الوحدة الرابعة

الحلقات والحقول
Rings and Fields

(1)، (2) الفصلان 24، 25 غير مطلوبين حتى نهايتهما.

الفصل 18 الحلقات والحقول: Rings and Fields

تركز عملنا السابق على المجموعات المعرّف عليها عملية ثنائية وحيدة، وقد تبين خلال سنوات من دراستنا للأعداد الصحيحة والحقيقية، أنّ دراسة المجموعات المعرّف عليها عمليتان ثنائيتان بالغتا الأهمية، وسيكون هذا النوع من البنية الجبرية محور دراستنا في هذا الفصل، الذي سيكون إلى حد ما أكثر تشويقًا من الفصول السابقة؛ لأن البنى الجبرية التي نحن بصدد دراستها ذات علاقة قريبة بالبنى الجبرية التي عملنا عليها في السنوات السابقة، وعلى الرغم من ذلك، فسوف نستمر بأسلوب المسلمات، بعبارة أخرى، تعدّ هذه الدراسة أكثر تعقيدًا من مبرهنة الزمرة؛ لأننا نتعامل مع عمليتين ثنائيتين ومسلمات أكثر.

البنية الجبرية المعرف عليها عمليتان ثنائيتان الأكثر عمومًا، التي سنقوم بدراستها تسمى حلقة (*ring*)، كما يظهر مثال 2.18 الذي يتبع تعريف 1.18، فقد تعاملنا كلنا مع الحلقات منذ الدراسة الابتدائية.

تعريفات وخصائص أساسية

1.18 تعريف الحلقة (***ring***) $\langle R, +, . \rangle$ هي مجموعة R معرّف عليها عمليتان ثنائيتان + و. التي نسميها الجمع (*addition*) والضرب (*multiplication*)، وتحقق المسلمات الآتية:

$\mathcal{R}_1$. $\langle R, + \rangle$ زمرة إبدالية.

$\mathcal{R}_2$. الضرب تجميعي.

$\mathcal{R}_3$. لكل $a,b,c \in R$ **قانون التوزيع من اليسار**.

$a.(b+c) = (a.b)+(a.c)$ (**Left distributive law**) **وقانون التوزيع من اليمين**

$(a+b).c =(a.c) + (b.c)$ (**right distributive law**) متحققان. ■

2.18 مثال الكل يدرك أنّ أيّ مجموعة جزئية من مجموعة الأعداد المركبة، بحيث تكون زمرة مع الجمع ومغلقة مع الضرب، فإنها تحقق المسلمات $\mathcal{R}_1$ ، $\mathcal{R}_2$ و $\mathcal{R}_3$ ، ومثال على ذلك:

$\langle \mathbb{Z}, +, . \rangle$، $\langle \mathbb{Q}, +, . \rangle$، $\langle \mathbb{R}, +, . \rangle$ و $\langle \mathbb{C}, +, . \rangle$ حلقات. ▲

■ **نبذة تاريخية**

نشأت مبرهنة الحلقات من دراسة نوعين محددين من الحلقات، هما: حلقات كثيرات الحدود بـ n من المتغيّرات على مجموعة الأعداد الحقيقية أو المركبة (فصل 22)، و"الأعداد الصحيحة" لحقل الأعداد الجبرية، حيث إنّ أول من قدّم مفهوم الحلقة المرتبط بالمثال 2.18، هو ديفيد هيلبرت (David Hilbert 1862- 1943)، ولكن هذا المفهوم لم يظهر قبل العقد الثاني من القرن العشرين، عندما ظهر تعريف كامل ومجرد للحلقة، وقد بُنيت لمبرهنة الحلقات الإبدالية قاعدة ثابتة من المسلمات من قبل إيمي نوثير (Emmy Noether 1882- 1935) في بحثها الضخم "مبرهنة المثاليات في الحلقات" الذي ظهر عام 1921م، فالموضوع الرئيس في هذا البحث هو شرط السلسلة المتصاعدة من المثاليات، وقد أثبتت نوثير أنّ في الحلقة التي يكون فيها لكل سلسلة متصاعدة من المثاليات عنصر أعظم، يكون كل مثالي فيها منتهي التولد.

حصلت إيمي نوثير على درجة الدكتوراة من جامعة إيرلانجن في ألمانيا عام 1907م، ودعاها هيلبرت للعمل في جامعة جوتنجن عام 1915م، ولكن جهوده في تأمين موقع لها في الجامعة باءت بالفشل بسبب جنسها، فاشتكى هيلبرت قائلًا: "لا أرى أنّ جنس المتقدّم للوظيفة عائق للحصول عليها؛ لأننا في جامعة، ولسنا في حمام سباحة"، وعلى الرغم من ذلك، تمكنت نوثير من أن تحاضر في الجامعة باسم هيلبرت، أخيرًا حصلت إيمي على الموقع الذي تستحقه في الجامعة عام 1923م، بعد التغييرات السياسية التي تبعت نهاية الحرب العالمية الأولى التي وصلت إلى جوتنجن، وقد كانت خلال السنوات العشر اللاحقة فاعلة ومؤثرة في تطوير المفاهيم الأساسية للجبر الحديث، وعلى الرغم من ذلك، فقد أرغمت هي وبعض أعضاء الكلية من اليهود على ترك جوتنجن عام 1933م، فأمضت آخر سنتين من عمرها في كلية براين مور بالقرب من فيلادلفيا.

من الشائع أن نرمز للضرب داخل الحلقة باستخدام ab بدلاً من $a.b$ دون حدوث أيّ التباس، وسوف نلاحظ أنه دون الأقواس، فإن الضرب يسبق الجمع، وعليه، فإن قانون التوزيع من اليسار على سبيل المثال يصبح:

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

دون استخدام الأقواس للجهة اليمنى من المعادلة، كذلك سنستعمل أسلوبًا مريحًا للدلالة على الحلقة $\langle R, +, . \rangle$، حيث سنسميها ببساطة R، وسنغض الطرف عن عدم دقّة هذا التعبير، تمامًا كما سمّينا الزمرة اختصارًا G بدلاً من $\langle G,* \rangle$، وذلك عندما لا يكون هناك أيّ التباس، وبوجه خاص، فإنّ $\mathbb{Z}$ تعني من الآن فصاعدًا $\langle \mathbb{Z}, +, . \rangle$ و $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ وهي الحلقات في المثال 2.18، وربما في مناسبة ما ستعني $\langle R, + \rangle$ الزمرة الجمعية للحلقة R (*additive group of the ring*).

3.18 مثال لتكن R أيّ حلقة، ولتكن $M_n(R)$ مجموعة المصفوفات من الدرجة $n \times n$ ومدخلاتها من الحلقة R، حيث إن عمليات الجمع والضرب المعرفة على R ستسمح لنا بجمع وضرب مصفوفات بالطريقة الاعتيادية، وهذا مشروح في الملحق، فيمكننا التحقق بسرعة من أنّ $\langle M_n(R), +, . \rangle$ زمرة إبدالية، ومن الجدير ذكره، أن تحقق قانون التجميع في ضرب المصفوفات وقانوني توزيع الضرب على الجمع في $M_n(R)$ تحتاج إلى عمل مضنٍ، ولكن الحسابات المباشرة توضح أنها تتحقق خصائص R نفسها، وسوف نفترض من الآن فصاعدًا أنه معلوم لدينا أن $M_n(R)$ حلقة، بوجه خاص $M_n(\mathbb{Q})$، $M_n(\mathbb{R})$، $M_n(\mathbb{C})$ حلقات.

