x^4 - 2$ كثيرة حدود غير قابلة للتحليل على Q ، وأن أحد جذورها $\sqrt[4]{2} \in L$ ولكن جذراً آخر وهو $i\sqrt[4]{2}$ لا ينتمي إلى L ، لذا فإن L ليس توسيعاً عادياً للحقل Q أي F .

هناك الكثير حول التوسيعات العادية يمكن التحدث عنه ، ولكننا نتجنب ذلك . دعنا الآن نعيد القول أن أي توسيع جبري لحقل بمميز صفر هو توسيع قابل للفصل ومن ناحية ثانية توجد حقول ذات مميزات موجبة (خصوصاً الحقول المنتهية) والتي جميع توسيعاتها الجبرية قابلة للفصل . والآن سوف نقتصر حديثنا على التوسيعات العادية المنتهية لحقول ذوات مميز صفر . على أية حال يجب التأكيد على أن معظم هذه النتائج يمكن برهنتها للتوسيعات العادية المنتهية والتوسيعات القابلة للفصل .

النظرية الآتية تعميم واضح للنتيجة 14-10 .

نظرية 14-15

ليكن K توسيعاً منتهياً لحقل F بمميز صفر . فإن K توسيع عادي للحقل F إذا وفقط إذا كان الحقل المثبت تحت زمرة جالوا $G(K, F)$ هو نفس F وعندما يكون K توسيعاً عادياً للحقل F فإن $[K : F] = o[G(K, F)]$.

البرهان

ليكن K حقل توسيع عادي للحقل F . حسب نظرية 13-50 فإن $K = F(\alpha)$ لبعض $\alpha \in K$. عليه كل كثيرة حدود غير قابلة للتحليل على F لها جذر في K ، تنفلق إلى عوامل خطية على K . بما أن α عنصر جبري على F نجد أن حقل الانفلاق K' لكثيرة الحدود الأصغرية $f(x)$ للعنصر α على F محتوى في K . من جهة أخرى $\alpha \in K'$ يعطي $F(\alpha) \subseteq K'$ أي أن $K \subseteq K'$. ومن ثم $K = K'$. عليه F هو الحقل المثبت تحت $G(K, F)$ (نتيجة 14-10) .

بالعكس ليكن F الحقل المثبت تحت $G(K, F)$. فإن K هو حقل انفلاق كثيرة الحدود الأصغرية $f(x)$ للعنصر α على F . عليه فإن K توسيع عادي للحقل F (نظرية 14-12) وهذا يكمل البرهان .

الجزء الثاني ينتج من نظرية 14-8 . □

اعتبر أي توسيع عادي منته K لحقل F بمميز صفر . ليكن $G = G(K, F)$ و H أية زمرة جزئية من G . لتكن :

$K_H = \{x \in K : \sigma(x) = x, \quad \forall \sigma \in H\}$ الحقل المثبت تحت H . لأي حقل جزئي E للحقل K يحوي F ، $G(K, E) = \{\sigma \in G \mid \sigma(x) = x, \quad \forall x \in E\}$.

$G(K, E)$ هي زمرة جميع $E-$ أوتومورفزمات الحقل K وهي زمرة جزئية من $G(K, F)$ نحن الآن في موضع لنبرهن النظرية الأساسية لنظرية جالوا (فقط في حالات الحقول التي مميزها صفر) بإعطاء ثنائية متميزة بين عائلة الحقول الجزئية للحقل K التي تحوي F وعائلة جميع الزمر الجزئية للزمرة $G(K, F)$.

نظرية 14-16 (النظرية الأساسية لنظرية جالوا)

ليكن K توسيعاً عادياً منتهياً لحقل F بمميز صفر ولتكن $G(K, F)$ زمرة جالوا للحقل K على F . فإن التقابل $E \leftrightarrow G(K, E)$ حيث E حقل جزئي من K يحوي F

هو تقابل أحادي بين عائلة الحقول الجزئية من K والتي تحوي F وعائلة جميع الزمر الجزئية من $G(K, F)$ ، مع تحقق الشروط الآتية :

إذا كان E حقلاً جزئياً من K حاوياً F و H زمرة جزئية من $G(K, F)$:

(i) $E = K_{G(K,E)}$.

(ii) $H = G(K, K_H)$.

(iii) $[K : E] = o[G(K, E)]$ و $[E : F]$ يساوي دليل $G(K, E)$ في $G(K, F)$.

(iv) E توسيع عادي للحقل F لذا وفقط إذا كانت $G(K, E)$ زمرة جزئية عادية من $G(K, F)$.

(v) عندما يكون E توسيعاً عادياً للحقل F ، فإن $G(E, F)$ أيزومورفية مع $G(K, F) / G(K, E)$.

البرهان

بما أن K توسيع عادي منته للحقل F و $F \subseteq E \subseteq K$ ، فإن K توسيع عادي منته للحقل E . عليه فإن E هو نفسه الحقل المثبت $K_{G(K,E)}$ (نظرية 14-15) . وهكذا حصلنا على (i) .

من التعريف $K_H = \{x \in K \mid \sigma(x) = x, \quad \forall \sigma \in H\}$ ، فإن كل $\sigma \in H$ عبارة عن K_H- أوتومورفزم للحقل K . عليه $H \subseteq G(K, K_H)$. من جهة أخرى $o(H) = [K : K_H]$ (نظرية 14-8) . في نفس الوقت ولكون K توسيع عادي للحقل K_H ، فإن نظرية 14-15 تبين أن K_H هو الحقل المثبت تحت $G(K, K_H)$. عليه فإن $[K : K_H] = o\,[G(K, K_H)]$ وهكذا فإن $o(H) = o\,[G(K, K_H)]$ ومنها $H = G(K, K_H)$ وهذا يبرهن (ii) .

والآن ولأن K توسيع عادي للحقل E ، فحسب نظرية 14-8 فإن $[K : E] = o[G(K, E)]$ وعليه يكون :

$$o\,[G(K, F)] = [K : F] = [K : E][E : F] = o\,[G(K, E)][E : F]$$

ومنها $[E : F] = \dfrac{o\,[G(K, F)]}{o\,[G(K, E)]}$ ، هذا يبرهن (iii) .

ليكن E توسيعاً عادياً للحقل F . اعتبر أي عنصر $a \in E$ ، فإن حقل انفلاق كثيرة الحدود الأصغرية للعنصر a على F محتوى في E وذلك يؤدي إلى أن كل مرافق للعنصر a على F في K ينتمي إلى E أيضاً . بما أن لأي $\sigma \in G(K, F)$ ، $\sigma(a)$ هو مرافق a ، تكون لدينا $\sigma(a) \in E$. عليه لكل $\eta \in G(K, E)$ يكون $\eta[\sigma(a)] = \sigma(a)$ ويكون $(\sigma^{-1}\eta\sigma)\,(a) = a$ وهذا يبرهن أن $\sigma^{-1}\eta\sigma \in G(K, F)$ لكل $\eta \in G(K, E)$ و $\sigma \in G(K, F)$. وبالتالي فإن $G(K, E)$ زمرة جزئية عادية للزمرة $G(K, F)$.

وبالعكس افرض أن $G(K, E)$ زمرة جزئية عادية من $G(K, F)$. اعتبر $a \in E$ بما أن K هو توسيع عادي للحقل F ، فإن K يحوي حقل انفلاق وليكن L لكثيرة الحدود الأصغرية $p(x)$ للعنصر a على L . اعتبر أي جذر b لكثيرة الحدود $p(x)$ في L فيكون b هو مرافق a على F . عليه يوجد F– أوتومورفزم σ للحقل K بحيث $\sigma(a) = b$. لأي $\eta \in G(K, E)$ ، $\sigma^{-1}\eta\sigma \in G(K, F)$ عليه $(\sigma^{-1}\eta\sigma)\,(a) = a$. إذاً $\eta[\sigma(a)] = \sigma(a)$ لكل $\eta \in G(K, F)$. على أية حال E هو حقل المثبت تحت $G(K, E)$. هذا يؤدي إلى أن $b = \sigma(a) \in E$. بالتالي $L \subseteq E$ وهذا يبرهن أن E هو توسيع عادي للحقل F . والذي يبرهن (iv) .

ليكن E توسيع عادي للحقل F . الآن $E = F(a)$ لبعض $a \in E$. لأي $\sigma \in G(K, F)$ ضع σ_E رمزاً لمقصور σ على E . بما أن $\sigma(a) \in E$ ، فإن $\sigma(E) \subseteq E$ ولأن $[\sigma(E) : F] = [E : F]$ فإن $\sigma(E) = E$ ، إذاً σ_E هو F– أوتومورفزم للحقل E

وعليه $\sigma_E \in G(E, F)$. عرف الراسم $\lambda : G(K, F) \to G(E, F)$ بحيث $\lambda(\sigma) = \sigma_E, \quad \forall \sigma \in G(K, F)$. من الواضح أنه لأي $\sigma, \eta \in G(K, F)$ ، $(\sigma\eta)_E = \sigma_E\eta_E$ وبالتالي λ عبارة عن هومومورفزم زمرة . اعتبر أي $\gamma \in G(E, F)$. الآن $\gamma(a)$ هو مرافق a على F . لذا فإنه يوجد F– أوتومورفزم σ للحقل K بحيث $\sigma(a) = \gamma(a)$. إضافة إلى ذلك فإنه لما كان σ و γ كلاهما يمثل المحايد على F والحقل E مولد بالعنصر a على F فإن $\sigma(x) = \gamma(x)$ لكل $x \in F(a) = E$.

أي أن $\gamma = \sigma_E = \lambda(\sigma)$. هذا يبين أن λ راسم فوقي . إذاً $\dfrac{G(K, F)}{\ker \lambda} \cong G(E, F)$. الآن $\sigma \in \ker \lambda$ إذا وفقط إذا كان σ_E هو الراسم المحايد على F بمعنى أنه إذا وفقط إذا كان $\sigma(x) = x$ لكل $x \in E$ أي إذا وفقط إذا كان $\sigma \in G(K, F)$. إذاً $\ker \lambda = G(K, E)$ ومنها نحصل على أن $G(E, F) \cong \dfrac{G(K, F)}{G(K, E)}$.

هذا يبرهن (v) . وتكون النظرية قد برهنت . □

في الملاحظات التالية F, K يحققان فروض النظرية السابقة .

ملاحظة 1 النظرية السابقة تبين أن عدد الحقول الجزئية من K والذي يحوي F عدد منته ، في الحقيقة هذا العدد هو عدد الزمر الجزئية للزمرة $G(K, F)$.

ملاحظة 2 بما أن كل زمرة جزئية من زمرة أبيلية هي زمرة جزئية عادية ، النظرية السابقة تبين أنه إذا كانت $G(K, F)$ زمرة أبيلية فإن كل حقل جزئي E من K يحوي F هو توسيع عادي للحقل F لتوضيح ذلك . افرض أن $K = F(a)$ حيث جميع مرافقات a هي قوة للعنصر a . علي سبيل المثال ليكن $F = Q$ و $K = Q(a)$ حيث $a = e^{\frac{2\pi i}{p}}$ (انظر مثال 4) . فإن العناصر $a, a^2, \ldots, a^{p-1}$ هي جذور كثيرة الحدود غير القابلة للتحليل $x^{p-1} + x^{p-2} + \ldots + x + 1$.

اعتبر أي عنصرين $\sigma, \eta \in G(K, F)$. بما أن $\eta(a), \sigma(a)$ كلاهما مرافق للعنصر a فإن $\sigma(a) = a^i$ و $\eta(a) = a^j$ لبعض i, j عندئذ يكون :

$$(\eta\sigma)(a) = \eta(\sigma(a)) = \eta(a^i) = [\eta(a)]^i = (a^j)^i = a^{ij}$$

بالمثل فإن $\sigma\eta(a) = a^{ij}$ بالتالي فإن $\sigma\eta = \eta\sigma$ والذي بين أن $G(K, F)$ هي زمرة أبيلية .

والآن نعطي مثالاً يوضح استخدام النظرية الأساسية لجالوا .

مثال 6 (a)

اعتبر $f(x) = x^4 - 5x^2 + 6$. بما أن $f(x) = (x^2 - 3)(x^2 - 2)$ فإن $\pm\sqrt{2}$ ، $\pm\sqrt{3}$ هي جذور $f(x)$ وأن $K = Q(\pm\sqrt{2}, \pm\sqrt{3}) = Q(\sqrt{2}, \sqrt{3})$ هو حقل انفلاق كثيرة الحدود $f(x)$ على Q . الآن $Q \subset Q(\sqrt{2}) \subset Q(\sqrt{2}, \sqrt{3})$ وللبرهنة على الاحتواء الفعلي الأخير يكفي البرهنة على أن $\sqrt{3} \notin Q(\sqrt{2})$. افرض أن هذا غير صحيح فيكون $\sqrt{3} = a + b\sqrt{2}$ لبعض $a, b \in Q$ وهذا بدوره يؤدي إلى أن :

$$3 = (a^2 + 2b^2) + 2\sqrt{2}ab \Rightarrow 2\sqrt{2}ab = 3 - a^2 - 2b^2$$

الآن $a = 0 \Rightarrow \sqrt{3} = b\sqrt{2} \Rightarrow \sqrt{6} = 2b = \sqrt{6}$

وأن $\sqrt{6}$ عدد نسبي وهذا لا يجوز أيضاً . إذا كان $b = 0$ فإن $\sqrt{3}$ يجب أن يكون عدداً نسبياً وهذا أيضاً لا يجوز . إذاً الاختيار الوحيد المتبقي هو أن $\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab}$ عدد نسبي ! وهذا يبين أن فرضنا غير صائب ، ونتيجة لذلك فإن $Q(\sqrt{2}, \sqrt{3}) \neq Q(\sqrt{2})$. وبالمثل يمكن تبيان أن $Q \subseteq Q(\sqrt{3}) \subset Q(\sqrt{2}, \sqrt{3})$. عليه نجد أن $[K : Q] = 4$. وبما أن رتبة زمرة جالوا $G(K, Q)$ يساوي 4 فإن هذه الزمرة إما أن تكون دائرية أو هي زمرة كلاين الرباعية . الآن K يحوي على الأقل حقلين جزئيين $Q(\sqrt{2})$ ، $Q(\sqrt{3})$ يقعان فعلياً بين Q و K فمن النظرية الأساسية لجالوا فإن $G(K, Q)$ تضم على الأقل زمرتين جزئيتين فعليتين بين $\{I\}$ والزمرة نفسها .

بمـا أن $[K : Q(\sqrt{2})] = 2$ و $[K : Q(\sqrt{3})] = 2$ فـإن $G(K, Q)$ لهـا علـى الأقـل زمرتين جزئيتين رتبتاهما 2 .

بالتالي فإن الزمرة $G(K, Q)$ لا يمكن أن تكون زمرة دائرية . عليه فهي أيزومورفية مع زمرة كلاين الرباعية . ولما كانت $x^2 - 2$ غير قابلة للتحليل على $Q(\sqrt{3})$ وجذراها هما $\sqrt{2}$ و $-\sqrt{2}$ ، وأن K توسيع عادي للحقل $Q(\sqrt{3})$ ، فحسب نتيجة 14-4 فإنه يوجد $Q(\sqrt{3})$ – أوتومـورفزم ولـيكن σ_2 للحقـل K بحيث $\sigma_2(\sqrt{2}) = -\sqrt{2}$ ومـن الواضـح أن $\sigma_3(\sqrt{3}) = \sqrt{3}$ وعليـه فـإن $\sigma_2(\sqrt{6}) = \sigma_2(\sqrt{2})\sigma_2(\sqrt{3}) = -\sqrt{6}$. بالمثـل باعتبـار $x^2 - 3$ ، نحصـل علـى أوتومـــورفزم σ_3 للحقـــل K بحيـــث $\sigma_3(\sqrt{2}) = \sqrt{2}$ ، $\sigma_3(\sqrt{3}) = -\sqrt{3}$ و $\sigma_3(\sqrt{6}) = -\sqrt{6}$ وهكـذا حصـلنا على ثلاثـة عناصـر في $G(K, Q)$ وهـي I, σ_2, σ_3 . ونحتـاج فقـط لعنصـر إضافي آخر .

مـرة ثانيـة $\sigma : Q(\sqrt{3}) \to Q(\sqrt{3})$ المعطـى حسـب $\sigma(a + b\sqrt{3}) = a - b\sqrt{3}$ هـو أوتومـورفزم للحقـل $Q(\sqrt{3})$ بحيث أن كثـيرة الحـدود المقابلـة لكثـيرة الحـدود $f(x) = x^2 - 2$ تحـت σ هـي $f_1(x) = x^2 - \sigma(2) = x^2 - 2 = f(x)$ ، الآن $\sqrt{2}$ ، $-\sqrt{2}$ همـا جـذرا كثيرتي الحـدود $f(x)$ ، $f_1(x)$ على الترتيـب ، كمـا أن $K = Q(\sqrt{3})(\sqrt{2}) = Q(\sqrt{3})(-\sqrt{2})$ عليـه حسـب نظريـة 13-32 يوجـد أوتومـورفزم σ_4 للحقـل K بحيـث $\sigma_4(\sqrt{2}) = -\sqrt{2}$ ، $\sigma_4(\sqrt{3}) = -\sqrt{3}$. بالتاي فإن $\sigma_4(\sqrt{6}) = \sigma_4(\sqrt{2})\sigma_4(\sqrt{3}) = \sqrt{6}$.

مـــن الواضـــح لأي $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ حيـــث $a, b, c, d \in Q$ فـــإن $I(\alpha) = \alpha$.

$$\sigma_2(\alpha) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \qquad \text{(i)}$$
$$\sigma_3(\alpha) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \qquad \text{(ii)}$$
$$\sigma_4(\alpha) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} \qquad \text{(iii)}$$

الآن الزمر الجزئية الفعلية للزمرة $G[K, Q]$ هي $H_1 = \{I, \sigma_2\}$ ، $H_2 = \{I, \sigma_3\}$ ، $H_3 = \{I, \sigma_4\}$. الآن $\alpha \in K_H$ إذا وفقط إذا كان $\sigma_2(\alpha) = \alpha$ أي أنه إذا وفقط إذا :

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

بمقارنة المعاملات نحصل على أن $\alpha \in K_H$ إذا وفقط إذا $b = 0 = d$. إذاً $K_{H_1} = \{a + c\sqrt{3} : a, c \in Q\} = Q(\sqrt{3})$ بالمثل فإن $K_{H_2} = Q(\sqrt{2})$ و $K_{H_3} = Q(\sqrt{6})$.

تعريف 14-16 (a)

ليكن n عدداً صحيحاً موجباً . يسمى العدد المركب ω بجذر نوني بدائي للواحد إذا كان $\omega^n = 1$ ولا يوجد عدد صحيح $m < n$ بحيث $\omega^m = 1$.

ملاحظة نعلم أن مجموعة الجذور النونية للواحد تشكل زمرة دائرية G رتبتها n تحت عملية ضرب الأعداد المركبة . وعليه فإن كل مولد للزمرة G هو جذر نوني بدائي للواحد وبالعكس .

مثال 6 (b)

$\frac{-1 + i\sqrt{3}}{2}$ هو جذر تكعيبي بدائي للواحد و $\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$ هو جذر خامس بدائي للواحد . للتحقق من هذه الادعاءات لاحظ أن $e^{\frac{2\pi i}{3}} = \frac{-1 + i\sqrt{3}}{2}$ و $\left(e^{\frac{2\pi i}{3}}\right)^3 = e^{2\pi i} = 1$ ولكن $\left(e^{\frac{2\pi i}{3}}\right)^1 = \frac{-1 + i\sqrt{3}}{2} \neq 1$ وأن :

$$\left(e^{\frac{2\pi i}{3}}\right)^2 = e^{\frac{4\pi i}{3}} = \frac{-1 - i\sqrt{3}}{2} \neq 1$$

مرة أخرى $\left(e^{\frac{6\pi i}{5}}\right)^5 = 1$ ولا يوجد عدد صحيح $0 < m < 5$ بحيث $\left(e^{\frac{6\pi i}{5}}\right)^m = 1$.

تعريف 16-14 (b)

لتكن S مجموعة جميع الجذور النونية البدائية للواحد ، عندئذ $\phi_n(x) = \prod_{\xi \in S} (x - \xi)$ تسمى كثيرة حدود سيكلوتومية (cyclotomic) من الدرجة n .

لاحظ أولاً أن $e^{\frac{2\pi i}{n}}$ جذر نوني بدائي للواحد ، عليه وحسب الملاحظة المذكورة سلفاً فإن جميع الجذور للواحد معطاة على أنها $1, \xi, \xi^2, \ldots, \xi^{n-1}$ حيث $\xi = \frac{2\pi i}{n}$. بالتالي فإن حقل انفلاق $x^n - 1$ على Q هو $Q(1, \xi, \xi^2, \ldots, \xi^{n-1}) = Q(\xi)$ حسب التعريف ξ يحقق $\phi_n(x)$. فإذا برهنا أن $\phi_n(x) \in Q[x]$ وأنها غير قابلة للتحليل على Q فإنه يكون بإمكاننا البرهنة على أن $[Q(\xi) : Q] = \varphi(n)$ (حيث $\varphi(n)$ هو دالة أويلر التوتيانية) لأن عدد الجذور البدائية للواحد يساوي عدد مولدات زمرة دائرية رتبتها n .

هدفنا التالي هو البرهنة على صواب جميع هذه الادعاءات . فبل أن نبرهن القضية التالية ، نلاحظ أن $\phi_n(x)$ كثيرة حدود واحدية من $Q(\xi)[x]$ لكون ξ جذر نوني بدائي للواحد .

قضية 16-14 (c)

$$x^n - 1 = \prod_{\substack{d / n \\ 1 \le d \le n}} \phi_d(x) \;.$$

البرهان

لما كانت جميع الجذور النونية للواحد تؤلف زمرة دائرية G رتبتها n ، فإن رتبة أي جذر نوني للواحد هي عامل للعدد n ، الآن :

$$x^n - 1 = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$$

حيث α_i هو جذر نوني للواحد . بإمكاننا ضم الجذور α_i المتساوية الرتبة . بما أن G دائرية، لكل عامل d من عوامل n يوجد α_i . افرض p هو حاصل ضرب جميع العوامل

$(x-\alpha_i)$ لكثيرة الحدود x^n-1 بحيث $d = \circ(\alpha_i)$ و d عامل لـ n . ندعي أن p ليس سوى $\phi_d(x)$. لتكن α الجذر رقم d للواحد . α هو أيضاً جذر نوني للواحد ، لأن $d \mid n \Rightarrow n = kd$ لبعض $k \in N$ هذا يؤدي إلى أن $\alpha^n = \alpha^{kd} = (\alpha^d)^k = 1$. بوجه خاص الجذور البدائية d للواحد هي جذور نونية للواحد، عليه كل واحد منها يجب أن يبرز عاملاً لـ p . إذاً $p = \phi_d(x)$ وكنتيجة لذلك فإن $x^n - 1 = \prod_{\substack{d|n \\ 1\le d\le n}} \phi_d(x)$. $\square$

هذه القضية تعطينا طريقة ملائمة لتحديد $\phi_n(x)$ بصورة واضحة لقيم n الصغيرة . وهكذا فإن $\phi_1(x) = x-1$. الآن :

$$x^2 - 1 = \phi_1(x)\phi_2(x) \Rightarrow \phi_2(x) = \frac{x^2-1}{x-1} = x+1$$

مرة أخرى

$$x^3 - 1 = \phi_1(x)\phi_3(x) \Rightarrow \phi_3(x) = \frac{x^3-1}{x-1} = x^2+x+1$$

وأخيراً

$$x^4 - 1 = \phi_1(x)\phi_2(x)\phi_4(x) \Rightarrow \phi_4(x) = \frac{x^4-1}{(x-1)(x+1)} = x^2+1$$

نظرية 14-16 (d)

$\phi_n(x) \in Z[x]$.

البرهان

نطبق الاستنتاج على n . عندما $n = 1$ ، $\phi_1(x) = x-1 \in Z[x]$ ليكن $n > 1$ ولنفرض أن $\phi_m(x) \in Z[x]$ لجميع $1 \le m < n$.

حسب القضية 14-16 (c) ، $x^n - 1 = \prod_{\substack{d|n \\ 1\le d\le n}} \phi_d(x) = q(x)\phi_n(x)$ حيث $q(x) = \prod_{\substack{d|n \\ 1\le d< n}} \phi_d(x)$. استناداً إلى فروض الاستقراء فإن $\phi_d(x) \in Z[x]$ لجميع $d < n$. إذاً

$q(x) \in Z[x]$. لما كانت $q(x)$ كثيرة حدود واحدية في $Z[x]$ ، فحسب خوارزمية القسمة في $Z[x]$ نحصل على $x^{n-1} = q(x)r(x) + s(x)$ حيث $r(x), s(x) \in Z[x]$ ، وأن $s(x) = 0$ أو $\deg s(x) < \deg q(x)$. لأن $Z \subseteq Q(\xi)$ ، ξ جذر نوني بدائي للواحد ، نجد أن $x^{n-1} = q(x)r(x) + s(x)$ حيث $r(x), s(x) \in Q(\xi)[x]$ وأنه إما $s(x) = 0$ أو $\deg s(x) < \deg q(x)$.

ولكن في $Q(\xi)[x]$ ، يكون $x^n - 1 = q(x)\phi_n(x)$ وحدانية ناتج القسمة والباقي يؤديان إلى أن $s(x) = 0$ و $\phi_n(x) = r(x)$. إذاً $\phi_n(x) \in Z[x]$. □

نتيجة 14-16 (e)

$\phi_n(x) \in Q[x]$. □

وأخيراً نبرهن أن $\phi_n(x)$ غير قابلة للتحليل على Q .

نظرية 14-16 (f)

$\phi_n(x)$ غير قابلة للتحليل على Q .

البرهان

على ضوء القضية 10-41 يكفي البرهنة على أن $\phi_n(x)$ غير قابلة للتحليل على Z . لتكن $h(x)$ كثيرة حدود غير قابلة للتحليل في $Z[x]$ بحيث $\phi_n(x) = h(x)g(x)$ لبعض $g(x) \in Z[x]$. بما أن $\phi_n(x)$ واحدية فإنه يمكن اختيار $h(x)$ ، $g(x)$ واحد بتان . الآن أي جذر لكثيرة الحدود $h(x)$ هو جذر لكثيرة الحدود $\phi_n(x)$ أي أنه جذر نوني بدائي للواحد . ليكن ξ أي جذر نوني بدائي للواحد فإن $h(\xi) = 0$ فإذا كان p عدداً أولياً بحيث $p < n$ و $p \nmid n$ فإننا ندعي أن ξ^p جذر لكثيرة الحدود $h(x)$. وعلى فرض أن ξ^p ليس جذراً لكثيرة الحدود $h(x)$ فإن $(p, n) = 1$ يؤدي إلى أن ξ جذر بدائي نوني للواحد ، وهذا يؤدي إلى أن :

$$\phi_n(\xi^p) = 0 \Rightarrow h(\xi^p)g(\xi^p) = 0 \Rightarrow g(\xi^p) = 0 \ (\text{لأن } h(\xi^p) \neq 0)$$

إذاً ξ^p جذر لكثيرة الحدود لـ $g(x)$ بعبارة أخرى ξ جذر لكثيرة الحدود $g(x^p)$. لكن $h(x)$ كثيرة حدود واحدية غير قابلة للتحليل تتحقق بالعنصر ξ ، فهي إذاً كثيرة حدود الأصغرية للعنصر ξ على Q . عليه $h(x) \mid g(x^p)$ في $Q[x]$. هذا بدوره يؤدي إلى أن $g(x^p) = h(x)l(x)$ بما أن $g(x^p), h(x) \in Z[x]$ ، فإن $l(x) \in Z[x]$ (استخدم المناقشة في نظرية 14-16 (d)) . عليه فإن $x^n - 1 = q(x)\phi_n(x)$ حيث :

$$q(x) = \prod_{\substack{d \mid n \\ 1 \le d < n}} \phi_d(x) \Rightarrow x^n - 1 = q(x)h(x)g(x)$$

الآن عرف $\theta : Z \to Z / < p >$ على النحو الآتي $\theta(n) = n + < p > = \bar{n}$

θ عبارة عن هومومورفزم فوقي تحث هومومورفزماً فوقياً $\phi : Z[x] \to \frac{Z}{< p >}[x]$ معرفاً كالآتي

$$\phi\left(\sum_{i=1}^{t} \alpha_i x^i\right) = \sum_{i=1}^{t} \bar{\alpha}_i x^i$$

فإذا رمزنا إلى $\phi(f(x))$ بالرمز $\bar{f}(x)$ فإن لأي $f(x) \in Z[x]$ يكون :

$$\phi(x^n - 1) = \phi[q(x)h(x)g(x)] \Rightarrow x^n - \bar{1} = \bar{q}(x)\bar{h}(x)\bar{g}(x) \qquad \ldots(1)$$

وبفرض أن $g(x) = \beta_0 + \beta_1 x + \ldots + \beta_r x^r$ فإنه حسب نظرية فيرمات (سؤال 30 ، بند 2 الفصل الثاني) إذا كان $a \in Z$ فإن $\bar{a}^p = \bar{a}$ هذا يؤدي إلى أن :

$$\begin{aligned}\bar{g}(x^p) &= \bar{\beta}_0 x^p + \ldots + \bar{\beta}_r x^{rp}) = (\bar{\beta}_0^p + \bar{\beta}_1^p x^p + \ldots + \bar{\beta}_r^p x^{rp}) \\ &= (\bar{\beta}_0 + \bar{\beta}_1 x + \ldots + \bar{\beta}_r x^r)^p = [\bar{g}(x)]^p\end{aligned}$$

الآن

$$\begin{aligned} g(x^p) = h(x)l(x) &\Rightarrow \bar{g}(x^p) = \bar{h}(x)\bar{l}(x) \\ &\Rightarrow [\bar{g}(x)]^p = \bar{h}(x)\bar{l}(x)\end{aligned}$$

إذا كان $\bar{t}(x)$ عاملاً غير قابل للتحليل لكثيرة الحدود $\bar{h}(x)$ في $\frac{Z}{< p >}[x1]$ ، فإن $\bar{t}(x) \mid [\bar{g}(x)]^p$ في $\frac{Z}{< p >}[x]$ هذا يؤدي إلى أن $\bar{t}(x) \mid \bar{g}(x)$ في $\frac{Z}{< p >}[x]$. باستخدام

(1) نجد أن $[\bar{f}(x)]^2 \mid x^n - \bar{1}$ في $\frac{Z}{<p>}[x]$ بالتالي فإن $x^n - \bar{I}$ غير قابلة للفصل على $Z/<p>$. ولكن :

$$\bar{f}(x) = x^n - \bar{I} \Rightarrow \left[\bar{f}(x)\right]' = nx^{n-1} \neq 0 \qquad (\text{لأن } p \nmid n)$$

هذا تناقض مع القضية 13-41 لذا فإن ادعائنا بكون ξ^p جذر لكثيرة الحدود $h(x)$ قد تحقق . ليكن ζ أي جذر لكثيرة الحدود $\phi_n(x)$. ζ جذر نوني بدائي للواحد ، وبما أن ξ هو أيضاً جذر نوني بدائي للواحد فإن $\xi^k = \zeta$ لبعض $k \in N$.

نفرض أن $k = p_1 p_2 \dots p_s$ حيث p_i أعداد أولية لكل $(1 \le i \le s)$ (ليس بالضرورة أن تكون مختلفة) بحيث $p_i < n$ لكل i . حيث أياً من p_i ليس عاملاً للعدد n . وإلا فإن $(k, n) \neq 1$ أي أن $\xi^k = \zeta$ لا يمكن أن يكون جذراً نونياً بدائياً للمحايد !

وبتكرار تطبيق ما برهناه فإن $\xi^{p_1}, (\xi^{p_1})^{p_2}, (\xi^{p_1 p_2})^{p_3}, \dots, (\xi^{p_1 p_2 \cdots p_{s-1}})^{p_s} = \xi$ هي جذور $h(x)$ وعليه فإن كل جذر لكثيرة الحدود $\phi_n(x)$ هو جذر لكثيرة الحدود $h(x)$. بالتالي $\phi_n(x) = h(x)$. إذاً $\phi_n(x)$ غير قابلة للتحليل على Z . □

باستخدام نتيجة 14-16 (e) ونظرية 14-16 (f) نحصل على النتيجة الآتية .

نتيجة 14-16 (g)

درجة حقل انفلاق $x^n - 1$ على Q يساوي $\varphi(n)$. □

مسائل

1- ليكن F حقل جالوا يحوي q عنصراً ، وليكن K حقل توسيع للحقل F درجته n . برهن أن K توسيع عادي للحقل F .

[**إرشاد** K عبارة عن حقل انفلاق كثيرة الحدود $x^{q^n} - x$ على F] .

2- ليكن K توسيعاً جبرياً للحقل F . إذا كانت $\{F_i\}_{i\in I}$ أية عائلة غير خالية لحقول جزئية تحوي F ، بحيث كل F_i هو توسيع عادي للحقل F ، برهن أن التقاطع $\bigcap_{i\in I} F_i$ هو أيضاً توسيع عادي للحقل F .

3- ليكن $F \subseteq K \subseteq L$ أي ثلاثة حقول بحيث F له مميز صفر ، K توسيع عادي ، منته للحقل F و L توسيع عادي منته للحقل K ، برهن الآتي :

إذا كان σ أي F- أوتومورفزم للحقل K ، فإنه يوجد F- أوتومورفزم η للحقل L بحيث أن σ هو مقصور η إلى K .

[**إرشاد** ليكن $K = F(a)$ ، $L = K(b)$. لأي $\sigma \in G(K, F)$ ، $\sigma(a)$ هو مرافق a على F مع كون $F(a) = F(\sigma(a))$. إضافة إلى ذلك L هو حقل انفلاق كثيرة الحدود الأصغرية للعنصر b على K تماماً مثل $F(\sigma(a))$] .

4- ليكن K توسيعاً منتهياً لحقل F . برهن الآتي :

(i) يوجد توسيع عادي أصغري للحقل F يحوي K .

[**إرشاد** ليكن $K = F(a_1, a_2, \ldots, a_n)$ ولكل i ، $f_i(x)$ هي كثيرة الحدود الأصغرية للعنصر a_i على F . إذا كان $f(x)$ حاصل ضرب كثيرات الحدود $f_i(x)$ هذه فإن حقل الانفلاق L لـ $f(x)$ على K هو الحقل المطلوب] .

(ii) K توسيع عادي على F إذا وفقط إذا كان يحقق الشرط الآتي : لكل توسيع K' للحقل K ، أي F - أيزومورفزم للحقل K في K' هو أساساً F - أوتومورفزم .

5- اذكر مثالاً لتوسيع عادي للحقل Q درجته 3 ومثالاً آخر لتوسيع جبري للحقل Q درجته 3 بحيث لا يكون توسيعاً عادياً .

[**إرشاد** اعتبر حقل انفلاق كثيرة الحدود $x^3 - 3x + 1$ على Q] .

6- لتكن $f(x)$ أية كثيرة حدود غير صفرية على حقل F وليكن K حقل انفلاق $f(x)$ على F . فإن الزمرة $G(K, F)$ تسمى زمرة جالوا لكثيرة الحدود $f(x)$. برهن أن الزمرة G ، زمرة جالوا لكثيرة الحدود $p_n(x) = x^n - 1$ على الأعداد النسبية تكون دائرية .

[**إرشاد** لاحظ أن $K = Q(\alpha)$ حيث $\alpha = e^{\frac{2\pi i}{n}}$ هو حقل انفلاق $x^n - 1$ على Q وكل مرافق للعنصر α هو قوة للعنصر α] .

7- ليكن K توسيعاً عادياً منتهياً لحقل F بمميز صفر بحيث $[K : F] = n$. ليكن $\sigma_1, \sigma_2, \dots, \sigma_n$ عبارة عن n من F - أوتومورفزمات الحقل K . لكل $x \in K$ ، عرف $N_{K/F(x)}$ و $T_{K/F(x)}$ (يسميان المعيار وأثر x على F على الترتيب) كما يلي :

$$N_{K/F(x)} = \prod_{i=1}^{n} \sigma_i(x), \quad T_{K/F(x)} = \sum_{i=1}^{n} \sigma_i(x)$$

برهن ما يلي :

(i) لأي F - أوتومورفزم σ للحقل K .

$$\sigma[N_{K/F(x)}] = N_{K/F(x)}, \quad \sigma[T_{K/F(x)}] = T_{K/F(x)}$$

عندئذ أو غير ذلك استنتج أن $N_{K/F(x)}$ و $T_{K/F(x)}$ كلاهما في F .

(ii) اعتبر $K = Q\left(\sqrt{-3}, \sqrt[3]{2}\right)$. احسب $N_{K/Q}\left(\sqrt[3]{2}\right)$ و $N_{K/Q}\left(\sqrt[3]{2}\right)$.

(iii) إذا كان E أي حقل جزئي من K يحوي F بحيث أن E هو توسيع عادي للحقل F ، فإنه لأي $x \in K$ يكون $N_{K/F(x)} = N_{E/F}\left[N_{K/E(x)}\right]$ و $T_{K/F(x)} = T_{E/F}\left[T_{K/E(x)}\right]$.

8- ليكن K توسيعاً منتهياً للحقل F . برهن أن K توسيع عادي قابل للفصل للحقل F ، إذا وفقط إذا كان F هو الحقل المثبت تحت الزمرة $G(K, F)$.

9- باستخدام سؤال 8 ، برهن النظرية الأساسية لنظرية جالوا تحت فرضية أن K توسيع عادي قابل للفصل للحقل F ودرجته منتهية .

10- ليكن K توسيعاً عادياً لحقل F بمميز صفر بحيث $[K : F] = 4$ أثبت أن أي حقل جزئي للحقل K يحوي F هو توسيع عادي للحقل F .

[**إرشاد** أية زمرة جزئية رتبتها 4 تكون إبدالية] .

3- التوسيعات الجذرية وقابلية الحل بواسطة جذور

في هذا البند والبند القادم سوف نناقش بعض التطبيقات البسيطة ولكنها أساسية لنظرية الحقل التي طبقت كثيراً على نظرية المعادلات والهندسة . قبل أن نتناول مفهوم قابلية حل كثيرة الحدود بواسطة جذور ، سوف نبرهن بعض النتائج العامة الإضافية حول نظرية الحقول .

قضية 14-17

أية زمرة جزئية منتهية للزمرة الضربية لأي حقل تكون دائرية .

البرهان

ليكن F حقلاً و S أية زمرة جزئية منتهية للزمرة الضربية F^* من F . بما أن S منتهية بإمكاننا إيجاد عنصر $z \in S$ الأكبر رتبة (بالنسبة للضرب) من بين عناصر S . عندئذ لكل $y \in S$ ، $o(y) \mid o(z)$ (قضية 4-25) . عليه إذا كان $o(z) = n$ فإن $y^n = e$ لكل $y \in S$ حيث e العنصر المحايد للحقل F . بالتالي كل عنصر في S هو جذر لكثيرة الحدود $ex^n - e$. الآن $e, x, x^2, \dots, x^n$ هي n من العناصر المختلفة في S . بما أن أية كثيرة حدود درجتها n على حقل لا يمكن أن يكون لها أكثر من n من الجذور فإن $e, z, z^2, \dots, z^{n-1}$ هي جميع عناصر S . إذاً $S =< z >$ زمرة دائرية (انظر نظرية 56-13) . □

بالأخص لكون F^* زمرة جزئية من نفسها نجد أنه إذا كانت F^* منتهية فإنها يجب أن تكون دائرية . الزمرة F^* منتهية حيثما يكون F حقل جالوا . ومن ذلك ينتج أن .

نتيجة 14-18

الزمرة الضربية لحقل جالوا تكون دائرية . □

تعريف 14-19

لعدد صحيح موجب n . يقال لعنصر ζ في حقل F أية جذر نوني للمحايد إذا كان $\zeta^n = e$ حيث e المحايد للحقل F .

ملاحظة من التعريف فإن كل جذر نوني للمحايد هو جذر لكثيرة الحدود $f(x) = x^n - e$. الآن $f'(x) = nx^{n-1}$. ليكن F حقلاً بحيث أن مميز F لا يقسم n . $f(x)$ هي كثيرة حدود على F . بما أن مميز F لا يقسم n فإن $f'(x) = nx^{n-1} = nex^{n-1} \neq 0$. الاحتمال الوحيد لجذر $f'(x)$ هو $x = 0$ والصفر ليس جذراً لـ $f(x)$. هذا يعطي أن $f(x)$ و $f'(x)$ ليس لهما جذر مشترك في أي حقل توسيع K للحقل F . بالتالي $f(x)$ ليس لها جذر مكرر في أي حقل توسيع للحقل F (قضية 13-41) . لهذا السبب بالأخص إذا كان K حقل انفلاق $f(x)$ على F فإن K يحوي n جذراً مختلفاً لكثيرة الحدود $f(x)$.

نظرية 14-20

ليكن F حقلاً بمميز صفر و K حقل انفلاق كثيرة الحدود $ex^n - e$ على F عندئذ يكون :

(i) مجموعة جميع جذور $f(x)$ هي زمرة دائرية بالنسبة للضرب ورتبتها n .

(ii) الزمرة $G(K, F)$ ، زمرة جالوا أيزومورفية مع زمرة جزئية من زمرة الأعداد الصحيحة M معيار عدد أولي نسبياً مع n . بالتالي فإن $G(K, F)$ زمرة إبدالية .

البرهان

(i) لنفرض أن S هي مجموعة جميع جذور كثيرة الحدود $x^n - e$ في K . فيكون عدد عناصرها n (انظر الملاحظة السابقة) . لنأخذ أي عنصرين ζ ، λ في S فإن $\lambda^n = e$ ، $\zeta^n = e$. هذا يبين أن $(\zeta\lambda^{-1})^n = \zeta^n(\lambda^n)^{-1} = ee^{-1} = e$. كذلك $\zeta\lambda^{-1}$ هو جذر لكثيرة الحدود $x^n - e$. إذاً $\zeta\eta^{-1} \in S$ ومن ثم فإن S زمرة جزئية منتهية من زمرة الضرب لـ K . بالتالي فإن S زمرة دائرية رتبتها n (قضية 14-17) .

(ii) ليكن θ مولداً للزمرة الدائرية S لجميع الجذور النونية لكثيرة الحدود $x^n - e$ وعددها n ، فإن رتبة θ بالنسبة لعملية الضرب هو n . إذاً θ جذر نوني بدائي للمحايد e . الآن كل عنصر آخر في S هو قوة للمولد θ بالتالي فإن $K = F(\theta)$.

ليكن σ أي F- أوتومورفزم للحقل K . لأي جذر نوني ζ للمحايد $\zeta^n = e$ يعطينا $e = \sigma(e) = \sigma(\zeta^n) = (\sigma(\zeta))^n$ عليه فإن $\sigma(\zeta) \in S$. بما أن σ راسم أحادي فإن مقصور σ على S هو أوتومورفزم للزمرة $S =< \theta >$. ويكون أيضاً $\sigma(\theta)$ هو مولداً للزمرة S فإذا كان $\sigma(\theta) = \theta^t$ ، فإن t عدد صحيح أولي نسبياً مع n . ليكن $\bar{t}$ فصل التكافؤ معيار n الذي ينتمي إليه t ، فإن $\bar{t} \in M$.

عرف الراسم $g : G(K, F) \to M$ بوضع $g(\sigma) = \bar{t}$ حيثما يكون $\sigma(\theta) = \theta^t$.

ندعي أن g معرف تعريفاً جيداً . لأجل ذلك افرض أن $\sigma(\theta) = \theta^u$ أيضاً فإن $\theta^{t-u} = e$. بالتالي $n \mid t - u$ إذاً $\bar{t} = \bar{u}$.

لأي عنصرين $\sigma, \eta \in G(K, F)$ ، افرض أن $g(\sigma) = \bar{t}_1, g(\eta) = \bar{t}_2$. فيكون $\sigma(\theta) = \theta^{t_1}, \eta(\theta) = \theta^{t_2}$. بالتالي فإن :

$$(\sigma\eta)(\theta) = \sigma[\eta(\theta)] = \sigma(\theta^{t_2}) = (\sigma(\theta))^{t_2} = (\theta^{t_1})^{t_2} = \theta^{t_1t_2}$$

أي أن $g(\sigma\eta) = \overline{t_1 t_2} = \bar{t}_1\bar{t}_2 = g(\sigma)g(\eta)$ وهذا يبين أن g يمثل هومومورفزم زمرة . للبرهنة على أن g راسم أحادي افرض أن $\sigma \in \ker g$ فإن $g(\sigma) = \bar{I}$ ويكون $\sigma(\theta) = \theta^1 = \theta$.

بما أن σ تمثل الراسم المحايد على F و $K = F(\theta)$ فإن σ تمثل الراسم المحايد على K . إذاً $\ker g = (I)$. هذا يثبت (ii) . □

ملاحظة 1 لاحظ أنه في إثبات (ii) لا نحتاج لوضع أي شرط على مميز F .

ملاحظة 2 ليكن F حقلاً بمميز صفر و $\alpha(\neq 0) \in F$.

نفرض أن K حقل توسيع للحقل F يحوي حقل انفلاق كثيرة الحدود $x^n - \alpha$ وجذراً بدائياً للمحايد وليكن θ ، مثلاً . عندئذ تكون $e, \theta, \theta^2, \ldots, \theta^{n-1}$ هي جميع الجذور النونية للمحايد . فإذا كان a أي جذر اختياري لكثيرة الحدود $x^n - \alpha$ في K ، فإن لكل θ^i ، $i = 0, 1, \ldots, n-1$ يكون $(\theta^i a)^n = \theta^{ni}a^n = e\alpha = \alpha$ والذي يبين أن كل واحد من $\theta^i a$ هو جذر لكثيرة الحدود $ex^n - \alpha$.

ومن ثم فإن جميع الجذور النونية لكثيرة الحدود $ex^n - \alpha$ هي $a, \theta a, \theta^2 a, \ldots, \theta^{n-1}a$.

ليكن L حقل انفلاق كثيرة الحدود $ex^n - \alpha$ على F محتوى في K . فإن $a, \theta a, \theta^2 a, \ldots, \theta^{n-1}a \in L$. وعندئذ فإن $F(\theta, a) \subseteq L$ ولكن $L = F(a, \theta a, \theta^2 a, \ldots, \theta^{n-1}a) \subseteq F(\theta, a)$ إذاً $L = F(\theta, a)$.

على وجه الخصوص إذا كان F يحوي جذراً نونياً بدائياً للمحايد ، فإن $\theta \in F$ و $L = F(a)$. فإننا نستطيع أيضاً أن نقول أن F يحوي جذراً نونياً بدائياً للمحايد وعندئذ لأي $(\alpha \neq 0) \in F$ يكون حقل الانفلاق L لكثيرة الحدود $ex^n - \alpha$ على F هو $F(a)$ حيث a أي جذر اختياري لكثيرة الحدود $ex^n - \alpha$.

قضية 14-21

إذا كان F حقلاً بمميز صفر يحوي جميع الجذور النونية للمحايد 1 (لعدد صحيح موجب ثابت n) فإنه لأي $F \ni (a \neq 0)$ فإن حقل الانفلاق L لكثيرة الحدود $x^n - \alpha$ هو $L = F(a)$ حيث a جذر اختياري لكثيرة الحدود $x^n - \alpha$ ، إضافة إلى ذلك فإن زمرة جالوا $G(L, F)$ هي أبيلية .

البرهان

ليكن ζ جذر نوني بدائي للمحايد في F وليكن a أي جذر لكثيرة الحدود $x^n - \alpha$ على F . كما وجدنا (ملاحظة 2) فإن $L = F(a)$ وجذور $x^n - \alpha$ في L هي $a, \zeta a, \zeta^2 a, \ldots, \zeta^{n-1} a$. اعتبر أي عنصرين σ و η في $G(L, F)$. الآن $\sigma(a)$ ، $\eta(a)$ جذران لكثيرة الحدود $x^n - \alpha$. بالتالي $\sigma(a) = \zeta^i a$ و $\eta(a) = \zeta^j(a)$ لبعض i, j . وبما أن σ هو F – أوتومورفزم فإن :

$$(\sigma\eta)\,(a) = \sigma(\eta(a)) = \sigma(\zeta^j a) = \zeta^i \sigma(a)$$

عليه فإن $\sigma\eta(a) = \zeta^j \zeta^i a = \zeta^{i+j} a$. بالمثل فإن $\eta\sigma(a) = \zeta^{i+j} a$. وهكذا فإن $\sigma\eta(a) = \eta\sigma(a)$. بالتالي $\sigma\eta = \eta\sigma$. إذاً $G(L, F)$ زمرة إبدالية . □

تعريف 14-22

يقال لحقل توسيع K للحقل F توسيع جذري إذا وجدت متتابعة من حقول :

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_r = K$$

بحيث لكل $1 \leq i \leq r$ فإن $F_i = F_{i-1}(\omega_i)$ لبعض $\omega_i \in F_i$ مع الخاصية $\omega_i^{r_i} \in F_{i-1}$ لبعض $r_i \geq 1$.

ملاحظة نلاحظ أن $K = F(\omega_1, \omega_2, \ldots, \omega_r)$ ، $F_i = F(\omega_1, \omega_2, \ldots, \omega_i)$ و $\omega_i^{r_i} \in F_{i-1}$. الآن $\omega_i^{r_i} \in F_{i-1}$ لذا فإن ω_i هو جذر لكثيرة الحدود $x^{r_i} - \omega_i^{r_i}$ على F_{i-1} عليه فإن F_i توسيع جبري بسيط للحقل F_{i-1} بالتالي فإن $[F_i : F_{i-1}]$ منتهي . إذاً :

$$[K : F] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}]...[F_1 : F]$$

وهذا يؤدي إلى أن K هو نفسه توسيع جبري منته للحقل F .

الآن نعطي تعريفاً دقيقاً لما نعنيه بقولنا أن كثيرة حدود ما قابلة للحل بواسطة جذور.

تعريف 14-23 (a)

يقال لكثيرة حدود غير ثابتة $p(x)$ على حقل F أنها قابلة للحل بواسطة جذور إذا كان حقل الانفلاق K لكثيرة الحدود $p(x)$ على F محتوى في توسيع جذري للحقل F .

مثال 7

لتكن $f(x) = x^2 + ax + 1$ كثيرة حدود تربيعية واحدية على Q ، حقل الأعداد النسبية . جذراها هما :

$$\alpha_1 = \frac{-a + \sqrt{a^2 - 4b}}{2}, \ \alpha_2 = \frac{-a - \sqrt{a^2 - 4b}}{2}$$

إذا أخذنا $L = \theta(\omega)$ حيث $\omega = \sqrt{a^2 - 4b}$ عندئذ نجد أن $\omega^2 \in Q$. عليه فإن L توسيع جذري للحقل Q . إضافة إلى ذلك فإن L نفسه حقل انفلاق $f(x)$ على Q . لذا فإن $f(x)$ قابلة للحل بواسطة جذور .

مثال 8

اعتبر $f(x) = x^3 + 3ax^2 + 3bx + c$ على Q ، حقل الأعداد النسبية . إذا أخذنا $z = x + a$ فإن المعادلة السابقة تصبح معادلة بالصيغة $g(z) = z^3 + 3b_1z + c_1$ حيث $b_1, c_1 \in Q$. فإذا علمنا جذور $g(z)$ فإنه يمكننا الحصول على جذور $f(x)$ من جذور $g(z)$ بطرح a من كل جذر من جذور $g(x)$. بما أن $a \in Q$ ، نجد أن حقل

انفلاق كثيرة الحدود $f(x)$ وحقل انفلاق نظيرتها $g(x)$ متساويان . صيغة كاردان يعطي أن جذور $g(z)$ هي $p+q$ ، $\omega p+\omega^2 q$ ، $\omega^2 p+\omega q$ حيث ω هو جذر تكعيبي تخيلي للمحايد (هنا الواحد) .

$$p=\sqrt[3]{-\frac{c_1}{2}+\sqrt{b_1^3+\frac{{c_1}^2}{4}}}$$

و
$$q=\sqrt[3]{-\frac{c_1}{2}-\sqrt{b_1^3+\frac{{c_1}^2}{4}}}$$

ضع
$$\alpha_1=\sqrt{b_1^3+\frac{{c_1}^2}{4}},\quad \alpha_2=\sqrt[3]{-\frac{c_1}{2}+\alpha_1},\quad \alpha_3=\sqrt{-3}$$

الآن ضع $F_0=Q$ ، $F_1=F_0(\alpha_1)$ ، $F_2=F_1(\alpha_2)$ ، $F_3=F_2(\alpha_3)$. نجد أن $F_0\subseteq F_1\subseteq F_2\subseteq F_3$ ، $\alpha_1^2\in F_0$ ، $\alpha_2^3\in F_1$ ، $\alpha_3^2\in F_2$.

إضافة إلى ذلك F_3 يحوي جميع جذور $g(z)$. عليه فإن $g(z)$ وبالتالي $f(x)$ قابلة للحل بواسطة جذور .

ملاحظة لأية كثيرة حدود $f(x)=x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ على F ، يمكننا القول أن $f(x)$ قابلة للحل بواسطة جذور إذا استطعنا الحصول على أي جذر من جذور $f(x)$ بإجراء عدد منته من عمليات الجمع ، الضرب ، الطرح ، القسمة على عناصر غير صفرية وبأخذ الجذر الميمي (لأي عدد صحيح موجب m) على معاملات $f(x)$.

نظرية 23-14

إذا كان E هو حقل توسيع منته بواسطة جذور للحقل F ، فإنه يوجد توسيع عادي منته K للحقل F يحوي E بحيث K هو توسيع للحقل F بواسطة جذور .

البرهان

بما أن E توسيع للحقل F بواسطة جذور ، توجد سلسلة من الحقول $F=F_0\subseteq F_1\subseteq F_2\subseteq\ldots\subseteq F_K=E$ بحيث أن كل $i=1,2,\ldots K$ يكون $F_i=F_{i-1}(\omega_i)$ لبعض $\omega_i\in F_i$ حيث $\omega_i^{r_i}\in F_{i-1}$ لعدد صحيح $1\le r_i$.

الآن كل واحد من ω_i هو عنصر جبري على F . لتكن $f_i(x)$ كثيرة الحدود الأصغرية للعنصر ω_i على F وأن
$$f(x) = f_1(x)f_2(x)\dots f_k(x)$$
فإذا كان K حقل انفلاق $f(x)$ على E ، فإن $E \subseteq K$. وحيث أن $\omega_1, \omega_2, \dots, \omega_k$ هي أيضاً جذور لكثيرة الحدود $f(x)$ فإن K هو حقل انفلاق $f(x)$ على F . من ذلك نجد أن K توسيع عادي للحقل F منتهي الدرجة . هذا يبين أن للحقل K عدد منتهي فقط $\sigma_0, \sigma_1, \dots, \sigma_m$ من F – أوتومورفزمات بحيث $\sigma_0 = I$ الأوتومورفزم المحايد على K .

عرف $\beta_{tk+i} = \sigma_t(\omega_i)$ لكل $t = 0, 1, \dots, m$ و $i = 1, 2, \dots, k$ بما أن $f_i(x)$ هي كثيرة الحدود الأصغرية للعنصر ω_i على F و σ_t هو F – أوتومورفزم للحقل K فإن العنصرين $\sigma_t(\omega_i)$ و ω_i مرافقان على F . عليه كل من b_{tk+i} هو جذر لكثيرة الحدود $f_i(x)$ وكذلك لكثيرة الحدود $f(x)$. اعتبر أي جذر c لكثيرة الحدود $f(x)$. فإن c جذر لبعض من $f_i(x)$. بما أن ω_i و c جذران لكثيرة الحدود $f_i(x)$ غير القابلة للتحليل على F ، فإنه يوجد F – أوتومورفزم σ_t للحقل K بحيث $\sigma_t(\omega_i) = c$ وعليه وفق التعريف $c = b_{tk} + i$. ومنها نجد أن جذور $f(x)$ هي فقط :

$$b_1, b_2, \dots, b_k, b_{k+1}, \dots, b_{mk+k}$$

هذا بدوره يؤدي إلى أن $K = F(b_1, b_2, \dots, b_{mh+k})$.

بما أنه لأي $s = 1, 2, \dots, k$ ، لدينا $b_{tk+s} = \sigma_t(\omega_s)$ فإن لكل $l = 1, 2, \dots, k$ يكون :

$$\begin{aligned}\sigma_t F(\omega_1, \omega_2, \dots, \omega_l) &= \sigma_t(F_l)\\ &= F(\sigma_t(\omega_1), \sigma_t(\omega_2), \dots, \sigma_t(\omega_l))\\ &= F(b_{tk+1}, b_{tk+2}, \dots, btk + l)\end{aligned}$$

ولما كان
$$\omega_l^{r_l} \in F_{l-1} = F(\omega_1, \omega_2, \dots, \omega_{l-1})$$

فإن
$$\begin{aligned}b_{tk+l}^{r_l} &= (\sigma_t(\omega_l))^{r_l}\\ &= \sigma_t(\omega_l^{r_l}) \in \sigma_t(F_{l-1})\\ &= F(b_{tk+1}, b_{tk+2}, \dots, b_{tk+l-1})\end{aligned}$$

إذا عرفنــا $k_{tk+l} = F(b_1, b_2, \ldots, b_{tk+1})$ لكــل $t = 0, 1, 2, \ldots, m$ ، $l = 1, 2, \ldots, k$ ويكــون لدينا $K_{tk+l} = K_{tk+l-1}(b_{tk+l})$ بحيث :

$$K_1 \subseteq K_2 \subseteq K_3 \subseteq \ldots \subseteq K_k \subseteq K_{k+} \ldots, \ldots, \subseteq K_{2k} \subseteq$$
$$\ldots \subseteq K_{mk} \subseteq K_{mk+1} \subseteq \ldots \subseteq K_{mk+k} = K \qquad (1)$$

كذلك

$$b_{tk+l}^{r_l} = [\sigma_t(\omega_l)]^{r_l}$$
$$= \sigma_t(\omega_l^{r_l}) \in \sigma_t(F_{l-1}) = F(b_{tk+1}, \ldots, b_{tk+l-1})$$
$$\subseteq F(b_1, b_2, \ldots, \ldots, b_{tk+l-1}) = K_{tk+l-1}$$

من هذه النتيجة ومتتابعة لحقول (1) نجد أن K توسيع جذري للحقل F . إذاً K توسيع عادي للحقل F يحوي E بحيث K أيضاً توسيع جذري للحقل F . □

نظرية 14-24

ليكن E توسيعاً عادياً لحقل F درجته n . إضافة إلى ذلك افرض أن F يحوي جذراً نونياً بدائياً للمحايد . عندئذ زمرة جالوا $G(E, F)$ تكون دائرية إذا وفقط إذا وجد $b \in F$ بحيث $x^n - b$ غير قابلة للتحليل على F و E حقل انفلاق $x^n - b$ على F .

البرهان

لتكن $x^n - b$ كثيرة حدود غير قابلة للتحليل على F لعدد صحيح موجب n ولعنصر $b \in F$ وليكن E حقل انفلاق كثيرة الحدود هذه على F . عندئذ يكون $E = F(c)$ (قضية 14-21) حيث c أي جذر لكثيرة الحدود $x^n - b$ ويكون $[E : F] = n$.

إذاً $G(E, F)$ من الرتبة n . الآن ليكن ξ أي جذر نوني بدائي للمحايد في F . (لاحظ إذا كان F يحوي جذراً نونياً بدائياً للمحايد فإنه يحوي جميع الجذور النونية البدائية للواحد !) . فإن $c, \xi c, \xi^2 c, \ldots, \xi^2 c, \ldots, \xi^{n-1} c$ هي جميع جذور كثيرة الحدود $x^n - b$

وعددها n (الملاحظة التي سبقت قضية 14-21) . لما كان ξ ، ξc مترافقان على F فإنه يوجد F – أيزومورفزم σ من $F(c)$ على $F(\xi c)$ بحيث $\sigma(c) = \xi c$. من ناحية أخرى $E = F(c) = F(\xi c)$ عليه فإن σ هو F – أوتومورفزم للحقل F . وهكذا فإن σ ينتمي إلى $G(E, F)$. الآن :

$$\sigma^2(c) = \sigma[\sigma(c)] = \sigma(\xi c) = \xi\sigma(c) = \xi^2 c$$

بصورة عامة $\sigma^k(c) = \xi^k c$ لكل $k = 1, 2, \dots, n$.

لما كان $\xi^n = 1$ و $c, \xi c, \dots, \xi^{n-1}c$ جميعها مختلفة فإن $I, \sigma, \sigma^2, \dots, \sigma^{n-1}$ هي عناصر $G(E, F)$ المختلفة وعددها n . ويكون $G(E, F) =< \sigma >$ زمرة دائرية رتبتها n .

بالعكس إذا كانت $G(E, F)$ زمرة دائرية رتبتها n ، فإن عناصرها $I, \sigma, \sigma^2, \dots, \sigma^{n-1}$ مستقلة خطياً على F (نظرية 14-1) .

ليكن ξ جذر نوني بدائي للمحايد في F . عندئذ $\xi \neq 0$ و $1 + \xi^{-1}\sigma + \xi^{-2}\sigma^2 + \dots + \xi^{-(n-1)}\sigma^{n-1}$ هو إندومورفزم غير صفري للحقل E كفضاء متجهي على F . عليه يوجد $a \in E$ بحيث :

$$c = I(a) + \xi^{-1}\sigma(a) + \xi^{-2}\sigma^2(a) + \dots + \xi^{-n+1}\sigma^{n-1}(a) \neq 0$$

الآن

$$\begin{aligned} \sigma(c) &= \sigma(a) + \xi^{-1}\sigma^2(a) + \xi^{-2}\sigma^3(a) + \dots + \xi^{-n+1}\sigma^n(a) \\ &= \xi\left[\xi^{-1}\sigma(a) + \xi^{-2}\sigma^2(a) + \dots + \xi^{-n+1}\sigma^{n-1}(a) + I(a)\right] \\ &= \xi c \qquad (\text{لأن } \xi^n = 1, \sigma^n = I) \end{aligned}$$

بصورة عامة $\sigma^k(c) = \xi^k c$ لكل $k = 1, 0, \dots, n-1$.

إذاً $\sigma^k(c^n) = \left[\sigma^k(c)\right]^n = \xi^{kn}c^n = c^n$ لأي $k = 1, 2, \dots, n-1$. عليه c^n ينتمي إلى الحقل المثبت تحت $G(E, F)$. من ناحية ثانية F هو الحقل المثبت تحت $G(E, F)$ (نظرية 14-15) .

عليه $c^n \in F$. ضع $b = c^n$ بالتالي فإن $x^n - b$ هي كثيرة حدود على F والتي جذورها هي $c, \xi c, \xi^2 c, \ldots, \xi^{n-1} c$. على أية حال فإن $\sigma^k(c) = \xi^k c$ يبين أن $c, \xi c, \xi^2 c, \ldots, \xi^{n-1} c$ تكون مترافقة على F . إذاً درجة كثيرة الحدود الأصغرية $f(x)$ للعنصر c على F هي على الأقل n . لما كان $f(x) \mid (x^n - b)$ فإن $f(x) = x^n - b$ ، وهي نفسها كثيرة الحدود الأصغرية للعنصر c . إذاً $x^n - b$ غير قابلة للتحليل على F . الآن $[F(c) : F] = n$ ، $[E : F] = n$ ، $F(c) \subseteq E$ يعطي أن $E = F(c)$. ومن ثم فإن E هو حقل انفلاق $x^n - b$ على F و x^{n-b} كثيرة حدود غير قابلة للتحليل على F وبهذا يكمل البرهان . □

تعريف 14-25

لتكن $p(x)$ أية كثيرة حدود (غير صفرية) على حقل F وليكن E حقل انفلاق $p(x)$ على F . زمرة جميع F – أوتومورفزمات الحقل E تسمى زمرة جالوا كثيرة الحدود $p(x)$ على F .

الآن نعطي علاقة بين طبيعة $p(x)$ وزمرة جالوا لها . من الآن فصاعداً نوقف أنفسنا على حالة الحقل F الذي يحوي جميع الجذور النونية البدائية للمحايد لكل n ، إلا إذا ذكر غير ذلك .

نظرية 14-26

إذا كان F حقلاً بمميز صفر يحوي جميع جذور المحايد ، فإن كثيرة حدود $p(x)$ على F تكون قابلة للحل بواسطة جذور إذا وفقط إذا كانت زمرة جالوا لها على F قابلة للحل .

البرهان

افرض أن $p(x)$ قابلة للحل بواسطة جذور . ذلك يعني أن حقل الانفلاق E لكثيرة الحدود $p(x)$ على F محتوى في توسيع جذري للحقل F . عندئذ نستطيع إيجاد متتابعة من الحقول .

$$F_0 = F \subseteq F_1 = F_0(\omega_1) \subseteq F_2 = F_1(\omega_2) \subseteq F_3 = F_2(\omega_3) \subseteq \dots$$
$$\subseteq F_k = F_{k-1}(\omega_k)$$

بحيث أن $\omega_1^{r_1} \in F_0, \omega_1^{r_2} \in F_1, \dots, \dots, \omega_k^{r_k} \in F_{k-1}$ لأعداد صحيحة $r_j \geq 1$ $(j = 1, 2, \dots, k)$ و $E \subseteq F_k$. حسب نظرية 14-23 يمكننا فرض أن F_k توسيع عادي للحقل F .

اعتبر الزمر $G_i = G(F_k, F_i)$ لكل $i = 0, 1, \dots, k-1$. لأي $i = 1, 2, \dots, k$ و $F_i = F_{i-1}(\omega_i)$ مع كون $\omega_i^{r_i} \in F_{i-1}$ يعطي أن ω_i جذر لكثيرة الحدود $x^{r_i} - \omega_i^{r_i}$ ، افرض ζ_i الجذر البدائي رقم r_i للمحايد في F . فإن $\zeta_i \in F_{i-1}$ وأن جذور كثيرة الحدود $x^{r_i} - \omega_i^{r_i}$ وهي $\omega_i, \zeta\omega_i, \dots, \zeta^{r_{i-1}}\omega_i$ وعددها r_i تنتمي جميعها إلى F_i . عليه فإن F_i هو حقل انفلاق لكثيرة الحدود $x^{r_i} - \omega_i^{r_i}$ على F_{i-1} .

حسب نظرية 14-21 فإن الزمرة $G(F_i, F_{i-1})$ أبيلية . الآن F_k هو أيضاً توسيع عادي للحقل F_{i-1} . من النظرية الأساسية لجالوا (نظرية 14-10) فإن $G_i = G(F_k, F_i)$ هي زمرة جزئية عادية من الزمرة $G_{i-1} = G(F_k, F_{i-1})$ و $G(F_i, F_{i-1}) \cong \dfrac{G_{i-1}}{G_i}$. عليه ففي السلسلة التنازلية $G_0 = G(F_k, F_0) \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_{k-1} \supseteq G_k = \{I\}$ كل G_i هي زمرة جزئية عادية من G_{i-1} و $\dfrac{G_{i-1}}{G_i}$ زمرة أبيلية . هذا يبرهن أن $G(F_k, F)$ زمرة قابلة للحل .

بما أن E توسيع عادي للحقل F فإن $G(F_k, E)$ زمرة جزئية عادية من $G(F_k, F)$ و $G(E, F) = \dfrac{G(F_k, F)}{G(F_k, E)}$ بما أن زمرة قسمة أية زمرة قابلة للحل تكون قابلة للحل فإن $G(E, F)$ زمرة قابلة للحل .

بالعكس لتكن $G(E, F)$ زمرة قابلة للحل . بإمكاننا إيجاد سلسلة عادية جزئية $G_0 = G(E, F) \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_{k-1} \supseteq G_k = \{I\}$ بحيث تكون $\dfrac{G_i}{G_{i+1}}$ زمرة دائرية لكل $i = 0, 1, ,2, \ldots, k-1$. ليكن F_i الحقل المثبت تحت G_i عندئذ G_i هي زمرة جميع F_i – أوتومورفزمات الحقل $F_k(= E)$ أي $G(E, F_i)$. ولما كانت G_{i+1} زمرة جزئية عادية من G_i ، فإن F_{i+1} توسيع عادي للحقل F_i و $G(F_{i+1}, F_i) \cong \dfrac{G_i}{G_{i+1}}$ هي زمرة دائرية . الآن F_i يحوي جميع الجذور النونية البدائية للمحايد لكل عدد صحيح موجب n كما يتحقق ذلك للحقل F .

حسب نظرية 14-24 يوجد $b_i \in F_i$ وعدد صحيح موجب r_i يجعل $x^{r_i} - b_i$ غير قابلة للتحليل على F_i و F_{i+1} هو حقل انفلاق $x^{r_i} - b_i$ على F_i . ليكن ω_i أي جذر لكثيرة الحدود $x^{r_i} - b_i$ في F_{i+1} . عندئذ $F_{i+1} = F_i(\omega_i)$ و $\omega_i^{r_i} \in F_i$. لذا فإن لدينا متتابعة $F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_k = E$ من حقول بحيث $F_{i+1} = F_i(\omega_i)$ لبعض $\omega_i \in F_{i+1}$ و $\omega_i^{r_i} \in F_i$ بالتالي فإن E توسيع بواسطة جذور للحقل F . هذا يبرهن أن $p(x)$ قابلة للحل بواسطة جذور . □

نظرية 14-27

كل كثيرة حدود من الدرجة الرابعة قابلة للحل بواسطة جذور .

البرهان

لتكن $p(x) = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4, a_0 \neq 0$ أية كثيرة حدود من الدرجة الرابعة على F وليكن E حقل انفلاقها على F . فإن $E = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$

حيث $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ هي جذور $p(x)$ الآن لأي $\sigma \in G(E, F)$ يكون $\sigma(\alpha_i)$ جذراً لكثيرة الحدود $p(x)$ لكل $i = 1, 2, 3, 4$. فإن σ يعطي تبديلاً للمجموعة $X = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ ، المجموعة X تحوي أربعاً أو أقل من عناصر مختلفة لأن بعض الجذور قد تكون متساوية .

افرض أن $| X | = m \leq 4$. الزمرة $A(X)$ ، زمرة جميع تباديل X هي أيزومورفية مع زمرة التناظرات S_m . بما أن زمر التناظرات S_1, S_2, S_3 و S_4 قابلة للحل فإننا نحصل على أن $A(X)$ قابلة للحل . عرف $f : G(E, F) \to A(X)$ كالآتي : $f(\sigma)$ هو مقصور σ على X .

هذا الراسم f هو مونومورفزم . لذا فإن $G(E, F) \cong \operatorname{Im} f$ بالتالي فإن $G(E, F)$ أيزومورفية لزمرة جزئية من الزمرة القابلة للحل $A(X)$ ، بالتالي فإن الزمرة $G(E, F)$ قابلة للحل ، ومن ثم فإن $p(x)$ قابلة للحل على F (نظرية 14-26) . □

من المثالين 7 و 8 والنظرية السابقة نستنتج أن جميع كثيرات الحدود من الدرجات 2، 3 و 4 على F تكون قابلة للحل بواسطة جذور .

اعتبر أي حقل F والحقل $F(x_1, x_2, \ldots, x_n)$ في n من غير المحددات على F . دع S_n زمرة التناظرات (التماثلات) من الدرجة n تؤثر على المجموعة $\{1, 2, \ldots, n\}$. لكل $\sigma \in S_n$ يمكننا تعريف أوتومورفزم σ' للحقل $F(x_1, x_2, \ldots, x_n)$ كالآتي :

اعتبر أية دالة نسبية $r(x_1, x_2, \ldots, x_n)$ فإن :

$$\sigma'[r(x_1, x_2, \ldots, x_n)] = r(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

عليه فإن $\sigma \to \overline{\sigma}$ مونومورفزم من S_n إلى زمرة جميع F – أوتومورفزمات الحقل $F(x_1, x_2, \ldots, x_2)$. وهكذا يمكن التعامل مع S_n على أنها زمرة F – أوتومورفزمات للحقل $F(x_1, x_2, \ldots x_n)$. ليكن S الحقل المثبت تحت S_n . كل عنصر في S يسمى دالة تماثل .

اعتبر

$$a_1 = x_1 + x_2 + \ldots + x_n$$

$$a_2 = \sum_{i<j} x_i x_j$$
$$a_3 = \sum_{i<j<k} x_i x_j x_k$$
$$\vdots$$
$$a_n = x_1 x_2 \dots x_n$$

على سبيل المثال عندما $n = 3$ ، فإن $a_1 = x_1 + x_2 + x_3$ ، $a_2 = x_1x_2 + x_1x_3 + x_2x_3$ ، $a_3 = x_1x_2x_3$. وعندما $n = 4$ فإن $a_1 = x_1 + x_2 + x_3 + x_4$ ، $a_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$ $a_3 = x_1x_2x_3 + x_2x_3x_4 + x_1x_2x_4 + x_1x_3x_4$ و $a_4 = x_1x_2x_3x_4$. يمكن بسهولة رؤية أن كلاً من $a_1, a_2, \dots, a_n$ هو دالة تماثل . أي أن $a_1, a_2, \dots, a_n$ جميعها تنتمي إلى S . كل من $a_1, a_2, \dots, a_n$ تسمى دالة تماثل أولية . لاحظ أن $S \supseteq F(a_1, a_2, \dots, a_n)$.

وسوف نثبت النظرية الآتية .

نظرية 14-28

ليكن F حقلاً و $F(x_1, x_2, \dots, x_n)$ حقل الدوال النسبية في n من غير المحددات $x_1, x_2, \dots, x_n$. إذا كان S حقل دوال التماثل ، فإن :

(i) $[F(x_1, x_2, \dots, x_n) : S] = n!$

(ii) $S = F(a_1, a_2, \dots, a_n)$ حيث $a_1, a_2, \dots, a_n$ هي دوال تماثل أولية في $x_1, x_2, \dots, x_n$.

(iii) زمرة جالوا $G(F(x_1, x_2, \dots, x_n), S)$ أيزومورفية مع S_n .

البرهان

(i) كما أشرنا سابقاً نعتبر S_n زمرة F – أوتومورفزمات للحقل $F(x_1, x_2, \dots x_n)$ و S الحقل المثبت تحت S_n . عليه حسب نظرية 14-8 فإن : $[F(x_1, x_2, \dots, x_n) : S] = \circ(S_n) = n!$.

(ii) بما أن $S \supseteq F(a_1, a_2, \dots, a_n)$ ،

$$[F(x_1, x_2, \ldots, x_n) : F(a_1, a_2, \ldots a_n)] \geq [F(x_1, x_2, \ldots, x_n) : S] = n!$$

اعتبر كثيرة الحدود
$$p(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} + \ldots + (-1^n)\, a_n$$
$$= (t - x_1)(t - x_2) \ldots (t - x_n)$$

كل واحد من $x_1, x_2, \ldots, x_n$ هو جذر لكثيرة الحدود $p(t)$ وهذه الجذور تولد $F(x_1, x_2, \ldots, x_n)$ على $F(a_1, a_2, \ldots, a_n)$. إذاً $F(x_1, x_2, \ldots, x_n)$ هو حقل انفلاق $p(t)$ على $F(a_1, a_2, \ldots, a_n)$ على أية حال $\deg p(t) = n$ فيكون $[F(x_1, x_2, \ldots, x_n) : F(a_1, a_2, \ldots, a_n)] \leq n!$ (نظرية 13-30) . ونستنتج أن :

$$[F(x_1, x_2, \ldots, x_n) : F(a_1, a_2, \ldots, a_n)] = n!$$

وعليه فإن
$$n! = [F(x_1, x_2, \ldots, x_n) : F(a_1, a_2, \ldots, a_n)]$$
$$= [F(x_1, x_2, \ldots, x_n) : S][S : F(a_1, a_2, \ldots, a_n)]$$
$$= n![S : F(a_1, a_2, \ldots, a_n)]$$

وهذا يعطي $[S : F(a_1, a_2, \ldots, a_n)] = 1$ وأن $S = F(a_1, a_2, \ldots, a_n)$ وهذا يبرهن (ii) .

(iii) بما أن $[F(x_1, x_2, \ldots, x_n) : S] = n!$ فإن $o\{G[F(x_1, x_2, \ldots, x_n), S]\} \leq n!$ من ناحية ثانية S_n زمرة رتبتها $n!$ محتواة في $G(F(x_1, x_2, \ldots, x_n), S)$. لذلك فإن $G(F(x_1, x_2, \ldots, x_n), S) = S_n$. هذا يبرهن (iii) . □

تعريف 14-29

ليكن $x_1, x_2, \ldots, x_n$ أي n في غير المحددات على أي حقل F ولتكن $a_1, a_2, \ldots, a_n$ أي n من الدوال المتماثلة الأولية في $x_1, x_2, \ldots, x_n$. عندئذ كثيرة الحدود $p_n(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} + \ldots + (-1)^n a_n$ تسمى كثيرة الحدود النونية العامة .

نظرية 14-30 (آبيل)

كثيرة الحدود النونية العامة $p_n(t)$ ذات الدرجة $n \geq 5$ غير قابلة للحل بواسطة جذور على $F(a_1, a_2, \ldots, a_n)$.

البرهان

بما أن زمرة جالوا لكثيرة الحدود $p_n(t)$ على $F(a_1, a_2, \ldots, a_n)$ هي S_n (نظرية 28-14) و S_n غير قابلة للحل عندما $n \geq 5$ (نتيجة 5-42) فإن $p_n(t)$ غير قابلة للحل بواسطة جذور . □

ملاحظة 1 لقد فرضنا أن F بمميز صفر ولكل عدد صحيح موجب n ، فإن F يحوي جميع الجذور النونية للواحد ومع ذلك فإنه في نظرية 14-28 لسنا بحاجة لفرض أية شروط على F . في الحقيقة أن الكثير من النتائج السابقة يمكن إثباتها لأي حقل بمميز صفر .

ملاحظة 2 النظرية السابقة تبين أنه لكل $n \geq 5$ توجد كثيرة حدود درجتها n على حقل مناسب هي غير قابلة للحل بوساطة جذور . بصورة عامة فإن كثيرات الحدود من درجة $n \geq 5$ غير قابلة للحل بواسطة جذور .

تمارين محلولة

تمرين 1

برهن أن كثيرة حدود متماثلة في $x_1, \ldots, x_n$ هي كثيرة حدود في دوال متماثلة أولية في $x_1, \ldots, x_n$.

الحل

عندما $n = 2$ ، $a_1 = x_1 + x_2$ ، $a_2 = x_1 x_2$. لتكن $f(x_1, x_2)$ كثيرة حدود متماثلة في x_1 و x_2 . بإعادة ترتيب $f(x_1, x_2)$ بقوة تنازلية لـ x_1 ، نحصل على $f(x_1, x_2) = A_t x_1^t + A_{t-1} x^{t-1} + \ldots + A_0$ حيث A_0 ، ... ، A_{t-1} ، A_t هي كثيرات حدود في x_2 . إذا عوضنا $a_1 - x_1$ بدلاً عن x_2 في $f(x_1, x_2)$ فإن $f(x_1, x_2)$ تصبح كثيرة حدود في x_1 ونجد أن $f(x_1, x_2) = B_u x_1^u + B_{u-1} x^{u-1} + \ldots + B_0 = g(x_1)$

حيث $B_u, B_{u-1}, \dots B_0$ كثيرات حدود في a_1 .

عندئــــذ $g(z) = B_u z^u + B_{u-1} z^{u-1} + \dots + B_0$. ضــــع $h(z) = z^2 - a_1 z + a_2$

وباستخدام خوارزمية القسمة في $F[a_1, a_2][z]$ نحصل على أن $g(z) = h(z)q(z) + Cz + D$

حيث $q(z) \in F[a_1, a_2][z]$ و $C, D \in F[a_1, a_2]$.

الآن $$g(x_1) = h(x_1)q(x_1) + Cx_1 + D \Rightarrow f(x_1, x_2) = Cx_1 + D$$

لأن $h(x_1) = 0$ علـى ضـوء حقيقـة أن $x_1^2 - (x_1 + x_2)x + x_1 x_2 = 0$ بتبـديل x_1 مـع x_2 والتذكر أن $f(x_1, x_2) = f(x_2, x_1)$ (لأن $f(x_1, x_2)$ كثيرة حدود متماثلة في x_2, x_1) نحصل على أن $f(x_1, x_2) = Cx_2 + D$ أي أن :

$$Cx_1 + D = Cx_2 + D \Rightarrow C(x_1 - x_2) = 0 \Rightarrow C = 0$$

وعليه $f(x_1, x_2) = D$. وهكذا فإن $f(x_1, x_2) \in F[a_1, a_2]$ ، بعبارة أخرى $f(x_1, x_2)$ كثيرة حدود في دوال تماثل أولية .

دعنا الآن نفرض أن $n > 2$ والنتيجة تتحقق لعدد $n - 1$ من غير المحددات . إذا كانت $t_1, t_2, \dots, t_n$ دوال تماثل أولية في $n - 1$ من غير المحددات $x_2, \dots, x_n$ ، يكون لدينا $a_1 = x_1 + t_1$; $a_2 = x_1 t_1 + t_2$; $a_3 = x_1 t_2 + t_3$ وهكذا إلى أن نصل $a_{n-1} = x_1 t_{n-2} + t_{n-1}$.

هذه الصيغ تؤدي إلى أن $t_1 = -x_1 + a_1$.

و $t_2 = -x_1 t_1 + a_2 = -x_1(-x_1 + a_1) + a_2 = x_1^2 - x_1 a_1 + a_2$

و $t_3 = -x_1(x_1^2 - x_1 a_1 + a_2) + a_3 = -x_1^3 + x_1^2 a_1 - x_1 a_2 + a_3, \dots,$

و $t_{n-1} = (-1)^{n-1}\left[x_1^{n-1} - x_1^{n-2} a_1 + \dots + (-1)^{n-1} a_{n-1}\right]$

لتكن $f(x_1, x_2, \dots, x_n)$ كثيرة حدود متماثلة في $x_1, x_2, \dots, x_n$ ترتيبها تنازليا في قوى x_1 نحصل على $$f(x_1, x_2, \dots, x_n) = A_p x_1^p + A_{p-1} x^{p-1} + \dots + A_0$$

حيث $A_0, A_1, \dots, A_p$ هي كثيرات حدود متماثلة في $x_2, x_3, \dots, x_n$ وحسب فروض الاستنتاج يمكن التعبير عنها ككثيرات حدود في $t_1, t_2, \dots, t_{n-1}$.

وباستخدام علاقات بين t_s و a_s نجد أنه بالإمكان التعبير عن $A_p, A_{p-1}, \dots, A_0$ ككثيرات حدود في $x_1, a_1, a_2, \dots, a_{n-1}$ (باستبدال $t_1, t_2, \dots, t_{n-1}$ بقيمها بدلالة $x_1, a_1, a_2, \dots, a_{n-1}$) .

إذاً
$$f(x_1, x_2, \dots, x_n) = B_m x_1^m + B_{m-1} x_1^{m-1} + \dots + B_0 = g(x_1)$$
حيث $B_m, B_{m-1}, \dots, B_0 \in F[a_1, a_2, \dots, a_{n-1}]$.

عندئذ $g(z) = B_m z^m + B_{m-1} z^{m-1} + \dots + B_0$. لتكن :
$$h(x) = z^n - a_1 z_1^{n-1} + a_2 z^{n-2} + \dots + (-1)^n a_n$$
باستخدام خوارزمية القسمة في $F[a_1, a_2, \dots, a_n][z]$ فإن :
$$g(z) = h(z)q(z) + C_{n-1} z^{n-1} + C_{n-2} z^{n-2} + \dots + C_0$$
حيث $C_{n-1}, C_{n-2}, \dots, C_0 \in F[a_1, a_2, \dots, a_n]$ ، وبما أن $h(x_1) = 0$ ، يكون $g(x_1) = C_{n-1} x_1^{n-1} + C_{n-2} x_1^{n-2} + \dots + C_0$ ، أي أن :
$$f(x_1, x_2, \dots, x_n) = C_{n-1} x_1^{n-1} + C_{n-2} x_1^{n-2} + \dots + C_0 \qquad (1)$$
بما أن $f(x_1, x_2, \dots, x_n)$ هي كثيرة حدود متماثلة في $x_1, x_2, \dots, x_n$ ، فتبديل x_1 مع x_2 نحصل على أن :
$$f(x_1, x_2, \dots, x_n) = C_{n-1} x_2^{n-1} + C_{n-2} x_2^{n-2} + \dots + C_0 \qquad (2)$$
بالمثل بتبديل x_1 بـ $x_3, x_4, \dots, x_n$ على الترتيب نحصل على :
$$f(x_1, x_2, \dots, x_n) = C_{n-1} x_3^{n-1} + C_{n-2} x_3^{n-2} + \dots + C_0 \qquad (3)$$
$$\dots \qquad \dots \qquad \dots \qquad \dots$$
$$f(x_1, x_2, \dots, x_n) = C_{n-1} x_n^{n-1} + C_{n-2} x_n^{n-2} + \dots + C_0 \qquad (4)$$
المعادلات من (1) إلى (n) تشير إلى أن $x_1, x_2, \dots, x_n$ هي جذور لكثيرة الحدود .
$$C_{n-1} u^{n-1} + C_{n-2} u^{n-2} + \dots + C_0 - f(x_1, x_2, \dots, x_n) \in F(a_1, a_2, \dots, a_n)[u]$$
وهذا غير معقول على ضوء نظرية 13-28 إلا إذا كان :
$$C_{n-1} = C_{n-2} = \dots = C_1 = C_0 - f(x_1, x_2, \dots, x_n) = 0$$
$$\Rightarrow f(x_1, x_2, \dots, x_n) = C_0 \in F[a_1, a_2, \dots, a_n]$$
بالتالي فإن $f(x_1, x_2, \dots, x_n)$ هي كثيرة حدود من الدوال المتماثلة الأولية $a_1, a_2, \dots, a_n$.

مسائل

-1 برهن أن الدوال المتماثلة الأولية في $x_1, x_2, \dots, x_n$ هي في الواقع دوال متماثلة في $x_1, x_2, \dots, x_n$.

-2 برهن متطابقات نيوتن ، أي إذا كانت $\alpha_1, \alpha_2, \dots, \alpha_n$ جذور كثيرة الحدود $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n$ وكان $s_k = \alpha_1^k + \alpha_2^k + \dots + \alpha_n^k$ ، فإن:

(a) $s_k + a_1s_{k-1} + a_2s_{k-2} + \dots + a_{k-1}s_1 + ka_k = 0$ لكل $k = 1, 2, \dots, n$.

(b) $s_k + a_1s_{k-1} + \dots + a_ns_{k-n} = 0$ لكل $k \geq n$.

-3 عبر عما يلي ككثيرات حدود من دوال متماثلة أولية في x_1, x_2, x_3 :

(a) $x_1^2 + x_2^2 + x_3^2$.

(b) $x_1^3 + x_2^3 + x_3^3$.

(c) $(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$.

[الجواب (a) $a_1^2 - 2a_2$. (b) $a_1^3 - 3a_1a_2 + 3a_2$.

(c) $-(4q^3 + 27r^2)$ حيث $r = -a_3 + \frac{a_1a_2}{3} - \frac{2a_1^3}{27}$ و $q = a_2 - \frac{a_1^2}{3}$] .

-4 ليكن K توسيعاً جذرياً عادياً لحقل F بمميز صفر . برهن ما يلي :

(i) توجد عناصر $a_1, a_2, \dots, a_n \in K$ وأعداد صحيحة موجبة $s_1, s_2, \dots, s_n$ بحيث $K = F(a_1, a_2, \dots, a_n)$ ولأي i ، $a_i^{s_i} \in F(a_1, a_2, \dots, a_{i-1})$ عندما $i = 2, 3, \dots, n$ و $a_1^{s_1} \in F$.

(ii) إذا كان $s = s_1s_2, \dots s_n$ وكان N حقل انفلاق $x^s - 1$ على K ، برهن أن N أيضاً هو توسيع عادي منته الدرجة للحقل F .

(iii) N يحوي جذراً . بدائياً (sth) للمحايد وليكن ζ .

(iv) إذا كان $L = F(\zeta)$ ، فإن L هو حقل انفلاق $x^3 - 1$ على F .

(v) $G(L, F)$ أبيلية .

(vi) عرف $L_0 = L$ ، $L_i = L(a_1, a_2, \ldots, a_i)$ لكل $i = 1, 2, \ldots, n$ برهن أن L_i توسيع عادي للحقل $L_i - 1$ بحيث $G(L_i, L_{i-1})$ أبيلية . استنتج أن $G(N, L)$ زمرة قابلة للحل .

(vii) $G(N, F)$ زمرة قابلة للحل .

(viii) $G(K, F)$ زمرة قابلة للحل .

[**إرشاد** (i) ينتج من التعريف . (ii) N هو حقل انفلاق لكثيرة الحدود $(x^s - 1)\, g(x)$ ، حيث $g(x)$ وهي كثيرة حدود بحيث K هو حقل انفلاق $g(x)$ على F . (v) ينتج من نظرية 14-20 . (vi) ينتج من القضية 14-21 . (vii) ينتج من (v) و (vi) (viii) ينتج من حقيقة أن $G(K, F) \cong \dfrac{G(N, F)}{G(N, K)}$] .

5- باستخدام سؤال 4 ، برهن أن أية كثيرة حدود $f(x)$ على حقل بمميز صفر قابلة للحل أو فقط إذا كانت زمرة جالوا كثيرة الحدود $f(x)$ على F قابلة للحل . (هذا يعمم نظرية 14-26) .

6- برهن أن $x^5 - 4x + 2$ غير قابلة للحل بواسطة جذور على Q .

4- إنشاءات بالمسطرة والفرجار

هناك العديد من المسائل في الهندسة الإقليدية حيرت الرياضيين منذ القدم ، ولكنها حلت أخيراً بواسطة تطبيقات في نظرية الحقول . في هذا البند سوف نطبق نظرية الحقول التي طورت سابقاً في الهندسة . وأخيراً سوف نحل المسائل القديمة التالية :

1- لإنشاء مربع له نفس مساحة دائرة معطاة بمسطرة وفرجار .

2- لإنشاء مكعب حجمه ضعف حجم مكعب معطى بمسطرة وفرجار .

3- لتقسيم زاوية معطاة إلى ثلاثة أجزاء متساوية بمسطرة وفرجار .

قبل دراسة هذه المسائل ، دعنا نفهم ما نعنيه بالإنشاء بمسطرة وفرجار . للتسهيل نقصد بالخط ، الخط المستقيم دائماً . في الهندسة الإقليدية ، تستخدم المسطرة فقط لرسم خط (مستقيم) يمر بنقطتين معينتين ، والفرجار مع المسطرة يستخدم لرسم دائرة مركزها نقطة معينة ونصف قطر يساوي البعد بين نقطتين معلومتين .

لتكن S مجموعة نقاط في المستوى تحوي عنصرين على الأقل . يقال لخط ما أنه قابل للإنشاء أو ممكن الإنشاء من S إذا كان يمر بنقطتين مختلفتين في S . يقال لدائرة بأنها قابلة للإنشاء من S إذا كان مركزها نقطة في S ونصف قطرها يساوي المسافة بين نقطتين في S . أية نقطة في المستوى هي تقاطع إما خطين مختلفين كلاهما قابل للإنشاء من S أو دائرتين مختلفتين كلاهما قابلة للإنشاء من S يقال عنها أنها قابلة للإنشاء بالمسطرة والفرجار أو ببساطة قابلة للإنشاء .

لتكن $s(S)$ مجموعة جميع النقاط القابلة للإنشاء من S . اعتبر أية نقطة P في S . بما أن S تحتوي على عنصرين على الأقل ، توجد نقطة Q في S ، تختلف عن P عندئذ الدائرة التي مركزها عند Q ونصف قطرها PQ والخط المار بالنقطتين P و Q كلاهما قابل للإنشاء من S ، إضافة إلى ذلك فإن P واحدة من نقطتين

تقاطعهما . بالتالي فإن P قابلة للإنشاء بمسطرة وفرجار ببساطة هي قابلة للإنشاء من S والذي يؤدي إلى أن $P \in s(S)$. إذاً $S \subseteq s(S)$.

إذا ثبتنا نظام إحداثي في المستوى ، فإننا نعلم أن أية نقطة في المستوى لها إحداثيان وحيدان وأنه يوجد تقابل أحادي بين النقاط والأزواج المرتبة (a, b) (إحداثيات النقاط) من الأعـــداد الحقيقيـــة ، ســـوف لا نميـــز بـــين نقطـــة في المســـتوى وإحداثييها . بالتالي لا نميز بين المستوى و $I\!R \times I\!R$ ، حيث $I\!R$ هي مجموعة الأعداد الحقيقية . النظام الإحداثي المأخوذ هنا نظام إحداثي متعامد بأخذ $X'OX$ كمحور سيني و $Y'OY$ كمحور صادي . اعتبر E المجموعة التي تحوي النقطتين $O(0, 0)$ و $I(1, 0)$ فقط هنا O تسمى نقة الأصل و I يسمى نقطة الوحدة . لتكن $E_1 = s(E)$. بأخذ $S = E$ في الفقرة السابقة يكون $E \subseteq E_1$. ضع $E_0 = E$.

والآن لاحظ ما يلي :

(i) بما أن $X'OX$ هو الخط المار بالنقطتين O و I المنتميتان إلى E ، فإن $X'OX$ قابل للإنشاء من E .

(ii) بما أن $OI = 1$ ، الدائرة التي مركزها عند O ونصف قطرها 1 قابلة للإنشاء من E (هذه الدائرة تسمى دائرة الوحدة) . دائرة الوحدة تلاقي $X'OX$ عند $I'(-1, 0)$ أيضاً . عليه فإن I قابلة للإنشاء أيضاً و $I' \in E_1$.

(iii) بما أن الدائرة التي مركزها I ونصف قطرها 1 قابلة للإنشاء من E وتقطع المحور X عند $A(2, 0)$ أيضاً ، فإن A قابلة للإنشاء من E . بالتالي $A \in E_1$.

نترك للقارئ إيجاد نقاط إضافية قابلة للإنشاء من E . حسب مبدأ الاستنتاج الرياضي لكل $n \geq 0$ ، نعرف $E_{n+1} = s(E_n)$. ضع $H = \bigcup_n E_n$. يقال لنقطة في المستوى أنها قابلة للإنشاء بمسطرة وفرجار (ببساطة قابلة للإنشاء) إذا وفقط إذا كانت تنتمي إلى H . لاحظ هنا أن $E_n \subseteq E_{n+1}$.

قضية 14-29

$s(H) = H$ ، أي أن كل نقطة قابلة للإنشاء من H تنتمي إلى H (أي أن كل نقطة قابلة للإنشاء من H هي قابلة للإنشاء) .

البرهان

اعتبر الخط l القابل للإنشاء من H . فإنه توجد نقطتين مختلفتين P و Q في H بحيث الخط المار بالنقطتين P و Q هو l . بما أن $H = \bigcup_n E_n$ ، $P \in E_n$ ، $Q \in E_m$ لبعض n ، m . إما $n \leq m$ أو $m \leq n$. وأكثر تحديداً ، افرض أن $n \leq m$ فإن $E_n \subseteq E_m$ و $P, Q \in E_m$. بالتالي فإن الخط l قابل للإنشاء من E_m .

اعتبر دائرة C قابلة للإنشاء من H . توجد ثلاثة نقاط A ، B و D بحيث A هي مركز C و BD نصف قطر الدائرة C . مرة ثانية لبعض أعداد صحيحة موجبة r, s, t فإن $A \in E_r$ ، $B \in E_s$ و $D \in E_t$. واحد من الأعداد r, s, t وليكن r هو الأكبر . عندئذ A, B, D جميعها تقع في E_r . وبالتالي الدائرة C قابلة للإنشاء من E_r . عليه أي خط أو دائرة قابلة للإنشاء من H فهي قابلة للإنشاء من بعض E_n .

لتكن P نقطة قابلة للإنشاء من H . من التعريف فإن P هي من نقاط تقاطع G_1 و G_2 ، حيث كل G_i هو إما خط أو دائرة قابلة للإنشاء من H . استناداً لما عرض في الفقرة السابقة فإن G_1 قابلة للإنشاء من E_n و G_2 قابلة للإنشاء من E_m لبعض n و m ، بما أنه إما $E_n \subseteq E_m$ أو $E_m \subseteq E_n$ بإمكاننا ولزيادة التحديد نفرض أن $E_n \subseteq E_m$. فإن G_1 و G_2 كلاهما قابلة للإنشاء من E_m . هذا يبين أن P قابلة للإنشاء من E_m بالتالي فإن $P \in S(E_m) = E_{m+1} \subseteq H$. إذاً $s(H) \subseteq H$. من ناحية أخرى $H \subseteq s(H)$ ومنها نحصل على أن $H = s(H)$. □

يقال لخط ما أو دائرة أنها قابلة لإنشاء إذا كان قابلاً للإنشاء من H . والآن دعنا نذكر الملاحظات التالية :

1- إذا كانت نقطة P قابلة للإنشاء تقع على خط l قابل للإنشاء فإن الخط المار من P والعمود على l يكون قابلاً للإنشاء أيضاً (سؤال 1) .

2- إذا كانت P نقطة قابلة للإنشاء ولا تقع على الخط l القابل للإنشاء ، فإن الخط المار من P موازي إلى l والخط المار من P وعمود على l كلاهما قابل للإنشاء (السؤالين 2 و 3) . لتوضيح هذا ، لاحظ أن النقطتين $I(1, 0)$ و $I'(-1, 0)$ هما نقطتان قابلتان للإنشاء .

ومن ثم فإن الدائرتين اللتين مركزيهما I', I ولهما نفس نصف القطر II' كلتاهما قابلة للإنشاء . بالتالي الخط المار بنقطتي تقاطعهما قابل للإنشاء . هذا الخط ليس سوى المحور Y . عليه فإن المحور y قابل للإنشاء . المحور y هو الخط المار بالنقطة القابلة للإنشاء O ، عمود على الخط القابل للإنشاء $X'OX$. رأينا سابقاً أن النقطة $A(20)$ قابلة للإنشاء والخط المار بنقطتي تقاطع دائرتين مركزاهما A, O ولهما نصف قطر 2 هو قابل للإنشاء وهذا الخط يوازي الخط القابل للإنشاء $Y'OY$ ويمر بالنقطة القابلة للإنشاء I .

يقال للعدد الحقيقي α أنه قابل للإنشاء إذا وفقط إذا كانت النقط $(\alpha, 0)$ قابلة للإنشاء . لتكن T مجموعة جميع الأعداد الحقيقية القابلة للإنشاء . بما أن $O(0, 0)$ و $I(1, 0)$ كلاهما قابل للإنشاء نجد أن $0, 1 \in T$. إضافة إلى ذلك يمكن أن نجد بسهولة أنه إذا كان عددان حقيقيان α و β قابلين للإنشاء فإن كلاً من $\alpha - \beta$ ، $a\beta^{-1}$ (إذا كان $\beta \neq 0$) قابلة للإنشاء (المسائل 5 ، 7 و 9) . عليه فإن T حقل جزئي من $I\!R$ ، حقل الأعداد الحقيقية . إضافة إلى ذلك إذا كان أي عدد حقيقي غير سالب α قابل للإنشاء فإن $\pm\sqrt{\alpha}$ قابل للإنشاء أيضاً (سؤال 11) . ولأننا لا نريد أن نرسم أي شكل

فإننا ننصح القراء بتصور أو تخيل إنشاء الأعداد الحقيقية المختلفة والقابلة للإنشاء ، برسم الأشكال بأنفسهم .

قضية 14-30

لأي عدد حقيقي α ، النقطة $(\alpha, 0)$ قابلة للإنشاء إذا وفقط إذا كانت $(0, \alpha)$ قابلة للإنشاء .

البرهان

افرض أن النقطة $(\alpha, 0)$ قابلة للإنشاء . بما أن نقطة الأصل O قابلة للإنشاء ، فإن الدائرة التي مركزها عند نقطة الأصل والتي تمر بالنقطة $(\alpha, 0)$ قابلة للإنشاء . هذه الدائرة تقطع المحور y عند النقطة $(0, \alpha)$. بما أن المحور y قابل للإنشاء ، فإن النقطة $(0, \alpha)$ قابلة للإنشاء .

بالعكس إذا كانت $(0, \alpha)$ قابلة للإنشاء ، فإن الدائرة التي مركزها O تمر بالنقطة $(0, \alpha)$ تقطع المحور x عند $(\alpha, 0)$. ومنها تتبع القضية . □

قضية 14-31

النقطة (α, β) قابلة للإنشاء إذا وفقط إذا كان العددان الحقيقيان α و β قابلتين للإنشاء .

البرهان

افرض أن العددين الحقيقيين α, β قابلين للإنشاء ، من تعريف العدد القابل للإنشاء والقضية 14-30 يستنتج أن النقطتين $A(\alpha, 0)$ و $B(0, \beta)$ قابلتين للإنشاء . بالتالي الخط المار من B موازياً للمحور x والخط المار من A موازياً للمحور y كلاهما قابل للإنشاء (سؤال 2) . هذان الخطان يتقاطعان عند (α, β) . بالتالي (α, β) قابلة للإنشاء .

بالعكس افرض أن النقطة $P(\alpha, \beta)$ قابلة للإنشاء . فإن الخط المار من P موازياً للمحور y يلاقي المحور x عند $(\alpha, 0)$. عليه فإن النقطة $(\alpha, 0)$ وبالتالي العدد الحقيقي α قابلان للإنشاء . مرة ثانية الخط المار من P موازياً للمحور x يلاقي المحور y عند $(0, \beta)$. عليه فإن النقطة $(0, \beta)$ قابلة للإنشاء . حسب قضية 14-30 النقطة $(\beta, 0)$ قابلة للإنشاء . إذاً حسب التعريف فإن β قابلة للإنشاء . □

يقال للعدد المركب $z = \alpha + is$ حيث α و β أعداد حقيقية و $i = \sqrt{-1}$ أنه قابل للإنشاء عندما تكون النقطة (α, β) قابلة للإنشاء . الآن نبرهن ما يلي .

نظرية 14-32

المجموعة L لجميع الأعداد المركبة القابلة للإنشاء عبارة عن حقل جزئي من C حقل الأعداد المركبة . كل جذر في C لكثيرة حدود تربيعية بمعاملات أعداد مركبة قابلة للإنشاء هو عدد مركب قابل للإنشاء (أي أن جذور أي تربيعي على L ينتمي إلى L) .

البرهان

لتكن T مجموعة جميع الأعداد الحقيقية القابلة للإنشاء. كما لوحظ سابقاً فإن T عبارة عن حقل جزئي لحقل الأعداد الحقيقية . ليكن $w = \alpha + ib$ عدداً مركباً . حسب التعريف w قابل للإنشاء إذا وفقط إذا كانت النقطة (α, β) قابلة للإنشاء . ولكن حسب القضية 14-31 النقطة (α, β) قابلة للإنشاء إذا وفقط إذا كان α, β قابلان للإنشاء بالتالي فإن w قابل للإنشاء إذا وفقط إذا كان $w \in T + T_i = T(i)$. عليه فإن $L = T(i)$ حقل جزئي من حقل الأعداد المركبة .

افرض أن العدد المركب t هو جذر لكثيرة حدود تربيعية ما $z^2 + az + b$ على L (دون أن نفقد العمومية نستطيع اختيار كثيرة الحدود التربيعية بحيث تكون واحدية) . عندئذ

$$t^2 + at + b = 0 \Rightarrow t = -\frac{a}{2} \pm \frac{1}{2}\sqrt{a^2 - 4b}$$

بما أن $\frac{-a}{2} \in L$ ، فإن $t \in L$ إذا وفقط إذا كان $\sqrt{a^2 - 4b} \in L$ وهكذا إذا برهنا أنه كل $w \in L$ يكون $\sqrt{w} \in L$ فمنها يتبع أن جذور أي كثيرة حدود تربيعية على L تنتمي إلى L . عليه اعتبر $w = \alpha + i\beta$ حيث $\alpha, \beta \in T$ وليكن :

$$z^2 = w = \alpha + i\beta \qquad (1)$$

الحالة I $\beta = 0$ إذا كان $\alpha \geq 0$ ، فإن $z = \pm\sqrt{\alpha}$ عدد حقيقي . بما أن الجذر التربيعي لعدد غير سالب في T قابل للإنشاء ، يكون لدينا $z \in T \subseteq L$. إذا كان $\alpha < 0$ فإن $-\alpha > 0$ و $-\alpha \in T$ أيضاً يعطي أن $\pm\sqrt{-\alpha} \in T$. من جهة أخرى $z = \pm i\sqrt{\alpha}$ ، هذا أيضاً يؤدي إلى $z \in T(i) = L$.

الحالة II $\beta \neq 0$ ليكن $z = x + iy$ ، x ، y أعداد حقيقية عندئذ (1) يؤدي إلى :

$$x^2 - y^2 = \alpha \qquad (2)$$
$$2xy = \beta \qquad (3)$$

(3) يؤدي إلى أن $x \neq 0$ و $y = \frac{\beta}{2x}$.

عليه حسب (2)

$$x^2 - \frac{\beta^2}{4x^2} = \alpha \Rightarrow x^4 - \alpha x^2 - \frac{\beta^2}{4} = 0$$

$$\Rightarrow \left(x^2 - \frac{\alpha}{2}\right)^2 = \frac{1}{4}(\alpha^2 + \beta^2) \qquad (4)$$

بما أن $\frac{1}{4}(\alpha^2 + \beta^2) > 0$ وينتمي إلى T ، لدينا $\sqrt{\frac{1}{4}(\alpha^2 + \beta^2)} \in T$ عليه وحسب (4) فإن

$$x^2 - \frac{\alpha}{2} = \pm\sqrt{\frac{1}{4}(\alpha^2 + \beta^2)} \in T$$

وحيث أن $\frac{\alpha}{2}$ قابل للإنشاء فهذا يؤدي إلى أن x^2 قابل للإنشاء . عندئذ الحالة (I) تؤدي إلى أن x قابل للإنشاء . هذا بدوره يؤدي إلى أن $x \in T$ وعليه $y = \frac{\beta}{2x} \in T$. ومن ثم $z = x + iy \in T(i) = L$. □

قضية 14-33

ليكن F حقل جزئي من حقل الأعداد الحقيقية ، أعطينا G_1 و G_2 $(G_2 \neq G_1)$ حيث كل من G_i إما خط أو دائرة جميع معاملات معادلتيها تقع في F وإذا كانت (x, y) نقطة من نقاط تقاطعها عندئذ إما كل من x و y يقع في F أو في توسيع تربيعي للحقل F .

البرهان

الحالة I إذا كان كل من G_1, G_2 خطاً . لتكن معادلتيهما :

$$ax + by + c = 0 \qquad (1)$$

و :

$$a'x + b'y + c' = 0 \qquad (2)$$

مع كون المعاملات في F ، هذان الخطان يمكن أن يتقاطعا فقط عندما لا يكونان متوازيان.

عندئذ نقطة تقاطعهما هي (x_1, y_1) حيث :

$$x_1 = \frac{bc' - b'c}{ab' - a'b}, y_1 = \frac{a'c - ac'}{ab' - a'b}$$

ومن الواضح أن $x_1, y_1 \in F$.