(لاحظ في هذه الحلقات كلها أن الضرب ليس إبداليًّا لـ $n \geq 2$.) ▲

4.18 مثال لتكن F مجموعة الدوال كلها $f : \mathbb{R} \to \mathbb{R}$. نعلم أن $\langle F,+\rangle$ زمرة إبدالية بالنسبة إلى جمع الدوال العادي،

$$(f+g)(x) = f(x) + g(x)$$

سنعرف الضرب على F بـ

$$(fg)(x) = f(x)\, g(x)$$

وهذا يعني أنّ fg هي الدالة التي قيمتها عند x تكون $f(x)g(x)$، ومن الممكن التحقق شفويًّا أنّ F حلقة، وسنترك توضيح ذلك لتمرين 34. لقد استخدمنا التعبير $\sigma\mu$ ليعني الدالة المركبة $\sigma(\mu(x))$ عندما ناقشنا الضرب التبديلي، وإذا استخدمنا ضرب الدوال وتركيبها في F، فسنستخدم التعبير $f \circ g$ للدالة المركبة، وعلى الرغم من ذلك، فإن استخدامنا لتركيب الدوال سيكون حصريًّا من التشاكلات التي سوف نرمز لها بالحروف اليونانية، ولن يؤدي هذا إلى أيّ تشويش مع الضرب المعرّف في هذا المثال، وخصوصًا عند ضرب كثيرات حدود $f(x)g(x)$. ▲

5.18 مثال تذكر من مبرهنة الزمرة، أنّ $n\mathbb{Z}$ زمرة جزئية دورية من $\mathbb{Z}$ بالنسبة إلى الجمع، وتتكوّن من مضاعفات الأعداد الصحيحة جميعها للعدد الصحيح n؛ لأن

$(nr)\,(ns) = n(nrs)$ فإن $n\mathbb{Z}$ مغلقة على الضرب، ولأن قانون التجميع وقانوني التوزيع متحققان في $\mathbb{Z}$ وهذا يؤكد لنا أنّ $\langle n\mathbb{Z}\ , +\ , .\ \rangle$ حلقة، ومن الآن فصاعدًا سنعدّ $n\mathbb{Z}$ هي هذه الحلقة في هذا الكتاب. ▲

6.18 مثال لتكن الزمرة الدورية $\langle \mathbb{Z}_n\ , +\ \rangle$، فإذا عرّفنا لـ $a,b \in \mathbb{Z}_n$ الضرب ab على أنه باقي قسمة ناتج ضرب الأعداد الصحيحة على n، فيمكننا إثبات أنّ $\langle \mathbb{Z}_n\ , +, . \rangle$ حلقة، ويمكنك استخدام هذه الحقيقة، فعلى سبيل المثال في: $\mathbb{Z}_{10}$، $(3)\,(7) = 1$، وتسمى هذه العملية على $\mathbb{Z}_n$ **بالضرب مقياس** n (**multiplication modulo**)، ولن نتحقق هنا من مسلمات هذه الحلقة؛ لأننا سنرى أنّ المسلمات متحققة من الفصل 26 من خلال مبرهنة طُوّرت هناك، ومن الآن فصاعدًا، فإنّ $\mathbb{Z}_n$ تعني الحلقة $\langle \mathbb{Z}_n\ , +, .\ \rangle$. ▲

7.18 مثال إذا كان $R_1, R_2, \ldots R_n$ حلقات، فيمكننا تعريف المجموعة $R_1 \times R_2 \times \ldots \times R_n$ المكوّنة من المتعددات من المرتبة n $(r_1, r_2, \ldots, r_n)$، حيث $r_i \in R_i$، وقد عُرّف الضرب والجمع على المتعددات من المرتبة n على كل حدّ مع ما يقابله (كما فعلنا مع الزمر)، ويمكننا ملاحظة أنّ مسلمات الحلقة متحققة على كل حدّ، ما يؤدي إلى أن المجموعة المكوّنة من المتعددات من المرتبة n تشكل حلقة تحت الجمع والضرب المعرّف على كل حدّ مع ما يقابله، حيث تسمّى هذه الحلقة **(direct product)** للحلقات R_i. ▲

سنأخذ في الحسبان الملاحظات الآتية: سنعدّ 0 العنصر المحايد لعملية الجمع لأيّ حلقة، والمعكوس الجمعي لأيّ عنصر a هو $-a$، وسنشير إلى المجموع

$$a + a + \ldots + a$$

n من المرّات بـ $n.a$ مستخدمًا النقطة، مع ذلك، فإنّ $n.a$ لا تعني حاصل ضرب n مع a في الحلقة؛ لأن العدد الصحيح n ليس عنصرًا في الحلقة أبدًا.

إذا كان $n < 0$، فلتكن:

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

$|n|$ من المرات، أخيرًا، نعرف

$$0.a = 0$$

لـ $0 \in \mathbb{Z}$ على الجهة اليسرى من المعادلة و $0 \in R$ على الجهة اليمنى، وفي الحقيقة، فإن المعادلة $a = 0$ 0 متحققة أيضًا لـ $0 \in R$ في جهتي المعادلة.

المبرهنة القادمة تثبت هذه الحقيقة وحقائق أخرى أساسية ومهمّة، ستلاحظ استخدامنا القوي لقانون التوزيع في إثبات هذه المبرهنة، حيث تركز المسلمة الأولى $\mathcal{R}_1$ في تعريف الحلقة على الجمع، وتركز الثانية $\mathcal{R}_2$ على الضرب؛ لذلك لإثبات أيّ شيء يعطي العلاقة بين هاتين العمليتين، فيجب علينا استخدام المسلمة الثالثة $\mathcal{R}_3$ ، على سبيل المثال: أوّل أمر سنوضّحه في المبرهنة 8.18 هو أن: $0a = 0$ لأي a في الحلقة R، وهذه العلاقة تشمل الجمع والضرب، حيث إنّ الضرب متمثل بـ $0a$ والجمع بـ 0؛ لذلك سنطور أسلوبًا يستخدم قانوني التوزيع في إثبات ذلك.

8.18 مبرهنة إذا كانت R حلقة والعنصر المحايد للجمع،0 فالخواص الآتية متحققة لكل $a,b \in R$:

-1 $0a = a0 = 0$

-2 $a(-b) = (-a)b = -(ab)$

-3 $(-a)(-b) = ab$

البرهان بالنسبة إلى الخاصية الأولى، لاحظ باستخدام المسلمتين $\mathscr{R}_1$ و $\mathscr{R}_2$،

$$a0 + a0 = a(0 + 0) = a0 = 0 + a0$$

ثم باستخدام قانون الحذف لزمرة الجمع $\langle R, + \rangle$، سنحصل على $a0 = 0$، وبالمثل:

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

ما يؤدي إلى $0a = 0$، وهذا إثبات الخاصية الأولى.

من أجل فهم إثبات الخاصية الثانية، يجب علينا تذكر– كما ورد في التعريف أن $-(ab)$ تعني أنه العنصر الذي عندما يضاف إلى ab نحصل على 0؛ لذلك لإثبات أن $a(-b) = -(ab)$، يجب علينا بالضبط إثبات أن $a(-b) + ab = 0$، باستخدام قانون التوزيع من اليسار،

$$a(-b) + ab = a(-b + b) = a0 = 0$$

لأنّ $a0 = 0$ كما بالخاصية 1، وبالمثل:

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

بالنسبة إلى الخاصية الثالثة، لاحظ أنه باستخدام الخاصية الثانية

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

ومرة أخرى باستخدام الخاصية الثانية،

$$-(a(-b)) = -(-(ab))$$

و $-(-(ab))$ هو العنصر الذي إذا أضيف إلى $-(ab)$ نحصل على 0، وهذا العنصر هو ab باستخدام تعريف $-(ab)$، وأن المعكوس الجمعي في الزمرة وحيد؛ لذلك فإن:

$$(-a)(-b) = ab.$$ ♦

من المهم جدًا فهم إثبات المبرهنة السابقة؛ لأنها ستسمح لنا باستخدام القوانين الاعتيادية للإشارات.

التشاكلات والتماثلات

من خلال عملنا على مبرهنة الزمرة، سيكون من الواضح كيف نعرف الدالة من الحلقة R إلى الحلقة R'.

9.18 تعريف للحلقتين R و R'، الدالة $\phi : R \to R'$ تشاكل (**homomorphism**)، إذا تحقق الشرطان الآتيان لأيّ $a,b \in R$

$$\phi(a+b) = \phi(a) + \phi(b) \qquad \textbf{-1}$$

$$\phi(ab) = \phi(a)\phi(b) \qquad \textbf{-2}$$

■

الشرط الأول في التعريف السابق هو العبارة التي تقول: إنّ ϕ هو دالة تشاكل من الزمرة الإبدالية $\langle R, + \rangle$ إلى $\langle R', + \rangle$، والمطلوب في الشرط الثاني: أن الدالة ϕ تعالج البنية الضربية للحلقتين R و R' في الوقت نفسه. لأن ϕ هي أيضًا تشاكل زمري، فإن النتائج جميعها المتعلقة بالتشاكلات الزمرية متحققة بالنسبة إلى البنية الجمعية للحلقتين، وبوجه خاص، الدالة ϕ واحد لواحد إذا وفقط إذا كانت النواة (**Kernel**) $\ker(\phi) = \{a \in R \mid \phi(a) = 0'\}$ هي فقط المجموعة الجزئية $\{0\}$ من R، ويمكن تعريف زمرة العامل باستخدام التشاكل ϕ للزمرة $\langle R,+\rangle$، إذ يُتوقع أنه يمكن تعريف حلقة العامل باستخدام التشاكل الحلقي، وهذا بالفعل ما سيحدث، سنؤجل مناقشة ذلك إلى الفصل 26، حيث ستكون معالجة هذا الأمر مشابهة لمعالجتنا لزمرة العامل في الفصل 14.