الحالة II واحد من G_1, G_2 هو خط والآخر دائرة . للتحديد أكثر افرض أن G_1 خط و G_2 دائرة . لتكن معادلتهما على الترتيب هما :

$$ax + by + c = 0 \qquad (3)$$

$$x^2 + y^2 + ex + fy + g = 0 \qquad (4)$$

مع كون المعاملات في F . في (3) على الأقل واحدة من a و b وليكن a يختلف عن الصفر . بحذف x من بين (3) و (4) نحصل على :

$$y^2\left(\frac{b^2}{a^2}+1\right)+y\left(\frac{2bc}{a^2}-\frac{be}{a}+f\right)-\frac{ec}{a}+\frac{c^2}{a^2}+g = 0$$

أي أن :

$$\alpha y^2+\beta y+\gamma = 0 \qquad (5)$$

حيث $\alpha = 1+\frac{b^2}{a^2}$ ، $\beta = \frac{2bc}{a^2}-\frac{eb}{a}+f$ ، $\gamma = \frac{c^2}{a^2}+g-\frac{ec}{a}$

(5) يؤدي إلى

$$y = \frac{-\beta}{2\alpha}\pm\frac{1}{2\alpha}\sqrt{\beta^2-4\alpha\gamma}$$

عليه نضع $d = \sqrt{\beta^2-4\alpha\gamma}$ ، لدينا $d^2 \in F$. هكذا فإن $[F(d) : F] \le 2$. من الواضح $y_1, y_2 \in F(d)$ حيث (x_1, y_1) و (x_2, y_2) هما إحداثيي نقطتي تقاطع G_1 و G_2 . (3) يؤدي إلى أن $x_1 = -\frac{c}{a}-\frac{b}{a}y_1$ و $x_2 = -\frac{c}{a}-\frac{b}{a}y$ ينتميان إلى $F(d)$.

الحالة III G_1 و G_2 كلاهما دائرة . افرض أن معادلتيهما على الترتيب هي :

$$x^2+y^2+ex+fy+g = 0 \qquad (6)$$

و :

$$x^2+y^2+e'x+f'y+g' = 0 \qquad (7)$$

مع كون المعاملات e, f, g, e', f', g' في F معادلة الخط المار بنقطتي تقاطعهما هي :

$$(e-e')x+(f-f')y+g-g' = 0 \qquad (8)$$

نقاط التقاطع لـ (6) و (7) هي نفس نقاط تقاطع G_1 مع الخط المعطى في 8 . عليه فإن الحالية (3) تتحول إلى الحالة II ، والقضية تتبع . □

نظرية 14-34

العدد المركب u يمكن إنشاؤه إذا وفقط إذا وجدت متتابعة $(F_j)_{0\le j\le n}$ لحقول جزئية من C ، بحيث :

$$Q = F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_n \qquad (1)$$
$$[F_j : F_{j-1}] \leq 2 \quad \forall j \quad 1 \leq j \leq n \qquad (2)$$
$$u \in F_n \qquad (3)$$

البرهان

لاحظ أن متتابعة ما (F_j) تحقق (1) ، (2) ، (3) تسمى متتابعة مقبولة للعنصر u . وأن (2) يؤدي إلى أن $F_j = F_{j-1}(c_j)$ لبعض $c_j \in F_j$.

الضرورة

نبرهن أولاً أنه إذا كان لعددين مركبين u و v متتابعتان مقبولتان فإن لهما متتابعة مقبولة مشتركة . افرض أن متتابعتيهما المقبولتين هما على التوالي $(F_i)_{0\leq i\leq n}$ و $(K_j)_{0\leq j\leq m}$. بما أن $[K_j : K_{j-1}] \leq 2$ فإن $K_j = K_{j-1}(\alpha_j)$ لبعض $\alpha_j \in K_j$ هذا يعطينا

$$K_1 = K_0(\alpha_1) = Q(\alpha_1)$$
$$K_2 = K_1(\alpha_2) = Q(\alpha_1, \alpha_2)$$
$$\vdots$$
$$K_j = Q(\alpha_1, \alpha_2, \dots, \alpha_j)$$

عندما $1 \leq j \leq m$. عرف المتتابعة $(L_k)_{0\leq k\leq m+1}$ على النحو الآتي :

$L_i = F_i$ عندما $0 \leq i \leq n$ و $L_{n+t} = F_n(\alpha_1, \alpha_2, \dots \alpha_t)$ عندما $1 \leq t \leq m$

هذا يؤدي إلى أن $L_{n+t} = L_{n+t-1}(\alpha t)$ عندما $0 \leq t \leq m$.

الآن $[L_i : L_{i-1}] = [F_i : F_{i-2}] \leq 2$ عندما $1 \leq i \leq n$. بما أن $K_{t-1} \subseteq L_{n+t-1}$ ودرجة α_t على K_{t-1} لا تتجاوز 2 ، فإن درجة α_t على L_{n+t-1} لا تتجاوز 2 . بالتالي $[L_{n+t} : L_{n+t-1}] \leq 2$. إضافة إلى ذلك $K_m \subseteq L_{n+m}$ يعطي $v \in L_{n+m}$. وهكذا فإن $(L_k)_{0\leq k\leq m+n}$ هي متتابعة مقبولة لكل من u و v .

من مبدأ الاستنتاج ينتج أنه إذا أعطينا عدداً منتهياً من الأعداد المركبة ولكل منها متتابعة مقبولة من حقول جزئية فإن لهذه الأعداد متتابعة مقبولة مشتركة لحقول جزئية . لكل عدد صحيح غير سالب n ، ضع D_n رمزاً لمجموعة جميع الأعداد الحقيقية x بحيث إما (x, y) أو (y, x) ينتمي إلى E_n لعدد حقيقي y . كذلك ضع $S = \{n \mid$ توجد متتابعة مقبولة لحقول جزئية في D_n ولكل عنصر عدد طبيعي ، $b\}$. بما أن $E_0 = \{(0, 0), (1, 0)\}$ ، فإن $D_0 = \{0, 1\}$. وحيث أن $0, 1 \in Q$ ، فلهما متتابعات مقبولة تافهة .

وعليه فإن $0 \in S$. افرض أن $n \in S$. اعتبر أي $x \in D_{n+1}$. من التعريف $(x, y) \in E_{n+1}$ أو $(y, x) \in E_{n+1}$ لعدد حقيقي y . ليكن $(x, y) \in E_{n+1}$. الآن (x, y) هي نقطة تقاطع G_1 و G_2 حيث كل من G_i إما خط أو دائرة قابلة للإنشاء من E_n . بما أن الخط القابل للإنشاء من E_n يتعين بنقطتين من E_n وكل دائرة قابلة للإنشاء من E_n تتحدد بثلاثة نقاط (المركز ، ونقطتان حيث المسافة بينهما تمثل نصف القطر) ، G_1 و G_2 كلاهما يتعينان بعدد منته من نقاط E_n . إذا كانت F مجموعة إحداثيات هذه النقاط المنتهية ، فمن الواضح أن F هي مجموعة جزئية منتهية من D_n . حسب فروض الاستنتاج كل عنصر في F له متتابعة مقبولة من حقول جزئية . بالتالي هذه الأعداد الحقيقية لها متتابعة مقبولة مشتركة ولتكن $(K_j)\ 0 \le j \le m$ ، بما أن جميع عناصر F تنتمي إلى K_m فإن معادلتي G_1 و G_2 هما على الحقل K_m . من قضية 14-33 كل من y, x يقع في حقل توسيع L للحقل K_m درجته على K_m لا تتجاوز 2 . لو وضعنا $K_{m+1} = L$ ، نرى أن $x, y \in K_{m+1}$ و $(K_j)_{0 \le j \le m+1}$ هي متتابعتهما المقبولة . نفس الشيء في حالة $(y, x) \in E_{n+1}$. إذاً لكل عنصر x في D_{n+1} متتابعة مقبولة لحقول جزئية . عليه فإن $n + 1 \in S$ ومن مبدأ الاستنتاج لكل $n \ge 0$ فإن لكل عنصر في D_n متتابعة مقبولة .

ليكن $u = x + iy$ عدداً مركباً قابلاً للإنشاء . فإن $(x, y) \in E_n$ لبعض n .
كما برهنا من قبل فإن لكل من x, y متتابعة مقبولة لحقول جزئية . عليه فإن لهما متتابعة مقبولة مشتركة ولتكن $(F_j)_{0 \le j \le q}$. نضع $F_{q+1} = F_q(i)$ ، فإن $\left[F_{q+1} : F_q\right] = 2$.

$$x, y \in F_q \subseteq F_q(i) \Rightarrow u = x + iy \in F_q(i) = F_{q+1}$$

إذاً $(F_j)_{0 \le j \le q+1}$ هي متتابعة مقبولة لحقول جزئية للعنصر u .

الكفاية افرض أن للعنصر $u = x + iy$ متتابعة مقبولة $(F_j)_{0 \le j \le q}$ لحقول جزئية . ليكن L حقل جميع الأعداد المركبة القابلة للإنشاء . نبرهن بالاستنتاج على j أن $F_j \subseteq L$. من الواضح أن $F_0 = Q \subseteq L$. افرض $F_j \subseteq L$ لبعض j . الآن $F_{j+1} = F_j(a_{j+1})$ لبعض $a_{j+1} \in F_{j+1}$. إذا كان $F_j = F_{j+1}$ فإنه من الواضح $F_{j+1} \subseteq L$ وإذا كان $F_j \neq F_{j+1}$ فإن a_{j+1} من الدرجة الثانية على F_j بالتالي على L . من ناحية أخرى كل جذر لكثيرة حدود تربيعية على L يقع في L . عليه $a_{j+1} \in L$ هذا يؤدي إلى أن $F_{j+1} \subseteq L$ ، بالتالي من الاستنتاج يكون $F_j \subseteq L$ لكل j . بالأخص $F_q \subseteq L$ فإن $u \in F_q$ يؤدي إلى أن $u \in L$ وعليه فإن u قابل للإنشاء . □

نتيجة 14-35

أي عدد مركب قابل للإنشاء هو جبري على Q ودرجته قوة للعدد 2 .

البرهان

ليكن u عدداً مركباً قابلاً للإنشاء . حسب النظرية السابقة فإن للعنصر u متتابعة مقبولة من حقول جزئية $Q = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_m$

هنا $u \in K_m$. الآن لكل j ، $1 \le j \le m$ ، $[K_j : K_{j-1}]$ يساوي إما 1 أو 2 .
من
$$[K_m : Q] = [K_m : K_{m-1}][K_{m-1} : K_{m-2}]\dots[K_1 : K_0]$$
نحصل على أن $[K_m : Q] = 2^r$ لبعض $r \le m$.

الآن $u \in K_m$ يؤدي إلى أن $Q(u) \subseteq K_m$. عليه فإن :
$$2^r = [K_m : Q] = [K_m : Q(u)][Q(u) : Q]$$
والذي يبين أن $[Q(u) : Q]$ هو قوة للعدد 2 . بالتالي فإن درجة u على Q هي قوة للعدد 2 . □

المثال الآتي يبين أنه إذا كان عدد مركب ما جبرياً على Q ودرجته قوة للعدد 2 فإنه ليس بالضرورة أن يكون قابلاً للإنشاء .

مثال 9

اعتبر كثيرة الحدود $f(x) = x^4 - 4x - 2$. حسب معيار أيرنستن $f(x)$ غير قابلة للتحليل على Q . وفقاً لطريقة فيراري فإن كثيرة حدودها التكعيبية هي $g(y) = y^3 - 2y - 2$.

إذا كان l جذراً لكثيرة الحدود $g(y)$ فإن :
$$x_1 = \frac{\sqrt{2l} + \sqrt{4\sqrt{l^2 - 2} - 2l}}{2} \,,\; x_2 = \frac{\sqrt{2l} - \sqrt{4\sqrt{l^2 - 2} - 2l}}{2}$$
هما جذران لكثيرة الحدود $f(x)$. الآن $g(y)$ غير قابلة للتحليل أيضاً ، عليه فإن درجة l على Q تساوي 3 . بالتالي l غير قابل للإنشاء (نتيجة 14-35) . إذا كان كل من x_1 ، x_2 قابلاً للإنشاء ، فإن $x_1 + x_2$ يكون قابلاً للإنشاء . هذا يؤدي إلى أن $\sqrt{2l}$ قابل للإنشاء والذي بدوره يؤدي إلى أن $l = \frac{1}{2}\left(\sqrt{2l}\right)^2$ قابل للإنشاء ، فهذا تناقض مما يعني أن واحداً على الأقل من x_1 ، x_2 غير قابل للإنشاء ، في حين درجة كل من x_1 و x_2 على Q هو $2^2 = 4$ قوة للعدد 2 .

يقال لقطعة مستقيم أنها قابلة للإنشاء إذا كانت نقطتين نهايتهما قابلة للإنشاء . يقال لخماسي أنه قابل للإنشاء إذا كان كل ضلع من أضلاعه قابلاً للإنشاء . يقال عن زاوية ما أنها قابلة للإنشاء إذا كان كلاً من رأسها وضلعيها قابلاً للإنشاء .

قضية 14-36

إذا كان قطعة مستقيم قابلة للإنشاء ، فإن طولها يكون عدداً قابلاً للإنشاء .

البرهان

اعتبر قطعة مستقيم قابلة للإنشاء نهايتيها $A(a_1, b_1)$ و $B(a_2, b_2)$ ، من التعريف A و B قابلتان للإنشاء ، بالتالي فإن a_1, a_2, b_1, b_2 هي أعداد قابلة للإنشاء . بما أن مجموعة جميع الأعداد الحقيقية القابلة للإنشاء تشكل حقلاً والجذر التربيعي لأي عدد حقيقي غير سالب قابل للإنشاء يكون قابلاً للإنشاء فإن $AB = \sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2}$ يكون قابلاً للإنشاء . عليه فإن القضية محققة . □

القضية السابقة تبين أن لقطعة مستقيم معطاة إذا كان بإمكاننا أن نبين أن طولها عدد غير قابل للإنشاء من ذلك يتبع أن قطعة المستقيم غير قابلة للإنشاء .

الآن نحن جاهزون لحل المسائل التي ذكرت في بداية البند .

قضية 14-37

كثيرة الحدود $8x^3 - 6x - 1$ غير قابلة للتحليل على حقل الأعداد النسبية .

البرهان

لتكن $f(x) = 8x^3 - 6x - 1$. يكفي أن نبرهن أن $f(x)$ غير قابلة للتحليل على Z (لماذا ؟) .

الآن :

$$f(x-1) = 8x^3 - 24x^2 + 18x - 3 \qquad (1)$$

كثيرة الحدود $f(x)$ غير قابلة للتحليل إذا وفقط إذا كانت $f(x-1)$ غير قابلة للتحليل .

الآن 3 عدد أولي لا يقسم المعامل القائد لكثيرة الحدود $f(x-1)$. ويقسم جميع المعاملات الأخرى ولكن $q = 3^2$ لا يقسم الحد الثابت . عليه وفق معيار آيزنستين فإن $f(x-1)$ غير قابلة للتحليل . بالتالي فهذا يثبت القضية . □

نظرية 14-38

بصورة عامة لا يمكن تثليث زاوية بمسطرة وفرجار .

البرهان

النتيجة تثبت إذا كان بإمكاننا أن نبين وجود زاوية قابلة للإنشاء ولا يمكن تثليثها .

النقطة $A\left(1, \sqrt{3}\right)$ قابلة للإنشاء (ارسم مخططاً) . $\frac{\pi}{3} = AOX >$ زاوية نصف قطرية . عليه فإن $AOX >$ قابلة للإنشاء . إذا كان بالإمكان تثليث هذه الزاوية بالمسطرة والفرجار يمكن رسم مستقيم ، OC بحيث $\frac{\pi}{q} = COX >$. لنفرض أن هذا الخط يلاقي دائرة الوحدة في D . عندئذ النقطة D وقطعة المستقيم DE العمود على OX (E على المحور x) قابلتان للإنشاء . بالتالي حسب قضية 14-36 $OE = \cos\frac{\pi}{9}$ قابل للإنشاء . ضع $x = \cos\frac{\pi}{9}$. بوضع $\theta = \frac{\pi}{9}$ في $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ نحصل على أن $4x^3 - 3x - \frac{1}{2} = 0$ أي أن $8x^3 - 6x - 1 = 0$.

وحسب قضية 14-37 فإن $8x^3-6x-1$ غير قابلة للتحليل على Q ، ونحصل على أن درجة x على Q يساوي 3 . ولكن 3 ليس قوة للعدد 2 . لذا فإن x غير قابل للإنشاء (نتيجة 14-35) ، هذا تناقض . إذاً نحصل على النتيجة . □

يجب التأكيد أن هناك زوايا مثل $\frac{\pi}{2}$ زاوية نصف قطرية يمكن تثليثها بواسطة مسطرة وفرجار .

المكعب الذي كل ضلع فيه وحدة واحدة يسمى مكعب وحده .

نظرية 14-39

لا يمكن إنشاء مكعب حجمه ضعف حجم مكعب الوحدة .

البرهان

حجم مكعب الوحدة يساوي 1 ، عليه إذا كان بالإمكان إنشاء مكعب حجمه ضعف حجم مكعب الوحدة بمسطرة وفرجار فإن حجمه يساوي 2 وعندئذ طول أي ضلع له يساوي $\sqrt[3]{2}$ ويكون قابلاً للإنشاء .

إذاً وحسب نتيجة 14-35 فإن درجة $\sqrt[3]{2}$ على Q هو قوة للعدد 2 . من ناحية ثانية كثيرة الحدود الأصغرية للعدد $\sqrt[3]{2}$ على Q هي x^3-2 ودرجتها ليست قوة للعدد 2 . هذا تناقض ، إذاً فإن النتيجة تتبع . □

نظرية 14-40

لا يمكن إنشاء مربع مساحته تساوي مساحة دائرة الوحدة بمسطرة وفرجار .

البرهان

مساحة دائرة الوحدة تساوي π . عليه إذا أمكن إنشاء مربع مساحته π ، فإن كل ضلع فيه $\sqrt{\pi}$. عليه فإن $\sqrt{\pi}$ عدد قابل للإنشاء ، وبالتالي $\left(\sqrt{\pi}\right)^2=\pi$ عدد قابل

للإنشـاء ويكـون π جـبري علـى Q (نتيجـة 14-35) . هـذا ينـاقض الحقيقـة أن π عـدد متسامي . إذاً حصلنا على النتيجة . $\square$

مسائل

ينصح الطلاب بإعطاء براهين تحليلية للمسائل من 1 إلى 11 .

1- إذا كانت P نقطة قابلة للإنشاء تقع على خط l قابل للإنشاء ، برهن أن الخط من P العمود على l قابل للإنشاء أيضاً .

[**إرشاد** توجد نقطة قابلة للإنشاء Q على l تختلف عن P . الدائرة التي مركزها P ونصف قطرها Pa تلاقي l عند نقطة أخرى ولتكن T . الدائرتان اللتان مركزهما عند Q ، T ولهما نصف القطر نفسه QT هما قابلتان للإنشاء ، خط تقاطعهما هو الخط المطلوب المار من P والعمود على l] .

2- إذا كانت P نقطة قابلة للإنشاء لا تقع على الخط القابل للإنشاء l ، فإن الخط من P العمود على l قابل للإنشاء .

[**إرشاد** اختر نقطة قابلة للإنشاء Q على l . الدائرة التي مركزها P نصف قطرها PQ يلاقي l بصورة عامة عند نقطتين ، إحداهما Q ولتكن الأخرى T . إذا كان T و Q متطابقتان فإن الخط المار بـ P و Q هو الخط المطلوب . إذا كانت T و Q مختلفتان ، فإن الدائرتان اللتان مركزاهما Q و T ولها نفس نصف القطر QT قابلتان للإنشاء . خط تقاطع هاتان الدائرتان هو الخط المطلوب] .

3- إذا كانت P نقطة قابلة للإنشاء لا تقع على الخط l القابل للإنشاء ، برهن أن الخط المار بـ P موازي إلى l قابل للإنشاء .

[**إرشاد** حسب سؤال 2 ، فإن الخط l' المار من P والعمود على l قابل للإنشاء . حسب سؤال 1 ، الخط m من P عمود على l' قابل للإنشاء فإن m هو الخط المطلوب] .

4- إذا كان α عدداً حقيقياً قابلاً للإنشاء ، برهن أن $\alpha -$ قابل للإنشاء .

[**إرشاد** النقطة $(\alpha, 0)$ قابلة للإنشاء . الدائرة التي مركزها نقطة الأصل والتي تمر بالنقطة $(\alpha, 0)$ قابلة للإنشاء . هذه الدائرة تلاقي المحور x عند $(-\alpha, 0)$] .

5- إذا كان عددان حقيقيان β, α قابلان للإنشاء ، برهن أن العددان الحقيقيان $\alpha \pm \beta$ قابلان للإنشاء .

[**إرشاد** الدائرة التي مركزها $A(\alpha, 0)$ ونصف قطرها OB حيث B هي $(\beta, 0)$ قابلة للإنشاء . هذه الدائرة تلاقي المحور x عند النقطتين $(\alpha + \beta, 0)$ و $(\alpha - \beta, 0)$] .

6- إذا كان α, β عددان موجبان قابلان للإنشاء ، برهن أن $\alpha\beta$ قابل للإنشاء .

[**إرشاد** الخط المار من $A(0, 1)$ و $B(\alpha, 0)$ قابل للإنشاء والخط المار من $E(0, \beta)$ يوازي AB قابل للإنشاء ويلاقي المحور x عند $(\alpha\beta, 0)$] .

7- استخدم سؤالي 4 و 6 للبرهنة على أن حاصل ضرب أي عددين حقيقيين قابلين للإنشاء يكون قابلاً للإنشاء .

8- إذا كان B عدداً موجباً قابلاً للإنشاء برهن أن $\frac{1}{B}$ قابل للإنشاء .

[**إرشاد** الخط المار بالنقطة $(1, 0)$ موازياً الخط الذي يربط $(\beta, 0)$ و $(0, 1)$ قابل للإنشاء وهو يلاقي المحور y عند $\left(0, \frac{1}{\beta}\right)$] .

9- باستخدام السؤالين 4 و 8 ، برهن أنه لأي عدد حقيقي قابل للإنشاء α يختلف عن الصفر فإن $\frac{1}{\alpha}$ قابل للإنشاء .

10- استنتج من المسائل 5 ، 7 و 9 أن مجموعة الأعداد الحقيقية القابلة للإنشاء تكون حقلاً تحت عمليتي الجمع والضرب للأعداد الحقيقية .

11- لأي عدد موجب قابل للإنشاء α ، برهن أن $\pm\sqrt{\alpha}$ قابلان للإنشاء .

[**إرشاد** الدائرة التي قطرها يربط النقطتين $(-\alpha, 0)$ و $(1, 0)$ قابلة للإنشاء وهي تقطع المحور y عند $(0, \sqrt{\alpha})$ و $(0,-\sqrt{\alpha})$ وعليه فإن $\pm\sqrt{\alpha}$ قابلان للإنشاء] .

12- برهن أن الزاوية التي قياسها α من الزوايا النصف قطرية قابلة للإنشاء إذا وفقط إذا كان العدد الحقيقي $\cos\alpha(\sin\alpha)$ قابل للإنشاء .

13- برهن أن زاوية α من الزوايا النصف قطرية قابلة للإنشاء إذا وفقط إذا كانت النقطة $(\cos\alpha, \sin\alpha)$ قابلة للإنشاء .

14- برهن أن A مجموعة جميع الأعداد الحقيقية α بحيث $\cos\alpha$ قابل للإنشاء تكون زمرة جزئية من زمرة الجمع للأعداد الحقيقية . وأن لكل $\alpha \in A$ يكون $\frac{\alpha}{2} \in A$.

15- *بين أن $\cos\frac{\pi}{5}$ قابل للإنشاء وأن $\frac{\pi}{5}$ زاوية قابلة للإنشاء .

16- *أعطيت عدداً صحيحاً موجباً n ، بين أن الزوايا التي قياسها n درجة قابلة للإنشاء إذا وفقط إذا كان n من مضاعفات 3 .

[**إرشاد** حسب سؤال 15 ، الزاوية التي قياسها 36 درجة قابلة للإنشاء . ومن سؤال 14 يتبع أن الزاوية التي قياسها 9 درجات قابلة للإنشاء ليكن t أصغر عدد صحيح موجب بحيث الزاوية التي قيمتها t درجة هي قابلة للإنشاء ، فإن $t \le 9$. اعتبر $9 - t$ استنتج أن $t = 3$] .

17- برهن أن المضلع النوني المنتظم (له n من الأضلاع) يكون قابلاً للإنشاء إذا وفقط إذا كانت الزاوية التي قياسها $\frac{\pi}{n}$ زاوية نصف قطرية قابلة للإنشاء .

18- باستخدام السؤالين 16 ، 17 استنتج أن المخمس المنتظم والمسدس المنتظم قابلان للإنشاء ، ولكن المضلع المنتظم ذو 9 أضلاع غير قابل للإنشاء .

19- برهن أن الزوايا التي قياسها 15 ، 6 ، 3 درجات لا يمكن تثليثها بمسطرة وفرجار .

20- برهن الآتي :

(i) $x^3 + x^2 - 2x - 1$ غير قابلة للتحليل على الأعداد النسبية .

(ii) $2\cos\dfrac{2\pi}{7}$ يحقق كثيرة الحدود في (i) .

(iii) $\dfrac{2\pi}{7}$ عدد غير قابل للإنشاء .

(iv) السباعي المنتظم غير قابل للإنشاء .

21- باستخدام حقيقة أنه لأي $n \geq 1$ ، كثيرة الحدود السيكوتومية $\phi_n(x)$ غير قابلة للتحليل على Q . برهن الآتي :

(i) كثيرة الحدود الأصغرية لجذر نوني بدائي للمحايد على Q هي $\phi_n(x)$.

(ii) باستخدام نظرية 14-34 استنتج أنه إذا كان جذر نوني بدائي للمحايد قابلاً للإنشاء فإن درجة $\phi_n(x)$ أي أن $\varphi(n)$ يساوي قوة للعدد 2 (حيث $\varphi(n)$ هي دالة أويلر (Totient) توتاينت) .

(iii) باستخدام حقيقة أن زمرة جالوا لجذر نوني بدائي u إبدالية وإن عكس نظرية لاجرانج تتحقق للزمر الأبيلية ، بين أنه إذا كان $\varphi(n)$ قوة لعدد n فإن u قابل للإنشاء .

(iv) بين أن المضلع المنتظم الذي n ضلعاً قابلاً للإنشاء إذا وفقط إذا كان جذر النوني البدائي للواحد قابل للإنشاء .

[**إرشاد** استخدم السؤالين 12 و 17 وتعريف عدد مركب قابل للإنشاء].

(v) (جاوس) المضلع المنتظم ذو n ضلعاً يكون قابلاً للإنشاء إذا وفقط إذا كان $\varphi(n)$ قوة للعدد 2 .

[**إرشاد** استخدم الأجزاء (ii) ، (iii) و (iv) السابقة] .

(vi) إذا كان P عدداً أولياً ، بين أن المضلع المنتظم ذو n ضلعاً يكون قابلاً للإنشاء إذا وفقط إذا كان P العدد الأولي لفيرمات ، أي أن $P = 2^{2^n} + 1$ لبعض $0 \le n$.

[**إرشاد** $\varphi(p) = P - 1$] .

15

حلقات تحقق شروط السلسلة

Rings with Chain Conditions

في القضية 10-27 أثبتنا أنه في ساحة مثاليات رئيسية (PID) كل سلسلة تصاعدية من المثاليات تتوقف بعد عدد منته من الحدود ، في هذا الفصل سنتعرض لدراسة بعض الخصائص للحلقات التي تحقق شروطاً مماثلة لمثاليات من جانب واحد ونعطي فكرة مختصرة عن الحلقات التي لا تستوعب سلسلة تنازلية لا نهائية تامة لمثاليات من جانب واحد .

1– الحلقات النويثيرية Noetherian Rings

تعريف 15-1

الحلقة التي فيها كل سلسلة تصاعدية تامة من مثاليات يمينية (يسارية) تكون منتهية تسمى حلقة نويثيرية يمينية (يسارية) .

بصورة مكافئة يمكننا أن نعرف حلقة نويثيرية يمينية (يسارية) بأنها تلك الحلقة التي فيها لكل سلسلة تصاعدية غير منتهية .

$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ من مثاليات يمينية (يسارية) يوجد عدد صحيح موجب n بحيث يكون $I_m = I_n$ لكل $m \geq n$.

ملاحظة حلقة نويثيرية يمينية (يسارية) معروفة أيضاً بأنها حلقة مع ACC (أي شرط السلسلة التصاعدية) على المثاليات اليمينية (اليسارية) .

تعريف 15-2

الحلقة التي يتحقق فيها شرط السلسلة التصاعدية للمثاليات اليمينية واليسارية معاً تسمى حلقة نويثيرية .

مثال 1

الحلقة Z هي حلقة نويثيرية لأنها ساحة مثاليات رئيسية (PID) وكل ساحة مثاليات رئيسية هي حلقة نويثيرية (قضية 10-27) .

مثال 2

من الواضح أن كل حلقة منتهية هي حلقة نويثيرية يمينية ويسارية .

مثال 3

اعتبر أية حلقة قاسمية D . بما أن المثاليات اليمينية للحلقة D هي فقط (0) و D نفسها . فإن D هي حلقة نويثيرية يمينية . لأسباب مماثلة فإن D حلقة نويثيرية يسارية أيضاً .

في نهاية الفصل سوف نعطي مثالاً لحلقة نويثيرية يمينية ليست يسارية .

تعريف 15-3

إذا كانت R حلقة بحيث كل مجموعة غير خالية من مثاليات يمينية (يسارية) فيها مرتبة جزئياً بعلاقة الاحتواء لها عنصر أعظم فإننا نقول أن شرط الأعظمية محقق للمثاليات اليمينية (اليسارية) للحلقة R .

لاحظ أننا بعنصر أعظمي من مجموعة غير خالية F مرتبة جزئياً بعلاقة $\leq$ نعني أن العنصر $A \in F$ حيث لا يوجد عنصر B في F يحقق $A < B$. بعبارة أخرى فإن A يكون عنصراً أعظمياً في F إذا وفقط إذا كان لكل $B \in F$ فإن :

$$A \leq B \Rightarrow A = B$$

ويمكن أن يكون لمجموعة ما أكثر من عنصر أعظمي واحد .

ملاحظة لأن نتائج الحلقات النويثيرية اليسارية في تشابه تام مع تلك التي للحلقات النويثيرية اليمينية فسوف نركز على الحلقات النويثيرية اليمينية فقط .

تعريف 4-15

يقال لمثالي يميني من حلقة R أنه منتهي التولد إذا كان مولداً بمجموعة جزئية منتهية من R .

اصطلاح إذا كانت المجموعة المولدة S تحتوي على n من العناصر $a_1, a_2, \ldots, a_n$ فإننا نكتب $I =< a_1, a_2, \ldots, a_n >_r$. يمكن التحقق من أن :

$$I =< a_1 >_r + < a_2 >_r + \ldots + < a_n >_r$$

نظرية 5-15

لأية حلقة R ، العبارات التالية متكافئة :

(1) R حلقة نويثيرية يمينية .

(2) شرط الأعظمية يتحقق للمثاليات اليمينية في R .

(3) كل مثالي يمني في R يكون منتهي التولد .

البرهان

$(2) \Leftarrow (1)$. لتكن F أية مجموعة غير خالية من مثاليات يمينية في R ولتكن I_1 مثالي يميني في F . إذا لم يكن I_1 عنصراً أعظم في F فبإمكاننا إيجاد مثالي يميني I_2 من R بحيث $I_2 \in F$ و $I_1 \subset I_2$. فإذا كانت F ليس بها عنصراً أعظم فإن العملية السابقة يمكن أن تستمر بصورة غير محددة ، وهكذا نحصل على سلسلة تصاعدية تامة غير منتهية $I_1 \subset I_2 \subset I_3 \subset \ldots$

من مثاليات يمينية في R . هذا يخالف حقيقة أن R حلقة نويثيرية يمينية . لذا فإن F لها عنصر أعظمي بالتالي $(2) \Rightarrow (1)$.

$(3) \Rightarrow (2)$. ليكن I مثالياً يمينياً في R ولتكن $F = \{ J \mid J \subseteq I$ مثالي يميني منته التولد $J \}$. من الواضح أن $(0) \in F$ أي أن F مجموعة غير خالية من مثاليات يمينية . حسب (2) فإن F تحوي عنصراً أعظم . افرض أن M عنصر أعظم في F . من الواضح أن M منته التولد . سوف نبرهن $I = M$. بما أن $M \in F$ ، $M \subseteq I$. فلو كان من الممكن فرض أن $I \neq M$ ، فإنه يوجد عنصر $a \in I$ ، $a \notin M$.

اعتبر المثالي اليميني $M + < a >_r$ فإن $M + < a >_r$ مثالي يميني منتهي التولد في R [هو مولد بالمجموعة $S \cup \{a\}$ حيث $M = < s >$] . بما أن $a \in I$ ، $M + < a >_r \subseteq I$. هذا يعطي أن $M + < a >_r \in F$. ولكن $a \notin M$ يؤدي إلى أن $M \subset M + < a >_r$. هذا يكسر أعظمية M . إذاً $I = M$. نتيجة لذلك فإن I منتهي التولد .

$(1) \Rightarrow (3)$. لتكن $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ سلسلة تصاعدية من مثاليات يمينية في R . اعتبر $I = \bigcup_i I_i$. المثالية I هي مثالية يمينية (قارن قضية 10-26) . الآن كل مثالي يميني هو منتهي التولد . لتكن $S = \{a_1, a_2, \ldots, a_n\}$ مجموعة مولدة للمثالي I أي أن $I = < a_1, a_2, \ldots, a_n >_r$. لكل $j \in \{1, 2, 3, \ldots, n\}$ ، $a_j \in I$ يؤدي إلى وجود عدد صحيح موجب i_j بحيث $a_j \in I_{ij}$. ليكن $k = \max\{i_1, i_2, \ldots, i_n\}$. فإن $a_j \in I_k$ لكل $j = 1, 2, 3, \ldots, n$. هذا يعطي أن $I \subseteq I_k$ ، ولكن $I_k \subseteq I$ بالتالي فإن $I = I_k$. الآن لكل $m \geq k$ ، $I_m \subseteq I = I_k$ يعطي أن $I_m = I_k$ ، عليه فإن R حلقة نويثيرية يمينية . □

تعريف 15-6

يقال للمثالي I من الحلقة R أنه نويثيري يميني إذا كانت كل سلسلة تصاعدية من مثاليات يمينية من R محتواة في I منتهية . حسب التعريف السابق ، فمن الواضح أن كل مثالي لحلقة نويثيرية يمينية هو نويثيري يميني .

قضية 15-7

الصورة الهومومورفية لحلقة نويثيرية يمينية تكون نويثيرية يمينية .

البرهان

لتكن S صورة هومومورفية لحلقة نويثيرية يمينية R . فإن $S \cong R / I$ لمثالي I من R . عليه يكفي أن نبرهن أن R / I نويثيرية يمينية .

لتكن $J_1 \subseteq J_2 \subseteq J_3 \subseteq \ldots$ سلسلة تصاعدية من مثاليات يمينية من R / I . الآن كل J_i هو بالصورة K_i / I حيث K_i مثالي يميني من R يحوي I . كذلك $J_i \subseteq J_{i+1}$ يؤدي إلى $K_i \subseteq K_{i+1}$ ، عليه فإن السلسلة التصاعدية أعلاه تعطينا السلسلة التصاعدية $K_1 \subseteq K_2 \subseteq K_3 \subseteq \ldots$ من مثاليات يمينية من R . ولكن لكون R نويثيرية يمينية فإنه يوجد عدد صحيح موجب n بحيث يكون $K_m = K_n$ لكل $m \geq n$ هذا يؤدي إلى أن $J_m = J_n$ لكل $m \geq n$. بالتالي فإن R / I نويثيرية . □

قضية 15-8 (قانون موديولر)

إذا كانت L, M, N مثاليات يمينية من الحلقة R بحيث كان $M \subseteq L$ ، فإن $L \cap (M + N) = M + (L \cap N)$.

البرهان

لأن كلاً من M و $L \cap N$ محتواة في L ، فإن $M + L \cap N \subseteq I$. إضافة إلى ذلك $L \cap N \subseteq N \Leftarrow M + L \cap N \subseteq M + N$. هذا يعطي أن

$M + (L \cap N) \subseteq L \cap (M + N)$. مرة أخرى ليكن $x \in L \cap (M + N)$ ، فإن $x \in L$ و $x = y + z$ لبعض $y \in M$ و $z \in N$ ، الآن $z = x - y \in L$ لأن $M \subseteq L$ وهذا يعطي أن $z \in L \cap N$. عليه فإن $x \in M + L \cap N$ وهكذا فإن $L \cap (M + N) \subseteq M + L \cap N$. بالتالي $L \cap (M + N) = M + (L \cap N)$. □

نظرية 9-15

ليكن I مثالي للحلقة R . فإن R نويثيرية يمينية إذا وفقط إذا كان كلاً من I و R / I نويثيرية يمينية .

البرهان

إذا كانت R نويثيرية يمينية ، فإنه حسب تعريف 6-15 يكون I نويثيري يميني وحسب قضية 7-15 فإن R / I نويثيرية يمينية أيضاً .

بالعكس افرض أن كلاً من I و R / I نويثيري يميني . ولتكن $J_1 \subseteq J_2 \subseteq J_3 \subseteq ...$ أية سلسلة تصاعدية من مثاليات يمينية من R . فإن $J_1 \cap I \subseteq J_2 \cap I \subseteq J_3 \cap I \subseteq ...$ هي سلسلة تصاعدية من مثاليات يمينية من R محتواة في I . بما أن I نويثيري يميني فإنه يوجد عدد صحيح موجب n بحيث $J_m \cap I = J_n \cap I, \quad \forall\, m \geq n$.

مرة أخرى $(J_1 + I) / I \subseteq (J_2 + I) / I \subseteq (J_3 + I / I) \subseteq ...$ هي سلسلة تصاعدية من مثاليات يمينية في R / I ولأن R / I نويثيرية يمينية فإنه يوجد عدد صحيح موجب t بحيث يكون $(J_m + I) / I = (J_t + I) / I$ ، لكل $m \geq t$. إذا كان $r = \max\{n, t\}$ ، فإن $J_m \cap I = J_r \cap I$ و $(J_m + I) / I = (J_r + I) / I$ لكل $m \geq r$ ولكن عندئذ يكون $J_m + I = J_r + I$ لكل $m \geq r$ فسوف نبرهن أن $J_r = J_m$ لكل $m \geq r$. الآن لكل $m \geq r$ يكون $J_m = J_m \cap (J_m + I) = J_m \cap (J_r + I)$

(لأن $J_m + I$ لكل $r \le m$)

$= J_r + J_m \cap I$ (لأن $J_r \subseteq J_m$ لكل $r \le m$ وحسب قانون موديولار)

$= J_r + J_r \cap I$ (لأن $J_m \cap I = J_r \cap I$)

$= J_r$ (لأن $J_r \cap I \subseteq J_r$)

بالتالي فإن $J_m = J_r$ لكل $m \ge r$ ونتيجة لذلك فإن R حلقة نويثيرية يمينية . □

الآن نعطي برهاناً لنظرية مشهورة لهلبرت .

نظرية 10-15 (نظرية القاعدة لهلبرت)

إذا كانت R حلقة نويثيرية يمينية بعنصر محايد ، فإن $R[x]$ ، حلقة كثيرات الحدود على R تكون نويثيرية يمينية .

البرهان

يكفي البرهنة على أن كل مثالي يميني في $R[x]$ هو منتهي التولد .

ليكن I مثالي يميني في $R[x]$ يختلف عن الصفر . لكل عدد صحيح $0 \le k$ ، ضع :

$$I_k = \{a \in R \mid a \ne 0 \text{ and } \exists \alpha_0 + \alpha_1 x + \dots + \alpha_{k-1}x^{k-1} + ax^k \in I\} \cup \{0\}$$

I_k مثالي يميني في R و $I_k \subseteq I_{k+1}$ لكل $k \ge 0$.

لما كانت R نويثيرية يمينية فإنه يوجد عدد صحيح موجب n بحيث $I_m = I_n$ لكل $m \ge n$ كذلك كل I_j مثالي يميني لحلقة نويثيرية يمينية فهو منتهي التولد . افرض أن $I_i = < a_{i_1}, a_{i_2}, a_{i_3}, \dots, a_{i_{m_i}} >$ لكل $i = 0, 1, 2, \dots, n$ حيث a_{ij} هو المعامل القائد لكثيرة حدود $f_{ij} \in I$ درجتها i . ندعي أن I مولد بعدد $m_0 + m_1 + m_2 + \dots + m_n$ من كثيرات الحدود $f_{01}, f_{02}, \dots, f_{0m_0}, f_{11}, f_{12}, \dots, f_{1m_1}, \dots, f_{n1}, f_{n2}, \dots, f_{nm_n}$

ليكن $J = < f_{01}, f_{02}, \ldots, f_{n1}, f_{n2}, \ldots, f_{nm_n} >_r$

لأن كل $f_{ij} \in I$ فإن $J \subseteq I$.

ليكن $f \neq 0 \in R[x]$ بحيث $f \in I$. عندئذ يكون :

$$f = c_0 + c_1x + c_2x^2 + \ldots + c_sx^s, c_s \neq 0$$

وسوف نطبق الاستنتاج على s عندما $s = 0$ ، $f = c_0 \in I_0$ ومن تعريف كثيرات الحدود f_{ij} فإن

$$a_{01} = f_{01}, a_{02} = f_{02}, \ldots, a_{0m_0} = f_{0m_0}$$

هي عناصر في I_0 تولد I_0 ، عليه فإن $I_0 \subseteq J$ ، ونحصل على أن $c_0 \in J$ ، هذا يبين أن $f \in J$.

الآن افرض أن جميع كثيرات الحدود غير الصفرية في I ذوات الدرجة $< s$ تنتمي إلى J ونفرض أن درجة $f = s$.

لتكن $s > n$. المعامل القائد c_s لكثيرة الحدود f ينتمي إلى I_s . لكن $I_s = I_n$ لأن $I_m = I_n$ لكل $m \geq n$. هذا يؤدي إلى أن $c_s \in I_n$ أي أن لبعض $b_1, b_2, \ldots, b_{mn} \in R$ يكون :

$$c_s = a_{n1}b_1 + a_{n2}b_2 + a_{n3}b_s + \ldots + a_{nm_n}b_{m_n} \in R \qquad (1)$$

كثيرة الحدود $g = f - (f_{n1}b_1 + f_{n2}b_2 + \ldots f_{nm_n}b_{m_n})\, x^{s-n}$ إما أنها صفرية أو درجتها أقل من s لأن معامل x^s في ويساوي :

$c_s - (a_{n1}b_1 + a_{n2}b_2 + \ldots + a_{nm_n}b_{m_n})$ وهو صفر حسب (1) .

إذا كان $g = 0$ فإن $g \in J$. وإذا كان $g \neq 0$ ، فمن فروض الاستنتاج يكون $g \in J$ وعليه في كل حالة فإن :

$$f = g + (f_{n1}b_1 + f_{n2}b_2 + \ldots f_{nm_n}b_{m_n})\, x^{s-n} \in J$$

إذا كان $s \leq n$ فإن $c_s \in I_3 \Rightarrow c_s = a_{s1}d_1 + a_{s2}d_2 + \ldots + a_{sm_s}d_{m_s}$

لبعض $d_1, d_2, \ldots, d_{m_s} \in R$.

كثـــيرة الحـــــدود $h = f - (f_{s1}d_1 + f_{s2}d_2 + \dots f_{sm_s}d_{m_s})$ إمـــا أنهـــا صـــــفرية أو درجتها $< s$ لأن معامل x^s في h هو :

$$c_s - (a_{s1}d_1 + a_{s2}d_2 + \dots + a_{sm_s}d_{m_s}) = 0$$

وعلى الفور مرة أخرى يكون $h \in J$ ، ومن ثم $f \in J$.

عليـه ففـي كـل حالـة تكـون كـل كثـيرة حـدود غـير صـفرية f محتـواة في I هـي في J أيضاً . هذا يعطي أن $J \subseteq I$ ، والذي بدوره يؤدي إلى أن $I = J$ وبالتالي فإن I منتهي التولد . إذاً $R[x]$ نويثيرية يمينية . □

2– الحلقات الأرتينية (Artinian Rings)

تعريف 15-11

الحلقة التي فيها كل سلسلة تنازلية تامة من مثاليات يمينية (يسارية) تكون منتهية تسمى حلقة أرتينية يمينية (يسارية) .

واختياراً يمكننا أن نعرف الحلقة الأرتينية اليمينية (اليسارية) بأنها الحلقة التي لكل سلسلة تنازلية غير منتهية من مثاليات يمينية (يسارية) $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$

يوجد عدد صحيح موجب n بحيث $I_m = I_n$ لكل $m \geq n$.

ملاحظة الحلقة الأرتينية اليمينية (اليسارية) معروفة أيضاً بأنها حلقة مع شرط السلسلة التنازلية (DCC) على المثاليات اليمينية (اليسارية) بها .

تعريف 15-12

الحلقة التي يتحقق فيها شرط السلسلة التنازلية للمثاليات اليمينية واليسارية معاً تسمى حلقة أرتينية .

مثال 4

كل حلقة قاسمية D هي أرتينية يمينية لأن المثاليان اليمينيان الوحيدان لها هما (0) و D نفسها . ولسبب مشابه فإن D حلقة أرتينية يسارية أيضاً .

مثال 5

كل حلقة منتهية هي أرتينية يمينية ويسارية معاً .

مثال 6

اعتبر المجموعة $Z(p^\infty)$ لجميع الأعداد النسبية بالصيغة $\frac{m}{p^n}$ بحيث $0 \le \frac{m}{p^n} < 1$ ، حيث p عدد أولي ثابت ، n أي عدد صحيح موجب و n تأخذ قيم جميع الأعداد الصحيحة غير السالبة . عندئذ تكون $Z(p^\infty)$ زمرة إبدالية تحت عملية الجمع معيار 1 . نجعل من $Z(p^\infty)$ حلقة بتعريف $ab = 0$ لكل $a, b \in Z(p^\infty)$.

لاحظ أن كل زمرة جزئية من $Z(p^\infty)$ هي مثالي للحلقة $Z(p^\infty)$. الآن لتكن I أي مثالي فعلي من $Z(p^\infty)$ وليكن k أصغر عدد صحيح موجب بحيث يكون لعدد صحيح موجب a ، $a / p^k \notin I$. لاحظ أن p لا يقسم a لأنه خلافاً لذلك يكون $b / p^{k-1} \notin I$ لعدد صحيح موجب b وهو خلاف اختيارنا للعدد k .

الآن $0, 1 / p^{k-1}, 2 / p^{k-1}, \dots (p^{k-1} - 1) / p^{k-1} \in I$. ندعي أن I تحوي بالضبط هذه العناصر . إذا كان ادعائنا غير صحيح فإنه يوجد عنصر $c / p^i \in I$ حيث c عدد صحيح موجب ، $k \le i$ و p لا يقسم c .

بما أن $(c, p) = 1$ فيمكننا إيجاد عددين صحيحين s, r بحيث $cr + ps = 1$.

الآن $(rp^{i-k})c / p^i = rc / p^k$ و $s / p^{k-1} = sp / p^k$ (كل مختزل معيار 1 يقع في I) . يتبع ذلك أن $rc / p^k + sp / p^k = (rc + sp) \mid p^k = 1 / p^k \in I$

مما يتناقض مع اختيار k ، إذاً $I = \{0, 1 / p^{k-1}, 2 / p^{k-1}, \dots, (p^{k-1} - 1) / p^{k-1}\}$

نرمز لهذا المثالي بالرمز I_{k-1} . وعليه نستنتج أن جميع المثاليات الفعلية للحلقة $Z(p^\infty)$ هي على شكل I_{j-1} لكل عدد صحيح موجب j ، بما أن كل مثالي فعلي في $Z(p^\infty)$ له عدد

منتـه مـن العناصـر ، فـإن شـرط السلسـلة التنازليـة (DCC) محققـة . إذاً $Z(p^{\infty})$ هـي حلقـة أرتينية .

في نهاية الفصل سنقدم مثالاً لحلقة أرتينية يمينية ليست أرتينية يسارية .

تعريف 15-13

إذا كان في الحلقة R كل مجموعة غير خالية في مثاليات يمينية (يسارية) في R ، مرتبة جزئياً بعلاقة الاحتواء ، يكون فيها عنصر أصغري فإننا نقول أن شرط الأصغرية يتحقق للمثاليات اليمينية (اليسارية) للحلقة R .

لاحظ ما نقصده بالعنصر الأصغري لمجموعة غير خالية F مرتبة جزئياً تحت العلاقة $\leq$ من أنه عنصر $A \in F$ حيث لا يوجد $B \in F$ يحقق $B < A$ بعبارة أخرى A عنصر أصغري في F إذا وفقط إذا كان $B \leq A \Rightarrow B = A$ كما في حالة العنصر الأعظمي فإن المجموعة قد يكون لها أكثر من عنصر أصغري واحد . وحيث أن نتائج الحلقات الأرتينية اليسارية تناظر تماماً تلك التي للحلقات الأرتينية اليمينية فإننا من الآن فصاعداً سوف نناقش فقط الحلقات الأرتينية اليمينية .

نظرية 15-14

لأية حلقة R ، العبارات الآتية متكافئة :

(1) R حلقة أرتينية يمينية .

(2) شرط الأصغرية يتحقق للمثاليات اليمينية في R .

البرهان

$(2) \Rightarrow (1)$. لتكن F مجموعة غير خالية من مثاليات يمينية في R . ليكن I_1 عنصراً في F . إذا لم يكن I_1 عنصراً أصغرياً ، يمكننا إيجاد مثالي يميني آخر I_2 في R بحيث

$I_1 \supset I_2$. إذا كانت F ليس فيها عنصر أصغري ، فإنه يمكن إعادة العملية بصورة غير محدودة لنحصل على سلسلة تنازلية تامة غير منتهية $I_1 \supset I_2 \supset I_3 \supset \ldots$ من مثاليات يمينية في R وهذا تناقض مع حقيقة كون R حلقة أرتينية يمينية . إذاً F يحوي عنصراً أصغرياً .

$(1) \Rightarrow (2)$. لتكن $I_1 \supseteq I_2 \supseteq I_3 \supseteq \ldots$ سلسلة تنازلية من مثاليات في R . اعتبر $F = \{I_i \mid i = 1, 2, 3, \ldots\}$. بما أن $I_1 \in F$ فإن F غير خالية . حسب (2) فإن F لها عنصر أصغري ، وليكن I_n لعدد صحيح موجب n . الآن لكل $m \geq n$ ، $I_m \subseteq I_n$. إذا كان $I_m \neq I_n$ ، فإن $I_m \notin F$ لأن I_n عنصر أصغري من F ، وهذا غير مقبول . إذاً $I_m = I_n$ لكل $m \geq n$. بالتالي R حلقة أرتينية يمينية . □

تعريف 15-15

يقال لمثالي I للحلقة R أنه أرتيني يميني إذا كانت كل سلسلة تنازلية تامة من مثاليات يمينية من R المحتواة في I هي سلسلة منتهية .

من الواضح أن كل مثالي I لحلقة أرتينية يمينية يكون أرتيني يميني نترك برهان النظريتين التاليتين للقارئ لأنهما مشابهتين تماماً للنتيجتين المناظرتين لهما في الحلقات النويثيرية اليمينية .

نظرية 15-16

الصورة الهومومورفية لحلقة أرتينية يمينية تكون أرتينية يمينية . □

نظرية 15-17

لتكن I مثالية لحلقة R ، فإن R أرتينية يمينية إذا وفقط إذا كان كل من I و R / I أرتينية يمينية . □

نظرية 15-18

الحلقة الأرتينية اليمينية التي تحوي أكثر من عنصر واحد وليس لها قواسم فعلية للصفر هي حلقة قاسمية .

البرهان

لتكن R حلقة أرتينية يمينية تحوي على الأقل عنصرين وليس لها قواسم فعلية للصفر . ليكن $a(\neq 0) \in R$. اعتبر السلسلة التنازلية :

$$< a >_r \supseteq < a^2 >_r \supseteq < a^3 >_r \supseteq \ldots$$

من مثاليات يمينية من R . لما كانت R أرتينية يمينية فإنه يوجد عدد صحيح موجب n بحيث أن $< a^m >_r = < a^n >$ لكل $m \geq n$. كحالة خاصة :

$$< a^{n+1} >_r = < a^n >_r \Rightarrow a^n \in < a^{n+1} >_r$$

$$\Rightarrow a^n = a^{n+1}r + ma^{n+1} \qquad (\text{لبعض } m \in Z, r \in R)$$

$$\Rightarrow a^n = a^n(ar + ma) = n^n e \qquad (\text{حيث } e = ar + ma \in R)$$

$$\Rightarrow a = ae \qquad (\text{لأن } a^{n-1}(\neq 0) \text{ تم حذفه})$$

$$\Rightarrow ae = ae^2 \Rightarrow a(e - e^2) = 0 \Rightarrow e = e^2$$

لأن $a \neq 0$ و R ليس لها قواسم فعلية للصفر .

كذلك $e \neq 0$ لأن $a \neq 0$.

الآن لأي $x \in R$ $\qquad e(ex - x) = 0 \Rightarrow ex = x$ و $(xe - x) = 0 \Rightarrow xe = x$

إذاً e هو المحايد للحلقة R . بالتالي $< a^n >_r = a^nR = < a^{n+1} >_r = a^{n-1}R$. الآن :

$$a^ne \in a^nR \Rightarrow a^ne \in a^{n+1}R \Rightarrow a^ne = a^{n+1}b$$

لبعض $b \in R$ ، هذا يؤدي إلى أن $ab = e$. بالتالي فإن R حلقة قاسمية . □

نتيجة 15-19

كل ساحة تامة أرتينية تحوي عنصرين على الأقل هي حقل .

نتيجة 15-20

في الحلقة الأرتينية الإبدالية R التي لها محايد ، كل مثالي أولي غير R هو أعظمي .

البرهان

إذا كان P مثالي أولي للحلقة R بحيث $P \neq R$ فإن R/P عبارة عن ساحة تامة أرتينية بعنصر محايد $1 + P$ إذاً R/P حقل (نتيجة 15-19) . هذا يؤدي إلى أن P مثالي أعظمي للحلقة R . □

نظرية 15-21

في الحلقة الأرتينية اليمينية كل مثالي يميني متلاشي (nil) يكون عديم القوة .

البرهان

لتكن I مثالي متلاشي للحلقة الأرتينية اليمينية R . للسلسلة التصاعدية اليمينية $\ldots \supseteq I^3 \supseteq I^2 \supseteq I$ ، يوجد عدد صحيح موجب n بحيث $I^m = I^n$ لكل $m \geq n$. بالأخص $I^{2n} = I^n$. ندعي أن $I^n = (0)$ ، إذا فرضنا غير ذلك فإن $I^{2n} \neq (0)$. ليكن $F = \{ A \mid AI^n \neq (0)$ بحيث R مثالي يميني في $A \}$.

F غير خالية لأن $I^n \in F$. بما أن R أرتينية يمينية ، F لها عنصر أصغري . ليكن K عنصراً أصغرياً في F . عندئذ $KI^n \neq (0)$ يؤدي على وجود $k \in K$ بحيث $kI^n \neq (0)$ ولكن $kI^n \subseteq K$ لأن K مثالي يميني في R . ليكن $kI^n \subset K$. مرة ثانية $(kI^n)\, I^n = kI^{2n} = kI^n \neq (0) \Rightarrow kI^n \in F$.

لأن kI^n مثالية يمينية في R . هذا يناقض أصغرية K . إذاً $kI^n = K$. بما أن $k \in K$ ، يوجد $a \in I^n$ بحيث $ka = k$ وحيث أن I هو مثالي يميني متلاشي

و $I^n \subseteq I$ فإن a عديم القوة . إذاً يوجد عدد صحيح موجب t بحيث $a^t = 0$. عندئذ يكون

$$k = ka = ka^2 = ka^3 = ... = ka^t = 0 \Rightarrow kI^n = (0)$$

وهذا تناقض مع اختيار k . إذاً $I^n = (0)$. بالتالي فإن I مثالي يميني عديم القوة . □

3– أمثلة وأمثلة مضادة

ننهي هذا الفصل بإعطاء بعض الأمثلة والأمثلة المضادة المفيدة .

مثال 7

Z حلقة نويثيرية ولكنها ليست أرتينية . في الحقيقة لكل عدد صحيح موجب n ، فإن السلسلة التنازلية التامة

$$< n > \supset < 2n > \supset < 4n > \supset ...$$

لمثاليات في Z هي سلسلة غير منتهية .

مثال 8

رأينا في مثال 6 أن $Z(p^\infty)$ حلقة أرتينية لأي عدد أولي ثابت p . ندعي أن $Z(p^\infty)$ ليست نويثيرية . نذكر أن كل مثالي في $Z(p^\infty)$ هو من نوع I_{k-1} لكل عدد صحيح موجب k . لاحظ أيضاً أن $x \in I_{k-1} \Leftarrow x = \frac{a}{p^{k-1}}$. لعدد صحيح a ، $0 \le a \le (p^{k-1} - 1)$ هذا يؤدي إلى أن :

$x = \frac{ap}{p^k}$ و $0 \le ap \le p^k - p < p^k - 1$ والذي يؤدي إلى أن $x \in I_k$.

إضافة إلى ذلك حسب تعريف I_{k-1} فإن $\frac{1}{p^k} \notin I_{k-1}$. عليه $I_{k-1} \subset I_k$. السلسلة التصاعدية التامة

$$(0) \subset I_1 \subset I_2 \subset I_3 \subset ...$$

غير منتهية . إذاً $Z(p^\infty)$ ليست نويثيرية . لاحظ أيضاً بالرغم من أن كل مثالي فعلي في $Z(p^\infty)$ منتهي التولد ، مع ذلك فإن $Z(p^\infty)$ نفسها ليست منتهية التولد .

مثال 9

لتكن S مجموعة غير منتهية ولتكن R مجموعة جميع المجاميع الجزئية من S (أي R هي مجموعة قوة S) . فإن $(R, \Delta, \cap)$ حلقة إبدالية بعنصر محايد .

تذكر أن لكل $A, B \in R$ ، $A \Delta B = (A - B) \cup (B - A)$.

ندعي أن R ليست نويثيرية ، لهذا الغرض يكفي أن نبين أنه يوجد مثالي في R ليس منته التولد . لتكن C مجموعة جزئية من R تحوي جميع المجاميع الجزئية المنتهية من S . من الواضح أن C مثالي في R .

افرض أن C منته التولد ، عندئذ $C = < C_1, C_2, C_3, \dots, C_t >$

حيث لكل $i = 1, 2, \dots, t$ ، C_i مجموعة جزئية منتهية من S . ليكن $A \in C$ ، فإن $A = (C_1 \cap D_1) \Delta (C_2 \cap D_2) \Delta \dots \Delta (C_t \cap D_t)$

لبعض المجاميع الجزئية $D_1, D_2, \dots, D_t$ من S . عندئذ لكل $y \in A$ لدينا $y \in (C_1 \cap D_1) \Delta \dots \Delta (C_t \cap D_t)$. هذا يؤدي إلى أن $y \in C_i \cap D_i$ على الأقل لبعض i و $1 \leq i \leq t$. عليه كل عنصر في a ينتمي لبعض C_i . وحيث أن S مجموعة غير منتهية و $\bigcup_{i=1}^{t} C$ مجموعة جزئية منتهي من S ، فإنه يوجد $x \in S$ ، $x \notin \bigcup_{i=1}^{t} C_i$. بعبارة أخرى $x \in S$ و $x \notin C_i$ لكل $i = 1, 2, \dots, t$. اعتبر الآن المجموعة المنتهية $\{x\}$ من S . حسب اختيارنا لـ C فإن $\{x\} \in C$. هذا غير مقبول على ضوء المناقشة المعطاة سلفاً . إذاً C ليست منتهية التولد ، بالتالي R ليست نويثيرية .

مثال 10

لتكن F حلقة جميع الدوال الحقيقية على R لأي عدد حقيقي $r > 0$ ، نعرف $I_r = \{f \in F \mid f(x) = 0 \quad \forall -r \leq x \leq r\}$ فإن I_r مثالي في F .

السلسلة التنازلية التامة من المثاليات $I_1 \supset I_2 \supset I_3 \supset \dots$

والسلسلة التصاعدية التامة من المثاليات $I_1 \subset I_{\frac{1}{2}} \subset I_{\frac{1}{3}} \subset \dots$

لن تنتهيان أبداً . إذاً F ليست نويثيرية ولا أرتينية .

الآن نبين بأمثلة أن الحلقة الجزئية لحلقة نويثيرية (أرتينية) ليست من الضروري أن تكون نويثيرية (أرتينية) .

مثال 11

اعتبر $Q[x]$. بما أن Q حلقة نويثيرية فإن $Q[x]$ حلقة نويثيرية (نظرية القاعدة لهلبرت) .

لتكن $R = \{ f \in Q[x] \mid$ الحد الثابت في f ينتمي إلى $Z\}$.

R حلقة جزئية من $Q[x]$. السلسلة التصاعدية التامة :

$$< x > \subset < x/2 > \subset < x/4 > \subset \dots$$

لن تنتهي أبداً ، إذاً R ليست نويثيرية .

مثال 12

لأن Q حقل فهو حلقة أرتينية . Z حلقة جزئية في Q ولكنها ليست أرتينية (انظر مثال 7) .

المثال الآتي يبين أن نظرية القاعدة لهلبرت غير متحققة للحلقات الأرتينية .

مثال 13

ليكن F حقلاً . فيكون F أرتيني . اعتبر $F[x]$. السلسلة التنازلية التامة :

$$< x > \supset < x^2 > \supset < x^3 > \supset \dots$$

من مثاليات في $F[x]$ غير منتهية . إذاً $F[x]$ ليست أرتينية .

لاحظ أنه لكون $F[x]$ ساحة تامة ، فلو كان $F[x]$ دائماً أرتينياً فسوف نحصل على أن $F[x]$ حقل حسب نتيجة 15-19 .

وأخيراً نعطي أمثلة على حلقات هي نويثيرية (أرتينية) يمينية ولكنها ليست نويثيرية (أرتينية) يسارية .

مثال 14

لتكن
$$R = \left\{ \begin{pmatrix} a & b \\ o & c \end{pmatrix} \middle| \, a \in Z; b, c \in Q \right\}$$

فإن R حلقة تحت عمليتي الجمع والضرب للمصفوفات . ندعي أن R نويثيرية يمينية ولكنها ليست نويثيرية يسارية .

لأي عدد صحيح غير سالب k ، اعتبر المجموعة :

$$A_k = \left\{ \begin{pmatrix} 0 & \frac{m}{2^k} \\ 0 & 0 \end{pmatrix} \middle| \, m \in Z \right\}$$

عندئذ A_k مثالي للحلقة R . إضافة إلى ذلك $A_k \subset A_{k+1}$ لأن $\frac{m}{2^k} = \frac{2m}{2^{k+1}}$ و $\begin{pmatrix} 0 & \frac{1}{2^{k+1}} \\ 0 & 0 \end{pmatrix} \notin A_k$.

وهكذا نحصل على سلسلة تصاعدية تامة غير منتهية :

$$A_0 \subset A_1 \subset A_2 \subset A_3 \subset \ldots$$

من مثاليات يسارية للحلقة R . هذا يبين أن R ليست نويثيرية يسارية .

للبرهنة على أن R نويثيرية يمينية يكفي التحقق من أن كل مثالي يميني يختلف عن الصفر في R هو منتهي التولد .

ليكن $A\,[\neq (0)]$ مثالي يميني من R وليكن $\alpha e_{11} + \beta e_{12} + \gamma e_{22} \in A$ حيث e_{ij} يرمز للمصفوفة التي فيها 1 في الموقع (i, j) وصفر من المواقع الأخرى و $\alpha \in Z$ ، $\beta, \gamma \in Q$. لاحظ أيضاً أن $e_{ij}e_{kl} = e_{il}$ إذا كان $j = k$ و $e_{ij}e_{kl} = 0$ إذا كان $j \neq k$ ، فإن هناك حالتان .

الحالــــة I $\alpha \neq 0$. لـــيكن δ أصـــغر عـــدد صـــحيح موجـــب بحيـــث أن $\delta e_{11} + be_{12} + ce_{22} \in A$ لبعض $b, c \in Q$. عندئذ ندعي أنه إما A مولدة بالمصفوفات $\delta e_{11}, e_{12}, e_{22}$ أو بالمصفوفتين δe_{11} و e_{12} . الآن :

$$(\delta e_{11} + be_{12} + ce_{22})\, e_{12} \in A \Rightarrow \delta e_{12} \in A \Rightarrow \delta e_{12}\left(\frac{1}{\delta}\right) e_{22} =$$

$$e_{12} \in A \Rightarrow be_{12} = e_{12}(be_{22}) \in A$$

كذلك

$$\delta e_{11} + be_{12} + ce_{22} \in A \Rightarrow (\delta e_{11} + be_{12} + ce_{22})e_{11} \in A$$

$$\Rightarrow \delta e_{11} \in A$$

لـذا حصـلنا علـى أن $ce_{22} \in A$. الآن في حالـة $c = 0$ لكـل مـا يماثـل δ و b فـإن A مولدة بـ δe_{11} و e_{12} وفي الحالة الأخرى فإن $ce_{22}\left(\frac{1}{c}\right) e_{22} \in A$ عندئذ A مولد بالمصفوفات $\delta e_{11}, e_{12}$ و e_{22} .

الحالـة II $\alpha = 0$. في هـذه الحالـة $be_{12} + ce_{22} \in A$. إذا كانـت جميع عناصر A هـي مـن النـوع $\lambda(b_{12} + ce_{22})$ لبعض $\lambda \in Q$ ، فـإن A مولـدة بمصـفوفة واحـدة $be_{12} + ce_{22}$. وغير ذلك يوجد $b_1, c_1 \in Q$ بحيث يكون $be_{12} + c_1e_{22} \in A$ ولكن $b_1c \neq bc_1$. عندئذ :

$$(bc_1 - b_1c)\, e_{12} \in A \Rightarrow (bc_1 - b_1c)\, e_{12}\left[\frac{1}{(bc_1 - b_1c)}\right] e_{22} \in A \Rightarrow$$

$$e_{12} \in A \Rightarrow e_{12}be_{22} \in A \Rightarrow be_{12} \in A \Rightarrow ce_{22} \in A$$

إمـا أن $c = 0$ أو $e_{22} \in A$. عليـه إمـا A مولـدة بالعنصـرين e_{12} و e_{22} أو بالعنصـر e_{12} فقط ، لذا فإن A منتهية التولد .

بالتالي فإن R نويثيرية يمينية .

مثال 15

لتكن $R = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a \in Q; b, c \in IR\right\}$

من الواضح أن R حلقة تحت عمليتي الجمع والضرب للمصفوفات . ندعي أن R حلقة أرتينية يمينية ولكنها ليست أرتينية يسارية .

باعتبار $I\!R$ فضاء متجهي على Q فهو ذو بعد غير منته . توجد أعداد حقيقية $a_1, a_2, \ldots, a_n$ مستقلة خطياً على Q . لكل عدد صحيح موجب k ضع :

$$A_k = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \middle| \; a \text{ عنصر في فضاء جزئي من } I\!R \text{ مولد بـ } a_k, a_{k+1}, \ldots \right\}$$

من اليسير التحقق من أن A_k مثالي يساري في R . إضافة إلى ذلك $A_k \supset A_{k+1}$ لأن $a_k \notin A_{k+1}$. بما أن المجموعة $\{a_1, a_2, a_3, \ldots\}$ غير منتهية . نحصل على سلسلة تنازلية تامة غير منتهية من مثاليات يسارية $I_1 \supset I_2 \supset I_3 \supset \ldots$ في R . هذا يثبت حقيقة أن الحلقة R ليست أرتينية يسارية . ولتكن $A_1 \supset A_2$ مثاليان يمينيان للحلقة R وأن $\alpha e_{11} + \beta e_{12} + \gamma e_{22} \in A_2$ حيث $\alpha \in Q$ ، $\beta, \gamma \in R$ وأن e_{ij} معرف كما في المثال السابق .

(e_{ij} هذه تسمى وحدة مصفوفة) . إذا كان $\alpha \neq 0$ ، فكما أثبتنا في المثال السابق إما $e_{22} \in A_2$ ، $e_{12} \in A_2$ ، $\alpha e_{11} \in A_2$ أو $\alpha e_{11} \in A_2$. $e_{12} \in A_2$ و $\gamma = 0$. من الموقف الأول يكون $(\alpha e_{11})\left(\frac{1}{\alpha}\right) e_{11} \in A_2$ بمعنى أن $e_{11} \in A_2$ وعليه فإن $A_2 = R$ ، وهو غير مقبول لأن $A_2 \subset A_1$. في الموقف الأخير A_2 مولد بالعنصرين e_{11} و e_{12} .

اعتبر $A_3 \subset A_2$ حيث $A_1 \supset A_2 \supset A_3$ مثالي يميني في R . الآن ليكن $ae_{11} + b_{12} \in A_3$. إذا كان $a \neq 0$ فإن $(ae_{11} + be_{12}) \frac{1}{a} e_{11} \in A_3 \Rightarrow e_{11} \in A_3$ عليه $b_{12} \in A_3$. الآن إذا كان $b \neq 0$ ، فهذا يؤدي إلى أن $be_{12}\left(\frac{1}{b}\right)e_{22} = e_{12} \in A_3$ وعليه $A_3 = A_2$ وهو تناقض . لذا فإن $b = 0$ وبالتالي A_3 مولدة بالعنصر e_{11} . هذا على الفور

يبرهن أن A_3 هو مثالي يميني أصغري في R . إذاً السلسلة التنازلية التامة من مثاليات يمينية $A_1 \supset A_2 \supset A_3 \supset (0)$ هي سلسلة منتهية .

وأخيراً إذا كان $\alpha = 0$ فإن $\beta e_{12} + \gamma e_{22} \in A_2$. إذا كانت جميع العناصر الأخرى في A_2 من النوع $\lambda(\beta e_{12} + \gamma e_{22})$ لبعض $\lambda \in R$ فإن A_2 مثالي يميني أصغري وأن $A_1 \supset A_2 \supset (0)$ هي السلسلة التنازلية التامة من المثاليات اليمينية . خلاف ذلك فكما رأينا في مثال سابق يكون A_2 مولد إما بالعنصرين e_{12}, e_{22} أو بالعنصر e_{12} فقط .

وفي حالة A_2 مولدة بالعنصر e_{12} فقط فهو مثالي يميني أصغري للحلقة R وبذلك أكملنا البرهان .

وفي الحالة A_2 مولد بالعنصرين e_{12} و e_{22} فإن مناقشة مشابهة لما سبق تبين أنه إذا كان $A_1 \supset A_2 \supset A_3$ لمثالي يميني A_3 في R فإنه إما A_3 مولد بالعنصر e_{12} أو بالعنصر $de_{12} + fe_{22}$ لبعض $d, f \in /R$. في كل حالة يكون A_3 مثالي يميني أصغري للحلقة R .

بالتالي فالحلقة R ليس لها سلسلة تنازلية تامة لانهائية من مثاليات يمينية . هذا يثبت حقيقة أن R أرتينية يمينية .

مسائل

1- بين أنه إذا كانت R نويثيرية فإن كل هومومورفزم من R فوقي على نفسه يكون أحادياً .

2- ليكن I مثالي لمساحة مثاليات رئيسية يختلف عن الصفر . برهن أن R/I حلقة أرتينية ونويثرية معاً .

3- برهن أنه في ساحات التحليل الوحيد (UFD) فإن شرط السلسلة التصاعدية يتحقق للمثاليات الرئيسية .

4- أثبت أن كل حلقة نويثيرية R بعنصر محايد لها مثالي أعظمي .

[**إرشاد** لتكن $F = \{ J \mid 1 \notin J$ و J مثالي في $R \}$] .

5- إذا كانت R حلقة إبدالية بعنصر محايد ، برهن أنه إذا كانت $R[x]$ نويثيرية فإن R نويثيرية .

[**إرشاد** $R[x]/(x) \cong R$] .

6- برهن أنه إذا كانت ساحة تامة ذات عنصر محايد لها عدد منته من المثاليات الأولية فإنها تكون حقلاً .

7- برهن أن كل حلقة أرتينية إبدالية لها عدد منته من المثاليات الأولية الفعلية .

8- برهن أن كل مثالي لحلقة نويثيرية إبدالية تحوي حاصل ضرب مثاليات أولية .

9- لتكن $R_1, R_2, \ldots, R_n$ هي n من الحلقات ، إذا كانت R مجموعة المرتبات النونية $(a_1, a_2, \ldots, a_n)$ مع كون $a_i \in R_i$ لكل $N = 1, 2, \ldots, n$ ، برهن أن R حلقة تحت عمليتي الجمع والضرب للمركبات . R تسمى المجموع المباشر للحلقات $R_1, R_2, \ldots, R_n$ ونكتب $R = R_1 \oplus R_2 \oplus \ldots \oplus R_n$.

10- ليكن R المجموع المباشر للحلقات $R_1, R_2, \dots, R_n$. لكل $i = 1, 2, \dots, n$ ضع :

$$R_i' = \{(0, 0, \dots, 0, a_i, \dots, 0) \mid a_i \in R\}$$

برهن (i) كل R_i' مثالي في R . (ii) لكل i ، $R_i' \cong R_i$.

11- إذا كانت R المجموع المباشر للحقلين R_1 و R_2 برهن أن $R / R_1' \cong R_2'$ و $R / R_2' \cong R_1'$ حيث R_1' و R_2' معرفتان كما في السؤال السابق .

12- ليكن R المجموع المباشر للحلقات $R_1, R_2, \dots, R_n$ ، برهن أن R هي نويثيرية (أرتينية) يمينية إذا وفقط إذا كانت كل R_i هي حلقة نويثيرية (أرتينية) يمينية .

[**إرشاد** طبق الاستنتاج على n واستخدم نظرية 15-9] .

13- إذا كانت R نويثيرية (أرتينية) يمينية ، برهن أن R_n ، حلقة المصفوفات ذات السعر $n \times n$ على R هي نويثيرية (أرتينية) يمينية .

14- (كلمر) إذا كانت R حلقة إبدالية بحيث $R[x]$ نويثيرية برهن أن R تحوي عنصراً محايداً .

15- إذا كانت في حلقة نويثيرية R كل مثالي مولد بعنصرين هو مثالي رئيسي برهن أن R هي حلقة مثاليات رئيسية .

16- لتكن R مجموعة جميع العناصر بالصيغة $\frac{f(t)}{g(t)}$ حيث $f(t)$ ، $g(t)$ كثيرتي حدود في $Z_2(t)$ ، حيث Z_2 هي حلقة الأعداد الصحيحة معيار 2 و $g(t) \neq 0$. برهن أن R أرتينية تحت الجمع والضرب الاعتياديين للدوال النسبية و $\theta : R \to R$ المعطاة حسب $\theta(x) = x^2$ هي هومومورفزم أحادي ليس فوقي .

ملاحظة هذا يبين أن ثنائية النتيجة المذكورة في سؤال 1 السابق ليست بالضرورة أن تكون صحيحة في الحلقات الأرتينية .

16

الصيغ القانونية Canonical Forms

في بند 4 في الفصل الثاني عشر ، برهنا أنه في مقابل كل اختيار لقاعدة فضاء متجهي V على حقل F فإن هناك مصفوفة وحيدة مرتبطة بكل تحويل خطي معلوم . لأغراض عملية غالباً ما يكون مرغوباً في اختيار قاعدة تجعل المصفوفة المرافقة في "صيغة شيقة" ونعني بذلك مصفوفة قريبة الشبه بمصفوفة قطرية مثل هذه الصيغ محببة في المعالجات الجبرية ، في هذا الفصل نناقش مسائل اختيار مثل هذه القاعدة لفضاء متجهي V لتحويل خطي معطى $T \in A(V)$.

1- كثيرات الحدود الأصغرية والجذور المميزة

تعريف 1.16

التحويل $T \in A(V)$ يسمى قابل للعكس يميناً أو يساراً إذا وجد $S \in A(V)$ بحيث $TS = I$ $(ST = I)$ حيث I هو التحويل المحايد على V .

ملحوظة

تسمى S بالمعكوس اليميني أو اليساري للتحويل T .

تعريف 2.16

$T \in A(V)$ يسمى تحويل قابل للعكس أو منتظم إذا كان T قابلاً للعكس من اليمين واليسار معاً .

قضية 3.16

إذا كان $T \in A(V)$ منتظماً فإنه يوجد $S \in A(V)$ بحيث $ST = TS = I$.

البرهان

بما أن T قابل للعكس من اليمين واليسار فإنه يوجد S'', S' في $A(V)$ بحيث $TS' = I$ و $S''T = I$.

الآن $S' = IS' = (S''T)S' = S''(TS) = S''I = S''$ بوضع $S = S' = S''$ نحصل على $TS = ST = I$.

ملاحظة

من الممكن بيان أنه إذا كان $T \in A(V)$ منتظماً فإنه يوجد تحويل خطي وحيد S بحيث يكون $TS = ST = I$ يسمى التحويل S بأنه معكوس T ويرمز له T^{-1} .

مثال 1

ليكن $V = R^2$ اعتبر القاعدة $\{e_1, e_2\}$ للفضاء حيث $e_2 = (0,1), e_1 = (1,0)$ عرف $T \in A(V)$ حسب $T(e_1) = 7e_1$ و $T(e_2) = 3e_2$ ندعي أن T تحويل منتظم . ليكن $S \in A(V)$ معرفاً حسب $S(e_2) = \frac{e_2}{3}, S(e_1) = \frac{e_1}{7}$ عندئذ يمكن بسهولة التحقق من أن $ST = TS = I$ أي أن T منتظم .

مثال 2

ليكن $V = R[x]$ ، الفضاء المنحني لكثيرات الحدود بمعاملات حقيقية . عرف $S, T \in A(V)$ حسب $T[f(x)] = \int_1^x f(t)\,dt \, , S[f(x)] = \frac{d}{dx}[f(x)]$ لكل $f(x) \in R[x]$.

الآن $ST[f(x)] = S\left(\int_1^x f(t)\,dt\right) = f(x) \Rightarrow ST = I$ هذا يبين أن S قابل للعكس من اليمين .

مرة ثانية $$TS[f(x)] = T\left[\frac{d}{dx} f(x)\right] = \int_1^x \left[\frac{d}{dt} f(t)\right] dt = [f(t)]_1^x = f(x) - f(1)$$

بما أن $f(1)\neq 0$ بصورة عامة فإن $TS\neq I$ أي أن S ليس تحويلاً منتظماً (انظر القضية 3.16 والملاحظات) .

تعريف 4.16

يقال للتحويل $T\in A(V)$ أنه مكافئ للتحويل $S\in A(V)$ إذا وجد تحويلان منتظمان $P,Q\in A(V)$ بحيث $T=PSQ$.

تعريف 5.16

يقال عن تحويل $T\in A(V)$ أنه مشابه للتحويل $S\in A(V)$.

إذا وجد تحويل منتظم $P\in A(V)$ بحيث $T=P^{-1}SP$.

فيما تبقى في الفصل (إلا إذا ذكر خلاف ذلك) فإن V هو فضاء متجهي ذو بعد منته $n>0$ على حقل F لقد تبين من نظرية 17.12 أن $A(V)=HomF(V,V)$ عبارة عن جبر ذو بعد n^2 على F .

لتكن $g(x)=\alpha_0+\alpha_1x+\ldots+\alpha_kx^k\in F[x]$ لتحويل خطي $T\in A(V)$ فإن $\alpha_0I+\alpha_1T+\ldots+\alpha_kT^k\in F[x]$ سوف نرمز لـ $\alpha_0I+\alpha_1T+\ldots+\alpha_kT^k$ بالرمز $g(T)$.

تعريف 6.16

يسمى $T\in A(V)$ جذر لكثيرة الحدود $g(x)\in F[x]$ إذا كان $g(T)=\bar{0}$ التحويل الصفري على V .

ملاحظة

لغرض التوافق سوف نستخدم O أو 0 محل $\bar{0}$ وسوف يكون واضحاً من سياق الكلام فيما إذا كان O أو 0 هو المعني به المتجه الصفري أو التحويل الخطي الصفري والصفر القياسي .

نظرية 7.16

لأي تحويل خطي غير صفري $T \in A(V)$ توجد كثيرة حدود واحدية وحيدة $m(x) \in F[x]$ بحيث :

i. $m(T)=0$.

ii. لأي $g(x) \in F[x]$ فإن $g(T)=0$ إذا وفقط إذا كانت $m(x)$ نقسم $g(x)$.

iii. $F[T] \cong \frac{F[x]}{<m(x)>}$.

البرهان

لتكن $F[T]=\{g(T): g(x) \in F[x]\}$ من السهل التحقق من أن $F[T]$ حلقة جزئية من $A(V)$ و $\sigma : F[x] \to F[T]$.

المعرف $\sigma[(x)]=g(T)$ عبارة عن إبيمورفزم حلقة إذاً $F[T] \cong \frac{F[x]}{\ker \sigma}$.

الآن $F[x]$ هي PID عليه $\ker \sigma =< pu,>$ لبعض $p(x) \in F[x]$.

لما كان بُعد $A(V)$ يساوي n^2 فإن العناصر $I, T, T^2, ..., T^{n^2}$ مرتبطة خطياً على F عليه يوجد $\left(0 \le i \le n^2\right)$ في F ليس جميعها صفراً بحيث $\alpha_0 I+\alpha_1 T+\alpha_2 T^2+..\alpha_{n^2} T^{n^2}=0$ بالتالي فإن كثيرة الحدود غير الصفرية $f(x)=\alpha_0+\alpha_1 x+\alpha_{n^2} x \in \ker \sigma$ لذا فإن $\ker \sigma \neq (0)$ ونتيجة لذلك $p(x) \neq 0$ ، $p(x)$ هي كثيرة حدود غير ثابتة لأن $T \neq 0$ إذن $0<\deg g(x)$ عليه يمكننا كتابة $p(x)=\alpha m x$ حيث α هو المعامل القائد لكثيرة الحدود $p(x)$ و $m(x)$ هي كثيرة حدود واحدية ، عندئذ $\ker \sigma =< m(x)>$. الآن حسب تعريف $\ker \sigma$ فإن $m(T)=0$ ولكل $g(x) \in F(x)$ فإن :

$$g(T)=0 \Leftrightarrow g(x) \in \ker \sigma =< m(x)> \Leftrightarrow m(x) | g(x)$$

وبالتالي فإن $m(x)$ تحقق (iii),(ii),(i) لتكن $m'(x)$ كثيرة حدود واحدية أخرى على F تحقق (ii),(i) عندئذ حسب (ii) فإن $m'(x) | m(x)$ و $m(x) | m'(x)$ بالتالي $m'(x)=\beta m(x)$

لبعض $\beta(\neq 0)\in F[x]$ بمقارنة المعامل القائد لكل من الطرفين وملاحظة أن كل من $m'(x), m(x)$ هي كثيرة واحدية نحصل على أن $\beta=1$ عليه فإن $m(x)=m'(x)$ هذا يبرهن واحدنية $m(x)$.

تعريف 8.16

ليكن $T(\neq 0)\in A(V)$ كثيرة الحدود الواحدية $m(x)=x^k-\alpha_1 x^{k-1}...-a_k$ على F تسمى كثيرة الحدود الأصغرية للتحويل T إذا كان :

(i) $m(T)=T^k-\alpha_1 T^{k-1}-\alpha_2 T^{k-2}-..\alpha_0 I=0$ و (ii) لأي $g(x)\in F[x]$ ، فإن $g(T)=0$ إذا وفقط إذا كان $m(x)$ يقسم $g(x)$.

من النظرية 7.16 يتبين أن كثيرة الحدود الأصغرية لتحويل خطي T على V هي كثيرة الحدود الواحدية ذات الدرجة الأصغر من بين كثيرات الحدود التي يكون T جدر لها . في إثبات هذه النظرية لوحظ أن T هو جذر لكثيرة حدود درجتها لا تتجاوز n^2 . في الواقع سوف نجد أنها لا تتجاوز n .

نظرية 9.16

ليكن $T(\neq 0)\in A(V)$ و $S\in A(V)$ قابلاً للعكس فإن T و $S^{-1}TS$ لهما نفس كثيرة الحدود الأصغرية .

البرهان

لأية كثيرة حدود $g(x)=\alpha_0+\alpha_1 x+...+\alpha_k x^k$ نجد أن :

$$g\left(S^{-1}TS\right)=\alpha I+\alpha\left(S^{-1}TS\right)+\alpha_2\left(S^{-1}TS\right)+...+\alpha_k\left(S^{-1}TS\right)^k$$

من ناحية ثانية $\left(S^{-1}TS^m\right)=S^{-1}\overset{m}{T}S$ لكل الأعداد الصحيحة $m\geq 0$ إذاً :

$$\begin{aligned} g\left(S^{-1}TS\right)&=\alpha_0 I+\alpha_1 S^{-1}TS+\alpha_2 S^{-1}T^2 S+...+\alpha_k S^{-1}T^k S \\ &=S^{-1}\left(\alpha_0 I+\alpha_1 T+\alpha_2 T^2+...+\alpha_k T^k\right)S=S^{-1}g(T)S \end{aligned}$$

ومنها يكون $g(T)=0 \Leftrightarrow g\left(S^{-1}TS\right)=0$ عليه إذا كانت $m(x)$ و $m'(x)$ هما كثيرتي الحدود الأصغريتان للتحويلين T و $S^{-1}TS$ على الترتيب ، فإن $m'(T)=\overline{0}, m(T)=0$ ، $m'\left(S^{-1}TS\right)=0$ ، $m\left(S^{-1}TS\right)=0'$ من تعريف كثيرة الحدود الأصغرية فإن $m(x)|m'(x)$ و $m'(x)|m(x)$ بالتالي $m(x)=m'(x)$ لأن كلتاهما واحدية وهذا يكمل البرهان .

لتكن $(v_1, v_2, ..., v_n)$ قاعدة مرتبة للفضاء المنحني V فإن $A(V)\cong M_n(F)$ حلقة المصفوفات من السعة $n\times n$ على F للراسم $\sigma : A(V) \to M_n(F)$ بحيث $\sigma(T)=(\alpha_{ij})\in M_n(F)$ حيث (α_{ij}) هي مصفوفة التحويل T نسبة للقاعدة المرتبة $(v_1, v_2, ..., v_n)$. بما أن σ إيزومورفزم فإنه لكل $g(x)\in F[x]$ ، يكون $g(T)=0$ إذا وفقط إذا $g(A)=0$ حيث $A=(\alpha_{ij})$ إذاً بالأخص يكون $m(A)=0$ حيث $m(x)$ هي كثيرة الحدود الأصغرية للتحويل T .

تعريف 9.16 (a)

يقال أيضاً أن $m(x)$ هي كثيرة الحدود الأصغرية للمصفوفة A .

نظرية 10.16

التحويل الخطي $T: V \to V$ يكون منتظماً إذا وفقط إذا كان الحد الثابت في كثيرة الحدود الأصغرية له تختلف عن الصفر .

البرهان

لتكن $m(x)=x^k-\alpha_1 x^{k-1}-\alpha_2 x^{k-1}-..\alpha_k$ كثيرة الحدود الأصغرية للتحويل T فإن $T^k-\alpha_1 T^{k-1}-...-\alpha_{k-1}T-\alpha_k I=0$ يؤدي إلى أن :

$$T\left(T^{k-1}-\alpha_1 T^{k-2}-...-\alpha_{k-1}I\right)=\left(T^{k-1}-\alpha_1 T^{k-2}-...-\alpha_{k-1}I\right)T=\alpha_k I \quad (1)$$

ليكن T منتظماً فإذا كان $\alpha_k=0$ فإن T^{-1} موجود و (1) يؤدي إلى أن $T^{k-1}-\alpha_1 T^{k-2}-...-\alpha_{k-1}I=0$ ، هذا يناقض حقيقة أن $\deg m(x)=k$ و T لا يمكن أن

يكون جذراً لأية كثيرة حدود غير صفرية على F ذات درجة $k > 0$ لذا $\alpha_k \neq 0$ بالعكس إذا كان $\alpha_k \neq 0$ فإن (1) يؤدي إلى أن $TT' = TT' = I$ حيث $T' = \alpha_k^{-1}\left(T^{k-1} - \alpha_{k-1}I\right)$ بالتالي فإن T منتظم .

نتيجة 11.16

إذا كان $T \in A(V)$ منتظماً فإن T^{-1} هو كثيرة حدود في T على F .

البرهان

إذا كانت $x^k - \alpha_1 x^{k-1} - \alpha_2 x^{k-2} - ... - \alpha_k$ هي كثيرة الحدود الأصغرية للتحويل T على F فإنه وكما رأينا في إثبات النظرية السابقة يكون $\alpha_k \neq 0$ و $T^{-1} = \alpha_k^{-1}\left(T^{k-1} - \alpha_1 T^{k-2} - ... - \alpha_{k-1}I\right)$ كثيرة حدود في T على F .

مثال 3

اعتبر $V = Q^3$ لتكن (e_1, e_2, e_3) قاعدتها القياسية . ليكن $T \in A(V)$ بحيث تكون المصفوفة A المقابلة له بالنسبة لهذه القاعدة هي $A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ عندئذ $A - 2I' = 0$ حيث $I' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ إذاً $T - 2I = 0$ هذا يبين أن T هو جذر لكثيرة الحدود الواحدية $x - 2$.

بما أن كثيرة الحدود الأصغرية للتحويل T هي كثيرة حدود واحدية وهي صاحبة الدرجة الموجبة من بين كثيرات الحدود التي يكون T جذراً لها نحصل على أن $x - 2$ هي كثيرة الحدود الأصغرية للتحويل T .

مثال 4

اعتبر التحويل الخطي $T : Q^3 \to Q^3$ بحيث $T(e_1) = e_2$ ، $T(e_2) = e_3$ ، $T(e_3) = e_1$ حيث (e_1, e_2, e_3) هي القاعدة القياسية للفضاء Q^3 ومصفوفة T نسبة لهذه القاعدة هي :

$$A=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}, A^2=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}, A^3=I'=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

عليه $T^3-I=0$ إذاً كثيرة الحدود الأصغرية $m(x)$ للتحويل T تقسم x^3-1 عندئذ $\deg m(x)\le 3$ والذي يؤدي إلى أن $m(x)=x-\alpha$ فإن $\deg m(x)=1$ إذا كان $\alpha\in Q$ لبعض $m(x)=x-\alpha$ أي أن $A=\alpha I'$ مصفوفة قطرية وهذا تناقض ، لذا فإن $\deg m(x)>1$ إذا كان $A-\alpha I'=0$ $\deg m(x)=2$ فإن $m(x)=x^2-\alpha x-\beta$ لبعض $\alpha,\beta\in Q$ إذاً $A^2-\alpha A-\beta I'=0$ يؤدي إلى أن

$$\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}-\begin{pmatrix}0&0&\alpha\\\alpha&0&0\\0&\alpha&0\end{pmatrix}-\begin{pmatrix}\beta&0&0\\0&\beta&0\\0&0&\beta\end{pmatrix}=\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}$$

أي أن

$$\begin{pmatrix}-\beta&1&-\alpha\\-\alpha&-\beta&1\\1&-\alpha&-\beta\end{pmatrix}=\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}$$

ونحصل على أن $1=0$ وهذا غير مقبول ! بالتالي فإن $\deg m(x)>2$ وحيث أن $m(x)\mid(x^3-1)$ نحصل على أن $\deg m(x)=3$ و $m(x)=x^3-1$ وهكذا فإن x^3-1 هي كثيرة الحدود الأصغرية للتحويل T على Q .

مثال 5

اعتبر الفضاء المتجهي V لجميع كثيرات الحدود على R والتي درجتها لا تتجاوز الثلاث ، ليكن $D:V\to V$ هو مؤثر التفاضل D تحويل خطي (الفصل 12 مثال 1) .

الآن $(1,x,x^2,x^3)$ قاعدة مرتبة للفضاء V لما كان $D(1)=0$ ، $D(x)=1$ ، $D(x^2)=2V$ ، $D(x^3)=3x^2$ فإن مصفوفة D نسبته إلى القاعدة المرتبة هذه هي :

$$A=\begin{pmatrix}0&1&0&0\\0&0&2&0\\0&0&0&3\\0&0&0&0\end{pmatrix}$$

من الممكن التحقق من أن $A^4 = 0$ ، $A^3 \neq 0$ عليه فإن كثيرة الحدود الأصغرية للتحويل D تقسم y^4 . بما أن $A^3 \neq 0$ والعوامل غير الثابتة لـ y^4 هي فقط y, y^2, y^3, y^4 نحصل على أن y^4 هي كثيرة الحدود الأصغرية للتحويل D .

تعريف 12.16

ليكن $T: V \to V$ تحويلاً خطياً فإن :

i. $v \in V$ يسمى متجه ذاتي للتحويل T إذا كان $T(v) = \alpha v$ لبعض $\alpha \in F$.

ii. $\alpha \in F$ يسمى قيمة ذاتية للتحويل T إذا كان $T(v) = \alpha v$ لمتجه غير صفري $v \in V$.

iii. لأي قيمة ذاتية α للتحويل T فإن المتجه $v \in V$ يسمى متجه ذاتي للتحويل T منتهي لـ α إذا كان $T(v) = \alpha v$ مجموعة جميع المتجهات الذاتية المنتمية للقيمة الذاتية α تسمى بالفضاء الذاتي لـ α .

لتكن A مصفوفة ذات سعة $n \times n$ على F و $T: V \to V$ تحويل خطي بحيث أن A هي مصفوفة T نسبة للقاعدة المرتبة $B = (v_1, v_2, ..., v_n)$ للفضاء V . نعني بقيمة ذاتية للمصفوفة A ، قيمة ذاتية للتحويل T إذا كان $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n$ متجهاً ذاتياً للتحويل T فإن المرتب النوني $(\alpha_1, \alpha_2, ..., \alpha_n)$ في F^n يسمى بالمتجه الذاتي للمصفوفة A .

المتجهات الذاتية والقيم الذاتية تسمى أيضاً بالمتجهات المميزة والقيم أو الجذور المميزة على الترتيب .

قضية 13.16

(a) إذا كان v متجهاً ذاتياً غير صفري للتحويل $T \in A(V)$ فإن العنصر $\alpha \in F$ حيث $T(v) = \alpha v$ يكون وحيداً .

(b) لأي قيمة ذاتية α للتحويل T فإن الفضاء الذاتي للقيمة الذاتية α هو فضاء جزئي غير صفري في الفضاء V .

البرهان

(a) ليكن $T(v)=\alpha v$ و $T(v)=\alpha' v$ لبعض $\alpha,\alpha'\in F$ عندئذ $(\alpha-\alpha')v=0$ ولما كان $v\neq 0$ نحصل على $\alpha-\alpha'=0$ أي أن $\alpha=\alpha'$ (قضية 3.11) وهذا يبرهن وحدانية α .

(b) ليكن W_α الفضاء الذاتي لـ α فمن تعريف القيمة الذاتية يوجد $v(\neq 0)\in V$ بحيث أن $T(v)=\alpha v$ وعليه فإن $v\in W_\alpha$ وبالتالي $W_\alpha\neq(0)$. ليكن $v,w\in W_\alpha$ ، $\lambda,\mu\in F$ عندئذ :

$$T(\lambda v+\mu w)=\lambda T(v)+\mu T(w)=\lambda(\alpha v)+\mu(\alpha w)=\alpha(\lambda v+\mu w)$$

إذاً $\lambda v+\mu w\in W_\alpha$ هذا يبرهن أن W_α هو فضاء جزئي من V (نظرية 11.16) .

تعريف 14.16

لكل $\alpha\in F$ ، بعد W_α الفضاء الذاتي لـ α يسمى التكرار الهندسي لـ α .

مثال 6

ليكن $T:Q\to Q$ تحويلاً خطياً بحيث كانت مصفوفة بالنسبة إلى القاعدة القياسية (e_1,e_2,e_3) هي $A=\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}$ عندئذ $T(e_1)=e_1=1e_1$ ، $T(e_2)=e_2=1e_2$ ، $T(e_3)=0=0e_3$ عليه فإن e_1,e_2,e_3 هي جميعها متجهات ذاتية و 0, 1, 1 هي القيم الذاتية المتناظرة .

بالرغم من أن e_1,e_2,e_3 هي مستقلة نجد أن 0, 1, 1 ليست مختلفة . دعنا نعين الفضاءات الذاتية لها ، ليكن W_1 الفضاء الجزئي المنتمي للقيمة الذاتية 1 فإن أي $\alpha e_1+\beta e_2+\delta e_3\in W_1$ إذا وفقط إذا كان

$$T(\alpha e_1+\beta e_2+\delta e_3)=1(\alpha e_1+\beta e_2+\delta e_3)$$

$$\Leftrightarrow\qquad \alpha T(e_1)+\beta T(e_2)+\delta T(e_3)=\alpha e_1+\beta e_2+\delta e_3$$

$$\Leftrightarrow \qquad \alpha e_1 + \beta e_2 = \alpha e_1 + \beta e_2 + \delta e_3 \Leftrightarrow \delta = 0$$

إذاً W_1 هو فضاء جزئية مولد بالمجموعة $\{e_1, e_2\}$ بالمثل فإن الفضاء الجزئي للقيمة الذاتية 0 هو الفضاء الجزئية المولد في $\{e_3\}$.

نظرية 14.16

ليكن $T(\neq 0) \in A(V)$ فإنه :

(a) إذا كان v متجهاً ذاتياً للتحويل T و $\alpha \in T$ بحيث $T(v) = \alpha v$ فإنه لأي $f(x) \in F[x]$ فإن v هو متجه ذاتي لـ $f(T)$ وأن $[f(T)](v) = f(\alpha)v$.

(b) إذا كانت $\alpha_1, \alpha_2, ..., \alpha_m$ قيم ذاتية مختلفة للتحويل T و $v_1, v_2, ..., v_n$ متجهات ذاتية غير صفرية تنتمي إلى $\alpha_1, \alpha_2, ..., \alpha_m$ على الترتيب فإن $v_1, v_2, ..., v_m$ مستقلة خطياً على F .

البرهان

(a) الآن :

$$T(v) = \alpha v \Rightarrow T^2(v) = T(Tv) = T(\alpha v) = \alpha T(v) = \alpha(\alpha v) = \alpha^2 v$$
$$T^3(v) = T\left[T^2(v)\right] = T\left(\alpha^2 v\right) = \alpha^2 T(v) = \alpha^2(\alpha v) = \alpha^3 v$$

بصورة عامة لأي عدد صحيح موجب k يكون $T^k(v) = \alpha^k v$.

عندئذ لأي $f(x) = \beta_0 + \beta_1 x + ... + \beta_m x^m F(x)$ فإن :

$$\begin{aligned}
[f(T)](v) &= \left(\beta_0 I + \beta_1 T + ... + \beta_m T^m\right)(v) \\
&= \beta_0 v + \beta_1 T(v) + \beta_2\left[T^2(v)\right] + ... + \beta_m\left[T^m(v)\right] \\
&= \beta_0 v + \beta_1(\alpha v) + \beta_2\left(\alpha^2 v\right) + ... + \beta_m\left(\alpha^m v\right) \\
&= \left(\beta_0 + \beta_1\alpha + ... + \beta_m\alpha^m\right)(v) = f(\alpha)v
\end{aligned}$$

هذا يبرهن (a) .

(b) إذا كان $m = 1$ فإن النتيجة تكون مباشرة أي متجه غير صفري يكون دائماً مستقلاً خطياً . نطبق الاستنتاج الرياضي على m . عليه افرض أن $m > 1$ والنتيجة محققة

لعـدد $m-1$ مـن المتجهـات الذاتيـة حسـب فـروض الاسـتنتاج فـإن المتجهـات $v_1, v_2, ..., v_{m-1}$ مسـتقلة خطيـاً علـى F كـذلك المتجهـات $v_2, v_3, ..., v_m$ مسـتقلة خطياً .

افرض أن المتجهـات $v_1, v_2, ..., v_m$ مرتبطة خطيـاً على F عندئذ فإنـه يوجـد $\beta_i \,(1 \le i \le m)$ ليس جميعها صفراً بحيث :

$$\beta_1 v_1 + \beta_2 v_2 + ... + \beta_m v_m = 0 \qquad (1)$$

إذا كان $\beta_m = 0$ فإن الاستقلالية الخطية للمجموعة $\{v_i\}_{1 \le i \le m-1}$ تؤدي إلى أن $\beta_i = 0$ لكل $i = 1, 2, ..., m-1$ هـذا يتناقض حقيقـة كون العناصر $\beta_i \,(1 \le i \le m)$ ليست جميعهـا أصفاراً ، عليه افرض أن $\beta_m \ne 0$ بتأثير T على (1) نحصل على أن :

$$\beta_1 T(v_1) + \beta_2 T(v_2) + ... + \beta_m T(v_m) = 0$$

من ناحية ثانية $T(v_i) = \alpha_i v_i, \,(1 \le i \le m)$

إذاً :

$$\beta_1 \alpha_1 v_1 + \beta_2 \alpha_2 v_2 + ... + \beta_m \alpha_m v_m = 0 \qquad (2)$$

بمـا أن $\beta_m \ne 0$ و $\alpha_m \ne \alpha_1$ فـإن المعامـل $\beta_m(\alpha_m - \alpha_1)$ للمتجـه v_m يختلـف عـن الصـفر إذاً حسـب (3) تكـون المتجهـات $v_2, v_3, ..., v_m$ مرتبطـة خطيـاً ، هـذا ينـاقض كـون المتجهـات $v_1, v_2, v_3, ..., v_m$ مستقلة خطياً .

نتيجة 15.16

التحويل الخطي T للفضاء المتجهي V لا يمكن أن يكون له أكثر من n من القيم الذاتية المختلفة حيث $n = \dim V$.

البرهان

كما رأينا في النظرية السابقة فإنه لأي m من القيم الذاتية المختلفة للتحويل T فإن المتجهات الذاتية المناظرة له وعددها m تكون مستقلة خطياً ، وبما أن $\dim V = n$ فإن V لا يحوي أكثر من n من المتجهات المستقلة خطياً وبالتالي فإن $m \le n$.

نتيجة 16.16

لتكن $\alpha_1,\alpha_2,...,\alpha_m$ قيم ذاتية مختلفة لتحويل خطي $T:V\to V$ إذا كانت $W_1,W_2,...,W_m$ فضاءات جزئية منتهية إلى $\alpha_1,\alpha_2,...,\alpha_m$ على الترتيب ، فإن المجموع $W_1+W_2+...+W_m$ هو مجموع مباشر .

البرهان

افرض أن $v_1+v_2+...+v_m=0$ لبعض $(1\le i\le m)$ ندعي أن جميع المتجهات v_i صفرية . لنفرض أن ادعاءنا غير صحيح فبإهمال المتجهات الصفرية من بين هذه المتجهات نحصل على :

$$v_{i1}+v_{i2}+..v_{it}=0 \qquad (1)$$

حيث $v_{ij}\ne 0$ لكل $1\le j\le t$ إذاً هذه المتجهات مرتبطة خطياً بالرغم من أن القيم الذاتية المناظرة α_{ij} حيث $(1\le j\le t)$ جميعها مختلفة وهذا يخالف النظرية السابقة . إذاً جميع المتجهات السابقة v_i صفرية . هذا يبرهن أن $W_1+W_2+...+W_m$ هو مجموع مباشر .

نظرية 17.16

إذا كان التحويل الخطي $T:V\to V$ له n في القيم الذاتية المختلفة $\alpha_1,\alpha_2,...,\alpha_n$ فإن للفضاء V قاعدة مرتبة $(v_1,v_2,...,v_n)$ تجعل مصفوفة T نسبة لهذه القاعدة هي :

$$\begin{pmatrix} \alpha_1 & 0 & 0 & ... & 0 \\ 0 & \alpha_2 & 0 & ... & 0 \\ ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & \alpha_n \end{pmatrix}$$

البرهان

ليكن v_i متجهاً ذاتياً للتحويل T ينتمي للقيمة الذاتية $(1\le i\le n)\alpha_i$ حسب نظرية 14.16 فإن المتجهات $v_1,v_2,...,v_n$ مستقلة خطياً على F إذاً $B=(v_1,v_2,...,v_n)$ هي قاعدة مرتبة للفضاء V (نتيجة 24.11) .

بما أن $T(v_i)=\alpha_i v_i$ لكل $i=1,2,...,n$ فإن مصفوفة T نسبة إلى B تساوي :

$$\begin{pmatrix} \alpha_1 & 0 & 0 & \dots & 0 \\ 0 & \alpha_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \alpha_n \end{pmatrix}$$

وهذا يكمل البرهان .

تعريف 18.16

يقال للتحويل $T \in A(V)$ إنه تحويل صفر (غير منفرد) إذا كان $\ker T$ يختلف عن الصفر (يساوي الصفر) .

ملاحظة

لفضاء متجهي منته البعد ، التحويل T غير منفرد وهذا إذا كان T تحويلاً منتظماً. النظرية التالية ذات شأن في تعيين القيم الذاتية .

نظرية 19.16

العنصر $\alpha \in F$ هو قيمة ذاتية إذا وفقط إذا كان $T-\alpha I$ منفرداً .

البرهان

لتكن α قيمة ذاتية للتحويل T يوجد $v(\neq 0)\in V$ بحيث $T(v)=\alpha v$ هذا يعطي أن $(T-\alpha I)V=T(v)-\alpha v=0$ عليه $v(\neq 0)\in \ker(T-\alpha I)$ أي أن $T-\alpha I$ منفرد .
بالعكس إذا كان $T-\alpha I$ منفرداً فإن $\ker(T-\alpha I)\neq(0)$ ومنها يتبين وجود $V(\neq 0)\in \ker(T-\alpha I)$ وعندئذ $(T-\alpha I)V=0 \Rightarrow T(v)=\alpha v$ يؤدي إلى أن α قيمة ذاتية للتحويل T .

نتيجة 20.16

إذا كان $T \in A(V)$ تحويلاً منفرداً فإن الصفر 0 هو دائماً قيمة ذاتية للتحويل T .

البرهان

بما أن $T - 0I = T$ منفرد فإن النتيجة تتبع في النظرية السابقة .

سوف نبين لاحقاً كل جذر لكثيرة الحدود الأصغرية لتحويل خطي T هو قيمة ذاتية للتحويل T . هنا نبرهن عكس العبارة المذكورة .

نظرية 21.16

كل قيمة ذاتية للتحويل $T \in A(V)$ هي جذر لكثيرة الحدود الأصغرية للتحويل T.

البرهان

لتكن $m(x)$ كثيرة الحدود الأصغرية للتحويل T وليكن $\alpha \in F$ قيمة ذاتية للتحويل T ، عندئذ لعنصر غير صفري $T(v) = \alpha v, v \in V$ استناداً إلى القضية 13.16 فإن $[f(T)](v) = f(\alpha)v$ لكل $f(x) \in F[x]$ بالأخص $[m(T)]v = m(\alpha)v$ هذا يؤدي إلى أن $m(\alpha)v = 0$ لأن $m(T) = 0$ وحيث أن $v \neq 0$ فإن $m(\alpha) = 0$ أي أن α جذر كثيرة الحدود الأصغرية للتحويل T .

الآن نناقش بعض الأمثلة الإضافية .