10.18 مثال لتكن F تعني الحلقة التي تحوي الدوال كلها من $\mathbb{R}$ إلى $\mathbb{R}$ والمعرّفة في المثال 4.18، إذ إنّ لكل عنصر $a \in \mathbb{R}$ لدينا **تشاكل التعويض** (**evaluation homomorphism**) $\phi_a : F \to \mathbb{R}$ حيث $\phi_a(f) = f(a)$ لكل $f \in F$، عرفنا هذا التشاكل للزمرة $\langle F, + \rangle$ في مثال 4.13، إلّا أنّنا لم نتعامل معه في مبرهنة الزمر، وسوف نتعامل معه كثيرًا فيما تبقى من هذا الكتاب، فلإيجاد الحل الحقيقي لمعادلة كثيرة حدود $p(x) = 0$، فإن هذا يكافئ إيجاد $a \in \mathbb{R}$، حيث $\phi_a(p) = 0$، ومعظم ما تبقى من هذا الكتاب يتعامل مع إيجاد حلول معادلات كثيرات حدود، سنترك توضيح تحقيق التشاكل ϕ_a للشرط الثاني إلى تمرين 35. ▲

11.18 مثال الدالة $\phi:\mathbb{Z}\to\mathbb{Z}_n$، حيث $\phi(a)$ باقي قسمة a مقياس n، تشاكل حلقات لأيّ عدد صحيح موجب n، ونعلم من مبرهنة الزمر أن $\phi(a+b)=\phi(a)+\phi(b)$. لإثبات خاصية الضرب خذ $a=q_1n+r_1$ و $b=q_2n+r_2$ وبحسب خوارزمية القسمة، فإن:

$ab=n(q_1q_2n+r_1q_2+q_1r_2)+r_1r_2$. ما يعني أنّ $\phi(ab)$ هو باقي القسمة r_1r_2 على n؛ لأن $\phi(a)=r_1$ و $\phi(b)=r_2$، يبيّن مثال 6.18 أنّ $\phi(a)\phi(b)$ هو الباقي نفسه لقسمة $\phi(ab)$ على n؛ لذلك: $\phi(ab)=\phi(a)\phi(b)$.

يمكننا أن نتوقع من مبرهنة الزمر أنّ الحلقة $\mathbb{Z}_n$ ربما تماثل حلقة العامل $\mathbb{Z}/n\mathbb{Z}$ وهذا بالفعل ما سيكون، سنناقش موضوع حلقات العامل في الفصل 26. ▲

ندرك أنه في حالة دراسة أيّ بنية رياضية، فإنّ الفكرة الأساسية الأكثر أهمية هي توافر نظامين متطابقين بالبنية (*structurally identical*)، أي يتشابهان في كل شيء عدا الأسماء، إذ يسمى هذا المفهوم في الجبر عادة تماثلًا (*isomorphism*).

كما حدث في الزمر، فإنّ مفهوم أنّ شيئين متشابهين في كل شيء عدا أسماء العناصر سيقودنا إلى التعريف الآتي:

12.18 تعريف التماثل (**isomorphism**) $\phi:R\to R'$ من الحلقة R إلى الحلقة R' هو تشاكل أحادي وغامر، والحلقتان R و R' عندها تكونان متماثلتين (**isomorphic**). ■

من خلال عملنا في مبرهنة الزمر، نتوقع أن التماثل يعطينا علاقة تكافؤ على أيّ مجموعة من الحلقات، ونحتاج إلى أن نفحص أنّ خاصية الضرب للتماثل متحققة لدالة المعكوس $\phi^{-1}:R'\to R$ (لاستكمال مناقشة التناظر).

يجب أن نفحص أيضًا أنه إذا كان $\mu:R'\to R''$ تماثل حلقات، فإنّ خاصية الضرب متحققة في الدالة المركبة $\mu\phi:R\to R''$ (لاستكمال مناقشة التعدي)، طبّق هذا في تمرين 36.

13.18 مثال الزمرتان الإبداليتان $\langle\mathbb{Z},+\rangle$ و $\langle 2\mathbb{Z},+\rangle$ متماثلتان بالنسبة إلى الدالة، $\phi:\mathbb{Z}\to\mathbb{Z}$ حيث $\phi(x)=2x$ لكل $x\in\mathbb{Z}$. هنا ϕ ليست تماثل حلقات؛ لأن $\phi(xy)=2xy$، بينما $\phi(x)\phi(y)=2x\,2y=4xy$. ▲

اسئلة ضربية: الحقول

كثير من الحلقات التي ذكرناها مثل $\mathbb{Z}$، و$\mathbb{Q}$ و$\mathbb{R}$ تملك العنصر المحايد في عملية الضرب، وهو 1، لكن $2\mathbb{Z}$ لا تملك عنصرًا محايدًا في عملية الضرب، لاحظ أيضًا أنّ الضرب ليس إبداليًّا في حلقات المصفوفات المشروحة في المثال 3.18.

$0 = 0 + 0$ و $0 = (0)(0)$ يعطينا الدليل على أنّ $\{0\}$ حلقة تسمى **الحلقة الصفرية (Zero ring)**، في هذه الحلقة 0 هو العنصر المحايد لعمليتي الضرب والجمع، وباستخدام المبرهنة 8.18، فإن هذه هي الحالة الوحيدة التي يكون فيها 0 هو العنصر المحايد في عملية الضرب؛ لأنه ينتج من $0a = 0$ أن $a = 0$، وتثبت المبرهنة 13.3 أنه إذا توافرت حلقة تملك العنصر المحايد في عملية الضرب، فإنه وحيد، حيث نرمز للعنصر المحايد الضربي في الحلقة بـ 1.

14.18 تعريف تسمى الحلقة التي يكون فيها الضرب إبداليًّا **حلقة إبدالية (Commutative ring)**، والحلقة التي تملك العنصر المحايد في عملية الضرب هي **حلقة بعنصر محايد (ring with unity)**؛ والعنصر المحايد في عملية الضرب (1) **يسمى محايدًا (unity)**. ■

يبين قانونا التوزيع في حلقة بعنصر محايد 1 أنّ:

$$(1 + 1 + \ldots + 1)\,(1 + 1 + \ldots + 1) = (1 + 1 + \ldots + 1)$$

nm من المرات $\quad$ m من المرات $\quad$ n من المرات

أي إن $(n.1)\,(m.1) = (nm).1$. المثال القادم تطبيق على هذه الملاحظة.

15.18 مثال ندَّعي أنه لعددين صحيحين r و s، حيث $\gcd(r,s) = 1$، فإن الحلقتين $\mathbb{Z}_{rs}$ و $\mathbb{Z}_r \times \mathbb{Z}_s$ متماثلتان، وبالنسبة إلى عملية الجمع، هما زمرتان إبداليتان دوريتان من الرتبة rs والمولدان لهما 1 و $(1,1)$ على الترتيب؛ لذلك فإن $\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ معرفة بـ $\phi(n.1) = n.(1,1)$ هي تماثل زمر على الجمع، ولفحص الشرط الثاني في التعريف 9.18،

سنستخدم الملاحظة التي سبقت هذا المثال بالنسبة إلى المحايد $(1,1)$ في الحلقة $\mathbb{Z}_r \times \mathbb{Z}_s$، ونحسب

$$\phi(nm) = nm.(1,1) = \big[n.(1,1)\big]\big[m.(1,1)\big] = \phi(n)\phi(m)$$ ▲

لاحظ أنّ الضرب المباشر $R_1 \times R_2 \times \ldots \times R_n$ للحلقات هو حلقة إبدالية أو يملك عنصرًا محايدًا إذا وفقط إذا كان كل R_i إبداليًّا أو يملك عنصرًا محايدًا على الترتيب.

في الحلقة R التي تملك عنصرًا محايدًا $0 \neq 1$، المجموعة R^* هي مجموعة العناصر غير الصفرية، إذا كانت هذه المجموعة مغلقة بالنسبة إلى عملية الضرب في الحلقة، فإنها ستكون زمرة ضربية إذا وجد المعكوس الضربي لكل عنصر فيها. إن **المعكوس الضربي** (**multiplicative inverse**) للعنصر a في حلقة R تملك عنصرًا محايدًا $0 \neq 1$، هو العنصر $a^{-1} \in R$، حيث $aa^{-1} = a^{-1}a = 1$ تمامًا كما في الزمر، فإن المعكوس الضربي لعنصر a في R وحيد إذا وجد (انظر تمرين 43)، تبين مبرهنة 8.18 أنه من المستحيل توافر معكوس ضربي لـ 0 إلا إذا كانت الحلقة هي $\{0\}$، حيث إن $0 = 0 + 0$ و $0 = (0)(0)$، وهذا يعني أن 0 هو العنصر المحايد في عملية الجمع وعملية الضرب؛ لذلك، يمكننا أن نركز مناقشتنا على توافر المعكوسات الضربية للعناصر غير الصفرية في أيّ حلقة تملك عنصرًا محايدًا غير صفري، وما لا يمكن تجنبه توافر الكثير من المصطلحات التي يجب تعريفها في هذا الفصل (المقدمة) عن الحلقات، وقد عرّفنا معظمها.

16.18 تعريف لتكن R حلقة تملك عنصرًا محايدًا $0 \neq 1$.

العنصر u في R هو **عنصر وحدة** (**unit**) في R، إذا كان له معكوس ضربي في R، فإذا كان كل عنصر غير صفري في R عنصر وحدة، فإن R تسمى **حلقة قسمة** (**Division ring**) أو حقل تخالف (**skew – field**). **الحقل** (**field**) هو حلقة قسمة إبدالية، إذ إنّ حلقة القسمة غير الإبدالية تسمى **حقلًا تخالفيًّا قطعيًّا** (**strictly skew – field**). ■

17.18 مثال لنجد عناصر الوحدة في $\mathbb{Z}_{14}$، بالطبع 1 و $-1 = 13$ هما عناصر وحدة؛ ولأن $(3)(5) = 1$ نرى أن 3 و 5 عناصر وحدة، لذلك $-3 = 11$ و $-5 = 9$ عناصر وحدة أيضًا، أمّا بقية العناصر في $\mathbb{Z}_{14}$ فليست عناصر وحدة؛ ولأنه لا يوجد مضاعف لكل من 2, 4, 6, 7, 8 أو 10، فيمكن أن تكون أكبر بواحد من أيّ مضاعف لـ 14؛ لذلك فإن العامل المشترك لأيّ منهم مع 14 إما 2 أو 7، سيبين الفصل 20 أنّ عناصر الوحدة في $\mathbb{Z}_n$ هي بالضبط العناصر $m \in \mathbb{Z}_n$، حيث $\gcd(m,n) = 1$. ▲

18.18 مثال $\mathbb{Z}$ ليس حقلاً؛ لأن 2 –على سبيل المثال– ليس له معكوس ضربي؛ لذلك فإن 2 ليس عنصر وحدة في $\mathbb{Z}$ عناصر الوحدة في $\mathbb{Z}$ هي 1 و -1 فقط، أما $\mathbb{Q}$ و $\mathbb{R}$ فهما حقلان، سنقدم في الفصل 24 مثالًا على حقل تخالفي قطعي. ▲

لدينا مفاهيم طبيعية لحلقة جزئية من حلقة وحقل جزئي من حقل، إذ إنّ **الحلقة الجزئية من حلقة** (**subring of a ring**) هي مجموعة جزئية من الحلقة، بحيث تكون حلقة بالنسبة إلى العمليات المعرفة على الحلقة الكلية، ويعرف **الحقل الجزئي** (**subfield**) بالطريقة نفسها لمجموعة جزئية من حقل، ولنقل في هذا المقام: إنه إذا توافرت بنية جبرية محدودة على مجموعة (algebriac structure)، مثل: زمرة، حلقة، حقل، حلقة تامة، فضاء متجهات، وهكذا، فإن أيّ مجموعة جزئية من هذه المجموعة ولها البنية الجبرية الطبيعية نفسها للبنية الجبرية للمجموعة الكلية، تسمّى بنية جزئية.

إذا كان K و L بنية، سنعدّ $K \leq L$ ترمز إلى أن K بنية جزئية من L، و $K < L$ ترمز إلى $K \leq L$، ولكن $K \neq L$. سيعطينا تمرين 48 معيارًا لمجموعة جزئية S من الحلقة R حتى تشكل حلقة جزئية من R.

أخيرًا، يجب علينا ألا نرتبك عند استخدامنا للمصطلحين عنصر وحدة (*unit*) وعنصر محايد (*unity*)، فالعنصر المحايد يعني العنصر المحايد لعملية الضرب، بينما يعني عنصر الوحدة عنصرًا له معكوس ضربي؛ لذلك، فإن العنصر المحايد لعملية الضرب هو عنصر وحدة، ولكن ليس كل عنصر وحدة عنصرًا محايدًا، فمثلاً: -1 عنصر وحدة في $\mathbb{Z}$، لكنه ليس عنصرًا محايدًا، أي إنّ: $1 \neq -1$.

■ **نبذة تاريخية**

على الرغم من أنّ الحقول كانت معروفة ضمنيًّا في عمل قديم على المعادلات القابلة للحل لأبيل وجالوا (Abel and Galois)، إلّا أنّ ليوبولد كرونكر (Kronecher 1823 – 1891) قدّم تعريفًا لما أسماه المجال النسبي من خلال عمل خاص له على الموضوع نفسه، الذي نشر أول مرة عام 1881م، فالمجال النسبي هذا $(R', R'', R''', \ldots)$ يحوي ... كل واحدة من هذه الكميات التي هي دوال نسبية للكميات $R', R'', R''', \ldots$ ذات المعاملات الصحيحة، ومع ذلك، فإن كرونكر الذي أصر على أن أيّ موضوع رياضي يمكن بناؤه بعدد منته من الخطوات، لم يعرض المجال النسبي بوصفه بنية متكاملة فحسب، ولكن بوصفه منطقة تقع فيها مجموعة من العمليات على عناصرها.

ريتشارد ديدكند (Richard Dedekind 1831 – 1916) مخترع تعريف العدد الحقيقي، عدّ الحقل بنية متكاملة، إذ نشر التعريف الآتي عام 1871م في ملحقه للطبعة الثانية لكتاب درشلت (Dirichlet) عن مبرهنة الأعداد: "نعني بالحقل أيّ نظام من عدد لانهائي من الأعداد الحقيقية أو المركبة، بحيث إنّ الجمع والطرح والضرب والقسمة لأيّ عددين من هذا النظام، فإنّه ينتج عدد من هذا النظام".

تعامل كل من كرونكر ويدكند مع هذه الأفكار المختلفة في هذا الموضوع قبل عام 1850م في محاضراتهما الجامعية، إذ إنّ أول تعريف مجرد للحقل شبيه لما هو متوافر في هذا الكتاب، قدمه هنريك ويبر (Heinrich Weber 1842 – 1913) في بحث له عام 1893م.

تعريف ويبر مختلف عن تعريف يدكند، فقد شمل الحقول التي تحوي عددًا منتهيًا من العناصر، إضافة إلى أنه شمل حقولًا أخرى، مثل حقول الدوال التي هي ليست حقولًا جزئية من حقل الأعداد المركبة.

تمارين 18

حسابات

في التمارين 1 إلى 6، احسب ناتج الضرب في الحلقة المعطاة:

1. (16) (12) في $\mathbb{Z}_{24}$

2. (3) (16) في $\mathbb{Z}_{32}$

3. (−4) (11) في $\mathbb{Z}_{15}$

4. (−8) (20) في $\mathbb{Z}_{26}$

5. (3,5) (2,3) في $\mathbb{Z}_5 \times \mathbb{Z}_9$

6. (−3,5) (2, −4) في $\mathbb{Z}_4 \times \mathbb{Z}_{11}$

في التمارين 7 إلى 13، قرر فيما إذا كانت العمليات الآتية من الجمع والضرب معرفة (مغلقة) على المجموعة، ثم أعطِ بنية الحلقة، وبيّن السبب إذا لم تشكل حلقة، أما إذا شكلت حلقة، فاذكر إذا كانت حلقة إبدالية، أو إذا كانت تملك عنصرًا محايدًا أو إذا كانت حقلًا.

7. $n\mathbb{Z}$ مع الجمع والضرب الاعتيادي.

8. $\mathbb{Z}^+$ مع الجمع والضرب الاعتيادي.

9. $\mathbb{Z}\times\mathbb{Z}$ مع الجمع والضرب على المركبات.

10. $2\mathbb{Z}\times\mathbb{Z}$ مع الجمع والضرب على المركبات.

11. $\left\{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\right\}$ مع الجمع والضرب الاعتيادي.