مثال 7

ليكن V الفضاء المتجهي لجميع كثيرات الحدود على Q التي درجتها لا تتجاوز 3، ليكن D المؤثر التفاضلي على V (مثال 5) افرض $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3$ متجه ذاتي للتحويل D فإنه لبعض $\alpha \in Q$ ، $Df(x) = \alpha f(x)$.

أي أن $\alpha_1+2\alpha_2x+3\alpha_3x^2=\alpha\left(\alpha_0+\alpha_1x+\alpha_2x^2+\alpha_3x^3\right)$

بمقارنة المعاملات نحصل على $\alpha_1=\alpha\alpha_0$ ، $2\alpha_2=\alpha\alpha_1$ ، $3\alpha_3=\alpha\alpha_2$ ، $0=\alpha\alpha_3$ عليه إذا كان $\alpha\neq 0$ فإن هذه المعادلات تعطينا $\alpha_3=0=\alpha_2=\alpha_1=\alpha_0$ أي أن $f(x)=0$ بالتالي لا يوجد عدد نسبي يختلف عن الصفر هو قيمة ذاتية لـ D ، إذا كان $\alpha=0$ نحصل في المعادلة السابقة أن $\alpha_1=0$ ، $\alpha_2=0$ ، $\alpha_3=0$ إذاً $f(x)\alpha_0$ ، α_0 ثابت ، بالتالي كل كثيرة حدود ثابتة هي متجه ذاتي لـ D .

الآن $D^2f(x)=2\alpha_2+6\alpha_3x$ إذا كانت $f(x)$ متجه ذاتي بالنسبة لـ D^2 ، عليه فإن $D^2f(x)=\alpha f(x)$ لبعض $\alpha\in F$ ، أي أن

$$2\alpha_2+6a_3x=\alpha(\alpha_0+\alpha_1x+\alpha_2x^2+\alpha_3x^3)$$

بمقارنة المعاملات نحصل على

$$\begin{aligned}2\alpha_2&=\alpha\alpha_0,\\6\alpha_3&=\alpha\alpha_1,\\0&=\alpha\alpha_2,\\0&=\alpha\alpha_3\end{aligned}$$

إذا كانت $\alpha\neq 0$ عليه فإن هذه المعادلات صالحة إذا كانت (كما ورد سابقاً) $f(x)=0$.

إذا كانت $\alpha=0$ ، فإننا نحصل على $\alpha_3=\alpha_2=0$

عليه $f(x)=\alpha_0+\alpha_1x$

هكذا D^2 تكون ليست ذات قيمة صغيرة ولكن تكون فقط ذات قيمة صغيرة إذا كانت D^2 من درجة أصغر من أو تساوي 1 .

مثال 8

اعتبر أن $V=R^2$ ، ولتكن (e_1,e_2) قاعدة أساسية ، وكذلك $T\in A(V)$ تعطى بالمعادلة التالية $T(e_1)=e_1+e_2$ و $T(e_2)=e_1-e_2$. افترض أن $V=\alpha_1e_1+\alpha_2e_2$ متجه ذاتي بالنسبة لـ T ولتكن لمجموع $\alpha\in F,$

$$T(\alpha_1e_1+\alpha_2e_2)=\alpha(\alpha_1e_1+\alpha_2e_2),$$

عليه $\alpha_1(e_1 + e_2) + \alpha_2(e_1 - e_2) = \alpha\alpha_1 e_1 + \alpha\alpha_2 e_2$

بمقارنة معاملات e_1, e_2 فإننا نحصل على :

$\alpha_1 + \alpha_2 = \alpha\alpha_1$ أي أن

$$\alpha_1(1-\alpha)+\alpha_2 = 0 \qquad (1)$$

$\alpha_1 - \alpha_2 = \alpha\alpha_2$ أي أن :

$$\alpha_1 - \alpha_2(1+\alpha) = 0 \qquad (2)$$

بضرب (2) في $(1-\alpha)$ وطرحها من (1) نجد أن :

$$\alpha_2\left(2-\alpha^2\right) = 0 \qquad (3)$$

عليه فإذا كان $\alpha \neq \pm\sqrt{2}$ فإن $\alpha_2 = 0$ و (2) يؤدي إلى أن $\alpha_1 = 0$ عليه فإن $v = 0$ بالتالي إذا كان $\alpha = \sqrt{2}$ ، (2) يؤدي إلى أن $\alpha_2 = \dfrac{\alpha_1}{1+\sqrt{2}}$ فبأخذ $\alpha_1 = 1$ نجد أن $v = e_1 + \dfrac{1}{1+\sqrt{2}} e_2$ هو متجه ذاتي غير صفري للتحويل T حيث $T(v) = \sqrt{2}v$ إذاً $\sqrt{2}$ هو قيمة ذاتية للتحويل T و $v_1 = e_1 + \dfrac{1}{1+\sqrt{2}} e_2$ هو متجه ذاتي ينتمي إلى $\sqrt{2}$.

إذا كان $\alpha = \sqrt{2}$ فإن $v_2 = \dfrac{1}{1-\sqrt{2}} v_1$ كما له خاصة فإن $-\sqrt{2}$ هو أيضاً قيمة ذاتية للتحويل T وأن $v_2 = e_1 - \dfrac{1}{1-\sqrt{2}}$ هو متجه ذاتي للتحويل T ينتمي إلى $-\sqrt{2}$ عليه فإن للتحويل T قيمتان ذاتيتان هما $\sqrt{2}$ و $-\sqrt{2}$ وحسب نتيجة 15.16 وحقيقة أن $\dim V = 2$ فإنه لا يمكن أن يكون للتحويل T أية قيم ذاتية أخرى ، نترك للقراء التحقق من أن $\{v_1, v_2\}$ مجموعة جزئية مستقلة خطياً وهكذا فإن $B = (v_1, v_2)$ هي قاعدة مرتبة للفضاء V . بما أن $T(v_2) = -\sqrt{2}v_2, T(v_1) = \sqrt{2}v_1$.

عليه فإن $\begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}$ هي مصفوفة T نسبة إلى B (انظر نظرية 16-17) .

نظرية 22.16

كثيرة الحدود الأصغرية للتحويل $T \in A(V)$ ذات درجة أصغر من أو تساوي n .

البرهان*

نطبق الاستنتاج على $\dim V = n$ إذا كان $n = 1$ فإنه لأي متجه غير صفري $v \in V$ يكون $V = Fv$ لذا فإن $T(v) = \alpha v$ لبعض $\alpha \in F$ هذا بدوره يؤدي إلى أن $(T - \alpha I)v = 0$ ، بما أن $\{v\}$ قاعدة للفضاء (V) نحصل على أن $T - \alpha I = 0$ ، بعبارة أخرى $x - \alpha$ هي كثيرة الحدود الأصغرية للتحويل T ، لما كانت درجة $x-1$ هي 1 فإن النظرية محققة عندما $n = 1$.

الآن افرض أن $n > 1$ والنظرية محققة لجميع الفضاءات المتجهة W ذات الأبعاد أصغر من n . ليكن $\dim V = n$ و $v(\neq 0) \in V$ فإن المتجهات $v, T(v), T^2(v), ..., T^n(v)$ التي عددها $n+1$ مرتبطة خطياً على F ، عليه يوجد $\alpha_i \in F$ ، $0 \le i \le \alpha_n$ ليس جميعها أصفاراً بحيث

$$\alpha_0 v + \alpha_1 T(v) + \alpha_2 T^2(v) + ... + \alpha_n T^n(v) = 0$$

من الواضح أن درجة كثيرة الحدود $f(x) = \alpha_0 + \alpha_1 x + ... + \alpha_n x^n$ أقل أو تساوي n وأن $[f(T)]v = 0$.

إذا كان $[f(T)]v = 0$ لكل $v \in V$ نحصل على أن $f(T) = 0$ وعليه $m(x) | f(x)$ حيث $m(x)$ هي كثيرة الحدود الأصغرية للتحويل T ومنها نحصل على أن $\deg m(x) \le n$ وهكذا فإن الحالة الوحيدة المتبقية للمناقشة هي عندما $[f(T)]V \neq (0)$. نفرض $W = \{v \mid [f(T)]v = 0\}$. W هو فضاء جزئي فعلي غير صفري في V .

افرض $dem W = k$ فإن $1 \le k < n$ ، ليكن T_1 مقصور T على W . بما أن لأي $w \in W$

$$\begin{aligned} & [f(T)]w = 0 \Rightarrow f(T)[T(w)] = [Tf(T)](w) = 0 \\ \Rightarrow \quad & T(w) \in W \Rightarrow T_1(w) \in W \Rightarrow T_1 \in A(w) \end{aligned}$$

* هذا البرهان يعود إلى *M.D.Burrow The Amer.Math.Monthly.December 1973* .

حسب فروض الاستنتاج فإن درجة $m_1(x)$ كثيرة الحدود الأصغرية للتحويل T_1 هي أقل أو تساوي k .

مرة أخرى اعتبر فضاء القسمة V/W .

بما أن $k \geq 1$ فإن $\dim V/W = n-k < n$ عرف $T_2 : v/W \to V/W$ كالآتي :

$$T_2(v+W) = T(v)+W, \forall v \in V$$

بما أنه لأي عنصرين $v, v' \in V$ ، $v+W = v'+W \Rightarrow v-v' \in W \Rightarrow T(v-v') \in W$

$$\Rightarrow \quad T(v)+W = T(v')+w$$

فإن T_2 معرف تعريفاً جيداً ، ويمكن التحقق بسهولة من أن $T_2 \in A(V/W)$. مرة أخرى من فروض الاستنتاج درجة $m_2(x)$ كثيرة الحدود الأصغرية للتحويل T_2 هي أصغر من أو تساوي $n-k$.

الآن $\quad m_2(T_2)(V/W) = \bar{0} \Rightarrow m_2(T)V \subseteq W$

عليه $\quad m_1(T)[m_2(T)V] \subseteq m_1(T)W = m(T_1)W = 0$

$$\Rightarrow \quad [m_1(T)m_2(T)]V = (0)$$
$$\Rightarrow \quad m(x) \mid m_1(x)m_2(x)$$
$$\Rightarrow \quad \deg m(x) \leq \deg m_1(x) + \deg m_2(x)$$
$$\Rightarrow \quad \deg m(x) \leq k+n=n$$

أي أن النظرية محققة للفضاءات المتجهة التي أبعادها n أيضاً .

مسائل

1. أوجد كثيرات الحدود الأصغرية لكل من المصفوفات الآتية على Q ، وإذا كانت أية واحدة منها غير منفردة أوجد معكوسها :

$$\begin{pmatrix} 2 & 0 & 0 \\ -1 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ ، } \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -2 & 3 \end{pmatrix} \text{ ، } \begin{pmatrix} 3 & -3 \\ -2 & 2 \end{pmatrix} \text{ ، } \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} .$$

[**إرشاد** : استخدم طريقة مشابهة لما في نظرية 22.16 للمصفوفات] .

2. برهن أن كثيرة الحدود الأصغرية للمصفوفة $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & -1 & 0 & 3 \end{pmatrix}$ هي $x^4 - 3x^3 + x - 1 = 0$

3. كون تحويلاً خطياً T على فضاء متجهي ثنائي البعد V على Q بحيث تكون كثيرة الحدود الأصغرية له هي $x^2 + 1$ ليكن A مصفوفة T نسبة لقاعدة مرتبة ما للفضاء V أوجد قيمة ذاتي للمصفوفة A معتبراً A كمصفوفة على C .

4. ليكن $A = (\alpha_{ij})$ مصفوفة سعتها $n \times n$ على F :

i. برهن أن أي $(\alpha_1, \alpha_2, ..., \alpha_n) \in F^{(n)}$ هو متجه ذاتي للمصفوفة A إذا وفقط إذا كان لبعض $\alpha \in F$ ، $\alpha(\alpha_1, \alpha_2, ..., \alpha_n) = (\alpha_1, \alpha_2, ..., \alpha_n)A$.

ii. لأي قيمة ذاتية α للمصفوفة A ، مجموعة المتجهات الذاتية للمصفوفة A المنتمية إلى α عبارة عن فضاء جزئي في $F^{(n)}$.

5. عين القيم الذاتية والمتجهات الذاتية لكل من المصفوفات المعطاة في المسألة (1) .

6. باستخدام نظرية 44.12 برهن أنه إذا كانت A مصفوفة $n \times n$ على حقل F لها n من القيم الذاتية المختلفة في F ، فإن A تشبه مصفوفة قطرية على F ، أي أنه توجد مصفوفة غير منفردة B في $M_n(F)$ بحيث تكون $B^{-1}AB$ مصفوفة قطرية .

7. ليكن $T \in A(V)$ ولتكن $\alpha_1, \alpha_2, ..., \alpha_n$ جميع قيمها الذاتية المختلفة ، افرض أن بعد الفضاء الذاتي لكل α_i هو 1 . برهن أن للفضاء V قاعدة مرتبة $(v_1, v_2, ..., v_n)$ بحيث تكون مصفوفة T بالنسبة إلى هذه القاعدة على الشكل $\begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_n \end{pmatrix}$ حيث A مصفوفة سعتها $kx(n-k)$ و V مصفوفة سعتها $(n-k)\times(n-k)$ و 0 هي المصفوفة الصفرية ذات السعة $(n-k)xk$.

8. بين أن القيم الذاتية للمصوفة $\begin{pmatrix} 3 & 2 & 5 \\ 0 & 10 & 9 \\ 0 & 0 & 6 \end{pmatrix}$ هي 10,3 و 6 على Q . حدد الفضاء الذاتي لكل من هذه القيم الذاتية تحقق من أن المجموع المباشر لهذه الفضاءات الذاتية هو Q^3 نفسه .

[**إرشاد** : استخدم نتيجة 16.16] .

9. ليكن $T \in A(v)$ بحيث $T^2 = T$ برهن أن $V = W_1 \oplus W_2$ حيث W_1, W_2 هما فضاءان جزئيان يحققان $T(W_1) = (0)$ و $T(w_2) = w_2$ لكل $w_2 \in W_2$.

10. اثبت أن التحويل $T \in A(V)$ منفرداً إذا وفقط إذا كان يوجد $S \in A(V)$ ، $S \neq 0$ بحيث $ST = TS = 0$.

11. برهن أنه $T \in A(V)$ قابل للعكس من اليمين إذا وفقط إذا كان قابلاً للعكس من اليسار (V فضاء منته البعد) هل النتيجة هذه صحيحة في الفضاءات المتجهة التي أبعادها غير منتهية ؟ [الجواب لا] .

12. ليكن V أي فضاء متجهي على C و $T \in A(V)$ يحقق $T^3 = T$. برهن $V = W_1 \oplus W_2 \oplus W_3$ حيث لكل $w_1 \in W_1$ ، $w_2 \in W_2$ ، $w_3 \in W_3$ ، $T(w_1) = 0$ ، $T(w_2) = w_2$ ، $T(w_3) = w_3$.

13. إذا كان مميز $F(char)=0$ برهن أن أي تحويل $T\in A(V)$ يمكن كتابته كمجموع تحويلين منتظمين .

14. تعريف يسمى الفضاء الجزئي W من الفضاء V أنه لا متغير تحت التحويل $T\in A(V)$ إذا كان $T(w)\subseteq W$.

ليكن S تحويل إسقاط على V و $T\in A(V)$ برهن أن $S(V)$ لا متغير تحت T إذا وفقط إذا كان $STS=TS$ واثبت أن كلاً من $S(V)$ و $\ker S$ لا متغير تحت T إذا وفقط إذا كان $ST=TS$.

15. برهن أن تحويلاً خطي غير صفري $T\in A(V)$ يكون منتظم إذا وفقط إذا كلما كان $V=W_1\oplus W_2$ حيث W_1,W_2 فضاءان جزئيان في V فإن $T(V)=T(W_1)\oplus T(W_2)$.

16. اعتبر IR^2 عرف $T\in A(IR^2)$ حسب $T(e_1)=2e_1$ ، $T(e_2)=e_1+2e_2$ حيث (e_1,e_2) هي القاعدة القياسية للفضاء IR^2 إذا كان W_1 الفضاء الجزئي في IR^2 المولد بـ e_1 .

a. برهن أن W_1 لا متغير تحت T .

b. برهن أنه لا يوجد أي فضاء جزئي W_2 في IR^2 يكون لا متغير تحت T وله الخاصية $IR^2=W_1\oplus W_2$.

2- معلومات إضافية حول كثيرات الحدود الأصغرية

كما في البند السابقة فإن V هو فضاء متجهي ذو بعد n على حقل F . ليكن $T(\neq 0)\in F[T]$ وكما نعلم فإن $F[T]$ حلقة جزئية من $A(V)$ لأي $\alpha\in F$ و $f(T)=\alpha_0 I+\alpha_1 T+...+\alpha_k T^k\in F[T]$ ، $\alpha_i\in F$ يكون :

$$\alpha f(T)=\alpha\alpha_0 I+\alpha\alpha_1 T+...+\alpha\alpha_k T^k\in F[T]$$

عليه فإن $F[T]$ هو فضاء جزئي من $A(V)$ ولما كان $dem_F A(V)=n^2$ ، $dem_F F[T]\leq n^2$ الآن لدينا الآتي :

قضية 23.16

إذا كانت درجة كثيرة الحدود الأصغرية $m(x)$ للتحويل T هي k فإن :

i. $\{1,T,T^2,...,T^{k-1}\}$ تشكل قاعدة للفضاء $F[T]$ على F .

ii. بعد $F[T]$ على F يساوي k .

البرهان

i. لتكن $m(x)=x^k-\alpha_1 x^{k-1}-\alpha_2 x^{k-2}-...-\alpha_n$ الآن $m(T)=0$ يؤدي إلى أن :

$$T^k=\alpha_1 T^{k-1}+\alpha_2 T^{k-2}+...+\alpha_k I \qquad (1)$$

$$T^{k+1}=T^kT=\alpha_1 T^k+\alpha_2 T^{k-1}+...+\alpha_k T$$

$$=\alpha_1\left(\alpha_1 T^{k-1}+\alpha_2 T^{k-1}+...+\alpha_k I\right)+\alpha_2 T+...+\alpha_k T \qquad (2)$$

من (2) يتضح أن T^{k+1} تركيب خطي في $I,T,T^2,...,T^{k-1}$.

مرة أخرى بضرب (2) في T والتعويض بقيمة T^k في (1) نحصل على أنه T^{k+2} أيضاً تركيب خطي في $I,T,T^2,...,T^{k-1}$ وبالاستنتاج نتوصل إلى أن كل $T^\ell(\ell\geq k)$ هو تركيب خطي في $I,T,T^2,...,T^{k-1}$ بما أن كل $f(T)=\lambda_0 I+\lambda_1 T+...+\lambda_5 T^5$ هو تركيب خطي في $I,T,T^2,...,T^5$ فإنه إذا كان $s>k-1$ فبالتعويض عن كل $T^\ell(\ell\geq k)$ بدلالة

$I,T,T^2,...,T^{k-1}$ نحصل على أن $f(T)$ هو تركيب خطي في $I,T,T^2,...,T^{k-1}$ إذاً $F[T]$ كفضاء متجهي على F مولد بالعناصر $I,T,T^2,...,T^{k-1}$ فلو كانت هذه العناصر مرتبطة خطياً على F فإنه لبعض $\beta_i(0 \le i \le k-1)$ ليست جميعها أصفاراً يكون لدينا :

$$\beta_0 I + \beta_1 T + ... + \beta_{k-1} T = 0$$

عليه فإن T هو جذر لكثيرة حدود غير صفرية على F درجتها أصغر من k ، حيث $\deg m(x) = k$ هذا يناقض نتيجة نظرية 7.16 بالتالي فإن $I,T,T^2,...,T^{k-1}$ مستقلة خطياً على F وتكون المجموعة $\{I,T,T^2,...,T^{k-1}\}$ قاعدة للفضاء $F[T]$.

(ii) ينتج مباشرة من (i) .

ملاحظة

على سبيل المثال في مثال 3 فإن $x-2$ هي كثيرة الحدود الأصغرية للتحويل الخطي T على Q^3 . بما أن درجة $x-2$ تساوي واحد نحصل على أن $\dim_Q Q[T]=1$ لكن Q قابل للغمر في $Q[T]$ عليه فإن $Q \cong Q[T]$ كحلقتين (بالتالي كحقلين) .

في مثال 4 كثيرة الحدود الأصغرية للتحويل الخطي T على Q^3 هي x^3-1 عليه يكون $\{I,T,T^2\}$ هي قاعدة للفضاء $Q[T]$ على Q . لاحظ أنه لكون x^3-1 غير قابلة للتحليل على Q فإن كثيرة الحدود الأصغرية لتحويل خطي ما ليست بالضرورة غير قابلة للتحليل (انظر نظرية 18.13) .

نظرية 24.16

إذا كان $T \in A(V)$ و $m(x)$ كثيرة الحدود الأصغرية للتحويل T على F فإنه لأي متجه غير صفري $v \in V$ يكون :

a. $F[T]v = \{[f(T)](v) | f(T) \in F[T]\}$ عبارة عن فضاء جزئي غير صفري في V يحوي المتجه v .

b. توجد كثيرة حدود واحدة فقط واحدية غير صفرية $m_v(x)$ على F بحيث :

i. $[m_v(T)](v)=0$.

ii. لأي $f(x)\in F[x]$ ، $[f(T)]v=0 \Rightarrow m_v(x)|f(x)$.

iii. $m_v(x)|m(x)$.

iv. $\deg m_v(x)=\dim_F F[T]v$ في الواقع $\{v,T(v),T^2(v),...,T^{t-1}(v)\}$ قاعدة للفضاء $F[T]v$ حيث $t=\deg m_v(x)$.

البرهان

a. من الواضح أن $0\in F[T]v$ كذلك لأي $[g(T)]v\in F[T]_v$ و $[f(T)]v$ و $\alpha\in F$ فإن :

$$[F(T)]v-[g(T)]V=[f(T)-g(T)]v\in F[T]v$$

وأن $\alpha[f(T)v]=[\alpha f(T)]v\in F[T]v$ ومنها ينتج أن $F[T]v$ فضاء جزئي في V .

بما أن $I\in F[T]$ فإن $v=Iv\in F[T]v$ وحيث أن v يختلف عن الصفر فإن $F[T]v$ فضاء جزئي غير صفري في V .

b. ليكن $W=\{f(x)|[f(T)]v=0\}$. بما أن $m(T)=0$ ، $m(x)\in W$ عليه فإن W مجموعة جزئية غير خالية في $F[x]$.

الآن لأي $f(x),g(x)\in W$ و $h(x)\in F[x]$ فإن $[f(T)](v)=0$ و $[g(T)](v)=0$ يؤدي إلى أن

$$[f(T)-g(T)](v)=[f(T)]v-[g(T)](v)=0$$

$$[h(T)][f(T)](v)=h(T)[f(T)](v)=0$$

بالتالي فإن $f(x)-g(x)\in W$ و $h(x)f(x)\in W$ بما أن $F[x]$ حلقة إبدالية $f(x)h(x)\in W$ إذاً W مثالي في $F[x]$ يختلف عن الصفر [تذكر أن $m(x)(\neq 0)\in W$.

لذا فإن W يتولد في كثيرة حدود واحدية وحيدة ولتكن $m_v(x)$.

هذا النوع من المنافسة قد استخدم سابقاً على سبيل المثال انظر نظرية 7.16 وهكذا فإن (i) قد برهنت كما في نظرية 7.16 فإن تعريف $m_v(x)$ يعطينا (ii) مباشرة ، بما أن $[m(T)]v=0$ فإن $(ii)\Rightarrow(iii)$.

وأخيراً ليكن $\deg m_v(x)=t$ فإنه لبعض $\lambda_i\in F$ يكون $m_v(x)=x^t-\lambda_{t-1}x^{t-1}-\lambda_{t-2}x^{t-2}---\lambda_0=0$.

أي أن $[m_v(T)]v=0$ يؤدي إلى أن $(T^t)v=\lambda_{t-1}T^{t-1}(v)+\lambda_{t-2}T^{t-2}(v)+...+\lambda_0 v$

باستخدام منافستان مشابهة لتلك التي في القضية السابقة نستنتج أن $\{v,T(v),..T^{t-1}(v)\}$ قاعدة للفضاء $F[T]v$ إذاً $\dim_F F[T]v=\deg m_v(x)$ بالتالي فإن (iv) برهنت .

هذه النظرية تحثنا على الآتي :

تعريف 25.16

ليكن T تحويلاً خطياً غير صفري على V لكل متجه غير صفري $v\in V$ ، كثيرة الحدود الواحدية $m(x)$ على F تسمى كثيرة الحدود الأصغرية للمتجه v نسبة إلى T إذا كان $[m_v(T)](v)=0$ ولكل $f(x)\in F[x]$ فإن $[f(T)]w=0$ يؤدي إلى أن $m_v(xs)$ يقسم $f(x)$.

ملحوظة

$\deg m_v(x)\geq 1$ لكل $v(\neq 0)\in V$.

تعريف 26.16

ليكن T تحويلاً خطياً على V يختلف عن الصفر .

لأي $v\in V$ المثالي $W=\{f(x)\in F[x]\| f(T)v=0\}$ في $F[x]$ يسمى المثالي المعدم للعنصر v بالنسبة إلى T .

من الواضح أن $m_v(x)$ مولد للمثالي W المعدم للعنصر v ، بذلك نجد أن كثيرة الحدود الأصغرية $m_v(x)$ للعنصر v نسبة إلى T هي عامل لكثيرة الحدود الأصغرية $m(x)$ للتحويل T وليس لكثيرة حدود غير صفرية $f(x)$ درجتها أقل من درجة $m_v(x)$ و $[f(T)](v)=0$ نحن نعتبر $m_v(x)$ لكل $v(\neq 0)\in V$ ولنفرض أن $m_1(x)$ هو المضاعف المشترك الأصغر لها . بما أن كل $m_v(x)$ هو عامل في $m(x)$ فإن $m_1(x)|m(x)$ و $[m_1(T)]v=0$ لكل $v\in V$ بذلك فإن $m_1(T)=0$ وبالتالي فإن $m(x)|m_1(x)$ إذاً $m_1(x)=m(x)$ ، المضاعف المشترك الأصغر لجميع $m_v(x)$ (لجميع $v(\neq 0)\in V$) .

ملحوظة

لما كان $m_v(x)|m(x)$ لكل $v(\neq 0)\in V$ و $\deg m(x)$ هو عدد صحيح موجب فإن عدد $m_v(x)$ المختلفة يجب أن يكون منتهياً ، هذا يسوغ لنا أنه بالإمكان التحدث في المضاعف المشترك الأصغر لجميع $m_v(x)$.

التعليل السابق يثمر النتيجة الآتية :

نتيجة 27.16

لأي تحويل خطي غير صفري $T\in A(V)$ فإن كثيرة الحدود الأصغرية له هي المضاعف المشترك الأصغر لكثيرات الحدود الأصغرية نسبة إلى T لجميع العناصر غير الصفرية في V .

مثال 9

اعتبر التحويل الخطي $T=Q^2\to Q^2$ مصفوفته نسبة إلى القاعدة القياسية (e_1,e_2) هي $A=\begin{pmatrix}0 & 3\\ 1 & 2\end{pmatrix}$.

بما أن $A^2-2A-3I'=0$ حيث $I'=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ ولأن المصفوفة A ليست قياسية (أي من النوع $\alpha I'$ لبعض $\alpha\in\ell$ فإن A لا يمكن أن يكون جذراً لكثيرة حدود من الدرجة 1 على Q .

إذاً x^2-2x-3 هي كثيرة الحدود الأصغرية للمصفوفة A بالتالي للتحويل T . الآن $T(e_1)=e_2$ ، $T(e_2)=3e_1+2e_2$ يثمر أن $T(e_1+e_2)=T(e_1)+T(e_2)=3(e_1+e_2)$ عليه طالما كان $v=e_1+e_2$ فإن $(T-3I)(v)=0$ لأن $x-3$ كثيرة حدود واحدية درجتها 1 و $(T-3I)(v)=0$ فإن $x-3$ هي نفسها كثيرة الحدود الأصغرية لـ v نسبة إلى T ويمكننا بالمثل نرى أن كثيرة الحدود الأصغرية للمتجه $w=3e_1+e_2$ نسبة إلى T هي $x+1$.

واضح أن x^2-2x-3 هو المضاعف المشترك الأصغر لكثيرتي الحدود $x+1$ و $x-3$. اعتبر $v=2e_1+e_2$ لأي $\alpha\in Q$ يكون

$$\begin{aligned}(T-\alpha I)(v)&=T(2e_1+e_2)-\alpha(2e_1+e_2)\\&=2T(e_1)+T(e_2)-2\alpha e_1-\alpha e_2=(4-\alpha)e_2+(3-2\alpha)e_1\neq 0\end{aligned}$$

ولأن لأي α $4-\alpha=0,$ و $3-2\alpha=0$ لا يمكن أن يتحقق في آن معاً ، لذا لا توجد كثيرة حدود واحدية درجتها تساوي 1 في المثالي المعدم للمتجه v نسبة إلى T .

هذه تبين أن درجة كثيرة الحدود الأصغرية للمتجه v يجب أن تكون على الأقل 2 .

بما أن $(T^2-2T-3)(v)=0v=0$ نجد أن x^2-2x-3 هي كثيرة الحدود الأصغرية للمتجه v نسبة إلى T ، لذا فإن Q^2 يحوي متجهاً كثيرة حدوده الأصغرية نسبة إلى T هي نفس كثيرة الحدود الأصغرية للتحويل T . هذه الحقيقة تتحقق في المواقف العامة كما سنرى فيما بعد .

قضية 25.16

إذا كان v,w متجهين غير صفريين في الفضاء المتجهي V بحيث كان كثيرتي حدودهما الأصغرية نسبة إلى تحويل خطي غير صفري T على V هما أوليتان نسبياً أحدهما مع الأخرى فإن كثيرة الحدود الأصغرية للمتجه $v+w$ عبارة عن ضرب كثيرتي الحدود الأصغريتين للمتجهين w,v .

البرهان

لتكن $f(x)$ و $g(x)$ كثيرتي الحدود الأصغريتين للمتجهين w,v على الترتيب . أُعطينا أن $(f(x),g(x))=1$.

الآن $[f(T)]v=0$ ، $[g(T)]v=0$ يؤدي إلى أن :

$$f(T)g(T)(v+w)=g(T)[f(T)v]+f(T)[g(T)v]=g(T)0+f(T)0=0$$

إذاً كثيرة الحدود الأصغرية $m(x)$ للمتجه $v+w$ يقسم $f(x)g(x)$.

بما أن $f(x),g(x)$ أوليتان نسبياً نحصل على $m(x)=f_1(x)g_1(x)$ لبعض $f_1(x),g_1(x)$ حيث $f_1(x)|f(x)$ و $g_1(x)|g(x)$ وأن $(f_1(x),g_1(x))=1$ لما كانت $m(x)$ كثيرة حدود واحدية فكل من $f_1(x),g_1(x)$ يمكن أخذها كثيرة حدود واحدية عندئذ يكون . افرض $f_1(x)\neq f(x)$ ، $\deg f_1(x)<\deg f(x)$ بالتالي فإن :

$$[f_1(T)]v\neq 0 \qquad (1)$$

كذلك

$$f_1(x)g_1(x)|\,f_1(x)g(x)\Rightarrow 0=f_1(T)g(T)(v+w)$$
$$=f_1(T)[g(T)](v) \qquad (2)$$

لأن $g(T)w=0$ وحيث أن $(f(x),g(x))=1$ فإنه يوجد $A(x),B(x)\in F[x]$ بحيث $f(x)A(x)+g(x)B(x)=1$ (نتيجة 20.10) بناء عليه في $F[T]$ يكون :

$$f(T)A(T)+B(T)g(T)=I$$

لذلك :

$$v=Iv=[B(T)g(T)]v \qquad (3)$$

لأن $[f(T)]v=0$ بتأثير $B(T)$ على (2) نحصل على :

(حسب 3) $0=[B(T)f_1(T)g(T)](v)=f_1(T)(Iv)=[f_1(T)]v$.

هذا يناقض (1) إذاً $\deg f_1(x)=\deg f(x)$ بعبارة أخرى $f_1(x)=f(x)$ وبالمثل يمكن تبيان أن $g_1(x)=g(x)$ إذاً $m(x)=f(x)g(x)$.

قضية 29.16

إذا كانت كثيرات الحدود الأصغرية للمتجهات غير الصفرية $v_i\ (i=1,2,...,s)$ نسبة إلى تحويل خطي T هي $f_i(x)\ (i=1,2,...,s)$ على الترتيب وكان أي اثنين في $f_i(x)$ أوليتان نسبياً فإن كثيرة الحدود الأصغرية للمتجه $v=v_1+v_2+...+v_5$ هي حاصل الضرب $f_1(x)f_2(x)...f_5(x)$.

البرهان

عندما $s=2$ فإن المطلوب ينتج في القضية 28.16 لكي نطبق الاستنتاج افرض $s>2$ والنتيجة محققة للعدد 1-5 أي أن كثيرة الحدود الأصغرية للمتجه $w=v_1+v_2+...+v_{5-1}$ هي $g(x)=f_1(x)f_2(x)...f_{5-1}(x)$ بما أن $(f_5(x),f_i(x))=1$ لجميع $1\le i<5$ فإن $(g(x),f_5(x))=1$ وفي القضية 23.16 تكون كثيرة الحدود الأصغرية للمتجه $v=v_1+v_2+v_5=w+v_5$ هي $g(x)f_5(x)f_2(x)...f_5(x)$ تتحقق من الاستنتاج .

القضية المساعدة التالية بسيطة ونترك إثباتها للقراء .

قضية 30.16

إذا كانت كثيرة الحدود الأصغرية لمتجه غير صفري $v\in V$ نسبة لتحويل خطي T على V هي $m(x)=f(x)g(x)$ حيث $f(x)$ و $g(x)$ كثيرتي حدود واحدتان في $F[x]$ فإن كثيرة الحدود الأصغرية لـ $f(T)v$ نسبة إلى T هي $g(T)$.

نظرية 31.16

إذا كان T تحويلاً خطياً غير صفري على V ، فإن V يحوي متجهاً v بحيث كثيرتي الحدود الأصغريتين للتحويل T والمتجه v نسبة إلى T متساويتين .

البرهان

لتكن $\{v_1, v_2, ..., v_n\}$ قاعدة للفضاء V .

افرض أنه لكل $i = 1, 2, ..., n$ كثيرة الحدود الأصغرية للمتجه v_i نسبة إلى T هي $f_i(x)$ ، بما أن $F[x]$ هو UFD نستطيع التعبير عن كثيرة الحدود f_i هذه كحاصل ضرب لقوى كثيرات حدود واحدية غير قابلة للتحليل .

$$f_i(x) = \pi_1^{\alpha_{1i}}(x)\pi_2^{\alpha_{2i}}(x)..\pi^{\alpha_{ti}}(x), (i = 1, 2, ..., n) \qquad (1)$$

حيث $0 \le \alpha_{ji}$ مثل i, j و $\Pi_1(x), \Pi_2(x), ..., \Pi_t(x)$ هي كثيرات حدود غير قابلة للتحليل (يمكننا أخذ نفس كثيرات الحدود غير القابلة للتحليل لجميع $f_i(x)$ وذلك بالسماح بالقوى الصفرية) ، و $\Pi_j^{\alpha ji}(x)$ $[\Pi_j(x)]^{\alpha ji}$ (انظر إثبات نظرية 31.10) لكل $j = 1, 2, ..., t$ ضع :

$$\alpha_j = \max\{\alpha_j 1, \alpha_j 2, ..., \alpha_{jn}\} \qquad (2)$$

عندئذ المضاعف المشترك الأصغر لكثيرات الحدود $f_1(x), f_2(x), ..., f_n(x)$ هو $f(x) = \Pi_1^{\alpha_1}(x)\Pi_2^{\alpha_2}(x)...\Pi_t^{\alpha t}(x)$.

الآن $\alpha_1 = \alpha_1 i_1$ لبعض i عليه $f_{t_1}(x) = \Pi_1^{\alpha_1}(x)\left[\Pi_2^{\alpha_2 i_1}(x)...\Pi_t^{\alpha_t i_1}(x)\right]$

فإذا كان v_i $w_1 = \left[\Pi_2^{\alpha_2 i_1}(T)...\Pi_t^{\alpha_t i_1}(T)\right]$ فإن كثيرة الحدود الأصغرية للمتجه w_1 هي $\Pi_1^{\alpha_1}(x)$ (قضية 30.16) وبالمثل باعتبار $\alpha_2, \alpha_3, ..., \alpha_t$ نحصل على متجهات $w_2, w_3, ..., w_t$ بحيث كثيرات الحدود الأصغرية لها نسبة إلى T هي على الترتيب $\Pi_2^{\alpha_2}(x), ..., \Pi_t^{\alpha_t}(x)$.

وحيث أن كل زوجين من كثيرات الحدود $\Pi_1^{\alpha_1}(x), ..., \Pi_t^{\alpha_t}(x)$ أوليان نسبياً فإنه حسب القضية 29.16 تكون كثيرة الحدود الأصغرية للمتجه $w = w_1 + w_2 + ... + w_t$ هي :

$$f(x) = \Pi_1^{\alpha_1}(x)\Pi_2^{\alpha_2}(x)..\Pi_t^{\alpha_t}(x)$$

لتكن $m(x)$ هي كثيرة الحدود الأصغرية للتحويل T افرض $v \in V$ فيكون $v = \beta_1 v_1 + \beta_2 v_2 + ... + \beta_n v_n$ لبعض $\beta_i \in F$ عليه :

$$[F(T)]v = \beta_1 f(T)v_1 + ... + \beta_n f(T)v_n = 0$$

(لأن $f_i(T)v_i = 0$ و $f_i(x)|f(x)$ لكل i) .

إذاً $f(T)=0$ ، هذا يؤدي إلى أن $m(x)|f(x)$ كذلك $f_i(x)|m(x)$ لكل $1\le \ell \le t$ (نظرية 24.16) و $f(x)$ هو المضاعف المشترك الأصغر لجميع كثيرات الحدود $f_i(x)$ فإننا نحصل على أن $f(x)|m(x)$ وهكذا فإن $f(x)|m(x)$ و $m(x)|f(x)$ ولكون كل منهما كثيرة حدود واحدية فإن $f(x)=m(x)$ إذاً كثيرة الحدود الأصغرية لكل من T,w هي نفسها أي $m(x)$.

الآن نظرية 22.16 بمثابة نتيجة مباشرة للنظرية السابقة .

نتيجة 32.16

لأي تحويل خطي غير صفري $T\in A(V)$ فإن درجة كثيرة الحدود الأصغرية له $\le n$ بعد الفضاء V .

البرهان

حسب نظرية 31.16 فإن V يحوي متجهاً v تكون كثيرة حدوده الأصغرية $f(x)$ نسبة إلى T هي نفسها كثيرة الحدود الأصغرية للتحويل T . بما أن $F[T]v$ فضاء جزئي من V فإن $\dim_F F[T]v \le n = \dim V$ من ناحية أخرى وحسب نظرية 24.16 يكون $\deg m(x) = \dim_F F[T]v$ إذاً $\deg m(x) \le n$ وهذا يثبت النتيجة .

نتيجة 33.16

لأي تحويل خطي غير صفري T على V كل جذر في F لكثيرة الحدود الأصغرية للتحويل T هو قيمة ذاتية للتحويل T .

البرهان

لتكن $m(x)$ كثيرة الحدود الأصغرية للتحويل T و α جذراً لها في F .

فإن $m(x)=(x-\alpha)m_1(x)$ حيث $m_1(x)\in F[x]$ استناداً إلى نظرية 31.16 يوجد متجه $v\in V$ كثيرة الحدود الأصغرية له نسبة إلى T هي $m(x)$.

عندئذ $m_1(T)v\neq 0$ وإذا كان $w=m_1(T)v$ نرى أن $0=m(T)v=(T-\alpha)w$ ويؤدي إلى أن $T(w)=\alpha w$ بالتالي فإن α قيمة ذاتية للتحويل T .

مثال 10

اعتبر كثيرة الحدود $f(x)=(x^2+1)^2=x^4+2x^2+1$ نعين تحويلاً خطياً على C^1 كثيرة حدوده الأصغرية له هي x^4+2x^2+1 لتكن (e_1,e_2,e_3,e_4) القاعدة القياسية المرتبة لـ C^4 عرف تحويلاً خطياً T على C^4 بحيث يكون $T(e_1)=e_2$ ، $T(e_2)=e_3$ ، $T(e_3)=e_4$ و $T(e_4)=-e_1-2e_3$ عليه $T^2(e_1)=e_3$ ، $T^3(e_1)=e_4$ ، $T^4(e_1)=Ie_1-2T^2(e_1)$ إذاً :

$$(T^4+2T^2+I)e_1=0 \qquad (1)$$

بما أن المتجهات الأربعة $e_1,T(e_1),T^2(e_1),T^3(e_1)$ مستقلة خطياً ، فإن درجة كثيرة الحدود الأصغرية للمتجه e_1 يجب أن تكون على الأقل أربعة (نظرية 24.16) بالتالي من (1) نستنتج أن x^4+2x^2+1 هي كثيرة الحدود الأصغرية للمتجه e_1 . الآن $eimC^4=4$ يؤدي إلى أن درجة كثيرة الحدود الصفرية للتحويل T لا تتجاوز 4 (نتيجة 32.16) من جهة أخرى x^4+2x^2+1 نقسم كثيرة الحدود الأصغرية للتحويل T لذا فإن x^4+2x^2+1 هي نفسها كثيرة الحدود الأصغرية للتحويل T مصفوفة T بالنسبة للقاعدة المرتبة (e_1,e_2,e_3,e_4) هي

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

ونترك للقراء تعيين القيم الذاتية والمتجهات الذاتية للتحويل T .

مثال 11

ليكن V الفضاء المتجهي لجميع كثيرات الحدود على $I\!R$ والتي درجتها لا تتجاوز 3 و D عملية التفاضل على V في مثال 5 وجدنا أن y^4 هي كثيرة الحدود الأصغرية للتحويل D . اعتبر المتجه $x^3 \in V$ بما أن $D(x^3)=3x^2$ ، $D^2(x^3)=6x$ ، $D^3(x^3)=6$ والمتجهات $x^3, 3x^3, 6x, 6$ مستقلة خطياً فإن $(x^3, D(x^3) D^2(x^3) D^3(x^3))$ مستقلة خطياً . بالتالي حسب نظرية 24.16 فإن كثيرة الحدود الأصغرية للتحويل D هي عامل واحدي لكثيرة الحدود y^4 ودرجتها على الأكثر 4 إذاً y^4 نفسها كثيرة الحدود الأصغرية لـ x^3 نسبة إلى D .

مسائل

1. لكل من التحويلات الخطية على Q^2 والتي مصفوفاتها نسبة إلى القاعدة القياسية هي $\begin{pmatrix}1&1\\2&2\end{pmatrix};\begin{pmatrix}1&2\\2&1\end{pmatrix};\begin{pmatrix}0&1\\1&3\end{pmatrix};\begin{pmatrix}5&2\\3&0\end{pmatrix}$ عين كثيرات الحدود الأصغرية المقابلة لها والمتجهات في Q^2 والتي كثيرات الحدود الأصغرية لها نسبة على التحويلات الخطية المقابلة تساوي كثيرات الحدود الأصغرية للتحويلات الخطية المقصودة .
2. تحقق من أن المصفوفة $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ ليس لها قيمة ذاتية في Q ولكن لها قيمة ذاتية في C
3. ليكن $T(\neq 0)\in A(V)$ و $v_1,v_2,\ldots,v_m$ أي m في المتجهات غير الصفرية بحيث كانت كثيرات الحدود الأصغرية الخاصة بها $f_1(x),f_2(x),\ldots,f_m(x)$ نسبة إلى T أولية نسبياً مثنى مثنى برهن أن مجموع الفضاءات $F(T)v_1,F(T)v_2,\ldots F(T)v_m$ هو مجموع مباشر .
4. كَوِّن أمثلة لتوضيح النتيجة في المسألة 3 .
5. لتحويل خطي ما T على V أعطينا متجهات $v_1,v_2,\ldots,v_m$ بحيث كان $V=\sum_{i=1}^{m}F[T]v_i$ ، برهن أن كثيرة الحدود الأصغرية للتحويل T هي المضاعف المشترك الأصغرية لكثيرات الحدود الأصغرية للمتجهات v_i $(1\leq i\leq m)$ نسبة إلى T .
6. في كل مطلب مما يأتي أوجد كثيرات الحدود الأصغرية لكل من المتجهات في القاعدة القياسية نسبة إلى التحويل الخطي المعطى T :

i. $T\in A(Q^2)$ ، $T(e_1)=e_2$ ، $T(e_2)=e_1+e_2$.

ii. $T\in A(Q^2)$ ، $T(e_1)=e_1-e_2$ ، $T(e_2)=e_1+e_2$.

iii. $T\in A(Q^2)$ ، $T(e_1)=e_1+2e_2$ ، $T(e_2)=e_1$.

iv. $T\in A(Q^3)$ ، $T(e_1)=e_2$ ، $T(e_2)=e_3,T(e_3)=e_1+e_2+e_3$.

v. $T\in A(Q^3)$ ، $T(e_1)=e_2$ ، $T(e_2)=e_3$ ، $T(e_3)=0$.

7. أوجد كثيرة الحدود الأصغرية لكل من التحويلات الخطية في المسألة ، وتحقق من أنها المضاعف المشترك الأصغر لكثيرات الحدود الأصغرية لمتجهات القاعدة .

3. صيغة جوردان القانونية

تعريف 34.16

إذا كانت $f(x)=x^k-\alpha_{k-1}x^{k-1}-..\alpha_1 x-\alpha_0$ أية كثيرة حدود واحدية على حقل F فإن المصفوفة $k\times k$

$$\begin{pmatrix} 0 & 0 & \dots & 0 & \alpha_0 \\ 1 & 0 & \dots & 0 & \alpha_1 \\ 0 & 1 & \dots & 0 & \alpha 2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \alpha_{k-1} \\ 0 & 0 & \dots & 1 & \alpha_{k-1} \end{pmatrix}$$

تسمى المصفوفة المصاحبة لها ويرمز لها بالرمز $c[f(x)]$.

مثال 2

المصفوفة المصاحبة لكثيرة الحدود $f(x)=x^3+3x^2+2x-1$ هي :

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -2 \\ 0 & 1 & -3 \end{pmatrix}$$

مثال 3

اعتبر كثيرة الحدود $f(x)=x^4-5x^2+1$ نستطيع كتابتها كالآتي $f(x)=x^4-0x^3 5x^2-0x+1$ وتكون مصفوفتها المصاحبة هي :

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 5 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

ننصح القراء بكتابة المصفوفات المصاحبة لكثيرات الحدود $x^6+4x^4+3x^3+2$ ، x^2+x+1 ، x^2+1 ، x^3+1 ، x^3+x^2+1 .

نظرية 35.16

لتكن $f(x) = x^m - \alpha_{m-1}x^{m-1} - \dots - \alpha_1 x - \alpha_0$ أية كثيرة حدود واحدية على حقل F عندئذ يوجد تحويل خطي T على فضاء متجهي W بعده m يساوي درجة كثيرة الحدود $f(x)$ بحيث تكون كثيرة الحدود الأصغرية للتحويل T هي $f(x)$.

البرهان

لتكن $(v_1, v_2, \dots, v_m)$ قاعدة مرتبة للفضاء V عرف التطبيق الخطي T على W بحيث $T(v_1) = v_2, T(v_2) = v_3, \dots, T(v_{m-1}) = v_m$ و $T(v_m) = \alpha_0 v_1 + \alpha_1 v_2 + \dots + \alpha_{m-1} v_{m-1}$.
الآن $\{v_1, T(v_1), T^2(v_2), \dots T^{m-1}(v_1)\} = \{v_1, v_2, \dots, v_n\}$ هي مجموعة مستقلة خطياً وتبعاً للنظرية 24.16 فإن درجة كثيرة الحدود الأصغرية للمتجه v_1 نسبة إلى T هي على الأقل m وبالتالي فهي m لأن $\dim W = m$ كذلك فإن درجة كثيرة الحدود الأصغرية لأي متجه أو تحويل خطي لا يمكن أن تتجاوز بعد الفضاء المتجهي الأساسي (نتيجة 32.16) والآن العلاقات المعرفة لـ T تعطينا :

$$T^m(v_1) = \alpha_0 v_1 + \alpha_1 T(v_1) + \alpha_2 T^2(v_1) + \dots + \alpha_{m-1} T^{m-1}(v_1)$$

أي أن

$$\left(T^m - \alpha_{m-1}T^{m-1} - \alpha_{m-2}T^{m-2} - \dots - \alpha_1 T - \alpha_0 I\right)v_1 = 0$$

إذاً $f(x) = x^m - \alpha_{m-1}x^{m-1} - \alpha_{m-2}x^{m-2} \dots - \alpha_0$ هي كثيرة الحدود الواحدية للمتجه v_1 نسبة إلى T . مرة ثانية استناداً إلى نظرية 24.16 (b) فقرة (iii) والنتيجة 32.16 إذا كانت درجة كثيرة الحدود الأصغرية $f(x)$ لتحويل خطي T على V تساوي بعد V فإن للفضاء V قاعدة مرتبة بحيث مصفوفة T نسبة إلى تلك القاعدة هي $C(f(x))$.

البرهان

افرض أن $f(x) = x^k - \alpha_{k-1}x^{k-1} - \dots - \alpha_0$ هي كثيرة الحدود الأصغرية للتحويل $T \in A(V)$ حيث $\dim V = k$ حسب نظرية 31.16 يوجد متجه $v_1 (\neq 0) \in V$ بحيث تكون $f(x)$ هي كثيرة الحدود الأصغرية للمتجه v_1 نسبة إلى T .

إذاً $\{v_1, T(v_1), T^2(v_1), \ldots, T^{k-1}(v_1)\}$ تمثل قاعدة للفضاء V (نظرية 24.16) .

ضع $v_2 = T(v_1), v_3 = T^2(v_1) = T(v_0) \ldots, v_k = T^{k-1}(v_1) = T(v_{k-1})$

الآن $(v_1, v_2, \ldots, v_k)$ قاعدة مرتبة للفضاء V بحيث :

$$T(v_1) = v_2 \,, T(v_2) = v_3, \ldots, T(v_{k-1}) = v_k$$

و

$$T(v_k) = T^k(v_1) = \alpha_0 v_1 + \alpha_1 T(v_1) + \ldots + \alpha_{k-1} T^{k-1}(v_1)$$

(لأن $f(T)v_1 = 0$ هذا يعطي $T(v_k) = \alpha_0 v_1 + \alpha_1 v_2 + \ldots + v_k - v_k$.

مصفوفة T نسبة إلى القاعدة المرتبة $(v_1, v_2, \ldots, v_k)$ هي

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & \alpha_0 \\ 1 & 0 & \ldots & 0 & \alpha_1 \\ 0 & 1 & \ldots & 0 & \alpha_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \alpha_{k-2} \\ 0 & 0 & \ldots & 1 & \alpha_{k-1} \end{pmatrix} = C(f(x)) .$$

نتيجة 37.16

لتكن A مصفوفة ذات سعة $n \times n$ على الحقل F إذا كانت درجة كثيرة الحدود الأصغرية $f(x)$ للمصفوفة A تساوي n فإنه توجد مصفوفة غير منفردة p على F بحيث يكون $P^{-1}AP$ هي $C(f(x))$.

البرهان

ليكن V فضاءاً متجهاً ذو بعد n على الحقل F و $B = (v_1, v_2, \ldots, v_n)$ قاعدة مرتبة له ، ليكن T تحويلاً خطياً على V ومصفوفة نسبة إلى B هي A حسب تعريف (a) 9.16 فإن كثيرة الحدود الأصغرية للتحويل T هي أيضاً $f(x)$ ، بما أن درجة $f(x)$ تساوي n فإنه توجد قاعدة مرتبة $B' = (w_1, w_2, \ldots, w_n)$ للفضاء V بحيث تكون مصفوفة T نسبة

إلى القاعدة $(w_1, w_2, ..., w_n)$ هي $A' = C(f(x))$ إذا كانت P مصفوفة $(v_1, v_2, ..., v_n)$ نسبة للقاعدة $(w_1, w_2, ..., w_n)$ فإن $A' = P^{-1}AP$ (نتيجة 40.12) إذاً $P^{-1}AP = C(f(x))$.

تعريف 38.16

يقال لتحويل خطي T على فضاء متجهي V إنه دوري إذا وجد $v \in V$ بحيث يكون $V = F[T]v$ في هذه الحالة يقال أن V فضاء دوري نسبة إلى T .

قضية 39.16

الفضاء المتجهي V دوري نسبة إلى تحويل خطي T على V إذا وفقط إذا كان $\dim_F V$ يساوي درجة كثيرة الحدود الأصغرية للتحويل T .

البرهان

إذا كان V دورياً نسبة إلى T فإنه يوجد $v \in V$ بحيث $V = F[T]v$ استناداً إلى نظرية 24.16 فإن $\dim_F F[T]v = \deg m_v(x)$ حيث $m_v(x)$ هي كثيرة الحدود الأصغرية للمتجه v نسبة إلى T ، عليه فإن $\deg m_v(x) = n = \dim V$ ، وحسب نظرية 24.16 ونتيجة 32.16 فإن $m_v(x)$ هي نفسها كثيرة الحدود الأصغرية للتحويل T .

بالعكس افرض أن درجة كثيرة الحدود الأصغرية $m(x)$ للتحويل T تساوي n حيث $n = \dim V$. الآن يوجد متجه v في V تكون كثيرة حدوده الأصغرية نسبة إلى T هي $m(x)$ ، وهكذا فإن $\dim F[T]v = n$ (نظرية 24.16 b (iv)) بالتالي فإن $V = F[T]v$ هذا يثبت أن V دوري نسبة إلى T .

تعريف 40.16

ليكن T تحويلاً خطياً دورياً على V و $f(x) = x^n - \alpha_{n-1}x^{n-1} - ... - \alpha_1 x - \alpha_0$ كثيرة حدود الأصغرية ، فإن المصفوفة المصاحبة لـ $f(x)$ نقصد

$$A=\begin{pmatrix} 0 & 0 & \dots & 0 & \alpha_0 \\ 1 & 0 & \dots & 0 & \alpha_1 \\ 0 & 1 & \dots & 0 & \alpha_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \alpha_{n-2} \\ 0 & 0 & \dots & 1 & \alpha_{n-1} \end{pmatrix}$$

تسمى مصفوفة جوردان للتحويل T .

نظرية 41.16

لتكن $f(x)=(q(x))^k$ كثيرة حدود واحدية على F ذات درجة n مع كون $q(x)$ كثيرة حدود درجتها m (أي أن $n=mk$) .

إذا كان T تحويلاً خطياً دورياً على V بحيث أن $f(x)$ هي كثيرة الحدود الأصغرية للتحويل T فإنه بالنسبة لقاعدة مرتبة ما للفضاء V تكون مصفوفة T على الصورة :

$$A=\begin{pmatrix} C & & N & & & \\ & \ddots & & \ddots & & \\ & & C & & N & \\ & & & \ddots & & \ddots \\ & & & & \ddots & & \ddots \\ & & & & & C & & N \end{pmatrix}$$

حيث $c=c(q(x))$ و N هي المصفوفة $m\times m$ التي على الشكل

$$\begin{pmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

البرهان

الآن لبعض $v\in V$ ، $V=F[T]v$.

عرف :

$$\left.\begin{array}{l} v_1=[q(T)]^{k-1}v\,,v_2=T[q(T)]^{k-1},\ldots,v_m=T^{m-1}[q(T)]^{k-1}\,v\,,\\ v_{m+1}=[q(T)]^{k-2}\,k\,,v_{m+2}=T[q(T)]^{k-2}\,k\,,\ldots,v_{2m}=T^{m-1}[q(T)]^{k-2}\,v\,,\\ v_{2m+1}=[q(T)]^{k-3}\,v\,,v_{2m+2}=T[q(T)]^{k-3}\,k\,,\ldots,v_{3m}=T^{m-1}[q(T)]^{k-3}\,v\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ v_{(k-1/m+1)}=v\,,v_{(k-1)m+2}=T(v),\ldots,v_{km}=T^{m-1}(v) \end{array}\right\}\qquad(1)$$

وهكذا فإن كل v_i هو بالصيغة $g(T)v$ مع كون $g_i(x)\neq 0$ و $\deg g_i(x)<n$.

افرض لبعض $\alpha_i \in F$ يكون $\sum_{i=1}^{km}\alpha_i v_i=0$ بحيث بعضاً من α_i لا يساوي الصفر ، أي أن $\left[\sum_i \alpha_i g_i(T)\right]v=0$ بملاحظة أن $g_i(x)$ كلها ذات درجات مختلفة فمن الممكن أن نجد $g(x)=\sum \alpha_i g_i(x)\neq 0$ ، $\deg g(x)<n$ و $g(T)v=0$ هذا يناقض حقيقة أن كثيرة الحدود الأصغرية للمتجه v نسبة إلى T هي $f(x)$ ودرجتها n ، بالتالي فإن المتجهات $v_1,v_2,\ldots,v_{km}(=v_n)$ والتي عددها n هي مستقلة خطياً .

لتكن :

$$q(x)=x^m-\alpha_{m-1}x^{m-1}-\ldots-\alpha_1 x-\alpha_0 \qquad (2)$$

من تعريف المتجهات v_i نحصل على أن :

$$\begin{aligned} &T(v_1)=v_1\\ &T(v_2)=v_3\\ &\ldots\ldots\ldots\ \ldots\ldots\\ &\ldots\ldots\ldots\ \ldots\ldots\\ &T(v_{m-1})=v_m\\ &T(v_m)=T^m[q(T)]^{k-1}v\\ &\qquad=[T^m-q(T)][q(T)]^{u-1}v\\ &\qquad=(\alpha_0 I+\alpha_1 T+\ldots+\alpha_{m-1}T^{m-1})[q(T)]^{k-1}v \end{aligned}$$

(لأن $[q(T)]^k v=0$.

$$= \alpha_0 [q(T)]^{k-1} v + \alpha_1 T [q(T)]^{k-1} v + ... + \alpha_{m-1} T^{m-1} [q(T)]^{k-1} v$$

وهذا يؤدي إلى أن

$$T(v_m) = \alpha_0 v_1 + \alpha_1 v_2 + ... + \alpha_{m-1} v_m$$
$$T(v_m + 1) = v_{m+2}$$
$$T(v_m + 2) = v_{m+3}$$
....
$$T(v_{2m-1}) = v_{2m}$$
$$T(v_{2m}) = T^m [q(T)]^{k-2} v$$
$$= [q(T)]^{k-1} v + [T^m - q(T)][q(T)]^{k-2} v$$
$$= v_1 + (\alpha_0 I + \alpha_1 T + ... + \alpha_{m-1} T^{m-1})[q(T)^{k-2}] v$$

هذا يعطي أن

$$T(v_{2m}) = v_1 + \alpha_0 v_{m+1} + \alpha_1 v_{m+2} + ... + \alpha_{m-1} v_{2m}$$

بالاستمرار بهذا الأسلوب نحصل على

$$T(v_{2m+1}) = v_{2m+2}$$
$$T(v_{2m+2}) = v_{2m+3}$$
....
$$T(v_{3m-1}) = v_{3m}$$
....

....
$$T(v_{(k-1)m+1}) = v_{(k-1)m+2}$$

....
$$T(v_{km-1}) = v_{km}$$
$$T(v_{km}) = v_{(k-2)m+1} + \alpha_1 v_{(k-1)m+1} + \alpha_1 v_{(k-1)m+2} + ... + \alpha_{m-1} v_{km}$$

باستخدام حقيقة أنه إذا كان $T(v_i) = \sum_{j=1}^{n=km} \alpha_i v_j$

فإن العنصر الواقع في العمود الذي ترتيبه i والصف الذي ترتيبه j في المصفوفة (α_{ij}) هو معامل v_j .

المعادلات السابقة جميعها تؤدي إلى أن مصفوفة T نسبة إلى $(v_1, v_2, ..., v_{km})$ هي :

$$\begin{pmatrix}
0 & 0 & \ldots & 0 & \alpha_0 & 0 & 0 & \ldots & 0 & 1 & \ldots & 0 & 0 & \ldots & 0 \\
1 & 0 & \ldots & 0 & \alpha_1 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\
0 & 1 & \ldots & 0 & \alpha_2 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & 1 & \alpha_{m-1} & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\
0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & \alpha_0 & \ldots & 0 & 0 & \ldots & 0 \\
0 & 0 & \ldots & 0 & 0 & 1 & 0 & \ldots & 0 & \alpha_1 & \ldots & 0 & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 1 & \alpha_{m-1} & \ldots & 0 & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & \alpha_0 \\
0 & 0 & \ldots & 0 & 0 & \ldots & 0 & \ldots & 0 & 0 & 1 & 0 & \ldots & 0 & \alpha_1 \\
\ldots & . & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & 0 & \alpha_{m-2} \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & 0 & 0 & 0 & 0 & \ldots & \ldots & o & 0 & 0 & \ldots & 1 & \alpha_{m-1}
\end{pmatrix}$$

$$= \begin{pmatrix}
c & N & 0 & 0 & \ldots & 0 & 0 \\
0 & C & N & 0 & \ldots & 0 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & 0 & \ldots & C & N \\
0 & 0 & 0 & 0 & \ldots & 0 & C
\end{pmatrix}$$

حيث C هي المصفوفة ذات السعة $m \times m$ التالية :

$$\begin{pmatrix}
0 & 0 & \ldots & 0 & \alpha_0 \\
1 & 0 & \ldots & 0 & \alpha_1 \\
0 & 1 & \ldots & 0 & \alpha_2 \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & 1 & \alpha_{m-1}
\end{pmatrix} = C(q(x))$$

و N هي المصفوفة ذات السعة $m \times m$ الآتية

$$\begin{pmatrix}
0 & 0 & \ldots & 1 \\
0 & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & 0
\end{pmatrix}$$

وهذا يكمل إثبات النظرية .

تعريف 42.16

لتكن $q(x)$ كثيرة حدود واحدية ، ولتكن درجتها m على الحقل F لأي عدد صحيح موجب k فإن المصفوفة ذات السعة $km \times km$ والتي تساوي

$$\begin{pmatrix} C & N & 0 & \dots & 0 & 0 \\ 0 & C & N & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & C & N \\ 0 & 0 & 0 & 0 & 0 & C \end{pmatrix}$$

حيث C هي المصفوفة المصاحبة لكثيرة الحدود $q(x)$ و N هي المصفوفة المصاحبة $m \times m$ الآتية

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots 0 \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

تسمى مصفوفة جوردان لكثيرة الحدود $f(x) = (q(x))$ نسبة إلى $q(x)$.

مثال 14

اعتبر $f(x) = (x^2+1)^3$ درجة $f(x)$ على Q هي 6 هنا $q(x) = x^2+1$ المصفوفة المصاحبة لكثيرة الحدود $q(x)$ هي $C = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

لدينا تحويل خطي T على Q^6 كثيرة حدود الأصغرية هي $f(x)$ (نظرية 35.16) وتوجد قاعدة مرتبة $B = (u_1, u_2, u_3, u_4, u_5, u_6)$ للفضاء Q^6 بحيث أن مصفوفة T نسبة لهذه القاعدة هي المصفوفة المصاحبة لكثيرة الحدود $f(x) = (x^2+1)^3 = x^6 + 3x^4 + 3x^2 + 1$ وهي :

$$A=\begin{pmatrix}0&0&0&0&0&-1\\1&0&0&0&0&0\\0&1&0&0&0&-3\\0&0&1&0&0&0\\0&0&0&1&0&-3\\0&0&0&0&1&0\end{pmatrix}$$

في نفس الوقت نظرية 41.16 تبين وجود قاعدة مرتبة $B'=(v_1,v_2,v_3,v_4,v_5,v_6)$ للفضاء Q^6 بحيث أن مصفوفة T نسبة على B' هي

$$A'=\begin{pmatrix}C&N&0\\0&C&N\\0&0&C\end{pmatrix}$$

حيث $N=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ وهكذا فإن

$$A'=\begin{pmatrix}0&-1&0&1&0&0\\1&0&0&0&0&0\\0&0&0&-1&0&1\\0&0&1&0&0&0\\0&0&0&0&0&-1\\0&0&0&0&1&0\end{pmatrix}$$

فإذا كانت P هي مصفوفة B' نسبة إلى B فإن $A'=P^{-1}AP$ إذاً A' و A مصفوفتان متشابهتان ، A' هي مصفوفة جوردان لكثيرة الحدود $f(x)$ نسبة إلى x^2+1 .

مثال 15

ليكن $\alpha\in F$ و $f(x)=(x-\alpha)^n$.

الآن $f(x)=x^n-c_1^n x^{n-1}\alpha+c_2^n x^{n-x}\alpha^2 ...+(-1)^n\alpha^n$ حيث $c_r^n=\dfrac{n(n-1)...(n-r+1)}{1.2.3..r}$ لكل $1\le r\le n$ بالتالي فإن المصفوفة المصاحبة لكثيرة الحدود $f(x)$ هي :

$$A=\begin{pmatrix}0&0&0&...&0&(-1)^{n+1}\alpha^n\\1&0&0&...&0&(-1)^n c_1^n\alpha^{n-1}\\0&1&0&...&0&(-1)^{n-1}C_2^n\alpha^{n-2}\\...&...&...&...&...&...\\0&0&0&...&1&C_1^n\alpha\end{pmatrix}$$

في نفس الوقت فإن المصفوفة المصاحبة لكثيرة الحدود $q(x)=x-\alpha$ هي (α) .

فإذا كان $N=(1)$ فإن المصفوفة من السعة $n\times n$.

$$A'=\begin{pmatrix} C & N & 0 & \dots & 0 \\ 0 & C & N & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & C & N \\ 0 & 0 & \dots & 0 & C \end{pmatrix}=\begin{pmatrix} \alpha & 1 & 0 & \dots & 0 & 0 \\ 0 & \alpha & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \alpha & 1 \\ 0 & 0 & 0 & \dots & 0 & \alpha \end{pmatrix}$$

بما أن A و A' هما مصفوفتان لنفس التحويل الخطي على $F^{(n)}$ فإن A',A متشابهتان ، أي أنه توجد مصفوفة غير منفردة $P\in M_n(F)$ بحيث أن $A'=P^{-1}AP$ (نتيجة 40.12) .

ملاحظة

علينا أن نتفحص مثال 15 بدقة أكثر حيث نلاحظ أننا إذا أعطينا $\alpha\in F$ فإن المصفوفة $n\times n$ الآتية :

$$A=\begin{pmatrix} \alpha & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \alpha & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & \alpha & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & \alpha \end{pmatrix}$$

وهي مصفوفة بحيث $f(x)=(x-\alpha)^n$ هي كثيرة الحدود الأصغرية لها (النظريتين 35.16 ، 41.16) بما أن كل قيمة ذاتية للمصفوفة هي جذر لكثيرة حدودها الأصغرية و α هو الجذر الوحيد لكثيرة الحدود $f(x)$ نستنتج أن α هو القيمة الذاتية الوحيدة للمصفوفة A هذه المصفوفة A والتي هي حالة خاصة من المصفوفة المعطاة في تعريف 42.16 تسمى لدى بعض المؤلفين بقالب جوردان .

وهكذا نستطيع القول مباشرة أن المصفوفات :

$$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 5 & 1 & 0 & 0 \\ 0 & 5 & 1 & 0 \\ 0 & 3 & 5 & 1 \\ 0 & 0 & 0 & 5 \end{pmatrix}$$

على الترتيب لها القيم الذاتية الوحيدة $2,-1,5$ لذلك إذا كان بإمكاننا إثبات أن مصفوفة معطاة هي شبيهة لقالب جوردان وفور معرفتنا الأخيرة يكون من السهل جداً تحديد قيمها الذاتية (التي يمكن أن تكون واحدة فقط) .

تعريف 34.16

ليكن T تحويلاً خطياً على فضاء متجهي V ، يقال للفضاء الجزئي W في V أنه فضاء جزئي لا متغير وفق T إذا كان $T(x) \in W$ لكل $x \in W$ [أي أن $T(W) \subseteq W$] .

ملاحظة

لأي تحويل $T \in A(V)$ الفضاءات V ، (0) ، $T(V)$ فضاءات جزئية لا متغيرة وفق التحويل T .

إذا كان W فضاءاً جزئياً في V لا متغير وفق التحويل T ، فإنه بإمكاننا تعريف تحويل خطي $T: W \to W$ بحيث يكون $T'(x) = T(x)$ لكل $x \in W$ ويقال أن T' مستحدث بـ T ، لدينا الآن ما يلي :

قضية 44.16

ليكن $V = V_1 \oplus V_2$ و T تحويل خطي في V إلى V بحيث أن V_2, V_1 فضاءان جزئيان في V كلاهما لا متغير وفق T ، إذا كان $T_i (i=1,2)$ تحويل خطي على $V_i (i=1,2)$ مستحدث في T فإن كثيرة الحدود الأصغرية $f(x)$ للتحويل T هي المضاعف المشترك الأصغر لكثيرتي الحدود الأصغرية لكل من T_1 و T_2 .

البرهان

لتكن $f_i(x)$ كثيرة الحدود الأصغرية للتحويل T_i ، بما أن $f(T)=0$ و T_i هو مقصور T على V_i ، يكون لدينا أيضاً $f(T_i)=0$ وحسب نظرية 7.16 يكون $f_i(x)|f(x)$ بالتالي فإن المضاعف المشترك الأصغر $g(x)$ لكثيرتي الحدود $f_2(x), f_1(x)$ يقسم $f(x)$ أيضاً.

الآن لأي $x_1 \in V_1$ فإن $g(T)x_1 = g(T_1)x_1 = 0$ لأن $g(T_1)=0$ [لاحظ أن $f_1(x)|g(x)$] بالمثل فإن $g(T)x_2 = 0$ لكل $x_2 \in V_2$.

إذاً $[g(T)]V_1 = (0)$ و $[g(T)]V_2 = (0)$ هذا يؤدي إلى أن $g(T)V = (0)$ لكون $V = V_1 \oplus V_2$ لذا فإن $g(T)=0$ وبالتالي $f(x)|g(x)$. وهكذا فإن $f(x)$ مصاحب لكثيرة الحدود $g(x)$ ، نتيجة لذلك يكون $f(x)$ هو المضاعف المشترك الأصغر لكثيرتي الحدود $f_1(x)$ و $f_2(x)$.

نظرية 45.16

ليكن T تحويلاً دورياً على فضاء متجهي V و $f(x)$ كثيرة حدوده الأصغرية إذا كان $f(x)=[f_1(x)]^{\alpha_1}[f_2(x)]^{\alpha_2}..[f_t(t)]^{\alpha_t}$ تحليلاً لكثيرة الحدود $f(x)$ كحاصل ضرب قوى لكثيرات حدود واحدية مختلفة غير قابلة للتحليل $f_i(x)$ على F ، عندئذ يكون $V = V_1 \oplus V_2 \oplus ... \oplus V_t$ لجملة فضاءات جزئية V_i في V لا متغيرة وفق T بحيث المقصور T_i للتحويل T على V_i هو تحويل خطي دوري على V_i بحيث تكون $[f_i(x)]^{\alpha_i}$ هي كثيرة حدوده الأصغرية .

البرهان

بما أن T تحويل دوري على V ، $V = F[T]v$ لبعض $v \in V$ و $f(x)$ هي كثيرة الحدود الأصغرية لـ v نسبة إلى T .

عرف $v_1 = [f_2(T)]^{\alpha_2}[f_3(T)]^{\alpha_3}..[f_t(T)]^{\alpha_t} v, v_2 = [f_1(T)]^{\alpha_1}[f_3(T)]^{\alpha_2}..[f_t(T)]^{\alpha_t} v$

$v_t = [f_1(T)]^{\alpha_1}[f_2(T)]^{\alpha_2}..[f_{t-1}(T)]^{\alpha_{t-1}}v$ ....

عندئذ كثيرة الحدود الأصغرية للمتجه v_1 هي $[f_1(x)]^{\alpha_1}$ (قضية 30.16) بصورة عامة كثيرة الحدود الأصغرية للمتجه v_i هي $[f_i(x)]^{\alpha_i}$ وهكذا استناداً إلى القضية 29.16 فإن كثيرة الحدود الأصغرية للمتجه

$$w = v_1 + v_2 + ..v_t \qquad (1)$$

هي

$$[f_1(x)]^{\alpha_1}[f_2(x)]^{\alpha_2}..[f_t(x)]^{\alpha_t} = f(x)$$

إذاً $\dim V = \deg f(x) = \dim F[T]w$ يؤدي إلى أن :

$$V = F[T]w \qquad (2)$$

ليكن $V_1 \le i \le t, V_i = F[T]v_i$ ، بما أن $TF[T]v_i \subseteq F[T]v_i$ فإننا نتوصل إلى أن V_i هو فضاء جزئي لا متغير وفق T ، عليه إذا كان T_i مقصور T على V_i نجد أن $V_i = F[T_i]v_i$ هو فضاء دوري نسبة إلى T_i ، بما أن $[f_i(x)]^{\alpha_i}$ هي كثيرة الحدود الأصغرية للمتجه v_i نسبة إلى T نجد أيضاً أن $[f_i(x)]^{\alpha_i}$ هي كثيرة الحدود الأصغرية للمتجه V_i نسبة إلى T_i إذاً $[f_i(x)]^{\alpha_i}$ هي كثيرة الحدود الأصغرية للتحويل T_i .

بما أن $w = v_1 + v_2 + ... + v_t$ يعني أن $V = F[T]w \subseteq F[T]v_1 + ..F[T]v_t$ فإن :

$$V = v_1 + v_2 + ... + v_t \qquad (3)$$

ندعي ان هذا المجموع هو مجموع مباشر ، افرض أن :

$$g_i(T)v_1 + g_2(T)v_2 + ... + g_t(T)v_t = 0 \qquad (4)$$

لبعض $g_i(T)v_i \in V_i = F[T]vli$ فإن :

$$[f_2(T)]^{\alpha_2}..[f_t(t)]^{\alpha_t}[g_1(T)v_1 + ... + g_t(T)v_t] = 0 \qquad (5)$$

بما أن $[f_i(T)]^{\alpha_i}v_i = 0$ لجميع i ، فإن (5) تؤدي إلى أن :

$$g_1[f_2(T)]^{\alpha_2}..[f_t(T)]^{\alpha_t}v_1 = 0$$

وحسب نظرية 24.16 فإن

$$[f_1(x)]^{\alpha_1} \mid g_1(x)[f_2(x)]^{\alpha_2}..[f_t(x)]^{\alpha_t}$$

بالتالي يكون $g_1(x)$ | $[f_1(x)]^{\alpha_1}$ لأن $[f_1(x)]^{\alpha_1}$ أولية نسبياً مع كل واحدة من $[f_i(x)]^{\alpha_i}$ حيث $i \geq 2$ إذاً $g_1(T)v_1 = 0$ بالمثل فإن $g_2(T)v_2 = 0, ..., g_t(T)v_t = 0$ وهكذا فإن كل حد من الطرف الأيسر في (4) يساوي صفراً ، إذاً $V = v_1 \oplus v_2 \oplus ... \oplus v_t$ وهذا يثبت صحة النظرية .

نظرية 46.16

ليكن T تحويلاً خطياً دورياً على فضاء متجهي V ولتكن $f(x) = [f_1(x)]^{\alpha_1}[f_2(x)]^{\alpha_2}...[f_t(x)]^{\alpha_t}$ كثيرة الحدود الأصغرية للتحويل T حيث $f_i(x)$ هي كثيرات حدود واحدية مختلفة غير قابلة للتحليل على F و $\alpha_i \geq 1$ ، عندئذ توجد قاعدة مرتبة B للفضاء V بحيث تكون مصفوفة T بالنسبة لها هي

$$\begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & ... & \\ & & & J_t \end{pmatrix}$$

حيث J_i $(i = 1, 2, ..., t)$ هي مصفوفة جوردان لـ $[f_i(x)]^{\alpha_i}$ نسبة إلى $f_i(x)$ (تعريف 42.16) .

البرهان

نستطيع أن نكتب :

$$V = V_1 \oplus V_2 \oplus ... \oplus V_t \qquad (1)$$

لبعض فضاءات جزئية V_i في V لا متغيرة وفق T بحيث يكون V_i دوري نسبة إلى T_i حيث T_i هو مقصور T على V_i و $[f_i(x)]^{\alpha_i}$ هي كثيرة الحدود الأصغرية للتحويل T_i (نظرية 42.16) . نستطيع إيجاد قاعدة مرتبة $B_i = (w_1^i, w_2^i, ..., w_{n_i}^i)$ للفضاء V_i بحيث تكون مصفوفة T_i نسبة إلى B_i هي مصفوفة جوردان J_i لكثيرة الحدود $[f_i(x)]$ نسبة إلى $f_i(x)$ (نظرية 41.16 وتعريف 42.16) .

الآن $B = (w_1^1, w_2^1, ..., w_{n_1}^1, w_1^2, w_2^2, ..., w_{n_2}^2, ..., w_1^t, w_2^t, ..., w_{n_t}^t)$

هي قاعدة مرتبة للفضاء V ، ليكن $J_i = \left(b_{im}^i\right)$ عندئذ يكون :

$$T\left(w_m^i\right) = T_i\left(w_m^i\right) = \sum_{\ell=1}^{nt} b_{\ell m}^i \, w_\ell^i \,, \forall_{i,m} \qquad (2)$$

لاحظ $T\left(w_m^i\right)$ يمكن التعبير عنه كتركيب خطي في $w_1^i, w_2^i, \ldots, w_{n_i}^i$ وأن المعاملات $B_{\ell m}^i$ مأخوذة من J_i بحفظ ذلك في الذاكرة فإننا نقتنع بسهولة أن مصفوفة T نسبة إلى B هي

$$\begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ldots & \\ & & & J_t \end{pmatrix}$$

وتَرِدُ على الفور النتيجة الآتية :

نتيجة 47.16

لتكن $A \in M_n(F)$ بحيث تكون درجة كثيرة حدودها الأصغرية $f(x)$ تساوي n ، فإذا كان $f(x) = \left[f_i(x)\right]^{\alpha_1} \ldots \left[f_t(x)\right]^{\alpha_t}$ حيث $f_i(x)$ هي كثيرات حدود واحدية غير قابلة للتحليل على F و $\alpha_i \geq 1$ عندئذ توجد مصفوفة غير منفردة P بحيث أن

$$P^{-1} A P = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ldots & \\ & & & J_t \end{pmatrix}$$

حيث J_i هي مصفوفة جوردان لكثيرة الحدود $\left[f_i(x)\right]^{\alpha_i}$ نسبة إلى $f_i(x)$.

في النظرية الأساسية للجبر نعلم أن أية كثيرة حدود درجتها n على C وحقل الأعداد المركبة تكون جميع جذورها في C وعددها n عليه إذا كانت $f(x)$ كثيرة حدود واحدية على C درجتها n فإننا نستطيع أن نكتب :

$$f(x) = \left(x - a_1\right)^{\alpha_1} \left(x - a_2\right)^{a_2} \ldots \left(x - a_t\right)^{\alpha_t}$$

حيث $a_1,a_2,...,a_t$ هي جذور مختلفة لكثيرة الحدود $f(x)$ و α_i هي أعداد صحيحة موجبة، كما رأينا سابقاً مصفوفة جوردان J_i لكثيرة الحدود $(x-a_i)^{\alpha_i}$ نسبة إلى $x-a_i$ هي قالب جوردان الآتي

$$\begin{pmatrix} a_i & 1 & 0 & ... & 0 \\ 0 & a_i & 1 & ... & 0 \\ 0 & 0 & a_i & ... & ... \\ 0 & 0 & 0 & ... & 1 \\ 0 & 0 & 0 & ... & a_i \end{pmatrix}$$

وهكذا فإن نظرية 46.16 تؤدي إلى النتيجة الآتية :

نتيجة 48.16

ليكن $A \in M_n(C)$ بحيث كانت درجة كثيرة الحدود الأصغرية $f(x)$ للعنصر A تساوي n إذا كان $a_1,a_2,...,a_t$ هي الجذور المختلفة لكثيرة الحدود $f(x)$ بتكرارات $\alpha_1,\alpha_2,...,\alpha_t$ على الترتيب ، فإنه يوجد مصفوفة غير منفردة P في $M_n(C)$ بحيث يكون

$$P^{-1}AP = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & ... & \\ & & & J_t \end{pmatrix}$$

حيث كل J_i هو قالب جوردان سعتها $\alpha_i \times \alpha_i$

$$\begin{pmatrix} a_i & 1 & 0 & ... & 0 \\ 0 & a_i & 1 & ... & 0 \\ ... & 0 & ... & 0 & ... \\ 0 & 0 & 0 & ... & a_i \\ 0 & 0 & 0 & ... & a_i \end{pmatrix}$$

تعريف 49.16

ليكن T تحويلاً خطياً دورياً على فضاء متجهي V_F ولتكن $f(x)=[f_1(x)]^{\alpha_1}..[f_i(x)]^{\alpha_t}$ كثيرة الحدود الأصغرية للتحويل T حيث $f_i(x)$ هي كثيرات حدود واحدية مختلفة وغير قابلة للتحليل على F فإن المصفوفة

$$\begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \dots & \\ & & & J_t \end{pmatrix}$$

حيث J_i هي مصفوفة جوردان لكثيرة الحدود $[f_i(x)]^{\alpha_i}$ نسبة إلى $f_i(x)$ تسمى المصفوفة القانونية الكلاسيكية أو صيغة جوردان القانونية للتحويل T ، المصفوفة السابقة تسمى أيضاً بالمصفوفة القانونية الكلاسيكية لكثيرة الحدود $f(x)$.

تعريف 50.16

ليكن T تحويلاً خطياً على فضاء متجهي V و $V_1, V_2, ..., V_t$ فضاءات جزئية لا متغيرة وفق T بحيث $V = V_1 \oplus V_2 \oplus ... \oplus V_t$ إذا كان T_i مقصور T على V_i فإن T يسمى المجموع المباشر للتحويلات $T_1, T_2, ..., T_t$ ويكتب $T = T_1 \oplus T_2 \oplus ... \oplus T_t$.

إذا كانت A_i مصفوفة T_i نسبة إلى قاعدة مرتبة ما B_i للفضاء V_i و B هي القاعدة المرتبة للفضاء V وهي اتحاد جميع القواعد التي فيها عناصر B_1 تسبق عناصر B_2 في الترتيب وعناصر B_3 تلي عناصر B_2 في الترتيب وهكذا . من الممكن أن نرى بسهولة أن مصفوفة A نسبة إلى B هي

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \dots & \\ & & & A_t \end{pmatrix}$$

نقول أن A هو مجموع مباشر من $A_1, A_2, ..., A_t$ وتكتب $A = A_1 \oplus A_2 \oplus ... \oplus A_t$.

مثال 16

ليكن T تحويلاً خطياً على $\overset{3}{Q}$ كثيرة حدوده الأصغرية هي $f(x) = (x^2+1)(x+1)$ و x^2+1 و $x+1$ هما عاملان مختلفان لكثيرة الحدود $f(x)$ وهما أحديان وغير قابلين للتحليل .

المصفوفتان المصاحبتان لهما هما $J_1=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, J_2=(-1)$. بالتالي فإن المصفوفة القانونية الكلاسيكية للتحويل T هي :

$$\begin{pmatrix}J_1 & 0\\ 0 & J_2\end{pmatrix}=\begin{pmatrix}0 & -1 & 0\\ 1 & 0 & 0\\ 0 & 0 & -1\end{pmatrix}$$

مثال 17

ليكن T تحويلاً خطياً على C^5 ، كثيرة حدوده الأصغرية هي $f(x)=(x-1)^2(x-2)(x-3)^2$ ، بما أن $\deg f(x) = \dim C^5$ فإن T تحويل خطي دوري .

مصفوفات جوردان لكثيرات الحدود $(x-1)^2, (x-2)$ و $(x-3)^2$ هي على الترتيب :

$$J_3=\begin{pmatrix}3 & 1\\ 0 & 3\end{pmatrix}, J_2=(2), J_1=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

عليه فإن المصفوفة القانونية الكلاسيكية للتحويل T هي :

$$\begin{pmatrix}J_1 & 0 & 0\\ 0 & J_2 & 0\\ 0 & 0 & J_3\end{pmatrix}=\begin{pmatrix}1 & 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 2 & 0 & 0\\ 0 & 0 & 0 & 3 & 1\\ 0 & 0 & 0 & 0 & 3\end{pmatrix}$$

لاحظ أن الأعداد 1 ، 2 و 3 التي تظهر على القطر هي قيم ذاتية للتحويل .

مثال 18

اعتبر التحويل الخطي T على Q^2 المعرف كما يلي $T(e_1)=e_1$ ، $T(e_2)=3e_1+2e_2$ حيث (e_1, e_2) هي القاعدة القياسية للفضاء Q^2 . بما ان $\{e_1, T(e_1)\}=\{e_1, e_2\}$ مستقلة خطياً فإن درجة كثيرة الحدود الأصغرية للعنصر e_1 نسبة إلى T هي على الأقل 2 ، وبما أن درجتها لا يمكن أن تتجاوز $\dim Q^2$ والذي يساوي 2 فإنها تساوي 2 ، عليه فإن T تحويل دوري .

مصفوفة T نسبة إلى (e_1,e_2) هي :

$$A=\begin{pmatrix}0 & 3\\ 1 & 2\end{pmatrix} \qquad (1)$$

بما أن $A^2-2A-3I=0$ و T دوري فإن $f(x)=x^2-2x-3=(x+1)(x-3)$ هي كثيرة الحدود الأصغرية للتحويل T .

الآن $x+1$ ، $x-3$ هما العاملان الوحيدان المختلفان لكثيرة الحدود $f(x)$ وكلاهما غير قابل للتحليل .

مصفوفتا جوردان لهما (هنا بالضبط المصفوفتان المصاحبتان) هما على الترتيب (-1) و (3) إذاً المصفوفة القانونية الكلاسيكية للتحويل T هي $\begin{pmatrix}-1 & 0\\ 0 & 3\end{pmatrix}$.

دعنا نحدد قاعدة مرتبة للفضاء Q^2 بحيث تكون مصفوفة T بالنسبة لها هي المصفوفة القانونية الكلاسيكية السابقة .

عرف :

$$u_1=(T-3I)e_1=T(e_1)-3I(e_1)=-3e_1+e_2 \qquad (2)$$
$$u_2=(T+I)e_1=T(e_1)+I(e_1)+e_1+e_2 \qquad (3)$$

u_2,u_1 مستقلان خطياً (أثبت ذلك) فتكون $B=(u_1,u_2)$ هي قاعدة مرتبة للفضاء Q^2 .

الآن :

$$T(u_1)=-3T(e_1)+T(e_2)=-3e_2+(3e_1+2e_2)=3e_1-e_2$$

أي أن $T(u_1)=-u$.

بالمثل فإن $T(u_1)=3u_2$. إذاً مصفوفة T نسبة إلى القاعدة (u_1,u_2) هي $A'=\begin{pmatrix}-1 & 0\\ 0 & 3\end{pmatrix}$ من (2) و (3)يتضح أن مصفوفة (u_1,u_2) نسبة إلى (e_1,e_2) هي $P=\begin{pmatrix}-3 & 1\\ 1 & 1\end{pmatrix}$.

ويمكن التحقق بسهولة من أن $A'=P^{-1}AP$.

مسائل

1. اكتب المصفوفات المصاحبة لكثيرات الحدود التالية :

i. $x+1$ ii. x iii. x^2+2x+5 iv. x^3+x^2+x+1

v. x^3-x+1 vi. x^3+1 vii. $x^4+x^3+x^2+1$ viii. x^4+20x^2+x

2. عَيِّن تحويلاً خطياً T :

i. على Q بحيث تكون كثيرة حدوده الأصغرية هي $x+1$.

ii. على Q^2 بحيث تكون كثيرة حدوده الأصغرية هي x^2+2x+5 .

iii. على Q^3 بحيث تكون كثيرة حدوده الأصغرية هي x^3-x+1 .

iv. على Q^4 بحيث تكون كثيرة حدوده الأصغرية هي x^4-20x^2+4 .

3. لتحويل خطي T ما على فضاء متجهي V ، الفضاء الجزئي W في V اللامتغير وفق T والذي هو بالصيغة $F[T]v$ ، $v\in V$ يسمى فضاء جزئي دوري لا متغير وفق T .

i. إذا كان $T\in A(Q^2)$ التحويل المعطى حسب $T(e_1)=e_2$ ، $T(e_2)=e_1$ و $T(e_3)=e_3$.
حدد $F[T]e_1$ ، $F[T]e_3$ الفضاءان الجزئيان الدوريان اللامتغيران وفق T .
[**إرشاد** : $F[T]e_1$ هو فضاء جزئي مولد من (e_1,e_2)] .

4. المصفوفات الآتية على Q هي مصفوفات مصاحبة لبعض كثيرات الحدود ، عين كثيرات الحدود تلك :

$\begin{pmatrix}0&2\\1&0\end{pmatrix}$ ، $\begin{pmatrix}0&-1\\1&1\end{pmatrix}$ ، $\begin{pmatrix}0&0\\1&1\end{pmatrix}$ ، $\begin{pmatrix}0&0&-5\\1&0&3\\0&1&0\end{pmatrix}$ ، $\begin{pmatrix}0&0&-1\\1&0&0\\0&1&0\end{pmatrix}$ ، $\begin{pmatrix}0&0&1\\1&0&-2\\0&1&3\end{pmatrix}$ ، (5) ، (-8) ، (10) .

5. (a) اكتب مصفوفات جوردان لكثيرات الحدود :

i. $f(x)=(x^2+1)^3$ نسبة إلى x^2+1 .

ii. $f(x)=(x^2+2x+1)^2$ نسبة على x^2+2x+1 .

iii. $f(x)=(x+1)^4$ نسبة إلى $x+1$.

(b) اكتب المصفوفات المصاحبة لكل من كثيرات الحدود في (a) برهن في كل حالة أن المصفوفة المصاحبة ومصفوفة جوردان متشابهتان .

6. لكل مصفوفة A في المسألة 4 عين $xI'-A$ حيث I' هي المصفوفة المحايدة التي لها نفس العدد من الصفوف والأعمدة كما للمصفوفة A . برهن أن محدد $xI'-A$ هو كثيرة الحدود الأصغرية لـ A (أي كثيرة الحدود التي تصاحبها المصفوفة A) .

7. لتكن A_2, A_1 أية مصفوفتين على حقل F . برهن أن المصفوفتين $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ و $\begin{pmatrix} A_2 & 0 \\ 0 & A_1 \end{pmatrix}$ متشابهتان .

[**إرشاد** : ليكن V_1 فضاءاً متجهاً على F مع القاعدة المرتبة $B_1=(u_1,u_2,...,u_t)$ بحيث A_1 هي مصفوفة لتحويل خطي T_1 على V_1 نسبة للقاعدة B_1] .

ليكن A_2 مصفوفة لتحويل خطي T_2 على فضاء متجهي V_2 على F نسبة لقاعدة مرتبة $B_2=(v_1,v_2,...,v_m)$ اعتبر $V=V_1\oplus V_2$ و $T=T_1\oplus T_2$ عندئذ مصفوفة T نسبة للقاعدة $B=(u_1,u_2,...,u_t,v_1,v_2,...,v_m)$ هي $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ ونسبة للقاعدة $B'=(v_1,v_2,...,v_m,u_1,u_2,...,u_t)$ هي $\begin{pmatrix} A_2 & 0 \\ 0 & A_1 \end{pmatrix}$]

8. لأي k من المصفوفات $C_1,C_2,...,C_k$ ولأي تبديل σ للمجموعة $\{1,2,3,...,k\}$ بين أن المصفوفتين

$$\begin{pmatrix} C_{\sigma(1)} & & & \\ & C_{\sigma(2)} & & \\ & & \cdots & \\ & & & C_{\sigma(k)} \end{pmatrix} \quad و \quad \begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \cdots & \\ & & & C_k \end{pmatrix}$$

متشابهان .

9. يقال لتحويل خطي T على فضاء متجهي V أنه عديم القوة إذا كان $T^k = 0$ لعدد صحيح موجب k . تعريف مشابه يمكن إعطاؤه لمصفوفة .

(a) بين أن المصفوفات :

$$A_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

عديمة القوة . في الواقع تحقق من أن :

i. $A_2^2 = 0, A_2 \neq 0$.

ii. $A_3^3 = 0$ لكن $A_4^2 \neq 0$.

iii. $A_4^4 = 0$ لكن $A_4^3 \neq 0$.

(b) إذا كان $T \neq 0$ تحويلاً عديم القوة على V بحيث كان $T^k = 0$ لكن $T^{k-1} \neq 0$ فإن k يسمى دليل المعدومية للتحويل T .

تعريف مشابه يُعطى لمصفوفة

إذا كانت $A_1, A_2, A_3, ..., A_t$ مصفوفات عديمة القوة وأدلة معدوميتها هي $k_1, k_2, ..., k_t$ على الترتيب ، برهن أن المصفوفة

$$A = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \cdots & \\ & & & A_t \end{pmatrix}$$

عديمة القوة وأن دليل انعدامها هو $k = \max k_i \ (1 \le i \le t)$.

(c) برهن أن التحويل الخطي العديم القوة ليس له قيم ذاتية تختلف عن الصفر .

[إرشاد : $T(v) = \alpha v \Rightarrow T^k(v) = \alpha_v^k, \forall k \ge 1$ **]**

4. بعض نظريات التحليل

نظرية 51.16

ليكن $T \in A(V)$ حيث كثيرة حدوده الأصغرية هي $f(x) = (P(x))^t$ لكثيرة حدوده p غير قابلة للتحليل وعدد صحيح $1 \le t$ بالإضافة إلى ذلك افرض أن $u \in V$ بحيث كانت كثيرة الحدود الأصغرية للمتجه u نسبة إلى T هي $f(x)$ نفسها . فإنه يوجد فضاء جزئي W في V لا متغير وفق T بحيث يكون $V = W \oplus F[T]u$.

البرهان

اعتبر F عائلة جميع الفضاءات الجزئية U في V اللامتغيرة وفق T والتي تقاطعها مع $F[T]u$ يساوي (0) . بما ان الفضاء الجزئي (0) لامتغير وفق T وواضح أن $(0) \cap F[T]u = (0)$ فإن $(0) \in F$ أي أن F عائلة غير خالية ، وحيث أنه لا يوجد عضو في F ذو بعد أكبر من n حيث $n = \dim V$ فإنه يمكننا العثور على عضو W في F بعد أكبر بعد من بين جميع أعضاء F .

وعليه فإن W هو فضاء جزئي في V لا متغير وفق T له أكبر بعد بحيث أن $W \cap F[T]u = (0)$.

ندّعي أن $V = W \oplus F[T]u$ افرض خلاف ذلك وهذا يعني أنه يوجد $v \in V$ بحيث $v \notin W + F[T]u$.

الآن $[p(T)]_v^0 = IV = v \notin W - F[T]u$ ولكن هو في $W + F[T]u$ ولكن $[p(T)]_v^t = 0$.

عليه يمكننا إيجاد عدد صحيح $t \geq \ell$ بحيث $[p(T)]_v^\ell \in W + F[T]u$ في حين $[p(T)]_v^{\ell-1} \notin W + F[T]u$ ضع $y = [p(T)]_v^{\ell-1}$ فإن y ينتمي إلى V و لا ينتمي إلى $W + F[T]u$.

كذلك $p(T)\,y = [p(T)]_v^\ell$ ينتمي إلى $W + F[T]u$ لذا فإن :

$$p(T)\,y = w + g(T)u \qquad (1)$$

لبعض $w \in W$ و $g(x) \in F(x)$ زد على ذلك أن :

$$0 = [p(T)]_y^t = [p(T)]^{t-1} p(T)\,y = [p(T)]_w^{t-1} + [p(T)]^{t-1}(T)u \qquad (2)$$

بما أن المجموع $W + F[T]u$ هو مجموع مباشر فإن $[p(T)]^{t-1} w = 0$ و $[p(T)]^{t-1} g(t)u = 0$

وعليه ولأن $[p(x)]^t$ هي كثيرة الحدود الأصغرية للعنصر u نسبة إلى T فإن $[p(x)]^t \big| [p(x)]^{t-1} g(x)$.

هذا يؤدي إلى أن $p(x) | g(x)$ عليه فإن $g(x) = p(x) g_1(x)$ لبعض $g_1(x) \in F[x]$ عندئذ يكون لدينا $p(T)\,y = w + p(T) g_1(T)u$ أي أن :

$$p(T)[y - g_1(T)u] = w \in W \qquad (3)$$

اعتبر W_1 الفضاء الجزئي اللامتغير وفق T حيث $W_1 = W + F[T][y - g_1(T)u]$ ، $W \subseteq W_1$ فإذا كان $y - g_1(T)u \in W$ فسوف نحصل على $y = g_1(T)u + w'$ لبعض $w' \in W$ عندئذ يكون $y \in F[T]u + W$ وهذا تناقض لذا فإن $y - g_1(T)u \notin W$ وهذا يبرهن أن W_1 يحوي W فعلياً .

فيكون $\dim W_1 > \dim W$ وحيث أننا اخترنا W فضاءاً جزئياً لا متغيراً وفق T وذو أكبر بعد بين الفضاءات الجزئية التي تحقق $W \cap F[T]u = 0$ فإن $W_1 \cap F[T]u \neq (0)$ إذاً يوجد عنصر غير صفري $w_1 \in W_1 \subset F[T]u$ بحيث :

$$w_1 = w' + h(T)[y - g_1(T)u] \qquad (4)$$

ولما كان $w' \in W$ و $w_1 \in F[T]u$ فإننا نحصل على :

$$w' + h(T)[y - g_1(T)u] = h'(T)u \qquad (5)$$

لبعض $h'(x) \in F[x]$ إذاً :

$$h(T)y = -w' + [h(T)g_1(T) + h'(T)]u \in W + F[T]u \qquad (6)$$

إذا كان $p(x) | h(x)$ ، فإن $h(x) = p(x)h_1(x), h_1(x) \in F[x]$.

بالتالي المعادلتين (3) و (4) تؤديان إلى أن $w_1 = w' + h_1(T)p(T)[y - g_1(T)u] \in W$

من جهة ثانية حسب (4) فإن $w_1 \in F[T]u$ عليه فإن $w_1 \in W_n F[T]u = (0)$ هذا يناقض حقيقة أن $w_1 \neq 0$ إذاً $p(x)$ لا يقسم $h(x)$ أي أن العامل المشترك الأكبر لكثيرتي الحدود $p(x)$ و $h(x)$ هو 1 وبناء عليه فإن $1 = a(x)h(x) + b(x)p(x)$ لبعض $a(x), b(x) \in F[x]$.

إذاً $1 = a(T)h(T) + b(T)p(T)$ ومنها $y = Iy = a(T)h(T)y + b(T)p(T)y$.

بما أن (1) $p(T)y \in W + F[T]u$ ومن (6) $h(T)y \in W + F[T]u$ و $W + F[T]u$ هو فضاء جزئي في V لا متغير وفق T فالمعادلة الأخيرة تبين أن $y \in W + F[T]u$ وهذا يناقض الفرض $y \notin W \in F[T]u$ إذاً $V = W \oplus F[T]u$.

نظرية 52.16

ليكن $T \in A(V)$ تحويلاً كثيرة حدوده الأصغرية هي $f(x) = (p(x))^k$ لكثيرة حدود واحدية غير قابلة للتحليل $p(x)$ ولعدد صحيح موجب k عندئذ يكون $V = F[T]u, \oplus F[T]u \oplus ... \oplus F[T]u_t$ لبعض المتجهات الغير صفرية $(1 \le i \le t)u_i$ بحيث كثيرة

الحدود الأصغرية للمتجهات u_i نسبة إلى T هي $(p(x))^{k_i}$ محققة الشرط $k=k_1 \geq k_2 \geq .. k_t > 1$ وهذه الأعداد k_i وحيدة التحديد بواسطة T .

البرهان

من نظرية 31.16 الفضاء V فيه عنصر غير صفري وليكن u_1 بحيث تكون كثيرة الحدود الأصغرية له نسبة إلى T هي $f(x)=(p(x))^{k_1}$ حيث $k=k_1$ (نظرية 31.16) ومن نظرية 51.16 فإن :

$$V = F[T]u_1 \oplus V_1 \qquad (1)$$

لفضاء جزئي V_1 في V تكون لا متغيراً وفق T إذا كان $V_1=(0)$ فقد تحقق المطلوب . لنفرض $V_1 \neq (0)$ فمن الواضح $\dim V_1 < \dim V$ ليكن T_1 مقصور T على V_1 فتكون كثيرة الحدود الأصغرية للتحويل T_1 وهي أحد عوامل كثيرة الحدود $f(x)=(p(x))^{k_1}$ فإنها تساوي $(p(x))^{k_1}$ لبعض $k_i \leq k_2$ إذا كان $k_2=0$ فإن $(p(x))^{k_2}=I$ يؤدي إلى أن $(0)=(p(T))^{k_2}V_1=IV_1=V_1$ وهذا تناقض لذا فإن $k_2 \geq 1$.

مرة أخرى فحسب نظرية 31.16 يمكننا العثور على متجه u_2 في v_1 بحيث تكون كثيرة الحدود الأصغرية لـ u_2 نسبة إلى T_1 (بالتالي نسبة إلى T تكون T_1 مقصور T) هي $(p(x))^{k_2}$ وإستناداً إلى نظرية 51.16 نحصل على أن :

$$V_1 = F[T]u_2 \oplus v_2 \qquad (2)$$

إذاً لفضاء جزئي V_2 من V يكون لا متغيراً وفق T_1 (بالتالي لا متغيراً وفق T)

$$V = F[T]u_1 \oplus F[T]u_2 \in V_2$$

إذا كان $V_2=(0)$ فإننا نكون قد أكملنا البرهان بخلاف ذلك فباعتبار T_2 مقصور T_1 (ومن ثم T) على V_2 فإننا نتابع ... بالنسبة للفضاء V أو V_1 ولما كان $\dim V_2 < \dim V_1 < \dim V$ و $\dim V$ منته ، فإن هذه العملية تنتهي بعد عدد منته من الخطوات ، عليه نحصل على أن :

$$V = F[T]u_1 \oplus F[T]u_2 \oplus \ldots \oplus F[T]u_t \qquad (3)$$

بحيث أن كثيرة الحدود الأصغرية لكل u_i هي $(p(x))^{k_i}$ مع تحقيق الشرط $k = k_1 \geq k_2 \geq k_3 \geq \ldots \geq k_t \geq 1$.

نحن نحاول بيان أن $k_1, k_2, \ldots, k_t$ مستقلة عن التحليل (3) من أجل ذلك نفرض أن:

$$V = F[T]u_1 \oplus F[T]u_2' \oplus \ldots \oplus F[T]u_5' \qquad (4)$$

بحيث أن كثيرة الحدود الأصغرية لكل u_i' هي $(p(x))^{k_i'}$ مع تحقق الشرط $k = k_1' \geq k_2' \geq \ldots \geq k_5' \geq 1$.

اعتبر $W = \{v \in V \,|\, p(T)v = 0\}$ فإن W فضاء جزئي في V كذلك لأي عنصر $w \in W$ فإن

$$p(T)[T(w)] = T[p(t)w] = 0 \Rightarrow Tw \in W$$

وهكذا فإن W فضاء جزئي في V وهو لا متغير وفق T ليكن $w \in W$ من (3) يكون $w = \sum_{i=1}^{t} g_i(T)u_i$ لبعض $g_i(x) \in F[x]$ ، $(1 \leq i \leq t)$ إذاً $p(T)w = 0$ يؤدي إلى أن :

$$p(T)g_1(T)u_1 + p(T)g_2(T)u_2 + \ldots + p(T)g_t(T)u_t = 0$$

طالما أن (3) مجموعاً مباشراً فإن $p(T)g_i(T)u_i = 0$ لكل $1 \leq i \leq t$ هذا يؤدي إلى أن $(p(x))^{k_i} \,|\, p(x)g_i(x)$ لأن $(p(x))^{k_i}$ هي كثيرة الحدود الأصغرية للعنصر u_i بالتالي $(p(x))^{k_i - 1} \,|\, g_i(x)$ أي أن $g_i(x) = h_i(x)(p(x))^{k_i - 1}$ عليه إذا وضعنا $w_i = (p_i(T))^{k_i - 1}u_i$ ، فإننا نرى أن $0 \neq w_i \in W$ وكل عضو من W هو بالصيغة $h_1(T)w_1 + h_2(T)w_2 + \ldots + h_t(T)w_t$.

إذاً $W = F[T]w_1 + F[T]w_2 + \ldots + F[T]w_t$ إضافة إلى ذلك يكون $F[T]w_i \subseteq F[T]u_i, (1 \leq i \leq t)$ وحسب (3) يكون مجموع الفضاءات $F[T]u_i$ مجموعاً مباشراً فإن مجموع الفضاءات $F[T]v_i$ هو أيضاً مجموع مباشر بعبارة أخرى :

$$W = F[T]w_1 \oplus F[T]w_2 \oplus \ldots \oplus F[T]w_t \qquad (5)$$

وبالمثل باستخدام (4) نحصل على أن :

$$W = F[T]w'_1 \oplus F[T]w'_2 \oplus \ldots \oplus F[T]w'_s \qquad (6)$$

حيث $0 \neq w'_i = [p(T)]^{k'_i-1}_{u'_i}$ ، $1 \leq i \leq 5$.

لأن أي عنصر غير صفري $w \in W$ يحقق $p(T)w = 0$ فإن كثيرة الحدود الأصغرية للعنصر w هي عامل من عوامل كثيرة الحدود $p(x)$. مرة أخرى بما أن كثيرة الحدود الأصغرية لمتجه غير صفري ذات درجة موجبة دائماً و $p(x)$ غير قابلة للتحليل فإننا نحصل على أن $p(x)$ هي نفسها كثيرة الحدود الأصغرية للعنصر w إذاً كثيرة الحدود الأصغرية لكل w_i أو w'_i هي $p(x)$.

اعتبر $K = \dfrac{F[x]}{< p(x) >}$ فإن K حقل (لماذا ؟) لأن مجموعة مصاحبة $\overline{g(x)} = g(x) + < p(x) >$ في K ولأي $w \in W$ عرف $g(x)w = g(T)w$.

هذا معرف تعريفاً جيداً لأننا إذا فرضنا $\overline{g(x)} = \overline{g_1(x)}$ لبعض $g(x), g_1(x) \in F[x]$ فإن $g(x) - g_1(x) \in < p(x) >$ أي أن $p(x) | (g(x) - g_1(x))$ من ذلك ولأن $p(T)w = 0$ يكون $[g(T) - g_1(T)]w = 0$ أي أن $g(T)w = g_1(T)w$ أي أن $\overline{g(x)}w = \overline{g_1(x)}w$ هذا يبين أن الضرب $\overline{g(x)}w$ معرف تعريفاً جيداً .

والآن المعالم واضحة لإثبات أن هذا التعريف يجعل W فضاءاً متجهاً على K .