12. $\left\{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\right\}$ مع الجمع والضرب الاعتيادي.

13. مجموعة الأعداد المركبة التخيلية النقية ri لكل $r \in \mathbb{R}$ مع الجمع والضرب الاعتيادي.

في التمارين 14 إلى 19، صف عناصر الوحدة في الحلقة المعطاة:

14. $\mathbb{Z}$ **15.** $\mathbb{Z}\times\mathbb{Z}$ **16.** $\mathbb{Z}_5$

17. $\mathbb{Q}$ **18.** $\mathbb{Z}\times\mathbb{Q}\times\mathbb{Z}$ **19.** $\mathbb{Z}_4$

20. خذ حلقة المصفوفات $M_2(\mathbb{Z}_2)$.

أ. أوجد رتبة الحلقة (**order**)، أي عدد العناصر فيها.

ب. اذكر عناصر الوحدة في الحلقة جميعها.

21. إذا كان ممكنًا، أعطِ مثالاً لتشاكل $\phi: R \to R'$، حيث R و R' حلقتان تملكان عنصرًا محايدًا $1 \neq 0$ و $1' \neq 0'$، وحيث $\phi(1) \neq 0'$ و $\phi(1) \neq 1'$.

22. (جبر خطي) لتكن الدالة det من $M_n(\mathbb{R})$ إلى $\mathbb{R}$، حيث $\det(A)$ هو محددة المصفوفة A لكل $A \in M_n(\mathbb{R})$. هل det تشاكل حلقات؟ لِمَ هو تشاكل حلقات؟ وإذا لم يكن تشاكل حلقات، فَلِمَ هو ليس كذلك؟

23. صف تشاكلات الحلقات كلها من $\mathbb{Z}$ إلى $\mathbb{Z}$.

24. صف تشاكلات الحلقات كلها من $\mathbb{Z}$ إلى $\mathbb{Z}\times\mathbb{Z}$.

25. صف تشاكلات الحلقات كلها من $\mathbb{Z}\times\mathbb{Z}$ إلى $\mathbb{Z}$.

26. ما عدد تشاكلات الحلقات من $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ إلى $\mathbb{Z}$؟

27. ليكن حلّ المعادلة $X^2=I_3$ في الحلقة $M_3(\mathbb{R})$.

$X^2=I_3$ يؤدي إلى، $X^2 - I_3 = 0$ المصفوفة الصفرية، سينتج $(X- I_3)(X+ I_3) = 0$ عندها إما $X= I_3$ أو $X= -I_3$. حلّل ذلك.

هل هذا الإثبات منطقي؟ إذا كان الجواب لا، فحدّد أين الخطأ في الإثبات، وإذا كان ممكنًا، فأعطِ مثالاً يناقض الجواب.

28. أوجد الحلول جميعها للمعادلة $x^2 + x - 6 = 0$ في الحلقة $\mathbb{Z}_{14}$ عن طريق تحليل كثيرة الحدود التربيعية. قارن بتمرين 27.

مفاهيم

في التمرينين 29 و 30، صحّح تعريف الحدّ المكتوب بخط مائل دون الرجوع إلى الكتاب –إذا كانت هناك حاجة للتصحيح – بحيث يكون بصيغة قابلة للنشر.

29. الحقل F حلقة فيها العنصر المحايد ليس صفرًا، حيث مجموعة العناصر غير الصفرية في F، هي زمرة تحت عملية الضرب.

30. عنصر الوحدة في الحلقة عنصر مقداره 1.

31. أعطِ مثالاً على حلقة فيها عنصران a وb، حيث $ab=0$، ولكن $a \neq 0$ و $b \neq 0$.

32. أعطِ مثالاً على حلقة فيها العنصر المحايد $1 \neq 0$، لها حلقة جزئية فيها العنصر المحايد $1' \neq 0$ و $1 \neq 1'$.

[مساعدة: خذ الضرب المباشر أو حلقة جزئية لـ $\mathbb{Z}_6$].

33. ضع إشارة صح أو إشارة خطأ:

_____ أ. كل حقل حلقة.

_____ ب. كل حلقة لها عنصر محايد في عملية الضرب.

_____ جـ. كل حلقة فيها عنصر محايد، يكون فيها على الأقل عنصرا وحدة.

_____ د. كل حلقة فيها عنصر محايد، يكون فيها على الأكثر عنصرا وحدة.

ـــــــــ هـ. من الممكن لمجموعة جزئية من حقل أن تكون حلقة لكنها ليست حقلًا جزئيًّا، وذلك بالنسبة إلى العملية نفسها.

ـــــــــ و. قانونا التوزيع على الحلقة غير مهمين.

ـــــــــ ز. الضرب في الحقل إبدالي.

ـــــــــ ح. العناصر غير الصفرية في الحقل تشكل زمرة تحت عملية الضرب.

ـــــــــ ط. الجمع في أيّ حلقة إبدالي.

ـــــــــ ي. كل عنصر في الحلقة له معكوس جمعي.

براهين

34. بيّن أن الضرب المعرّف على مجموعة الدوالّ F في المثال 4.18 يحقق المسلمتين $\mathscr{R}_2$ و $\mathscr{R}_3$ للحلقة.

35. بيّن أنّ دالة التعويض ϕ_a في المثال 10.18 تحقق متطلبات الضرب للتشاكل.

36. أكمل المناقشة التي ذكرت بعد تعريف 12.18؛ لتوضيح أنّ التماثل يعطي علاقة تكافؤ على مجموعة من الحلقات.

37. بيّن أنه إذا كانت U مجموعة عناصر الوحدة كلها في الحلقة $\langle R, +, \cdot \rangle$ التي فيها عنصر محايد، فإن $\langle U, \cdot \rangle$ زمرة.

(تحذير: تأكد أن U مغلقة بالنسبة إلى عملية الضرب).

38. بيّن أن $a^2 - b^2 = (a + b)(a - b)$ لكل a و b في الحلقة R، إذا وفقط إذا كانت R إبدالية.

39. لتكن $\langle R, + \rangle$ زمرة إبدالية. بيّن أن $\langle R, +, \cdot \rangle$ حلقة، إذا عرفنا $ab = 0$ لكل

$a, b \in R$.

40. بيّن أنّ الحلقتين $2\mathbb{Z}$ و $3\mathbb{Z}$ غير متماثلتين، وبيّن أنّ الحلقتين $\mathbb{R}$ و $\mathbb{C}$ غير متماثلتين.

41. قوى الطالب المبتدئ (Freshman exponentiation) ليكن p عددًا أوليًّا. بيّن أنه في الحلقة $\mathbb{Z}_p$ يكون

$(a+b)^p = a^p + b^p$ لكل $a, b \in \mathbb{Z}_p$. [مساعدة: لاحظ أنّ مفكوك ثنائي الحدّ الاعتيادي لـ $(a+b)^p$ متحقق في الحلقة الإبدالية].

42. بيّن أنّ العنصر المحايد في الحقل الجزئي هو العنصر المحايد نفسه في الحقل الكلي، بخلاف الحلقات، كما في تمرين 32.

43. بيّن أنّ المعكوس الضربي لعنصر الوحدة في حلقة فيها عنصر محايد يكون وحيدًا.

44. العنصر a في الحلقة R يسمّى متساوي القوى (**idempotent**)، إذا كان $a^2 = a$.

أ. بيّن أنّ مجموعة العناصر متساوية القوى كلها في حلقة إبدالية مغلقة على عملية الضرب.

ب. أوجد العناصر **متساوية القوى** كلها في الحلقة $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

45. (جبر خطي) تذكر أنه للمصفوفة A من الدرجة $m \times n$ ، المنقول A^T (*transpose*)، هي المصفوفة التي يكون العمود رقم j فيها هو الصف رقم j من A. بيّن أنه إذا كانت A مصفوفة من الدرجة $m \times n$ بحيث A^TA ذات معكوس، فإن مصفوفة الإسقاط (*Projection matrix*) $P = A(A^TA)^{-1} A^T$ هي عنصر متساوي القوى في حلقة المصفوفات من الدرجة $n \times n$.

46. العنصر a في R يسمى **معدوم القوى (nilpotent)**، إذا كان $a^n = 0$ لـ $n \in \mathbb{Z}^+$ بيّن إذا كان a و b عنصري معدومي القوى في حلقة إبدالية، فإن $a+ b$ معدوم القوى أيضًا.

47. بيّن أنه لا يوجد أي عنصر معدوم القوى غير صفري في R، إذا وفقط إذا كان 0 هو الحل الوحيد لـ $x^2 = 0$ في R.

48. بيّن أنّ المجموعة الجزئية S من الحلقة R هي ح لقة جزئية من R، إذا وفقط إذا كانت الشروط الآتية متحققة:

$$0 \in S$$

$$a,b \in S \text{ لكل } (a-b) \in S$$

$$a,b \in S \text{ لكل } ab \in S$$

49. بيّن أنّ تقاطع حلقات جزئية في R هي حلقة جزئية من R.

بيّن أنّ تقاطع حقول جزئية في الحقل F هو حقل جزئي من F.

50. لتكن R حلقة، وليكن a عنصرًا ثابتًا في R، وليكن $I_a = \{x \in R \mid ax = 0\}$. بيّن أنّ I_a هي حلقة جزئية من R.

51. لتكن R حلقة، وليكن a عنصرًا ثابتًا في R، ولتكن R_a تعني الحلقة الجزئية من R، التي تمثل تقاطع الحلقات الجزئية كلها من R التي تحوي a (انظر تمرين 49)، الحلقة R_a **هي الحلقة الجزئية من *R* المولدة من *a***
(**subring of *R* generated by *a***). بيّن أنّ الزمرة الإبدالية $\langle R_a, + \rangle$ مولدة (كما في الفصل 7) من المجموعة $\{a^n \mid n \in \mathbb{Z}^+\}$.

52. (مبرهنة الباقي الصينية لتطابقين) خذ عددين صحيحين موجبين r و s، حيث: ق.م.أ $(r,s) = 1$. استخدم التماثل في المثال 15.18 لتبيّن أنه لـ $m, n \in \mathbb{Z}$ يوجد عدد صحيح x، حيث (مقياس r) $x \equiv m$ و(مقياس s) $x \equiv n$.

53. أ. اذكر التعميم لمثال 15.18 وأثبته للضرب المباشر لـ n من العوامل.

ب. أثبت مبرهنة الباقي الصينية: خذ $a_i, b_i \in \mathbb{Z}^+$ لكل $i = 1, 2, \ldots, n$، وليكن

$gcd(b_i, b_j) = 1$ لـ $i \neq j$. عندها يوجد $x \in \mathbb{Z}^+$، حيث (مقياس b_i) $x \equiv a_i$ لـ $i = 1, 2, \ldots n$

54. اعتبر $\langle S, +, \cdot \rangle$، حيث S مجموعة و $+$ و $\cdot$ عمليات ثنائية على S حيث $\langle S, + \rangle$ زمرة $\langle S^*, \cdot \rangle$ زمرة، حيث S^* تحوي العناصر كلها في S عدا العنصر المحايد في عملية الجمع $a(b+c) = (ab) + (ac)$ و $(a+b)c = (ac) + (bc)$ لكل $a, b, c \in S$.

بيّن أنّ $\langle S, +, \cdot \rangle$ حلقة قسمة. [مساعدة: طبق قانوني التوزيع على $(a+b)(1+1)$ لتثبيت أنّ الجمع إبدالي].

55. الحلقة R **حلقة بولينية (Boolean ring)**، إذا كان $a^2 = a$ لكل $a \in R$، أي إنّ كل عنصر متساوي القوى. بيّن أنّ الحلقة البولينية إبدالية.

56. (خاص بالطلاب الذين يملكون بعض المعرفة لقوانين مبرهنة المجموعة). لأي مجموعة S دع $\mathcal{P}(S)$ تحوي المجموعات بالطلاب كلها من S. لندع العمليات الثنائية $+$ و $\cdot$ على $\mathcal{P}(S)$ تعرف على النحو الآتي:

$$A + B = (A \cup B) - (A \cap B) = \{ x \mid x \in A \text{ أو } x \in B \text{ لكن } x \notin (A \cap B) \}$$

و

$$A.B = A \cap B$$

لـ $A, B \in \mathcal{P}(S)$

أ. أوجد جدولي الجمع والضرب على $\mathcal{P}(S)$ حيث $S = \{a, b\}$. [مساعدة: $\mathcal{P}(S)$ فيها أربعة عناصر].

ب. بيّن أنه لأي مجموعة S، $\langle \mathcal{P}(S), +, \cdot \rangle$ هي حلقة بولينية. (انظر تمرين 55).

الفصل 19 الحلقات التامة Integral Domains

على الرغم من أننا لن نعالج كثيرات الحدود بطريقة موسعة قبل الفصل 22، إلّا أننا سنستخدمها بشكل مبسط في هذا الفصل بدافع التحفيز.

قواسم الصفر والحذف

إن من أهم الخصائص الجبرية لنظام الأعداد الاعتيادي أنّ حاصل ضرب عددين يساوي صفرًا، إذا كان على الأقل أحدهما صفرًا، وقد استخدمنا هذه الحقيقة مرات عدّة في حلّ المعادلات، وربما دون أن ندرك أننا نستخدمها. افترض – على سبيل المثال – أنه طلب منّا أن نحلّ المعادلة:

$$x^2 - 5x + 6 = 0$$

فإنّ أول شيء نفعله هو تحليل الطرف الأيسر من المعادلة:

$$x^2 - 5x + 6 = (x - 2)(x - 3).$$

وبعدها نستنتج أنّ القيم المحتملة الوحيدة لـ x هي 2 و3. لماذا؟ السبب، لأنه إذا استبدلنا x بأي عدد a، فإنّ ناتج الضرب

$(a - 2)(a - 3)$ هو 0، إذا وفقط إذا كان $a - 2 = 0$ أو $a - 3 = 0$.

1.19 مثال حلّ المعادلة $x^2 - 5x + 6 = 0$ في $\mathbb{Z}_{12}$.

الحل إنّ تحليل $x^2 - 5x + 6 = (x - 2)(x - 3)$ يبقى صحيحًا، إذا اعتقدنا أنّ x تمثِّل أي عدد من $\mathbb{Z}_{12}$ وليس فقط $a0 = 0a = 0$ لكل $a \in \mathbb{Z}_{12}$، ولكن كذلك

$$(2)(6) = (6)(2) = (3)(4) = (4)(3) = (3)(8) = (8)(3)$$
$$= (4)(6) = (6)(4) = (4)(9) = (9)(4) = (6)(6) = (6)(8)$$
$$= (8)(6) = (6)(10) = (10)(6) = (8)(9) = (9)(8) = 0$$

في الحقيقة نجد أنه ليس 2 و3 هما فقط حلّا معادلتنا، ولكن أيضًا 6 و11؛ لأن $(4)(3) = (6-3)(6-2) = (9)(8) = (11-3)(11-2) = 0$ في $\mathbb{Z}_{12}$. ▲

2.19 تعريف إذا كان a و b عنصرين من الحلقة R ليس أي منهما صفرًا، حيث $ab=0$، فإن a وb **تقسم الصفر** (**أو قواسم الصفر**). ■

يبيِّن مثال 1.19 أنّ العناصر 9, و8, و6, و4, و3, و2 و10 هي قواسم 0 في $\mathbb{Z}_{12}$. لاحظ أنّ هذه الأعداد هي فقط الأعداد التي في $\mathbb{Z}_{12}$، وليست أوليَّة بالنسبة إلى العدد 12، أي إنّ القاسم المشترك الأكبر لأي عدد من هذه الأعداد والعدد 12 ليس 1. مبرهنتنا القادمة مثال على الحالة العامة.

3.19 مبرهنة قواسم ألـ 0 في الحلقة $\mathbb{Z}_n$ هي بالضبط العناصر غير الصفرية من $\mathbb{Z}_{12}$ التي ليست أولية نسبيًّا مع n.

البرهان

خذ $m \in \mathbb{Z}_n$، حيث $m \neq 0$، ودع القاسم المشترك الأكبر بين m وn هو $d \neq 1$،

فإن $m(\frac{n}{d}) = (\frac{m}{d})n$

و $(\frac{m}{d})n = 0$

لأنه من مضاعفات n؛ لذلك، فإن $m\left(\frac{n}{d}\right) = 0$ في $\mathbb{Z}_n$.

بينما ليس m ولا $\frac{n}{d}$ أصفارًا، لذلك m قاسم لـ 0.

من جهة أخرى، لنفرض أن $m \in \mathbb{Z}_n$ أولى بالنسبة إلى n، إذا كان $s \in \mathbb{Z}_n$ حيث $ms = 0$، فإن n تقسم ms حاصل ضرب m وs، وهما عنصران في $\mathbb{Z}$. لأنّ n أولى بالنسبة إلى m، توضح الخاصية المؤطرة 1 التي تبعت مثال 9.6 أنّ n تقسم s؛ لذلك، فإن $s=0$ في $\mathbb{Z}_n$. ♦

4.19 نتيجة إذا كان p عددًا أوليًّا، فإنه لا يوجد قواسم لـ 0 في $\mathbb{Z}_p$.