من الواضح أن $kw = \overline{F[x]}w = F[T]w$ عندئذ من (5) يكون $W = kw_1 \oplus kw_2 \oplus \ldots \oplus kw_t$ هذا يبين أن $\dim_k W = t$ بالمثل من (6) فإن $\dim_k W = s$ إذاً $t = s$ وهذا يثبت أن العدد t يتحدد بصفة وحيدة بواسطة T لذا يبقى أن نبين أن $k_1 = k'_1, k_2 = k'_2, \ldots, k_t = k'_t$ ومن أجل هذا نطبق الاستنتاج على بعد الفضاء المتجهي فنفرض أن النتيجة محققة لجميع الفضاءات المتجهة ذات الأبعاد أصغر من $\dim V$ اعتبر $V' = p(T)V$ بما أن $T(V') = p(T)[TV] \subseteq p(T)V$ فإن V' فضاء جزئي في V لا متغير وفق T ، بالإضافة إلى

أن $(0)=p(T)^k V=[p(T)]^{k-1}V'$ لكــن $[p(T)]^{k-1}V\neq 0$ فنحصــل علــى أن $V'\neq V$ أي أن $\dim V'<\dim V$ عليه إذا كـان T' مقصور على V' فمن فروض الاستنتاج تكون النتيجة محققـة لـ V' و T' بمـا أن $k=k_1\geq k_2\geq\ldots\geq k_t\geq 1$ فبالإمكـان العثـور علـى $\alpha\geq 0$ بحيـث $k_i=1$ لكــــل $i>\alpha$ ولكـــن $k_i>1$ عنــــدما $i\leq\alpha$ عندئـــذ عنــــدما يكــــون $i>\alpha$ $p(T)u_i=[p(T)]^{k_i}u_i=0$ لكن عندما يكون $i\leq\alpha$ فإن $p(T)u_i\neq 0$.

مرة أخرى من (3) يكون

$$V'=p(T)V=F[T]p(T)u_1\oplus\ldots\oplus F(T)p(T)u_\alpha$$
$$=F[T]v_1\oplus\ldots\oplus F(T)v_\alpha \qquad (7)$$

حيث $v_i=p(T)u_i$ ، $(1\leq i\leq\alpha)$ له كثيرة الحدود الأصغرية تساوي $[p(x)]^{k_i-1}$ نسبة إلى T بالتالي نسبة إلى T' بالمثل نحصل على أن :

$$V'=F[T]v_1'\oplus F[T]v_2'\oplus\ldots\oplus F[T]v_\beta \qquad (8)$$

حيث β هـو عـدد صـحيح بحيث يكـون $k_i'=1$ لكـل $i>\beta$ و $k_i'>1$ عنـدما $i\leq\beta$ وإن $v_i'=p(T)u_i'$ له $[p(x)]^{k_i'-1}$ ككثيرة حدود أصغرية $v_i'=p(T)u_i'$ نسبة إلى T (بالتـالي نسبة إلى T') .

مـن فـروض الاسـتنتاج لـدينا $\alpha=\beta$ ، $k_i-1=k_i'-1$ لكـل $i\leq\alpha$ أي أن $k_i=k_i'$ عنـدما يكون $i\leq\alpha$ ونظراً لأن $k_i=1$ ، $k_i'=1$ عندما $i>\alpha$ فمن الواضح أن $k_i=k_i'$ لكل $i>\alpha$ هذا يبرهن أن $k_i=k_i'$ لكل i بذلك يكمل إثبات النظرية .

نظرية 53.16

ليكن T تحويلاً خطياً على V وكثيرة حدوده الأصغرية هي :

$$f(x)=[p_1(x)]^{k_1}[p_2(x)]^{k_2}\ldots[p_v(x)]^{k_v}$$

حيث $p_1(x),p_2(x),\ldots,p_v(x)$ هي كثيرات حدود واحدية مختلفة غير قابلة للتحليل وجميع k_i أعــداد صــحيحة موجبــة فإنــه توجــد فضــاءات جزئيــة وحيــدة $V_1,V_2,\ldots,V_v$ في V

ولا متغيرة وفق T بحيث أن $V=V_1\oplus V_2\oplus\ldots\oplus V_r$ ، $T=T_1\oplus T_2\oplus\ldots\oplus T_r$ حيث T_i هو مقصور T على V_i وأن $[p_i(x)]^{k_i}$ تمثل كثيرة حدوده الأصغرية .

البرهان

ليكن $g_i(x)=\dfrac{f(x)}{[p_i(x)]^{k_i}}$ لكل $1\le i\le r$.

$g_i(x)$ عبارة عن حاصل ضرب جميع كثيرات الحدود $[p_j(x)]^{k_j}$ التي لها $j\ne i$.

عرف :

$$V_i=g_i(T)v \text{ ، } 1\le i\le r \qquad (1)$$

وهو فضاء جزئي في V لا متغير وفق T ، بما أن :

$$[p_i(T)]^{k_i}V_i=[p_i(T)]^{k_i}g_i(T)V=f(T)v=(0)$$

نحصل على أن كثيرة الحدود الأصغرية لمقصور T للتحويل T هي $[p_i(x)]^{k_i}$ بما أن العامل المشترك الأكبر لـ $g_1(x),g_2(x),\ldots,g_r(x)$ هو 1 فإنه يوجد كثيرات حدود $q_1(x),q_2(x),\ldots,q_r(x)$ بحيث :

$$1=g_1(x)q_1(x)+g_2(x)q_2(x)+\ldots+g_r(x)q_r(x) \qquad (2)$$

إذاً :

$$I=g_1(T)q_1(T)+g_2(T)q_2(T)+\ldots+g_r(T)q_r(T) \qquad (3)$$

عندئذ لأي $v\in V$.

$$\begin{aligned} v=I(v)&=g_1(T)q_1(T)v+g_2(T)q_2(T)v+\ldots+g_r(T)q_r(T)v\\ &=v_1+v_2+\ldots+v_r \end{aligned}$$

حيث $v_i=g_i(T)q_i(T)v\in V_i=g_i(T)V$ إذاً $V=V_1+V_2+\ldots+V_r$.

ولبيان أن هذا المجموع هو مجموع مباشر افرض لبعض $x_i\in V_i$ $(1\le i\le r)$ أن :

$$x_1+x_2+\ldots+x_r=0 \qquad (4)$$

وحيث أنه لأي i يكون $[p_j(x)]^{k_j}/g_i(x)$ عندما $j\ne i$ وأن $[p_j(T)]^{k_j}V_j=(0)$ فإننا نجد $g_i(T)V_j=(0)$ عندما $i\ne j$ لذا من (4) نحصل على أن :

$$g_i(T)x_i=0 \qquad (5)$$

الآن $[p_i(x)]^{k_i}$ و $g_i(x)$ أوليـان نسـبياً ، عليـه لكثـيرتي حـدود $a(x)$ و $b(x)$ في $F[x]$ يكون :

$$I=a(x)g_i(x)+b(x)[p_i(x)]^{k_i} \qquad (6)$$

هكذا فإن :

$$I=a(T)g_i(T)+b(T)[p_i(T)]^{k_i} \qquad (7)$$

بالتالي فإن $x_i=I(x_i)=a(T)g_i(T)x_i+b(T)[p_i(T)]^{k_i}x_i=0$ لأن $g_i(T)x_i=0$ (حسب 5) و $[p_i(T)]^{k_i}V_i=(0)$ إذاً في (4) يكون كل $x_i=0$ ومن ثم فإن :

$$V=V_1\oplus V_2\oplus\ldots\oplus V_r \qquad (8)$$

لكي نبين واحدانية الفضاءات V_i افرض أن :

$$V=W_1\oplus W_2\oplus\ldots\oplus W_r \qquad (9)$$

لبعض فضاءات جزئية $W_i(1\le i\le r)$ لا متغيرة وفق T بحيث أن كثيرة الحدود الأصغرية للتحويل T_i (مقصور T على W_i) هي $[p_i(x)]^{k_i}$ وبما أن $[p_i(x)]^{k}|g_i(x)$ لكل $i\ne j$ يكون لدينا $g_i(T)w_j=(0)$ عندما $i\ne j$ ، عليه من (9) نحصل على $g_i(T)V=g_i(T)W_i\subseteq W_i$ أي أن $V_i\subseteq W_i$ من ناحية أخرى لأي $w_i\in W$ فمن (7) يكون

$$\begin{aligned} v_i &= g_i(T)a(T)w_i+b(T)[p_i(T)]^{k_i}w_i \\ &= g_i(T)a(T)w_i\in g_i(T)V=V_i \end{aligned}$$

إذاً $W_i\subseteq V_i$ لذلك فإن $W_i=V_i$ هذا يثبت أن الفضاءات V_i تتحدد بصفة وحيدة .

ملاحظة

نـدعي أن $V_i=\{v\in V\,|\,\exists\alpha_i\ge 0,[p_i(T)]^{\alpha_i}v=0\}$ بما أن $[p_i(T)]^{k_i}V=(0)$ فإن $p_i(T)^{k_i}v=0$ لجميع $v\in V_i$ ، بالعكس افرض أن $v\in V$ يحقق $[p_i(T)]^{\alpha_i}v=0$ لبعض $\alpha_i\ge 1$.

بمـا أن العامـل المشـترك الأكـبر لكثـيرتي الحـدود $[p_i(x)]^{\alpha_i}, g_1(x)$ يسـاوي 1 فـإن $1 = g_i(x)a_1(x) + [p_i(x)]^{\alpha_i} b_1(x)$ لبعض كثيرتي حدود $a_1(x), b_1(x) \in F(x)$ إذاً :

$$v = Iv = g_i(T)a_1(T)v + b_1(T)\{p_i(T)\}^{\alpha_i} v = g_i(T)a_1(T)v \in V_i$$

بالتالي $$V_i = \{v \in V \mid \exists \alpha_i \geq 1 [p_i(T)]^{\alpha_i} v = 0\}$$

نظرية 54.16 (النظرية الأساسية للمجموع المباشر)

ليكن V أي فضاء متجهي بعده $n > 0$ على حقل F و T تحويل خطي على V فإنه توجد كثيرات حدود وحيدة $q_1(x), q_2(x), ..., q_m(x)$ كل واحدة تكون قوة لكثيرة حدود واحدية ، وتوجد فضاءات جزئية دورية $W_1, W_2, ..., W_m$ (ليست بالضرورة وحيدة) لا متغيرة وفق T بحيث $V = W_1 \oplus W_2 \oplus ... \oplus W_m$ وأن كل مقصور T_i من T على W_i له كثيرة حدود أصغرية $q_i(x)$.

البرهان

افرض $f(x) = [p_1(x)]^{k_1}[p_2(x)]^{k_2} .. [p_x(x)]^{k_r}$ هي كثيرة الحدود الأصغرية للتحويل T حيث $p_1(x), p_2(x), ..., p_r(x)$ كثيرات حدود واحدية مختلفة وغير قابلة للتحليل على F و k_i أعداد صحيحة موجبة .

من نظرية 53.16 والملاحظة التالية لها ، نجد أن :

$$V = V_1 \oplus V_2 \oplus ... \oplus V_r \qquad (1)$$

حيث V_i فضاء جزئي في V لا متغير وفق T بحيث تكون كثيرة الحدود الأصغرية للتحويل L_i وهو مقصور T على V_i هي $[p_i(x)]^{k_i}$ وأن :

$$V_i = \{v \in V \mid \exists \alpha_i \geq 1, [p_i(x)]^{\alpha_i} = 0\}$$

واستناداً إلى نظرية 52.16 يمكن كتابة :

$$V_i = F[T]u_{r_1} \oplus F[T]u_{i_2} \oplus ... \oplus F[T]u_{it_i} \qquad (2)$$

لبعض المتجهات غير الصفرية u_{ij} في $V_i\,(1\le j\le t_i)$ بحيث كثيرة الحدود الأصغرية للمتجه u_{ij} نسبة إلى L_i هي $[p_i(x)]^{k_{ij}}$ وتحقق الشرط $k_i=k_{i1}\ge k_{i2}\ge\ldots\ge k_{it}$ الأعداد الصحيحة k_{ij} هذه تحدد بطريقة وحيدة بواسطة L_i وحيث أن L_i هو مقصور T على V_i نحصل أيضاً على أن كثيرة الحدود الأصغرية لكل u_{ij} نسبة إلى T هي $p_i(x)]^{k_{ij}}$ عليه إذا كتبنا :

$$1\le j\le t_i\,,1\le i\le r\,,W_{ij}=F[T]u_{ij} \qquad (3)$$

فإننا في (1) و (2) نحصل على أن :

$$V=W_{11}\oplus W_{12}\oplus\ldots\oplus W_{1t1}\oplus\ldots\oplus W_{r1}\oplus\ldots\oplus W_{rtr} \qquad (4)$$

كل W_{ij} هو فضاء جزئي دوري لا متغير وفق T بحيث أن المقصور T_{ij} لـ T على الفضاء W_{ij} له كثيرة الحدود الأصغرية $[p_i(x)]^{k_{ij}}$ وهي قوة لكثيرة حدود واحدية غير قابلة للتحليل . فالنظرية يكمل برهانها إذا بينّا أن كثيرات الحدود الواحدية هذه تحدد بصفة وحيدة بواسطة T ، لتنفيذ ذلك افرض أن :

$$W=W_1\oplus W_2\oplus\ldots\oplus W_m \qquad (5)$$

حيث كل W_i هو فضاء جزئي دوري لا متغير وفق T بحيث أن $q_i(x)$ هي كثيرة الحدود الأصغرية لمقصور T على W_i ، وأن $q_i(x)$ هي قوة لكثيرة حدود واحدية غير قابلة للتحليل، عندئذ تكون $f(x)=[p_1(x)]^{k_1}..[p_r(x)]^{k_r}$ هي المضاعف المشترك الأصغر لكثيرات الحدود $q_1(x),q_2(x),\ldots,q_m(x)=[p_{j(x)}(x)]^{\alpha_i}$ لبعض $1\le\alpha_i\le k_j(i),\alpha_i$ أو لبعض i و $\alpha_i=k_j(i)$ حسب الملاحظة التي تلت نظرية 53.16 يكون $W_i\subseteq V_{j(i)}$ إضافة إلى ذلك لكل $i=1,2,..,r$ فإن بعضاً من $q_j(x)$ يجب أن يكون قوة لكثيرة الحدود $p_i(x)$ بالتالي لكل $i=1,2,\ldots,r$ ونأخذ U_i كمجموع الفضاءات W_j التي فيها $q(x)$ قوة لكثيرة الحدود $p_i(x)$ فنحصل على أن $U_i\subseteq V_i$ ومنها :

$$V=U_1\oplus U_2\oplus\ldots\oplus U_r \qquad (6)$$

U_i فضاء جزئي في V وهو لا متغير وفق T و $U_i\subseteq V_i$.

اعتبر أي عنصر $x \in V_i$ حسب (6) يكون $x = u_1 + u_2 + ... + u_r$ هذا يؤدي إلى أن :

$$x - u_i = \sum_{j \neq i} u_j \in V_i \cap \left(\sum_{j \neq i} V_j \right) = (0)$$

لأن $u_j U_j \in\subseteq V_j$ لجميع j فإن $x = u_i \in U_i$ ، نتيجة لذلك فإن $U_i = V_i$ لكل $1 \leq i \leq r$.

الآن U_i (وكذلك V_i) هو المجموع المباشر لتلك الفضاءات الجزئية الدورية W_j والتي كثيرة الحدود الأصغرية لمقصور T على W_i هي $q_j(x)$ وهي قوة لكثيرة الحدود $p_i(x)$. من نظرية 52.16 فإن عدد العناصر $w_j \in W_i$ يساوي t_i (من (2)) وأن $q_j(x)$ تساوي $(1 \leq j \leq t_i), [p_i(x)]^{k_{ij}}$ وهكذا فإن كثيرات الحدود $q_j(x)$ هذه تتحدد بصفة واحدة بواسطة T وهذا يكمل البرهان .

تعريف 55-16

ليكن T تحويلاً خطياً على فضاء متجهي V و $V = W_1 \oplus W_2 \oplus ... \oplus W_m$ تحليلاً للفضاء V إلى فضاءات جزئية دورية لا متغيرة بالنسبة إلى T بحيث كثيرة الحدود الأصغرية للتحويل T_i وهو مقصور T على W_i هي $q_i(x)$ وهي قوة كثيرة حدود واحدية غير قابلة للتحليل $q_1(x), q_2(x), ..., q_m(x)$ تسمى القواسم الأولية للتحويل T .
إذا كانت A مصفوفة T نسبة لقاعدة مرتبة ما للفضاء V فإن القواسم الأولية للتحويل T تسمى أيضاً بالقواسم الأولية للمصفوفة A .

ملاحظة

كثيرات الحدود $q_i(x)$ السابقة ليست بالضرورة مختلفة ، وسوف نرى ذلك لاحقاً علماً بأنه من نظرية 54.16 فإن $q_i(x)$ تتحدد بطريقة وحيدة بواسطة T .

نتيجة 56-16

أي جذر في F لقاسم أولي لتحويل خطي T على V_F هو قيمة ذاتية للتحويل T .

البرهان

الآن $V = W_1 \oplus W_2 \oplus \ldots \oplus W_m$ مـن الاصـطلاح في التعريـف السـابق ، بمـا أن W_i فضاء جزئي دوري لا متغير وفق T_i فإنه يوجد $w \in W_i$ كثيرة حدوده الأصغرية نسبة إلى T_i (بالتالي نسبة إلى T) هي $q_i(x)$.

اعتـبر أي جـذر α لكثـيرة الحـدود $q_i(x)$ في F فسـيكون $q_i(x) = g(x)(x-\alpha)$ لـبعض $g(x) \in F[x]$.

بما أن $\deg g(x) < \deg q_i(x)$ ، $[g(T)]w \neq 0$ ضع $v = g(T)w$ ، عندئذ :

$$(T-\alpha)v = (T-\alpha)[g(T)w] = q_i(T)w = 0$$

يؤدي إلى أن $T(r) = \alpha v$ إذاً α هو قيمة ذاتية للتحويل T .

مثال 19

اعتـبر Q^4 لـيكن T تحـويلاً خطيـاً علـى Q^4 بحيـث $T(e_1) = e_2$ ، $T(e_2) = 0$ ، $T(e_3) = e_4$ ، $T(e_4) = 0$ حيث (e_1, e_2, e_3, e_4) هي القاعدة القياسية للفضاء Q^4 .

واضح أن $T^2 = 0$ وأن $T \neq 0$. عليه فإن كثيرة الحدود الأصغرية للتحويل T هي x^2 وهي قوة لكثيرة الحدود $p(x) = x$ ومن الواضح أن $p(x) = x$ غير قابلة للتحليل .

الآن $Q^4 = Q[T]e_1 \oplus Q[T]e_3$ هو مجموع مباشر لفضائيين جزئيين دوريين . بما أن كثيرة الحدود الأصغرية لكل من e_3, e_1 نسبة إلى T هي x^2 فمن اليسير أن نقول أن كثيرتي الحـدود الأصـغرية للتحويـل T وهـو مقصـور T علـى $Q[T]e_1$ و T_3 وهـو مقصـور T علـى $Q[T]e_3$ هما x^2, x^2 على الترتيب .

فيكون حسب المصطلحات في تعريف 53.16 x^2, x^2 هما القاسمان الأوليان للتحويل T وهما في هذه الحالة متساويان .

مثال 20

اعتبر المصفوفة $A=\begin{pmatrix}1&0&0\\0&0&-1\\0&1&2\end{pmatrix}$ ليكن T التحويل الخطي على Q^3 بحيث أن A هي مصفوفته نسبة إلى قاعدة مرتبة (v_1,v_2,v_3) للفضاء Q^3 . عندئذ يكون :

$T(v_1)=v_1$ $T(v_2)=v_3$ ، $T(v_3)=-v_2+2v_3$.

من الواضح أن كثيرة الحدود الأصغرية للمتجه v_1 نسبة إلى T هي $x-1$ وحيث أن درجتها 1 يؤدي إلى أن $F[T]v_1=Q_{v1}$.

$(T-I)^2v_2=\left(T^2-2T+I\right)v_2=0$ ولكن $(T-I)v_2\neq 0$ فطالما أن $(x-1)$ غير قابلة للتحليل فإن $(x-1)^2$ هي كثيرة الحدود الأصغرية للمتجه v_2 نسبة إلى T ، إذاً $Q[T]v_2$ هو الفضاء المتولد في $\{v_2,T(v_2)\}$ أي في (v_2,v_3) بالتالي فإن $Q[T]v_2=Qv_2+Qv_3$ وهكذا فإن

$$Q^3=Q\,y_1\oplus(Q\,y_2\oplus Q\,y_3)=Q[T]v_1\oplus Q[T]v_2$$

وبناء عليه فإن $(x-1)^2$ ، $x-1$ هما القاسمان الأوليان للتحويل T .

مثال 21

اعتبر المصفوفة $A=\begin{pmatrix}0&1&0&0&1\\1&2&0&0&0\\0&0&0&0&-1\\0&0&1&0&4\\0&0&0&1&0\end{pmatrix}$

ليكن T تحويلاً خطياً على Q^5 مصفوفته نسبة إلى القاعدة (القياسية) (e_1,e_2,e_3,e_4,e_5) للفضاء Q^5 هي A .

إذا كان $A_1=\begin{pmatrix}0&1\\1&2\end{pmatrix}$ ، $A_2=\begin{pmatrix}0&0&-1\\1&0&4\\0&1&0\end{pmatrix}$ ، وكما أن $A=A_1\oplus A_2$ فإننا نحصل على أن $W_1=<e_1,e_2>$ ، $W_2=<e_3,e_4,e_5>$ هما فضاءان جزئيان من V لا متغيران بالنسبة إلى T

وأن $V=W_1\oplus W_2$ ليكن كل T_i مقصور T على $W_i\,(i=1,2)$ فإن مصفوفة T_i هي A_i . الآن A_1 هي المصفوفة المصاحبة لكثيرة الحدود غير القابلة للتحليل x^4-2x-1 .

بما أن $T(e_1)=e_2$ فإن $W_1=F[T]e_1$ هو فضاء جزئي دوري وأن كثيرة الحدود الأصغرية للتحويل T_1 هي x^2-2x-1 مرة ثانية لأن $T(e_3)=e_4$ ، $T(e_4)=e_5$ لدينا أيضاً $W_2=F[T]e_3$ فضاء جزئي دوري ، وحيث أن A_2 هي المصفوفة المصاحبة لكثيرة الحدود غير القابلة للتحليل x^3-4x+1 فهذا يؤدي إلى أن كثيرة الحدود الأصغرية للتحويل T هي x^3-4x+1 إذاً كثيرة الحدود الأصغرية للتحويل T هي $(x^2-2x-1)(x^3-4x+1)$ والقواسم الأولية له اثنان هما x^2-2x-1 و x^3-4x+1 .

ملاحظة

أعطينا عدداً منتهياً من كثيرات الحدود الواحدية $q_1(x),q_2(x),...,q_t(x)$ على حقل F ، كل واحدة منها هي قوة لبعض كثيرة حدود غير قابلة للتحليل على F ، يمكننا إنشاء تحويل خطي T على فضاء متجهي V_F ذو بعد يساوي مجموع درجات كثيرات الحدود المعطاة . فهي تكون $q_1(x),q_2(x),...,q_t(x)$ هي قواسم أولية للتحويل T. لذلك ضع $A_i\,(1\le i\le t)$ يمثل المصفوفات المصاحبة لـ $q_i(x)$.

ليكن $\deg q_i(x)=m_i$ و W_i فضاء متجهي على F بعده m_i ، عندئذ يوجد تحويل خطي T_i على W_i مصفوفته نسبة إلى قاعدة مرتبة B_i هي A_i وكثيرة حدوده الأصغرية هي $q_i(x)$ (النظريتان 35.16 و 36.16) .

كما رأينا في إثبات نظرية 35.16 فإن W_i فضاء دوري بالنسبة إلى T_i عندئذ إذا كان $V=W_1\oplus W_2\oplus...\oplus W_t$ و $T=T_1\oplus T_2\oplus...\oplus T_t$ يكون لدينا W_i فضاء جزئي دوري في V نسبة إلى T بحيث T_i يساوي مقصور T على W_i و $q_i(x)$ هي كثيرة الحدود الأصغرية للتحويل T_i . إذاً $q_1(x),q_2(x),...,q_t(x)$ هي القواسم الأولية للتحويل T .

مثال 22

لتكن $(x+1)$ و $(x+1)^2$ و $(x+1)$ و (x^2+x+1) هي أربع كثيرات حدود ، واضح أن كل واحدة منهن هي قوة لكثيرة حدود غير قابلة للتحليل على Q ومصفوفاتها المصاحبة هي على الترتيب :

$A_1=(-1)$ ، $A_2=\begin{pmatrix}0 & -1\\ 1 & -2\end{pmatrix}$ ، $A_3=(-1)$ ، $A_4=\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$.

الآن

$$A_1\oplus A_2\oplus A_3\oplus A_4=\begin{pmatrix}-1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & -1 & 0 & 0 & 0\\ 0 & 1 & -2 & 0 & 0 & 0\\ 0 & 0 & 0 & -1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & -1\\ 0 & 0 & 0 & 0 & 1 & -1\end{pmatrix}$$

عليه إذا كان T تحويلاً خطياً على Q^6 مصفوفته مشابهة للمصفوفة السابقة فإن $(x+1)$ و $(x+1)^2$ و $(x+1)$ و (x^2+x+1) هي القواسم الأولية للتحويل T .

مسائل

1. في كل من التمارين التالية بين أن كثيرة الحدود الأصغرية للتحويل T هي قوة لكثيرة حدود غير قابلة للتحليل ، ومن ثم مثّل الفضاء المتجهي V كمجموع مباشر لفضاءات جزئية دورية وفق T .

a. $V=Q^2$ ، $T(e_1)=2e_1$ ، $T(e_2)=2e_2$.

b. $V=Q^2$ ، $T(e_1)=-e_2$ ، $T(e_2)=e_1$.

c. $V=Q^3$ ، $T(e_1)=e_1-e_2$ ، $T(e_2)=2e_1-e_2$.

d. $V=Q^3$ ، $T(e_1)=e_1$ ، $T(e_2)=2e_1-e_2+e_3$.

e. $V=Q^3$ ، $T(e_1)=e_2$ ، $T(e_2)=e_3$ ، $T(e_3)=-e_1+4e_2$.

f. $V=Q^3$ ، $T(e_1)=e_1$ ، $T(e_2)=e_3$ ، $T(e_3)=2e_1$.

g. $V=Q^4$ ، $T(e_1)=e_2$ ، $T(e_2)=e_1$ ، $T(e_3)=-e_4$ ، $T(e_4)=e_3$.

h. $V=Q^4$ ، $T(e_1)=e_1$ ، $T(e_2)=e_2$ ، $T(e_3)=2e_2-e_3+e_1$ ، $T(e_4)=4e_2-4e_3+4e_4$.

i. $V=Q^4$ ، $T(e_1)=e_2+2e_3-2e_4$ ، $T(e_2)=-3e_1+4e_2-2e_3-6e_4$ ، $T(e_3)=-2e_2+2e_3+e_4$ ، $T(e_4)=-2e_1+4e_2-3e_3-6e_4$.

2. برهن أنه لأي تحويل خطي T على فضاء متجهي V_F فإن مجموع درجات القواسم الأولية للتحويل T يساوي بعد V_F .

3. برهن أن أي تحويلين خطيين T و T' على فضاء متجهي V لهما نفس القواسم الأولية إذا وفقط إذا كانت مصفوفتهما نسبة إلى قاعدة ما للفضاء V متشابهين .

4. برهن أن كثيرة الحدود الأصغرية لتحويل خطي ما T هي عامل لحاصل ضرب قواسم الأولية أن وكل قاسم أولي هو عامل لكثيرة حدوده الأصغرية .

5. أوجد القواسم الأولية لكل من التحويلات الخطية الآتية وعبر عن الفضاء المتجهي V كمجموع مباشر لفضاءات جزئية دورية لا متغيرة نسبة إلى T :

a. $V=Q^2$ ، $T(e_1)=e_1$ ، $T(e_1)=e_1$ ، $T(e_2)=3e_2$.

b. $V=Q^2$ ، $T(e_1)=e_2$ ، $T(e_2)=e_1$.

c. $V=Q^2$ ، $T(e_1)=5e_2$ ، $T(e_2)=3e_2$.

d. $V=Q^3$ ، $T(e_1)=e_1+e_2+e_3$ ، $T(e_2)=-e_3$ ، $T(e_3)=2e_2+3e_3$.

e. $V=Q^3$ ، $T(e_1)=2e_1-e_2-2e_3$ ، $T(e_2)=-6e_1-3e_2+2e_3$ ، $T(e_3)=8e_1+3e_2-3e_3$

f. $V=Q^4$ ، $T(e_1)=e_2$ ، $T(e_2)=e_1$ ، $T(e_3)=e_4$ ، $T(e_4)=e_3$.

g. $V=Q^4$ ، $T(e_1)=-e_2$ ، $T(e_2)=e_1+e_2+e_3$ ، $T(e_3)=e_4$ ، $T(e_4)=e_3+e4$.

6. إذا كانت كثيرة الحدود الأصغرية لتحويل خطي ما T على فضاء متجهي V_F هي $(p(x))^k$ حيث $p(x)$ غير قابلة للتحليل ، فما هي القواسم الأولية المختلفة للتحويل T؟

5. صيغة جوردان العادية

ليكن $A=(\alpha_{ij})$ مصفوفة سعتها $n\times n$ على حقل F و V فضاء متجهي على F بعده n ، و $B=(b_1,b_2,...,b_n)$ قاعدة مرتبة للفضاء V فإذا كان T تحويل خطي على V معرفاً حسب $1\le j\le n, T(b_i)=\sum_{i=1}^{n}\alpha_{ij}b_i$ فإن A هي مصفوفة T نسبة إلى $B1$. افرض أن $q_1(x),q_2(x),...,q_m(x)$ هـي القواسـم الأوليـة للتحويـل T فـإن $V=W_1\oplus W_2\oplus...\oplus W_m$ ، $T=T_1\oplus T_2\oplus...\oplus T_m$ لفضاءات جزئية دورية $(1\le i\le n),W_i$ لا متغيرة وفق T بحيث تكون $q_i(x)$ هي كثيرة الحدود الأصغرية للتحويل T_i وهو مقصور T على W_i (نظرية 54.16) بما أنه كل W_i هو فضاء جزئي دوري لا متغير وفق T_i ومن نظرية 46.16 تكون له قاعدة B_i بحيث تكون مصفوفة T_i نسبة إلى B_i هي مصفوفة جوردان لكثيرة الحدود $q_i(x)$ نسبة على كثيرة حدود غير قابلة للتحليل تكون $q_i(x)$ قوة لها .

$T=T_1\oplus T_2\oplus...\oplus T_m$ يـؤدي إلى أن للفضـاء V قاعـدة $B'=(b'_1,b'_2,...,b'_n)$ بحيـث تكـون مصـفوقة T نسبة إلى B' هي $J=J_1\oplus J_2\oplus...\oplus J_n$ عندئذ تكون A مشابهة للمصفوفة J (نتيجة 40.12) تسمى J صيغة جوردان العادية للمصفوفة A ، بما أن القواسم الأولية للتحويل T تتحدد بصفة وحيدة (نظرية 54.16) فإن صيغة جوردان العادية للمصفوفة A تتحدد بصفة وحيدة عدا للترتيب الذي يكتب به J_i .

إذا كانـت كثـيرة الحـدود $q(x)$ هـي قـوة لكثـيرة حـدود واحديـة غـير قابلـة للتحليـل $p(x)$ فـإن مصـفوفة جـوردان لكثـيرة الحـدود $q(x)$ نسـبة إلى $p(x)$ سـوف تسـمى ببسـاطة بمصفوفة جوردان لكثيرة الحدود $q(x)$.

نظرية 57.16

لأي $A\in M_n(C)$ ، صيغة جوردان العادية للمصفوفة A هي بالشكل

$$\begin{pmatrix} J_1 & 0 & 0 & \dots & 0 \\ 0 & J_2 & 0 & 0 & 0 \\ 0 & 0 & J_3 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & J_m \end{pmatrix}$$

حيث كل J_i هي بالصورة
$$\begin{pmatrix} \alpha_i & 1 & 0 & \dots & 0 & 0 \\ 0 & \alpha_i & 1 & \dots & 0 & 0 \\ 0 & 0 & \alpha_i & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \alpha_i & 0 \\ 0 & 0 & 0 & \dots & 0 & \alpha_i \end{pmatrix}$$

وكل α_i هو قيمة ذاتية للمصفوفة A .

البرهان

لتكن $q_1(x),\dots,q_m(x)$ القواسم الأولية لـ A ، بما أن كثيرات الحدود غير القابلة للتحليل على C هي فقط تلك التي درجتها واحد ، وأن كل $q_i(x)$ هي قوة لكثيرة حدود غير قابلة للتحليل ، يكون لدينا $q_i(x)=(x-\alpha_i)^{k_i}$ لبعض العناصر $\alpha_i \in C$ ولأعداد صحيحة موجبة k_i ، عندئذ تكون مصفوفة جوردان لكثيرة الحدود $q_i(x)$ هي :

المصفوفة من السعة $k_i \times k_i$ الآتية
$$J_i = \begin{pmatrix} \alpha_i & 1 & 0 & \dots & 0 & 0 \\ 0 & \alpha_i & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \alpha_i & & 1 \\ 0 & 0 & 0 & \dots & 0 & \alpha_i \end{pmatrix}$$

إذاً صيغة جوردان العادية للمصفوفة A هي :

$$J_1 \oplus J_2 \oplus \dots \oplus J_m = \begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & J_m \end{pmatrix}$$

الجزء التالي من النظرية يتحقق من نتيجة 56.16 .

مثال 23

اعتبر كثيرات الحدود $(x+1)$ ، $(x+1)^2$ ، $(x-i)^2$ ، $(x+i)^2$ على C مصفوفات جوردان المقابلة لها (قوالب جوردان) هي على الترتيب :

$J_1=(-1)$ ، $J_2=\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}$ ، $J_3=\begin{pmatrix}i & 1\\ 0 & i\end{pmatrix}$ و $J_4=\begin{pmatrix}-i & 1\\ 0 & -1\end{pmatrix}$.

المصفوفة ذات السعة 7×7 التالية :

$$\begin{pmatrix} J & 0 & 0 & 0\\ 0 & J_2 & 0 & 0\\ 0 & 0 & J_3 & 0\\ 0 & 0 & 0 & J_4\end{pmatrix}=\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & -1 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & i & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & i & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & -i & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & -i\end{pmatrix}$$

هي بصيغة جوردان العادية وقواسمها الأولية هي كثيرات الحدود المذكورة سابقاً ، وأن $-i,i,-1,1$ هي قيمها الذاتية المختلفة .

تعريف 58.16

يقال لتحويل خطي T على فضاء متجهي V إنه عديم القوة بدليل $1\leq k$ إذا كان $T^k=0$ ولكن $T^{k-1}\neq 0$.

على غرار ذلك يمكن إعطاء تعريف مماثل لمصفوفة عديمة القوة ، وعلى الفور يتبين أن تحويلاً خطياً T يكون عديم القوة بدليل k إذا وفقط إذا كانت مصفوفة المناظرة عديمة القوة بالدليل k .

وعلى سبيل المثال فإن أية مصفوفة $n\times n$ العناصر التي على القطر وتحته يساوي الصفر تكون عديمة القوة بدليل $n\geq$.

نظرية 59.16

إذا كان $T \in A(V)$ عديم القوة بدليل k فإنه توجد قاعدة مرتبة B للفضاء V بحيث تكون مصفوفة T نسبة إلى B على الصورة

$$\begin{pmatrix} M_{k_1} & 0 & 0 & \dots & 0 \\ 0 & M_{k_2} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & M_{k_r} \end{pmatrix}$$

حيث $k = k_1 \geq k_2 \geq \dots \geq k_r$ ولكل عدد صحيح موجب t . M_t هي المصفوفة $t \times t$ المعطاة بالصورة

$$M_t = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

البرهان

بما أن $T^k = 0$ كثيرة الحدود الأصغرية $m(x)$ للتحويل T يقسم x^k إذاً $m(x) = x^\ell$ لعدد $\ell \leq k$.

وحيث أن $T^{k-1} = 0$ ، $\ell \leq |k - 1$ ، فإن $\ell = k$ عليه تكون $m(x) = x^k$. لتكن $q_1(x), q_2(x), \dots, q_r(x)$ هي القواسم الأولية للتحويل T ولأن كل واحدة منها تقسم كثيرة الحدود الأصغرية $m(x) = x^k$ فإن $q_i(x) = x^{k_i}$ لعدد $k_i \leq k$. عليه بإمكاننا إعادة ترتيب كثيرات الحدود $q_i(x)$ بحيث $k_1 \geq k_2 \geq \dots \geq k_v$.

بما أن المضاعف المشترك الأصغر لكثيرات الحدود $q_i(x)$ هو كثيرة الحدود x^k نحصل على أن $k = k_1$ الآن مصفوفة جوردان لكثيرة الحدود $q_i(x) = x^{k_i}$ نسبة إلى x حسب مثال 15 هي المصفوفة ذات السعة $k_i \times k_i$ التالية :

$$M_{k_i} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

بما أن أية مصفوفة تكون مشابهة لمصفوفة جوردان العادية لها ، فإن للفضاء V قاعدة مرتبة B بحيث تكون مصفوفة T نسبة إلى B هي

$$\begin{pmatrix} M_{k1} & 0 & 0 \\ 0 & M_{k2} & 0 \\ 0 & 0 & M_{kr} \end{pmatrix}$$

ملاحظة

بما أن القواسم الأولية للتحويل T السابقة تتحدد بصفة وحيدة ، فإن الأعداد الصحيحة $k_1, k_2, \dots, k_r$ في النظرية السابقة تتحدد بصفة وحيدة بواسطة T . هذه الأعداد الصحيحة تسمى لا متغيرات للتحويل الخطي T العديم القوة .

مثال 24

اعتبر المصفوفة ذات السعة $n \times n$ بالصورة :

$$M = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

هذه المصفوفة هي المصفوفة المصاحبة لكثيرة الحدود $f(x) = x^n$ كثيرة الحدود الأصغرية للمصفوفة M هي x^n ولأن درجتها n فهذا يعطينا أن M لها قاسم أولي واحد هو نفس x^n . الآن مصفوفة جوردان لكثيرة الحدود x^n نسبة إلى x هي كثيرة الحدود من السعة $n \times n$ الآتية :

$$J=\begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

إذاً صيغة جوردان العادية للمصفوفة M هي J ولا متغيرها الوحيد هو n .

مثال 25

اعتبر كثيرة الحدود x^3 . دعنا نحدد جميع صيغ جوردان العادية للمصفوفات من السعة 6×6 والتي لها كثيرة حدود أصغرية تساوي x^3 ، جميع هذه المصفوفات عديمة القوة ، بدليل تساوي 3 . لتكن A أية واحدة من هذه المصفوفات فإذا كانت لا متغيراتها هي $k_1,k_2,...,k_r$ فإنه يكون $3=k_1\geq k_2\geq ...\geq k_r$ وأن العدد 6 يمكن التعبير عنه بهذه الصيغة فقط بالطرق الثلاثة الآتية :

$3+3, 3+2+1, 3+1+1+1$ إذا صيغ جوردان العادية المحتملة هي فقط :

$$A_i=\begin{pmatrix} 0 & 1 & 0 & \vdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \vdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \vdots & 0 & 0 & 0 \\ \ldots & \ldots & \ldots & \vdots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \vdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \vdots & 0 & 0 & 1 \\ 0 & 0 & 0 & \vdots & 0 & 0 & 0 \end{pmatrix}$$

$$A_2=\begin{pmatrix} 0 & 1 & 0 & \vdots & 0 & 0 & & 0 \\ 0 & 0 & 1 & \vdots & 0 & 0 & & 0 \\ 0 & 0 & 0 & \vdots & 0 & 0 & & 0 \\ \ldots & \ldots & \ldots & \vdots & \ldots & \ldots & \vdots & \ldots \\ 0 & 0 & 0 & \vdots & 0 & 1 & \vdots & 0 \\ 0 & 0 & 0 & \vdots & 0 & 0 & \vdots & 0 \\ & & & \vdots & \ldots & \ldots & \vdots & \ldots \\ 0 & 0 & 0 & & 0 & 0 & \vdots & 0 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

نُوعِزُ القراء بتحديد مصفوفات جوردان العادية من السعة 8×8 التي هي عديمة القوة وبأدلة 3 , 5 , 6 , 7 .

مثال 26

اعتبر المصفوفة $A = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}$ $A^3 = (0)$ ولكن $A^2 \neq (0)$ أي أن A عديمة القوة ودليلها يساوي 3 . بما أن المصفوفة الوحيدة ذات السعة 3×3 من صيغة جوردان العادية وتكون عديمة القوة ودليلها 3 هي فقط المصفوفة $J = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ ، والمصفوفة A مشابهة للمصفوفة J .

اعتبر المصفوفة $B = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$ هذه المصفوفة عديمة القوة ودليلها هو ... واضح أن B, A غير متشابهتين .

بما أن الطريقة الوحيدة لكتابة 3 بالصيغة $3 = k_1 + k_2 + ... + k_1$ حيث k_i أعداد صحيحة موجبة تحقق $2 = k_1 \geq k_2 \geq ... \geq k_r$ هي $3 = 2 + 1$ نحصل على أن صيغة جوردان العادية للمصفوفة B هي $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

مسائل

1. اثبت أن تحويلين خطيين في $A(V)$ متشابهان إذا وفقط إذا كان لهما نفس القواسم الأولية .
2. ليكن $T \in A(V)$ تحويلاً خطياً كثيرة حدوده الأصغرية هي $F(x)=[p_1(x)]^{m_1}[p_2(x)]^{m_2}..[p_t(x)]^{m_t}$ حيث $p_i(x)$ هي كثيرات حدود واحدية مختلفة وغير قابلة للتحليل وأن $m_i \geq 1$. برهن أن مصفوفة T في صيغة جوردان العادية يمكن وضعها بالشكل

$$A=\begin{pmatrix} R_1 & 0 & 0 & \dots & 0 \\ 0 & R_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & R_t \end{pmatrix}$$

بحيث أن
$$R_i = \begin{pmatrix} C(p_i(x)e_{i_2} & & \\ & \ddots \; C(p_i(x)e_{i_2} & \\ & & \ddots \; C(p_i(x)e_{i_2} \end{pmatrix}$$

وبحيث يكون $m_i = e_{i1} \geq e_{i2} \geq \ldots \geq e_{iti}$ وأي كثيرة حدود $C\left(g(x)^m\right), g(x)$ ترمز إلى مصفوفة جوردان للمصفوفة $[g(x)]^{m_i}$ نسبة إلى $g(x)$. (المصفوفة تسمى كذلك بمصفوفة في صيغة قانونية قياسية)

[إرشاد : إذا كان $q_1(x),\ldots,q_i(x)$ هي القواسم الأولية للتحويل T ، فإن كل واحد منها هو قوة لكثيرة حدود $p(x)$. ضم جميع كثيرات الحدود $q_j(x)$ هذه التي هي قوة لنفس كثيرة الحدود $p_i(x)$] .

3. إذا كانت جميع الجذور المميزة للتحويل $T \in A(V)$ تقع في F اثبت أن مصفوفة T بصيغة جوردان العادية هي مصفوفة مثلثية نعني أن جميع عناصرها تحت القطر مساوية للصفر .

4. اعط برهاناً باستخدام حسابات مصفوفية أنه إذا كانت A مصفوفة مثلثية من السعة $n \times n$ وعناصرها القطرية هي $\lambda_1, \lambda_2, ..., \lambda_n$ فإن $(A-\lambda_1 I')(A-\lambda_2 I')...(A-\lambda_n I')=0$ حيث I' هي مصفوفة الوحدة ذات السعة $n \times n$.

5. أوجد صيغة جوردان العادية للمصفوفة التي تمثل T في كل من الحالات الأتية :
   - i. $T \in A(Q^2)$ له القاسمين الأوليين $x-2$ ، $x+3$.
   - ii. $T \in A(Q^3)$ له القاسم الأولي x^2+2x-1 .
   - iii. $T \in A(Q^3)$ له كثيرة الحدود الأصغرية x^3+x+1 .
   - iv. $T \in A(R^4)$ له القاسمين الأوليين $x^2+\pi, x^2+x+1$.
   - v. $T \in A(C^6)$ له كثيرة الحدود الأصغرية x^6-1 .

6. اكتب جميع المصفوفات ذات سعة 4×4 في صيغة جوردان العادية على R/ ولها قيم ذاتية 1 , 2 , 3 .

7. أوجد صيغة جوردان العادية لكل من المصفوفات الآتية :

   i. $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ ii. $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

   iii. $\begin{pmatrix} 2 & -1 & -1 \\ -4 & -1 & 1 \\ 4 & 3 & 1 \end{pmatrix}$ iv. $\begin{pmatrix} 2 & 0 & 0 \\ -4 & -2 & 0 \\ 4 & 4 & 2 \end{pmatrix}$.

8. اكتب جميع المصفوفات من السعة 6×6 على Q بحيث تكون بصيغة جوردان العادية عندما :

i. $x^2(x^2+1)$ هي كثيرة الحدود الأصغرية لكل منها .

ii. $(x^2+1)(x+1)(x+2)$ هي كثيرة الحدود الأصغرية لكل منها .

iii. $(x+1)^2(x+2)^3(x+1)$ هي كثيرة الحدود الأصغرية لكل منها .

iv. كل منها عديمة القوة بدليل أقل أو يساوي 4 .

9- كثيرات الحدود المميزة

تعريف 60.16

إذا كانت $A=(\alpha_{ij})$ أية مصفوفة $n\times n$ على حقل ما F فإن محددة المصفوفة :

$$xI' - A = \begin{pmatrix} x-\alpha_{11} & -\alpha_{12} & \dots & \dots & -\alpha_{1n} \\ -\alpha_{21} & x-\alpha_{22} & \dots & \dots & -\alpha_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ -\alpha_{n1} & -\alpha_{n2} & \dots & \dots & x-\alpha_{nn} \end{pmatrix}$$

تسمى كثيرة الحدود المميزة للمصفوفة A (I' يرمز إلى مصفوفة الوحدة ذات السعة $n\times n$) .

كثيرة الحدود المميزة للمصفوفة A واحدية ودرجتها n . في الواقع هي بالصيغة :

$$x^n - x^{n-1}\left(\sum \alpha_{ii}\right)+\dots+(-1)^n \det A$$

مثال 27

لتكن $A=\begin{pmatrix} 0 & 1 \\ 2 & 33 \end{pmatrix}$ فإن $xI'-A=\begin{pmatrix} x-0 & -1 \\ -2 & x-3 \end{pmatrix}$

$$\det(xI'-A)=x(x-3)-2=x^2-3x-2$$

عليه x^2-3x-2 هي كثيرة الحدود المميزة للمصفوفة A ، يمكن التحقق بسهولة من أن A جذر لكثيرة حدودها المميزة .

قضية 61.16

أي مصفوفتين متشابهتين لهما نفس كثيرة الحدود المميزة .

البرهان

لتكن $A,B\in M_2(F)$ وأن $B=P^{-1}AP$ لكثيرة حدود غير منفردة P في $M_n(F)$

فإن

$$\begin{aligned} \det(xI'-B) &= \det\left(xP^{-1}I'P-P^{-1}AP\right) \\ &= \det\left[P^{-1}(xI'-A)P\right] \\ &= \det P^{-1}\det(xI'-A)\det P \\ &= \det(xI'-A) \end{aligned}$$

(لأن $\det P.\det P^{-1}=1$) .

إذاً B,A لهما نفس كثيرة الحدود المميزة .

تعريف 62.16

ليكن $T\in A(V)$ و A مصفوفة T نسبة إلى قاعدة مرتبة للفضاء V فإن كثيرة الحدود المميزة للمصفوفة A تسمى أيضاً بكثيرة الحدود المميزة للتحويل T .

كل تحويل خطي له كثيرة حدود مميزة وحيدة إذا كانت A و A' مصفوفتان لتحويل خطي $T\in A(V)$ نسبة على القاعدتين المرتبتين B',B على الترتيب ، فإن B,A متشابهتان (نتيجة 40.12) إذاً حسب القضية 61.16 يكون A',A لهما نفس كثيرة الحدود المميزة .

الغرض الرئيسي لهذا البند هو إثبات أن كل تحويل خطي T هو جذر لكثيرة حدوده المميزة والقيمة الذاتية للتحويل T هي جذر لكثيرة حدوده المميزة .

سوف نبرهن هذا أولاً باستخدام صيغة جوردان العادية لمصفوفة ، وبعدها برهاناً مستقلاً، سوف نفرض أن القراء على دراية بالمحددات على الأعداد المركبة . تعريف المحددات وبعض خصائصها الأساسية على الأعداد المركبة يمكن توسيعها للمحددات على أي حقل وسوف نستخدم هذه النتائج دون إثباتها . على سبيل المثال أي مصفوفة $A\in M_n(F)$ تكون قابلة للعكس (أي غير منفردة) إذا وفقط إذا كان $\det A\neq 0$. عليه فإن تحويل خطي ما T على V هو غير منفرد أو منفردة تبعاً لمحدد مصفوفته المصاحبة A من حيث كونه مختلفاً عن الصفر أو يساوي الصفر .

نظرية 63.16

ليكن $T \in A(V)$ فإن العنصر $c \in F$ هو قيمة ذاتية للتحويل T إذا وفقط إذا كان $\det(cI' - A) = 0$ حيث A هي مصفوفة T نسبة لقاعدة مرتبة للفضاء V .

البرهان

الآن $(I' - A)$ هي مصفوفة $cI - T$ و c قيمة ذاتية للتحويل T إذا وفقط إذا كان متجه غير صفري $v \in V$:

$$T(v) = cv \Leftrightarrow (CI - T)v = 0 \Leftrightarrow$$
$$cI - T$$

ولكننا نعلم أن تحويلاً خطياً ما يكون منفرداً إذا كان محدد مصفوفته يساوي صفراً ، بالتالي فإن c قيمة ذاتية للتحويل T إذا وفقط إذا كان $\det(cI' - A) = 0$.

قضية 64.16

لأي كثيرة حدود واحدية $f(x) = x^n - \alpha_{n-1}x^{n-1} - \ldots - \alpha_0$ على الحقل F كثيرة الحدود المميزة للمصفوفة المصاحبة لها هي $f(x)$ نفسها .

البرهان

نبرهن النتيجة بالاستنتاج على درجة كثيرة الحدود إذا كان $n = 1$ ، فإن $f(x) = x - \alpha_0$ والمصفوفة المصاحبة لها هي $A = (\alpha_0)$ وكثيرة الحدود المميزة للمصفوفة A تساوي $\det(xI' - A) = x - \alpha_0 = f(x)$.

إذاً النتيجة محققة عندما $n = 1$ لتطبيق الاستنتاج نفرض أن النتيجة محققة لجميع كثيرات الحدود الواحدية والتي درجتها $< n$.

الآن المصفوفة المصاحبة لكثيرة الحدود $f(x)$ هي :

$$A=\begin{pmatrix} 0 & 0 & \dots & 0 & \alpha_0 \\ 1 & 0 & \dots & 0 & \alpha_1 \\ 0 & 1 & \dots & 0 & \alpha_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \alpha_{n-1} \end{pmatrix}$$

وكثيرة الحدود المميزة للمصفوفة A هي :

$$\det(xI'-A)=|\,xI'-A=\begin{vmatrix} x & 0 & 0 & \dots & 0 & -\alpha_0 \\ -1 & x & 0 & \dots & 0 & -\alpha_1 \\ 0 & -1 & x & \dots & 0 & -\alpha_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & -1 & x-\alpha_{n-1} \end{vmatrix}$$

بملء المحدد باستخدام العمود الأول نحصل على أن :

$$|\,xI'-A|=x\begin{vmatrix} x & 0 & \dots & 0 & -\alpha_1 \\ -1 & x & \dots & 0 & -\alpha_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -1 & x-\alpha_{n-1} \end{vmatrix}+\begin{vmatrix} 0 & 0 & 0 & \dots & 0 & -\alpha_0 \\ -1 & x & 0 & \dots & 0 & -\alpha_2 \\ 0 & -1 & x & \dots & 0 & -\alpha_3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & -1 & x-\alpha_{n-1} \end{vmatrix}$$

$$=xB+C \qquad (1)$$

حيث :

$$B=\begin{vmatrix} x & 0 & \dots & 0 & -\alpha_1 \\ -1 & x & \dots & 0 & -\alpha_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & -1 & x & -\alpha_{n-1} \end{vmatrix},C=\begin{vmatrix} 0 & 0 & 0 & \dots & 0 & -\alpha_0 \\ -1 & x & 0 & \dots & 0 & -\alpha_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & -1 & x-\alpha_{n-1} \end{vmatrix}$$

من الواضح أن B هي كثيرة الحدود المميزة للمصفوفة المصاحبة لكثيرة الحدود $x^{n-1}-\alpha_{n-1}x^{n-2}-\dots-\alpha_1$.

بما أن كثيرة الحدود هذه درجتها $n>n-1$ فإنه حسب فروض الاستنتاج يكون :

$$B=x^{n-1}-\alpha_{n-1}x^{n-2}-\dots-\alpha_1 \qquad (2)$$

بملء C على الصف الأول نحصل على أن :

$$C=(-1)^{n-1}(-\alpha_0)\begin{vmatrix} -1 & x & 0 & 0 & \ldots & 0 \\ 0 & -1 & x & 0 & \ldots & 0 \\ 0 & 0 & -1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & -1 \end{vmatrix}$$

[محدد له $(n-1)$ صفاً] وعليه :

$$C=(-1)^{n-2}(-\alpha_0)(-1)^{n-2}=-\alpha_0 \qquad (3)$$

من (1) ، (2) و (3) نحصل على أن $|xI'-A|=x\left(x^{n-1}-\alpha_{n-1}x^{n-2}-\ldots-\alpha_1\right)-\alpha_0$

$$=x^n-\alpha_{n-1}x^{n-1}-\ldots-\alpha_1x-\alpha_0=f(x)$$

عليه النتيجة محققة عندما $\deg f(x)=n$ بالتالي النتيجة محققة لجميع قيم n .

قضية 65.16

لأي كثيرة حدود $g(x)=[f(x)]^m$ حيث $f(x)$ كثيرة حدود واحدية فإن كثيرة الحدود المميزة لمصفوفة جوردان لكثيرة الحدود $g(x)$ نسبة إلى $f(x)$ هي نفسها $g(x)$.

البرهان

افرض أن $\deg f(x)=k$ فتكون مصفوفة جوردان لكثيرة الحدود $g(x)$ نسبة إلى $f(x)$ هي المصفوفة A ذات السعة $km\times km$ وهي على الصورة :

$$A=\begin{pmatrix} C & N & 0 & 0 & \ldots & 0 \\ 0 & C & N & 0 & \ldots & 0 \\ 0 & 0 & C & N & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & C \end{pmatrix}$$

حيث C هي المصفوفة المصاحبة لكثيرة الحدود $f(x)$ و N هي المصفوفة ذات السعة $k\times k$

$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$ كثيرة الحدود المميزة للمصفوفة A هي :

$$|xI' - A| = \begin{vmatrix} xI'' - C & -N & 0 & \dots & 0 \\ 0 & xI'' - C & -N & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & & \\ 0 & 0 & 0 & & xI'' - C \end{vmatrix}$$

حيث I'', I' هما مصفوفتا الوحدة من السعة $km\times km$ والسعة $k\times k$ على الترتيب .

باستخدام المفكوك القالبي للمحدد نجد أن $|xI' - A| = |xI'' - C|^m$.

لأنه في محدد القالب جميع العناصر تكون على القطر الرئيسي هي تساوي صفر .

الآن حسب القضية 64.16 $|xI'' - C| = f(x)$.

بذلك فإن $|xI' - A| = [f(x)]^m = g(x)$ وهذا يثبت النظرية .

القضية التالية يمكن إثباتها بسهولة .

قضية 66.16

لأية مصفوفة A من الصيغة $\begin{pmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & A_t \end{pmatrix}$ حيث A_i هي أيضاً مصفوفات ، فإن كثيرة الحدود المميزة للمصفوفة A تساوي ضرب كثيرات الحدود المميزة للمصفوفات $A_i .(i = 1, 2, \dots, t)$.

نظرية 67.16 (نظرية كيلي – هاملتون)

أي تحويل خطي على فضاء متجهي V هو جذر لكثيرة حدوده المميزة .

البرهان

افرض أن $m(x)$ هي كثيرة الحدود الأصغرية للتحويل T . فلكي نثبت أن T هو جذر لكثيرة حدوده المميزة $f(x)$ يكفي أن نثبت أنه $m(x)$ يقسم $f(x)$.

الآن افرض أن $q_1(x), q_2(x), ..., q_t(x)$ هي القواسم الأولية للتحويل T (تعريف 55.16) ومن نظرية 54.16 فإن كثيرة الحدود الأصغرية للتحويل T هي المضاعف المشترك الأصغر لكثيرات الحدود $q_i(x)$.

الآن صيغة جوردان العادية لمصفوفة T هي
$$A = \begin{pmatrix} J_1 & 0 & 0 & \dots & 0 \\ 0 & J_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & J_t \end{pmatrix}$$

حيث كل J_i هو مصفوفة جوردان القانونية لكثيرة الحدود $q_i(x)$.

الآن حسب القضية 66.16 كثيرة الحدود المميزة $f(x)$ للمصفوفة A (بالتالي للتحويل T) هي حاصل ضرب كثيرات الحدود المميزة للمصفوفات J_i ، $(j = 1, 2, ..., t)$.

واستناداً إلى القضية 65.16 كثيرة الحدود المميزة لكل J_i هي $q_i(x)$ بذلك فإن :

$$f(x) = q_1(x) q_2(x) ... q_t(x) \qquad (4)$$

بما أن كثيرة الحدود الأصغرية $m(x)$ للتحويل T هي المضاعف المشترك الأصغر لكثيرات الحدود $(i = 1, 2, ..., t). q_i(x)$ فإن المعادلة (4) تؤدي إلى أن $m(x)$ تقسم $f(x)$.

بالتالي $f(T) = 0$ وهذا يثبت النتيجة .

ملاحظة

البرهان السابق في الحقيقة تبيّن أن كثيرة الحدود المميزة لتحويل خطي ما T تساوي حاصل ضرب قواسمه الأولية .

برهان بديل لبرهان نظرية نظرية 67.16

لتكن A مصفوفة T نسبة لقاعدة مرتبة B للفضاء V فتكون كثيرة الحدود المميزة للتحويل T هي $|xI'-A|$.

افرض أن $|xI'-A| = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n$ حيث العناصر $a_i \in F$.

لتكن $B(x)$ المصفوفة المرافقة $(Adjoint)$ للمصفوفة $xI'-A$. بما أن عناصر $B(x)$ هي العوامل المرافقة لعناصر المصفوفة $xI'-A$ فهي كثيرات حدود من x درجتها أصغر من أو تساوي $n-1$ هذا يؤدي إلى أن $B(x) = B_0 + B_1 x + \ldots + B_{n-1}x^{n-1}$

حيث لكل $i = 0,1,2,\ldots,n-1$: B_i هي مصفوفة سعتها $n \times n$ على F .

بمعنى آخر العناصر B_i مستقلة عن x ومن المعلوم جيداً حول خاصية الترافق في المصفوفات فإن :

$$[Adj(xI'-A')](xI'-A) = [B(x)](xI'-A) = |xI'-A|\,I'$$

عليه فإن :

$$\left(B_0 + B_1 x + \ldots + B_{n-1}x^{n-1}\right)(xI'-A) = \left(a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n\right)I'$$

بمقارنة معاملات القوة المتساوية لـ x في الطرفين ، نحصل على :

$$\begin{aligned}
&-B_0 A = a_0 I' \\
&-B_1 A + B_0 = a_1 I' \\
&\ldots\ldots \quad \ldots\ldots \quad \ldots\ldots \\
&-B_{n-1}A + B_{n-1} = a_{n-1} I' \\
&B_{n-1} = I'
\end{aligned}$$

بضرب هذه المعادلات المصفوفية في $A^{n-1}, \ldots A^2, A, I'$ و A^n على الترتيب نحصل على أن :

$$-B_0 A = a_0 I'$$
$$-B_1 A^2 + B_0 A = a_1 A$$
$$\ldots\ldots \qquad \ldots\ldots\ldots\ldots$$
$$-B_{n-1} A^n + B_{n-2} A^{n-1} = a_{n-1} A^{n-1}, \; B_{n-1} A^n = A^n$$

بجمع هذه المعادلات المصفوفية نحصل على أن :

$$a_0 I' + a_1 A + \ldots + a_{n-1} A^{n-1} + A^n = 0$$

وهذا بدوره يؤدي إلى أن :

$$a_0 I + a_1 T + \ldots + a_{n-1} T^{n-1} + T^n = 0$$

أي أن T هو جذر لكثيرة حدوده المميزة .

تمارين محلولة

تمرين 1

تعريف : يقال عن مصفوفة (أو تحويل خطي) أنها قابلة للتمثيل القطري إذا كانت مشابهة لمصفوفة قطرية (له قاعدة تكون مصفوفته نسبة لهذه القاعدة مصفوفة قطرية) .

إذا كان T تحويلاً في $A(V)$ فإن T قابل للتمثيل القطري (عندما تكون جميع جذوره كثيرة حدوده الأصغرية في F) إذا وفقط إذا كان $(T-\lambda I)^m v = 0$ حيث $v \in V$ ، $\lambda \in F$ فإن $(T-\lambda I)v = 0$.

الحل

لتكن $m(x)$ كثيرة الحدود الأصغرية للتحويل T ، بما أن جميع جذورها تقع في F ، يمكننا أن نكتب $m(x) = (x-\lambda_1)^{n_1}(x-\lambda_2)^{n_2}\ldots(x-\lambda_k)^{k_n}$ حيث كل λ_i عناصر مختلفة في F وأن n_i أعداد صحيحة أكبر من أو تساوي 1 لكل $i = 1, 2, \ldots, k$.

إذاً $V=V_1\oplus V_2\oplus\ldots\oplus V_k$ حيث كل V_i هو فضاء جزئي في V لا متغير بالنسبة إلى V بحيث تكون كثيرة الحدود الأصغرية لـ T_i هو مقصور T على V_i هي $(x-\lambda_i)^{n_i}$ توجد قاعدة للفضاء V بحيث A مصفوفة T نسبة لهذه القاعدة على الصورة $\begin{pmatrix} J_1 & 0 & 0 & \ldots & 0 \\ 0 & J_2 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & J_n \end{pmatrix}$ حيث J_i هي مصفوفة جوردان لكثيرة الحدود $(x-\lambda)^{n_t}$ نسبة إلى $x-\lambda_i$ بما أن $(T_i-\lambda_i I)^{n_i}(v_i)=0$ لكل $v_i\in V_i$ نحصل على أن $(T-\lambda_i I)v_i=0$ لذا فإن كثيرة الحدود الأصغرية لـ T_i على V_i هي $x-\lambda_i$ أي أن $n_i=1$ لكل $i=1,2,\ldots,k$.

بالتالي فإن J_i مصفوفة قطرية لجميع قيم $i=1,2,\ldots,k$ وكل عنصر قطري هو λ_i نتيجة لذلك فإن A نفسها مصفوفة قطرية فيكون T قابل للتمثيل القطري .

بالعكس افرض أن T قابل للتمثيل القطري توجد قاعدة مرتبة $(e_1,e_2,\ldots,e_n)$ للفضاء V بحيث أن $T(e_i)=\lambda_i e_i$ لكل $i=1,2,\ldots,n$ إذا كان $v=0$ فإن النتيجة محققة بوضوح .

افرض أن $0\neq v\in V$ بحيث $\left[(T-\lambda I)^m\right]v=0$ لبعض $\lambda\in F$ ، $m\in N$ ، الآن :

$$v=\sum_{i=1}^{n}\mu_i e_i\ ,\mu_i\in F$$
$$=\sum_{j=1}^{t}\mu_{ij}\ e_{ij}$$

حيث $\{e_1,e_2,\ldots,e_n\}\supseteq\{e_{i_1},e_{i_2},\ldots,e_{i_t}\}$ وكل μ_{ij} عنصر في F يختلف عن الصفر .

إضافة إلى ذلك فإن

$$\left[(T-\lambda I)^m\right]r=0\Rightarrow\sum_{j=1}^{t}\mu_{ij}(T-\lambda I)^m e_{ij}=0$$

مرة أخرى $T(e_i)=\lambda_i e_i$ يعطينا $T^2(e_i)=\lambda_i T(e_i)=\lambda_i^2 e_i$ بالاستمرار على هذا المنوال يمكن بيان أن لكل عدد صحيح موجب r فإن $T^r(e_i)=\lambda_i^r(e_i)$.

وهكذا $(T-\lambda I)^m e_{ij}=(\lambda_{ij}-\lambda)^m e_{ij}$ لكل $i=1,2,\ldots,t$ وأن :

$$\{\lambda_{i1},\lambda_{i2},\dots,\lambda_{it}\}\subseteq\{\lambda_1,\lambda_2,\dots,\lambda_m\}$$

وبالتالي فإن

$$\left[(T-\lambda I)^m\right]r=0\Rightarrow\sum_{j=1}^{t}\mu_{ij}\left(\lambda_{ij}-\lambda\right)^m e_{ij}=0$$
$$\Rightarrow\qquad \mu_{ij}\left(\lambda-\lambda_{ij}\right)^m=0$$

لكل j لأن $e_{i_1},e_{i_2},\dots,e_{i_t}$ متجهات مستقلة خطياً على F ، بما أن $\mu_{ij}\neq 0$ لكل i_j فإن هذا يؤدي إلى أن $\lambda_{ij}=\lambda$ لكل $j=1,2,\dots,t$ بالتالي فإن :

$$(T-\lambda I)v=\sum_{j=1}^{t}\mu_{ij}(T-\lambda I)e_{ij}=\sum_{j=1}^{t}\mu_{i_j}\left(\lambda_{i_j}-\lambda\right)e_{ij}=0$$

تمرين 2

برهن أنه إذا كان T تحويلاً خطياً على V يحقق $T^2=T$ فإن T قابل للتمثيل القطري ، وإنه إذا كان T,S تحويلان خطيان على V $(S,T\in A(V))$ بحيث $T^2=T,S^2=S$ فإن T,S متشابهان إذا وفقط إذا كان لهما نفس المرتبة .

الحل

لاحظ أن حل الجزء الأول من التمرين يتطلب تحقق الشرط $\left[(T-\lambda I)^m\right]v=0$ وهو يؤدي إلى أن $(T-\lambda I)v=0$ لجميع $v\in V$ ولجميع الجذور لكثيرة الحدود الأصغرية $m(x)$ للتحويل T بشرط أن جميع جذور $m(x)$ تقع في F ، في هذا التمرين $T^2=T$ يعطينا $m(x)\mid x^2-x$. عليه فإن الجذور الوحيدة المحتملة لكثيرة الحدود $m(x)$ هي $0,\ 1$ وهما عنصران في F .

الآن $\left[(T-0I)^m\right]v=0\Rightarrow T^m(v)=0$ لأي $m\in N$ إذا كان $m=1$ فذلك يعطينا $T(v)=0$ وإذا كان $m\geq 2$ فمن العلاقة $T^2=T$ ، $T^m=T$ مرة ثانية نحصل على أن $\left[(T-0I)^m\right]v=0\Rightarrow T(v)=0$.

مرة أخرى لاحظ أن $(T-I)^2=T^2-2T+I=I-T$

أي أن $(I-T)^2 = I-T$. مثل السابق هذا يؤدي إلى أنه لجميع $m \geq 2$ يكون $(I-T)^m = I-T$ ، بالتالي :

$$\left[(T-I)^m\right]v = 0 \Rightarrow \left[(I-T)^m\right]v = 0 \Rightarrow \left[(I-T)\right]v = 0 \Rightarrow \left[(T-I)\right]v = 0$$

عليه فإن الشرط في الجزء الأول في تمرين 1 السابقة محقق ، إذاً T قابل للتمثيل القطري .

الآن افرض أن T,S متشابهان ، فإنه يوجد تحويل غير منفرد $U \in A(V)$ بحيث $S = UTU^{-1}$

لذا $r(S) = r\left(uTu^{-1}\right) = r\left(u^{-1}uT\right) = r(T)$

وبالعكس افرض أن $r(S) = r(T) = k$ ، بما أن $S^2 = S$ و $T^2 = T$ فإن كلاً من S و T قابل للتمثيل القطري وتوجد قاعدتين مرتبتين $(e_1, e_2, ..., e_n)$ و $(f_1, f_2, ..., f_n)$ للفضاء V بحيث :

$S(e_i) = e_i$ لكل $1 \leq i \leq k$.

$S(e_i) = 0$ لكل $k < i \leq n$.

$T(f_i) = f_i$ لكل $1 \leq i \leq k$.

$T(f_i) = 0$ لكل $k < i \leq n$.

عرف $u \in A(V)$ كالآتي $u(e_i) = f_i$ لكل $i = 1, 2, ..., n$ فإن u تحويل غير منفرد وأن :

$uS(e_i) = 0 = T(f_i) = Tu(e_i)$ هذا يعطينا $uS = Tu \Rightarrow T = usu^{-1}$

وهكذا فإن S,T متشابهان .

مسائل

1. اثبت أن كثيرة الحدود المميزة لتحويل خطي تساوي كثيرة حدوده الأصغرية إذا وفقط إذا كان التحويل الخطي دورياً .
2. اكتب مصفوفة جوردان القانونية لكل من كثيرات الحدود الآتية على Q وحدد كثيرة حدودها المميزة $\left(x^2+1\right)^2$ و $(x+1)^3$ و $\left(x^3+2x+1\right)^2$ و x^3-2 .
3. اثبت أن مصفوفة ما A ذات سعة $n\times n$ مشابهة لمصفوفة قطرية إذا وفقط إذا كانت كثيرة حدودها الأصغرية $m(x)$ تساوي $(x-\alpha_1)(x-\alpha_2)...(x-\alpha_m)$ لبعض عناصر مختلفة $\alpha_1,\alpha_2,...,\alpha_m$ في F . **[إرشاد** : استخدم صيغة جوردان العادية**]** .
4. بين بحسابات مباشرة أنه لا توجد واحدة من المصفوفات التالية على Q مشابهة لمصفوفة قطرية $\begin{pmatrix}0&-2&0&0\\1&0&0&0\\0&0&0&0\\0&0&1&0\end{pmatrix},\begin{pmatrix}0&1&0\\0&1&0\\0&0&2\end{pmatrix},\begin{pmatrix}0&-1\\1&0\end{pmatrix}$.
5. بين أن المصفوفتين $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ و $\begin{pmatrix}0&-2&0&1\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$ كمصفوفتين على C متشابهتين لمصفوفتين قطريتين .
6. أوجد كثيرة الحدود المميزة لكل من المصفوفات التالية على Q :
$\begin{pmatrix}-4&1\\0&4\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\\3&1&2\end{pmatrix},\begin{pmatrix}2&3&0\\0&2&3\\3&2&0\end{pmatrix},\begin{pmatrix}1&0&0\\2&3&0\\-2&-2&1\end{pmatrix}$.

7. إذا كان $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$ مع كون إما $b \neq 0$ أو $c \neq 0$ ، بين أن كثيرة الحدود المميزة للمصفوفة A هي $f(x)=x^2-x(a+d)+ad-bc$ وأن $f(x)$ هي أيضاً كثيرة الحدود الأصغرية للمصفوفة A . استنتج أن A مشابهة لمصفوفة قطرية على IR إذا وفقط إذا كان $(a+d)^2-4(ad-bc)>0$.

الملاحـق

جدول الكتل الذرية المحايدة

Atom	A	Mass	Atom	A	Mass	Atom	A	Mass
$_1$H	1	1.007825	($_4$Be)	8*	8.005305	($_6$C)	13	13.003355
	2	2.014102		9	9.012182		14*	14.003242
	3*	3.016049		10*	10.013534		15*	15.010599
$_2$He	3	3.016029		11*	11.021658	$_7$N	13*	15.003739
	4	4.002603	$_5$B	8*	8.024606		14	14.003074
	5*	5.01222		9*	9.013329		13	15.000109
	6*	6.018886		10	10.012937		16*	16.006100
$_3$Li	5*	5.01254		11	11.009305		17*	17.008450
	6	6.015121		12*	12.014353	$_8$O	14*	14.008595
	7	7.016003	$_6$C	10*	10.016856		15*	15.003065
	8*	8.022486		11*	11.011433		16	15.994915
$_4$Be	7*	7.016928		12	12.000000		17	16.999131

(continued)

* Radioactive isotope.

Note: Masses are in u: 1 u = 931.5 MeV/c^2. Some other masses: Two electrons, 0.001097 $^1_0$n, 1.008665 $^1_1$p, 1.007276

The last figure shown isn't necessarily the last significant figure of the mass.

Sources: Data were extracted from the *1983 Atomic Mass Table*, A. H. Wapstra and G. Audi, Nuc. Phys. A432, 1 (1985); *Chart of the Nuclides*.

Atom	A	Mass
($_{8}$O)	18	17.999160
	19*	19.003577
	20*	20.004076
$_{9}$F	17*	17.002095
	18*	18.000937
	19	18.998403
	20*	19.999981
	21*	20.999948
$_{10}$Ne	18*	18.005710
	19*	19.001880
	20	19.992436
	21	20.993843
	22	21.991383
	23*	22.994465
	24*	23.993613
$_{11}$Na	21*	20.997650
	22*	21.994434
	23	22.989768
	24*	23.990961
	25*	24.989953
	26*	25.992586
$_{12}$Mg	22*	21.999574
	23*	22.994124
	24	23.985042
	25	24.985837
	26	25.982594
	27*	26.984341
	28*	27.983877
$_{13}$Al	25*	24.990429
	26*	25.986892
	27	26.981539
	28*	27.981910
	29*	28.980446
$_{14}$Si	26*	25.992330
	27*	26.986704
	28	27.976927
	29	28.976495
	30	29.973770
	31*	30.975362
	32*	31.974148
$_{15}$P	29*	28.981803
	30*	29.978307
	31	30.973762
	32*	31.973907
	33*	32.971725

Atom	A	Mass
$_{16}$S	30*	29.984903
	31*	30.979554
	32	31.972071
	33	32.971458
	34	33.967867
	35*	34.969032
	36	35.967081
	37*	36.971126
$_{17}$Cl	33*	32.977452
	34*	33.973763
	35	34.968853
	36*	35.968307
	37	36.965903
	38*	37.968011
	39*	38.968005
$_{18}$Ar	34*	33.980269
	35*	34.975256
	36	35.967546
	37*	36.966776
	38	37.962732
	39*	38.964314
	40	39.962384
	41*	40.964501
	42*	41.963050
$_{19}$K	37*	36.973377
	38*	37.969080
	39	38.963707
	40*	39.963999
	41	40.961825
	42*	41.962402
	43*	42.960717
$_{20}$Ca	38*	37.976318
	39*	38.970718
	40	39.962591
	41*	40.962278
	42	41.958618
	43	42.958766
	44	43.955481
	45*	44.956185
	46	45.953689
	47*	46.954543
	48	47.952533
	49*	48.955672
$_{21}$Sc	43*	42.961150
	44*	43.959404
	45	44.955910

Atom	A	Mass
($_{21}$Sc)	46*	45.955170
	47*	46.952409
	48*	47.952235
$_{22}$Ti	44*	43.959690
	45*	44.958124
	46	45.952629
	47	46.951764
	48	47.947947
	49	48.947871
	50	49.944792
	51*	50.946616
	52*	51.946898
$_{23}$V	48*	47.952257
	49*	48.948517
	50*	49.947161
	51	50.943962
	52*	51.944778
	53*	52.944340
$_{24}$Cr	48*	47.954033
	49*	48.951338
	50	49.946046
	51*	50.944768
	52	51.940510
	53	52.940651
	54	53.938882
	55*	54.940842
	56*	55.940643
$_{25}$Mn	52*	51.945568
	53*	52.941291
	54*	53.940361
	55	54.938047
	56*	55.938907
	57*	56.938285
$_{26}$Fe	52*	51.948114
	53*	52.945310
	54	53.939613
	55*	54.938296
	56	55.934939
	57	56.935396
	58	57.933277
	59*	58.934877
	60*	59.934078
$_{27}$Co	57*	56.936294
	58*	57.935755
	59	58.933198

Atom	A	Mass
($_{27}$Co)	60*	59.933820
	61*	60.932478
$_{28}$Ni	56*	55.942134
	57*	56.939799
	58	57.935346
	59*	58.934349
	60	59.930788
	61	60.931058
	62	61.928346
	63*	62.929670
	64	63.927968
	65*	64.930086
$_{29}$Cu	61*	60.933461
	62*	61.932586
	63	62.929599
	64*	63.929766
	65	64.927793
	66*	65.928872
	67*	66.927747
$_{30}$Zn	62*	61.934332
	63*	62.933214
	64	63.929145
	65*	64.929243
	66	65.926035
	67	66.927129
	68	67.924846
	69*	68.926552
	70	69.925325
	71*	70.927727
$_{31}$Ga	67*	66.928204
	68*	67.927982
	69	68.925580
	70*	69.926028
	71	70.924700
	72*	71.926365
	73*	72.925169
$_{32}$Ge	68*	67.928096
	69*	68.927969
	70	69.924250
	71*	70.924954
	72	71.922079
	73	72.923463
	74	73.921177
	75*	74.922858
	76	75.921402
	77*	76.923548

Atom	A	Mass
$_{33}$As	73*	72.923827
	74*	73.923928
	75	74.921594
	76*	75.922393
	77*	76.920646
$_{34}$Se	73*	72.926768
	74	73.922475
	75*	74.922522
	76	75.919212
	77	76.919912
	78	77.917308
	79*	78.918498
	80	79.916520
	81*	80.917991
	82	81.916698
	83*	82.919117
$_{35}$Br	77*	76.921378
	78*	77.921144
	79	78.918336
	80*	79.918528
	81	80.916289
	82*	81.916802
	83*	82.915179
$_{36}$Kr	77*	76.924610
	78	77.920396
	79*	78.920084
	80	79.916380
	81*	80.916590
	82	81.913482
	83	82.914135
	84	83.911507
	85*	84.912531
	86	85.910616
	87*	86.913360
$_{37}$Rb	83*	82.915144
	84*	83.914390
	85	84.911794
	86*	85.911172
	87*	86.909187
	88*	87.911326
$_{38}$Sr	83*	82.917566
	84	83.913430
	85*	84.912937
	86	85.909267
	87	86.908884
	88	87.905619

Atom	A	Mass
($_{38}$Sr)	89*	88.907450
	90*	89.907738
$_{39}$Y	87*	86.910882
	88*	87.909508
	89	88.905849
	90*	89.907152
	91*	90.907303
$_{40}$Zr	88*	87.910225
	89*	88.908890
	90	89.904703
	91	90.905644
	92	91.905039
	93*	92.906474
	94	93.906315
	95*	94.908042
	96	95.908275
	97*	96.910950
$_{41}$Nb	91*	90.906991
	92*	91.907192
	93	92.906377
	94*	93.907281
	95*	94.906835
$_{42}$Mo	90*	89.913933
	91*	90.911755
	92	91.906808
	93*	92.906813
	94	93.905085
	95	94.905841
	96	95.904678
	97	96.906020
	98	97.905407
	99*	98.907711
	100	99.907477
	101*	100.910343
$_{43}$Tc	95*	94.907657
	96*	95.907870
	97*	96.906364
	98*	97.907215
	99*	98.906254
	100*	99.907657
$_{44}$Ru	94*	93.911361
	95*	94.910414
	96	95.907599
	97*	96.907556
	98	97.905287

(continued)

Atom	A	Mass
($_{44}$Ru)	99	98.905939
	100	99.904219
	101	100.905582
	102	101.904348
	103*	102.906323
	104	103.905424
	105*	104.907744
$_{45}$Rh	101*	100.906159
	102*	101.906814
	103	102.905500
	104*	103.906651
	105*	104.905686
$_{46}$Pd	101*	100.908287
	102	101.905634
	103*	102.906114
	104	103.904029
	105	104.905079
	106	105.903478
	107*	106.905127
	108	107.903895
	109*	108.905954
	110	109.905167
	111*	110.907660
$_{47}$Ag	105*	104.906520
	106*	105.906662
	107	106.905092
	108*	107.905952
	109	108.904756
	110*	109.906111
$_{48}$Cd	105*	104.909459
	106	105.906461
	107*	106.906613
	108	107.904176
	109*	108.904953
	110	109.903005
	111	110.904182
	112	111.902757
	113*	112.904400
	114	113.903357
	115*	114.905430
	116	115.904755
	117*	116.907228
$_{49}$In	111*	110.905109
	112*	111.905536
	113	112.904061
	114*	113.904916
	115*	114.903882

Atom	A	Mass
$_{50}$Sn	111*	110.907741
	112	111.904826
	113*	112.905176
	114	113.902784
	115	114.903348
	116	115.901747
	117	116.902956
	118	117.901609
	119	118.903311
	120	119.902199
	121*	120.904239
	122	121.903440
	123*	122.905722
	124	123.905274
	125*	124.907785
$_{51}$Sb	119*	118.903948
	120*	119.905077
	121	120.903821
	122*	121.905179
	123	122.904216
	124*	123.905938
	125*	124.905252
$_{52}$Te	119*	118.906411
	120	119.904048
	121*	120.904947
	122	121.903050
	123*	122.904271
	124	123.902818
	125	124.904428
	126	125.903310
	127*	126.905221
	128	127.904463
	129*	128.906594
	130	129.906229
	131*	130.908528
$_{53}$I	125*	124.904620
	126*	125.905624
	127	126.904473
	128*	127.905810
	129*	128.904986
$_{54}$Xe	123*	122.908469
	124	123.905894
	125*	124.906397
	126	125.904281
	127*	126.905182
	128	127.903531
	129	128.904780

Atom	A	Mass
($_{54}$Xe)	130	129.903509
	131	130.905072
	132	131.904144
	133*	132.905888
	134	133.905395
	135*	134.907130
	136	135.907214
	137*	136.911557
$_{55}$Cs	131*	130.905444
	132*	131.906431
	133	132.905429
	134*	133.906696
	135*	134.905885
$_{56}$Ba	129*	128.908642
	130	129.906282
	131*	130.906902
	132	131.905042
	133*	132.905988
	134	133.904486
	135	134.905665
	136	135.904553
	137	136.905812
	138	137.905232
	139*	138.908826
$_{57}$La	137*	136.906460
	138*	137.907105
	139	138.906347
	140*	139.909471
	141*	140.910896
$_{58}$Ce	134*	133.908890
	135*	134.909117
	136	135.907140
	137*	136.907780
	138	137.905985
	139*	138.906631
	140	139.905433
	141*	140.908271
	142*	141.909241
$_{59}$Pr	139*	138 908917
	140*	139.909071
	141	140.907647
	142*	141.910039
	143*	142.910814
$_{60}$Nd	141*	140.909594
	142	141.907719
	143	142.909810

Atom	A	Mass
($_{60}$Nd)	144*	143.910083
	145*	144.912570
	146	145.913113
	147*	146.916097
	148	147.916889
	149*	148.920145
	150	149.920887
	151*	150.923825
$_{61}$Pm	143*	142.910930
	144*	143.912588
	145*	144.912743
	146*	145.914708
	147*	146.915135
	148*	147.917473
	149*	148.918332
$_{62}$Sm	143*	142.914626
	144	143.911998
	145*	144.913409
	146*	145.913053
	147*	146.914894
	148*	147.914819
	149*	148.917180
	150	149.917273
	151*	150.919929
	152	151.919728
	153*	152.922094
	154	153.922205
	155*	154.924636
$_{63}$Eu	149*	148.917926
	150*	149.919702
	151	150.919847
	152*	151.921742
	153	152.921225
	154*	153.922975
	155*	154.922889
$_{64}$Gd	152*	151.919786
	153*	152.921745
	154	153.920861
	155	154.922618
	156	155.922118
	157	156.923956
	158	157.924099
	159*	158.926384
	160	159.927049
	161*	160.929664
$_{65}$Tb	157*	156.924023

Atom	A	Mass
($_{65}$Tb)	158*	157.925411
	159	158.925342
	160*	159.927163
	161*	160.927566
$_{66}$Dy	156*	155.924277
	157*	156.925460
	158	157.924403
	159*	158.925735
	160	159.925193
	161	160.926930
	162	161.926795
	163	162.928728
	164	163.929171
	165*	164.931700
$_{67}$Ho	163*	162.928731
	164*	163.930285
	165	164.930319
	166*	165.932281
	167*	166.933127
$_{68}$Er	161*	160.929996
	162	161.928775
	163*	162.930030
	164	163.929198
	165*	164.930723
	166	165.930290
	167	166.932046
	168	167.932368
	169*	168.934588
	170	169.935461
	171*	170.938027
$_{69}$Tm	167*	166.932848
	168*	167.934170
	169	168.934212
	170*	169.935798
	171*	170.936427
$_{70}$Yb	167*	166.934946
	168	167.933894
	169*	168.935186
	170	169.934759
	171	170.936323
	172	171.936378
	173	172.938208
	174	173.938859
	175*	174.941273
	176	175.942564
	177*	176.945253

Atom	A	Mass
$_{71}$Lu	173*	172.938929
	174*	173.940336
	175	174.940770
	176*	175.942679
	177*	176.943752
$_{72}$Hf	174*	173.940044
	175*	174.941507
	176	175.941406
	177	176.943217
	178	177.943696
	179	178.945812
	180	179.946546
	181*	180.949096
$_{73}$Ta	179*	178.945930
	180*	179.947462
	181	180.947992
	182*	181.950149
	183*	182.951369
$_{74}$W	179*	178.947067
	180	179.946701
	181*	180.948192
	182	181.948202
	183	182.950220
	184	183.950928
	185*	184.953416
	186	185.954357
	187*	186.957153
$_{75}$Re	183*	182.950817
	184*	183.952530
	185	184.952951
	186*	185.954984
	187*	186.955744
$_{76}$Os	183*	182.953290
	184	183.952488
	185*	184.954041
	186*	185.953830
	187	186.955741
	188	187.955830
	189	188.958137
	190	189.958436
	191*	190.960920
	192	191.961467
	193*	192.964138
$_{77}$Ir	189*	188.958712
	190*	189.960580

(continued)

Atom	A	Mass
($_{77}$Ir)	191	190.960584
	192*	191.962580
	193	192.962917
	194*	193.965069
$_{78}$Pt	190*	189.959917
	191*	190.961665
	192	191.961019
	193*	192.962977
	194	193.962655
	195	194.964766
	196	195.964926
	197*	196.967315
	198	197.967869
	199*	198.970552
$_{79}$Au	195*	194.965013
	196*	195.966544
	197	196.966543
	198*	197.968217
	199*	198.968740
$_{80}$Hg	195*	194.966640
	196	195.965807
	197*	196.967187
	198	197.966743
	199	198.968254
	200	199.968300
	201	200.970277
	202	201.970617
	203*	202.972848
	204	203.973467
	205*	204.976047
Tl	201*	200.970794
	202*	201.972085
	203	202.972320
	204*	203.973839
	205	204.974401
	206*	205.976084
Pb	202*	201.972134
	203*	202.973365
	204	203.973020
	205*	204.974458
	206	205.974440
	207	206 975872
	208	207.976627
	209*	208.981065
i	207*	206.978446
	208*	207.979717

Atom	A	Mass
($_{83}$Bi)	209*	208.980374
	210*	209.984095
	211*	210.987255
$_{84}$Po	208*	207.981222
	209*	208.982404
	210*	209.982848
	211*	210.986627
	212*	211.988842
$_{85}$At	209*	208.986149
	210*	209.987126
	211*	210.987469
	212*	211.990725
$_{86}$Rn	211*	210.990576
	219*	219.009479
	220*	220.011368
	222*	222.017571
$_{87}$Fr	212*	211.996130
	221*	221.014230
	222*	222.017560
	223*	223.019733
$_{88}$Ra	223*	223.018501
	224*	224.020186
	225*	225.023604
	226*	226.025403
	228*	228.031064
$_{89}$Ac	225*	225.023205
	226*	226.026084
	227*	227.027750
	228*	228.031015
$_{90}$Th	229*	229.031755
	230*	230.033128
	232*	232.038051
	234*	234.043593
$_{91}$Pa	231*	231.035880
	232*	232.038565
	233*	233.040242
	234*	234.043303
$_{92}$U	232*	232.037130
	233*	233.039628
	234*	234.040947
	235*	235.043924
	236*	236.045563
	237*	237.048725
	238*	238.050785

Atom	A	Mass
$_{93}$Np	235*	235.044056
	236*	236.046550
	237*	237.048168
	238*	238.050941
	239*	239.052933
$_{94}$Pu	236*	236.046032
	238*	238.049555
	239*	239.052158
	240*	240.053808
	241*	241.056846
	242*	242.058737
$_{95}$Am	240*	240.055278
	241*	241.056824
	242*	242.059542
	243*	243.061375
$_{96}$Cm	243*	243.061382
	244*	244.062747
	245*	245.065484
	246*	246.067218
	247*	247.070347
	248*	248.072343
	250*	250.078352
$_{97}$Bk	245*	245.066357
	247*	247.070300
	249*	249.074980
$_{98}$Cf	248*	248.072183
	249*	249.074845
	250*	250.076400
	251*	251.079580
	252*	252.081621
$_{99}$Es	251*	251.079986
	252*	252.082944
	253*	253.084818
	254*	254.088019
$_{100}$Fm	252*	252.082466
	253*	253.085173
	254*	254.086846
	255*	255.089948
	256*	256.091767
	257*	257.095099
$_{101}$Md	255*	255.091081
	256*	256.093960
$_{102}$No	252*	252.08895
	254*	254.09095

Atom	A	Mass	Atom	A	Mass	Atom	A	Mass
($_{102}$No)	256*	256.09425	$_{104}$Rf	259*	259.1055	$_{106}$	263*	263.1182
	257*	257.09685		261*	261.1087	$_{107}$	262*	262.1229
	259*	259.10093	$_{105}$Ha	260*	260.1110			
$_{103}$Lr	259*	259.10290		261*	261.1118			
	260*	260.10532		262*	262.1138			

قائمة المصطلحات

المصطلــح	وصفــه
Abelian group	زمرة أبيلية
Addition modulo n	جمع معيار أو مقياس n
Admissible sequence	متتابعة مقبولة
Algebraically closed	مغلق جبرياً
Algebraic closure	الانغلاق الجبري
algebraic extension	توسيع جبري
Alternating group A_n	الزمرة المتناوبة A_n
Annihilator	معدم
Artinian ring	حلقة أرتينية
Ascending chain condition (ACC)	شرط السلسلة التصاعدية
Automorphism	أتومورفزم
Basis	قاعدة
Bijection	تقابل أو تناظر أحادي
Cartesian product	الضرب الديكارتي أو الكارتيزي
Centralizer	مركز
Center of group	مركز الزمرة
Characteristic	مميز
Characteristic polynomial	كثيرة الحدود المميزة
Class	فصل أو صف
Class equation	معادلة صف
Classical canonical matrix	المصفوفة القانونية الكلاسيكية
Co domain	انطباق المصاحب
Co-maximal	متعاظمة ، أعظمية مترافقة

وصفه	المصطلح
حلقة إبدالية	Commutative ring
مبادلة	Commutator
المصفوفة المصاحبة	Companion matrix
متمم أو مكمل فضاء جزئي	Complement of a subspace
سلسلة تركيبية	Composition series
مرافق	Conjugate
قابل للانتشار	Constructible
عناصر أولية نسبياً	Co-prime elements
نظرية التقابل	Correspondence theorem
مجموعة مصاحبة	coset
مجموعة قابلة للعد	Countable set
دورة	Cycle
زمرة دائرية أو دورية	Cyelic group
فضاء دوري	Cyclic space
كثيرة حدود سايكلوتومية	Cyclotomic polynomial
مجموعة قابلة للترقيم	Denumerable set
الزمرة المشتقة	Derived group
شرط السلسلة التنازلية	Descending chain condition (*DCC*)
قابل للتمثيل القطري	Diagonalizable
الزمرة الدايهيدرالية	Dihedral group
بعد	Dimension
الضرب المباشر	Direct product
حد مجموع مباشر	Direct summand
مجموع مباشر	Direct sum
قابل للقسمة	Divisible
خوارزمية القسمة	Division algorithm

المصطلح	وصفه
Division ring	حلقة قاسمية
Domain	ساحة
Dual	ثنائي
Eigen value	قيمة ذاتية
Eigen vector	متجه ذاتي
Eisenstien's Criterion	معيار أيزنستن
Elementary divisors	قواسم أولية أو ابتدائية
Elementary symmetric function	دالة تماثل أولية
Embedding theorems for rings	نظريات الأغمار للحلقات
Endomorphism	إندومورفزم
Epimorphism	أبيمورفزم
Equipotent sets	مجموعات متكافئة
Equivalence class	فصل تكافؤ
Equivalent matrices	مصفوفات متكافئة
Euclidean algorithm	خوارزمية إقليدس
Euclidean domain	ساحة إقليدية
Even permutation	تبديل زوجي
Extension	توسيع
Factorization domain	ساحة تحليل
Field of quotients	حقل قواسم
Fixed field	الحقل المثبت
Galois extension	توسيع جالوا
Galois theory	نظرية جالوا
Gaussian domain	ساحة جاوسيان
Geometric multiplicity	تكرار هندسي ، تعددية هندسية
Gram-Schmiat orthogonalization process	طريقة جرام شميدث للتعامد

المصطلـح	وصفــه
Highest common factor (*HCF*)	عامل مشترك أعلى
Ideal	مثالي
Identity	محايد
Image	صورة
Inclusion map	راسم الاحتواء
Index of a subgroup	دليل زمرة جزئية
Inner automorphism	أتومورفزم داخلي
Inner product space	فضاء ضرب داخلي
Integral domain	ساحة تامة
Invariant subgroup	زمرة جزئية لا متغيرة
Invertible element	عنصر قابل للعكس
Jordan block	قالب جوردان
Jordan normal from	صيغة جوردان القانونية
Kernel	نواة
Klein's 4-group	زمرة كلاين الرباعية
Leadiny coefficient	المعامل القائد
Least common multiple (*LCM*)	المضاعف المشترك الأصغر
Linear combination	تركيب خطي
Linearly dependent (L.D.)	مرتبط خطياً
Linearly independent (L.I.)	مستقلة خطياً
Linear transformation	تحويل خطي
Mapping	راسم
Maximal	أعظمي
Maximal normal subgroup	زمرة جزئية عادية أعظمية
Minimal	أصغري
Minimal polynomial	كثيرة حدود أصغرية

المصطلـح	وصفـه
Monomorphism	مونومورفزم
Multiplicative subset	مجموعة جزئية ضربية
Nilpotent	عديم القوة
Norm	معيار
Normal extension	توسيع عادي
Normalizer	منظم
Nullity	صفرية
Null space	الفضاء الصفري
Odd permutation	تبديل فردي
Order	رتبة
Ordered basis	قاعدة مرتبة
Orthogonal	عمود
Orthonormal	عياري متعامد
Partial ordering	ترتيب جزئي
Permutation	تبديل
Polynomial	كثيرة حدود
Primary	ابتدائي
Prime	أولي
Prime subfield	حقل أولي
Primitive	ابتدائي
Principal	رئيسي
Projection	إسقاط
Quaternion group	الزمرة الكوانيرنسية
Quotient ring	حلقة القسمة
Radical extension	توسيع جذري
Range	مدى

المصطلـح	وصفـه
Rank	مرتبة
Refinement	تحسين
Regular	منتظم
Restriction	مقصور أو مقيد
Separable	قابل للفصل
Singular	منفرد
Splitting field	حقل انغلاق
Solvable	قابل للحل
Surjection	فوقي
Symmetric	متناظر ، متماثل
Sylow's theorems	نظريات سايلو
T-invariant	لا متغير وفق T
Transcendental	متسامي
Transitive	متعددي
Transpose	منقول أو مدور
Unit of a ring	وحدة في حلقة
Valuation ring	حلقة تقييم
Vector space	فضاء متجهي
Zero divisor	قاسم صفري

المراجع

1. Adamson, I. T., *Elementary Rings and Modules*. Edinburgh: Oliver &: Boyd,1972.
2. Adamson, I. T., *Introduction to Field Theory*. London: Oliver & Boyd, 1964.
3. Albert, A. A., *Fundamental Concepts of Higher Algebra*. Chicago: University of Chicago Press. 1956.
4. Ames, D. B., *An Introduction to Abstract Algebra*. Scranton, Pennsylvania: International Text Book Company. 1969.
5. Ames, D. B., *Fundamentals of Linear Algebra*. Scranton, Pennsylvania: International Text i Book Company, 1970. .
6. Artin, E., *Galois Theory*. Notre Dame, Indiana: University of Notre Dame Press, 1955.
7. Artin, E., C. Nesbitt and R. Thrall, *Rings with Minimum Condition*. Ann. Arbor, Michigan: University of Michigan Press, 1944.
8. Atiyah. M. F. and I. G. Macdonald, *Introduction to Commutative Algebra*. Reading. Massachusetts: Addison-Wesley, 1969.
9. Auslander, M. and D. A. Buchsbaum, *Groups, Rings, Modules*. New York: Harper & Row, 1974.
10. Barnes, W. E., *Introduction to Abstract Algebra*. Boston: Heath, 1963.
11. Barshay, J., *Topics in Ring Theory*. New York: W. A. Benjamin, Inc., 1969.
12. Baumslag, B. and B. Chandler. *Theory and Problems of Group Theory*. New York: Mc Graw-Hill Book Company, 1968.
13. Behrens, E.A., *Ring Theory*. New York: Academic Press, 1972.
14. Birkhoff, G. and S. Maclane. *A Survey of Modern Algebra*. New York: Macmillan, 1965.
15. Birkhoff, G. and S. Maclane. *Algebra*. New York: Macmittan, 1979.
16. Bourbaki. N., *Commutative Algebra*. Reading, Massachusetts: Addison-Wesley, 1972.
17. Burnside. W., *Theory of Groups of Finite Order*. New York: Dover, 1955.
18. Burton, D. M., *A First Course in Rings and Ideals*. Reading, Massachusetts: Addison Wesley, 1968.
19. Burton, D. M., *Abstract and Linear Algebra* Addison-Wesley 1972.

20. Charmichael, R. D., *Introduction to the Theory of Groups of Finite Order*. New York: Dover, 1956.

21. Chevalley, C., *Fundamental Concepts of Algebra*. New York: Academic Press, 1956.

22. Coho, P. M., *Algebra,* Vol. I. New York: John Wiley & Sons, 1974.

23. Coho, P. M., *Algebra,* Vol. II. New York: John Wiley & Sons, 1977.

24. Dean, R. A., *Elements of Abstract Algebra,* New York: Wiley, 1966.

25. Dixon, J. D., *Problems in Group Theory*. Waltham, Massachusetts: Blaisdell, 1967.

26. Dubreil, P. and M. L. Dubreil Jacotin, *Lectures on Modern Algebra*. New York: Hafner Publishing Company, 1967.

27. Durbin, J. R., *Modern Algebra, An Introduction*. New York: John Wiley, 1979.

28. Finkbeiner H, D. T., *Introduction to Matrices and Linear Transformations*. Tokyo: Toppan Company Ltd., *1965*.

29. Fraleigh, J. B., *A First Course in Abstract Algebra*. Reading, Massachusetts: Addison-Wesley, 1968.

30. Fuchs, L., *Abelian Groups*. Oxford: Pergamon Press, 1960.

31. Fuchs, L., *Infinite Abelian Groups,* Vol. I. New York: Academic Press, 1970.

32. Fuchs, L., *Infinite Abelian Groups,* Vol. It. New York: Academic Press, 1973.

33. Gaal. L., *Galois .Theory with Examples*. New York: Chelsea, 1973.

34. Goldhaber, J. K. and G. Ehrlich. *Algebra*. London: Macmillan, 1970.

35. Goldstein. L. R., *Abstract Algebra, a First Course*. Englewood Cliffs, New Jersey: Prenctice-Hall, 1973.

36. Gorenstein, D., *Finite Groups*. New York: Harper and Row, 1968.

37. Gray, M., *A Radical Approach to Algebra*. Reading, Massachusetts: Addison-Weslet, 1970.

38. Green, J. A.. *Sets and Groups*. London: Routledge and Kegan Paul, 1965.

39. Greub. W. H., *Linear Algebra*. Berlin: Springer-Verlag, 1967.

40. Griffith, P. A., *Infinite Abelian Group Theory*. Chicago: The University of Chicago Press, 1970.

41. Hall Jr., M., *TIe Theory of Groups*. New York: Macmillan, 1959

42. Halmos, P., *Finite-dimensional Vector Spaces*. Princeton, New Jersey: Von Nostrand, 1958.

43. Halmos, P., *Naive Set Theory*. Princeton, New Jersey: Von Nostrand, 1960.

44. Herstein, I. N., *Topics in Algebra*. Delhi: Vikas, 1971.

45. Hilton, P. J. and Y-C. Wu, *A Course in Modern Algebra*, New York: John Wiley, 1974.

46. Hoffman, K. and R. Kunze, *Linear Algebra*. Englewood Cliffs; New Jersey: Prentice-Hall, 1961.

47. Hungeford, T. W.. *Algebra*. New York: Holt, Rinehart and Winston, 1974.

48. Huppert. B., *Endliche Gruppen I,* Berlin: Springer-Verlag, 1967.

49. Hu, S. T., *Elements of Modern Algebra*. San Francisco; California: Holden Day Inc., 1965.

50. Jacobson, N., *Basic Algebra*. Vol. I. San Francisco: W, H. Freeman, 1974.

51. Jacobson, N., *Lectures in Abstract Algebra,* Vol. I. Princeton, New Jersey: Von Nostrand, 1951.

52. Jacobson, N., *Lectures in Abstract Algebra,* Vol. II. Von Nostrand, 1953.

53. Jacobson, N., *Lectures of Abstract Algebra,* Vol. III. Von Nostrand, 1964.

54. Jacobson, N., *Structure of Rings*. Providence. American Mathematical Society, 1964.

55. Kaplansky, I., *Conzmututive Rings*. Boston. Massachusetts: Allyn & Bacon, 1970.

56. Kaplansky, I., *Fields and Rings*. Chicago: The University of Chicago Press, 1969.

57. Kargapolov. M. I. and Ju I. Merzljakav, *Fundamentals of the Theory of Groups*. New York: Springer-Verlag, 1979.

58. Kochendorfer, R., *Group Theory*. London: McGraw-Hill, 1970.

59. Kuczkowski, J. E. and J. L. Gerstins, *Abstract Algebra. a First Look*. New York: Marcel Dekker, 1977.

60. Kurosh, A. G., *The Theory of Groups,* (Two volumes). New York: Chelsea. 1960.

61. Lambek, J., *Lectures on Rings and Modules*. Waltham, Massachusetts: Blaisdell, 1966.

62. Lang. S., *Algebra*. Reading, Massachusetts: Addison-Wesley, 1965.

63. Lang. S., *Linear Algebra*. Reading, Massachusetts: Addison-Wesley. 1968.

64. Ledermann, W., *An Introduction to the Theory of Finite Groups*. London: Oliver & Boyd., 1964.

65. Ledermann, W., *Introduction to Group Theory*. London: Longman, 1973.

66. Lewis, D. J., *Introduction to Algebra*. New York: Harper & Row, 1965.

67. Macdonald, I. D., *Tire Theory 01 Groups*. Oxford: Oxford University Press, 1968.

68. Macduffee, C. C., *An Introduction to Abstract Algebra*. New York: Dover, 1964.

69. Marcus, M., *Introduction to Modern Algebra*. New York: Marcel Dekker, 1978.

70. Mc Carthy, P., *Algebraic Extension 01 Fields*. Waltham, Massachusetts: Blaisedll, 1966.

71. Mc Coy. N. H., *The Theory 01 Rings*. New York: Macmillan, 1964.

72. Mc Coy. N. H., *Introduction to Modern Algebra*. Boston: Allyn & Bacon, 1975.

73. Mc Coy. N. H., *Fundamentals 01 Abstracts Algebra*. Allyn &. Bacon, 1972.

74. Mc Coy. N. H., and T. R. Berger, *Algebra, Groups, Rings and other Topics*. Allyn & Bacon, 1977.

75. Moore, J. T., *Elements of Abstract Algebra*. New York: Macmillan, 1967.

76. Moore, J. T., *Introduction to Abstract Algebra*. New York: Academic Press; 1975.

77. Mostow, G. D., J. H. Sampson and J. Meyer, *Fundamental Structures of Algebra*. New York: McGraw-Hill, 1963.

78. Nagata,.M., *Field Theory*. New. York: Marcel Dekker, 1977.

79. Niven, I., *Irrational Numbers*. New York: Carus Monographs No. II, John Wiley & Sons, 1956.

80. Paley, H. and P. M. Weichsel, *A First Course in Abstract Algebra*. New York: Holt, Rinehart and Winston, 1966.

81. Passman, D. S., *Permutation Groups*. New York: W. A. Benjamin, 1969.

82. Perlis, S., *Introduction to Algebra*. Waltham; Massachusetts: Blaisdell, 1966.

83. Polites, G. W., *An Introduction to the Theory 01 Groups*. Scranton; International Text Book Company, 1968.

84. Postinikov, M. M., *Foundations 01 Galois Theory*. Oxford: Pergamon Press, 1962.

85. Redei, L., *Algebra*. Vol. I. Oxford: Pergamon Press, 1967.

86. Ribenboim, P., *Rings and Modules*. New York: Interscience, 1969.

87. Rose, John S., *A Course on Group Theory*. Cambridge: Cambridge University Press, 1978.

88. Rotman, J. J., *Theory 01 Groups*. Boston: Allyn & Bacon, *1965*.

89. Sah, C. H., *Abstract Algebra*. New York: Academic Press, 1967.

90. Samuel, P.. *Algebraic Theory of Numbers*. London: Kershaw Publishing Company Ltd., 1972. ,

91. Saracino Dam, *Abstract Algebra*, *a First Course*. Reading, Massachusetts: Addison-Wesley, 198O.

92. Satake, J., *Linear Algebra*. New York: Marcel Dekker, 1975,

93. Schwerdtfeger, H., *Introduction 10 Group Theory*. Leyden: No-ordhoff International Publishing, 1976.

94. Scott, W. R., *Group Theory*. Englewood Cliffs, New Jersey: Prentice-Hall. 1964.

95. Shapiro, L. W., *Introduction to Abstract Algebra,* New York: McGraw. Hill Book Company, 1975.

96. Shephard, O. C., *Vector Spaces of Finite*. *Dimension*. London: Oliver & Boyd, 1966.

97. Sigler, L.E., *Algebra* New York: Springer-Verloy, 1976.

98. Smirnov, V.L., *Linear Algebra and Group Theory*, New York: Dover, 1961.

99. Stewart, I., *Galois Theory*, London: Chapman and Hall, 1973.

100. Van Der Waerden, B. L., *Modern Algebra*, Vol. I. New York: Unger. 1545.

101. Van Der Waerden, B. L., *Modern Algebra*, Vol. II. New York: Unger, 1950.

102. Wallace, D.A.R., *Groups*, London: George Allen & Unwin Ltd., 1974.

103. Warner, S., *Classical Modern Algebra*, Englewood Cliffs, New Jersey: Prentice Hall, 1971.

104. Warner, S., *Modern Algebra* (Two Volumes). Prentice Hall, 1965.

105. Weilandt, H., *Finite Permutation Groups*, New York: Academic Press. 1964.

106. Zariski, O. and P. Samuel, *Commutative Algebra*, Vol. I. Princeton, New Jersey: Von Nostrand, 1954.

107. Zariski, O. and P. Samuel, *Commutative Algebra*, Vol. II. Ven Nostrum, 1960.

108. Zassenhans, H., *The Theory of Groups*, New York: Chelscu, 1958.