البرهان هذه النتيجة تأتي مباشرة من المبرهنة 3.19. ♦

نشير إلى أهمية أخرى لمفهوم قواسم الصفر تظهر في المبرهنة المقبلة، خذ الحلقة R، وخذ $a, b, c \in R$ **قوانين الحذف (Cancellation laws)** متحققة في R، إذا كان $ab = ac$، حيث: $a \neq 0$، فإن $b=c$ و $ba = ca$ حيث: $a \neq 0$ فإن $b = c$. هذه هي قوانين الحذف لعملية الضرب، وبالطبع قوانين الحذف لعملية الجمع متحققة في R؛ لأن $\langle R, + \rangle$ زمرة.

5.19 مبرهنة قوانين الحذف متحققة في الحلقة R، إذا وفقط إذا لم يكن في الحلقة R قواسم لـ 0.

البرهان لتكن R حلقة تحقق قوانين الحذف، افترض أنّ $ab = 0$ لـ $a,b \in R$. علينا أن نبيّن أن a أو b تكون 0، وإذا كانت $a \neq 0$، فإن $ab = a0$ تؤدي إلى $b = 0$ باستخدام قوانين الحذف، وكذلك إذا كان $b \neq 0$، فإن $a = 0$، ما يعني أنه لا توجد قواسم لـ 0 في R إذا تحققت قوانين الحذف.

من جهة أخرى، افترض أنَّ R حلقة ليس فيها قواسم لـ 0، افترض أنّ $ab = ac$، حيث $a \neq 0$. فإن:

$$ab - ac = a(b-c) = 0$$

لأن $a \neq 0$؛ ولأن الحلقة R ليس فيها قواسم لـ 0، فإن $b-c = 0$ أي $b = c$. وباتباع الخطوات نفسها يمكن إثبات أنه إذا كان $ba = ca$، حيث $a \neq 0$، فإن $b = c$. ♦

افترض أنَّ الحلقة R ليس فيها قواسم لـ 0، فإن المعادلة $ax=b$، حيث $a \neq 0$، لها حل وحيد x في R على الأكثر؛ لأنه إذا كان $ax_1=b$ و $ax_2=b$ فإن $ax_1 = ax_2$، باستخدام المبرهنة 5.19، فإن $x_1 = x_2$ لأن R ليس فيها قواسم لـ 0. إذا احتوت R على عنصر محايد $1 \neq 0$، وa هو عنصر وحدة في R، حيث a^{-1} هو المعكوس الضربي لـ a، فإن الحل x للمعادلة $ax=b$ هو $a^{-1}b$. عندما تكون R إبدالية، وبوجه خاص إذا كانت R حقلًا، فمن المشهور أن نرمز لـ $a^{-1}b$ وba^{-1} (هما متساويان؛ لأن R إبدالية) باستخدام القسمة $\frac{b}{a}$. هذه القسمة لا يجب استخدامها إذا كانت الحلقة R غير إبدالية؛ لأنه في هذه الحالة لا نعلم إذا كانت $\frac{b}{a}$ ترمز إلى $a^{-1}b$ أو إلى ba^{-1}، وبوجه خاص، المعكوس الضربي a^{-1} للعنصر غير الصفري a في حقل يمكن كتابته على الصورة $\frac{1}{a}$.

الحلقات التامة

إن الأعداد الصحيحة هي نظام الأعداد الأكثر شهرة، باعتبار الخصائص الجبرية، فإننا نناقش حقيقة أنَّ $\mathbb{Z}$ هي حلقة إبدالية فيها عنصر محايد، ولا تحوي قواسم لـ 0، بالتأكيد هذا ما كان وراء الاسم المعطى لمثل هذه البنية في التعريف المقبل.

6.19 تعريف ***Iintegral domain*** حلقة إبدالية فيها عنصر محايد $1 \neq 0$ ولا تحوي قواسم لـ 0. ■

لذلك، إذا كانت معاملات كثيرة حدود في حلقة تامة، فنستطيع أن نحل معادلة كثيرة حدود عن طريق تحليل كثيرة الحدود إلى عوامل خطية بالأسلوب الاعتيادي، من خلال جعل كل معامل يساوي 0.

في سلسلتنا من البنى الجبرية، تقع الحلقة التامة بين الحلقات الإبدالية ذات العنصر المحايد والحقول، كما سوف نوضح، وقد بيّنت المبرهنة 5.19 أنّ قوانين الحذف للضرب متحققة في الحلقة التامة.

7.19 مثال لاحظنا أنّ $\mathbb{Z}$ و $\mathbb{Z}_p$ حلقات تامة لأي عدد أولي p، ولكن $\mathbb{Z}_n$ ليست حلقة تامة إذا كانت n عددًا غير أولي، وعند التفكير لحظة، يتضح أنّ الضرب المباشر $R \times S$ للحلقتين غير الصفريتين R وS ليس حلقة تامة، فقط لاحظ أنه لأي $r \in R$ و $s \in S$، بحيث إن كليهما لا يساوي صفرًا، فإن $(r,0)(0,s) = (0,0)$. ▲

8.19 مثال بيّن أنه على الرغم من أنّ $\mathbb{Z}_2$ حلقة تامة، فإن حلقة المصفوفة $M_2(\mathbb{Z}_2)$ تحتوي على قواسم للصفر.

الحل نحتاج إلى أن نلاحظ أنَّ :

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

▲

مبرهنتنا المقبلة توضح أنّ بنية الحقول ما زالت هي الأكثر تحديدًا (أي الأغنى) فيما قمنا بتعريفه.

9.19 مبرهنة أي حقل F هو حلقة تامة.

البرهان لتكن $a, b \in F$، وافترض أنّ $a \neq 0$. إذا كان $ab=0$، فإن:

$$\left(\frac{1}{a}\right)(ab) = \left(\frac{1}{a}\right) 0 = 0$$

وعليه، فإن

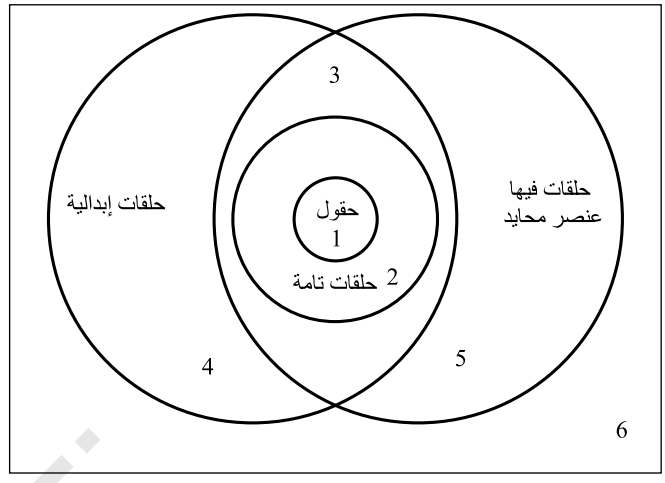
$$0 = \left(\frac{1}{a}\right)(ab) = \left[\left(\frac{1}{a}\right) a\right] b = 1b = b$$

إذن، فقد وضحنا أنّ $a\,b = 0$، حيث $a \neq 0$ يؤدي إلى $b=0$ في F، وهذا يعني أنّ الحقل F لا يحوي قواسم للصفر، وبالطبع، فإن F هو حلقة إبدالية، ويملك عنصرًا محايدًا، وعليه، فإن مبرهنتنا أُثبتت.

♦

يعطي الشكل 10.19 رسوم فن البيانية التي تبين العلاقات بين البنى الجبرية المعرف عليها عمليتان ثنائيتان والتي هي محور اهتمامنا، وسنطلب منك في تمرين 20 أن تعيد رسم هذا الشكل مرة أخرى، بعد أن تضيف له حلقات القسمة.

الحقول المعلومة لدينا حتى الآن هي $\mathbb{Q}$، و $\mathbb{R}$ و$\mathbb{C}$، وستكشف لنا النتيجة التي تعقب المبرهنة المقبلة عن بعض الحقول منتهية الرتبة، إذ إنّ إثبات المبرهنة المقبلة ذو نكهة خاصة، ويعتمد على العدّ، الذي يُعدّ من أهم التقنيات القوية في الرياضيات.



الشكل 10.19 مجموعة من الحلقات

11.19 مبرهنة كل حلقة تامة منتهية تكون حقلاً.

البرهان افترض أنّ

$$0,\ 1,\ a_1,\ \ldots,\ a_n$$

هي عناصر الحلقة التامة المنتهية D، ونريد أن نبين أنه لـ $a \in D$ حيث $a \neq 0$، يوجد $b \in D$ بحيث $ab=1$. خذ

$$a1,\ aa_1,\ldots,\ aa_n$$

ندَّعي أن هذه العناصر مختلفة في D؛ ولأنّ قوانين الحذف متحققة في أي حلقة تامة، فإن $aa_i = aa_j$ يؤدي إلى $a_i = a_j$، كذلك لأنّ D ليس فيها قواسم لـ 0، فليس أيّ من هذه العناصر يساوي 0، وباستخدام مبدأ العد (*counting*) نجد أن $a1,\ aa_1,\ldots,\ aa_n$ هي العناصر نفسها $1,\ a_1,\ \ldots\ a_n$ ولكن بترتيب معين، وهذا يعني أنه إما $a1 = 1$ أي $a = 1$ أو $aa_i = 1$ لعدد i، ما يعني أن a لها معكوس ضربي. ♦

12.19 نتيجة إذا كان p عددًا أوليًّا، فإن $\mathbb{Z}_p$ حقل.

البرهان هذه النتيجة تأتي مباشرة من حقيقة أن $\mathbb{Z}_p$ حلقة تامة بحسب المبرهنة 11.19 ♦

بينت النتيجة السابقة أنه عندما ندرس الحلقة $M_n\left(\mathbb{Z}_p\right)$، فإننا نتكلم عن حلقة مصفوفات على حقل (*field*)، وفي مادة الجبر الخطي لمستوى البكالوريوس استخدمنا في معظم تلك المادة خصائص حقل الأعداد الحقيقية أو الأعداد المركبة، إضافة إلى أنّ بعض المفاهيم، مثل اختصار المصفوفة لحل أنظمة المعادلات الخطية، والمحددات، وقانون كريمر، والقيم الذاتية، والمتجهات الذاتية والتحويلات التشابهية لتحويل المصفوفة إلى مصفوفة قطرية، متحققة باستخدام المصفوفات على أي حقل؛ لأنها تعتمد فقط على الخواص الحسابية للحقل، ولكن في الجبر الخطي الذي يحتوي على بعض مفهوم المقدار، مثل أصغر المربعات لتقريب الحلول أو أساسات متعامدة معايرة، فإن هذه المفاهيم لها معنًى فقط إذا استخدمنا الحقول التي فيها

فكرة المقدار.

العلاقة $p \cdot 1 = 1 + 1 + \cdots + 1 = 0$ من الحدود

تبين أنه لا يمكن أن يكون هناك مفهوم طبيعي للمقدار في الحقل $\mathbb{Z}_p$.

مميزة الحلقة

خذ أي حلقة R، يمكننا أن نتساءل: هل يوجد عدد صحيح موجب مثل n، حيث $n.a = 0$ لكل $a \in R$، حيث $n.a$ يعني $a + a + \ldots + a$، n مرة، كما تقدم شرحه في الفصل 18، على سبيل المثال: العدد الصحيح m يملك هذه الخاصية في الحلقة $\mathbb{Z}_m$.

13.19 تعريف إذا توافر لحلقة مثل R عدد صحيح موجب n، بحيث $n.a = 0$ لكل $a \in R$، فإن أصغر عدد صحيح موجب يحقق هذه الخاصية يسمى **مميز الحلقة** R (***characteristic of the ring***)، وإذا لم يوجد مثل هذا العدد الصحيح الموجب، فإن الحلقة R **مميزها** 0. ■

سنستخدم في المقام الأول مفهوم المميز للحقول، حيث يطلب منا تمرين 29 أن نبين أنّ مميز الحلقة التامة إما 0 أو عددًا أوليًّا p.

14.19 مثال مميز الحلقة $\mathbb{Z}_n$ هو n، بينما $\mathbb{Z}$، و $\mathbb{Q}$، و $\mathbb{R}$ و $\mathbb{C}$ كلها مميزها 0. ▲

من الوهلة الأولى يبدو أن معرفة مميز الحلقة عمل شاق، إلّا إذا كان من الواضح أنّ الحلقة مميزها 0. هل حقًّا نحتاج إلى أن نختبر كل عنصر a في الحلقة كما هو منصوص عليه في التعريف 13.19؟ تبين مبرهنتنا الأخيرة في هذا الفصل، أنه إذا توافر عنصر محايد في الحلقة، فيكفي أن نختبر $a = 1$ فقط.

15.19 مبرهنة لتكن R حلقة تحتوي على عنصر محايد، وإذا كان $n.1 \neq 0$ لكل $n \in \mathbb{Z}^+$ فإن مميز الحلقة R هو 0، أما إذا توافر $n \in \mathbb{Z}^+$ حيث $n.1 = 0$، فإن أصغر عدد صحيح n له هذه الخاصية سيكون مميز الحلقة R.

البرهان إذا كان $n.1 \neq 0$ لكل $n \in \mathbb{Z}^+$ فبالتأكيد لا يمكن أن يوجد $n \in \mathbb{Z}^+$، بحيث $n.a = 0$ لكل $a \in R$، لذلك وباستخدام التعريف 13.19؛ فإن مميز R هو 0.

افترض أنه يوجد عدد صحيح موجب n حيث $n.1 = 0$، فإنه لأي $a \in R$ سيكون

$n.a = a + a + \ldots + a = a(1 + 1 + \ldots + 1) = a(n.1) = a0 = 0$ وبذلك تثبت مبرهنتنا مباشرة. ♦

تمارين 19

حسابات

1. أوجد الحلول جميعها للمعادلة $x^3 - 2x^2 - 3x = 0$ في $\mathbb{Z}_{12}$.

2. حلّ المعادلة $3x = 2$ في الحقل $\mathbb{Z}_7$ والحقل $\mathbb{Z}_{23}$.

3. أوجد الحلول جميعها للمعادلة $x^2 + 2x + 2 = 0$ في $\mathbb{Z}_6$.

4. أوجد الحلول جميعها للمعادلة $x^2 + 2x + 4 = 0$ في $\mathbb{Z}_6$.

في التمارين 5 إلى 10، أوجد مميز الحلقة المعطاة.

5. $2\mathbb{Z}$ **6.** $\mathbb{Z} \times \mathbb{Z}$ **7.** $\mathbb{Z}_3 \times 3\mathbb{Z}$

8. $\mathbb{Z}_3 \times \mathbb{Z}_3$ **9.** $\mathbb{Z}_3 \times \mathbb{Z}_4$ **10.** $\mathbb{Z}_6 \times \mathbb{Z}_{15}$

11. لتكن الحلقة الإبدالية R مع عنصر محايد ومميزها 4. لـ $a, b \in R$، احسب $(a+b)^4$ وبسِّطه.

12. لتكن الحلقة الإبدالية R مع عنصر محايد ومميزها 3. لـ $a, b \in R$، احسب $(a + b)^9$ وبسِّطه.

13 لتكن الحلقة الإبدالية R مع عنصر محايد ومميزها 3. لـ $a, b \in R$ احسب $(a + b)^6$ وبسِّطه.

14. أثبت أنّ المصفوفة $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ قاسم للصفر في $M_2(\mathbb{Z})$.

مفاهيم

في التمرينين 15 و16، صحح تعريف الحد المكتوب بخط مائل دون الرجوع إلى الكتاب –إذا كانت هناك حاجة للتصحيح – بحيث يكون بصيغة قابلة للنشر.

15. إذا كان $ab = 0$، فإن a و b قواسم للصفر.

16. إذا كان $n.a = 0$ لكل a في الحلقة R، فإن n مميز R.

17. ضع إشارة صح أو إشارة خطأ:

_____ أ. $n\mathbb{Z}$ تحتوي على قواسم للصفر إذا لم يكن n عددًا أوليًّا.

_____ ب. يكون كل حقل حلقة تامة.

_____ جـ. مميز $n\mathbb{Z}$ هو n.

_____ د. الحلقة $\mathbb{Z}$ تماثل الحلقة $n\mathbb{Z}$ لكل $n \leq 1$.

_____ هـ. قانون الحذف متحقق في أي حلقة تماثل حلقة تامة.

_____ و. كل حلقة تامة مميزها 0 غير منتهية.

_____ ز. الضرب المباشر لحلقتين تامتين يعطي حلقة تامة.

_____ ح. في حلقة إبدالية فيها عنصر محايد، لا يكون لقاسم الصفر معكوس ضربي.

_____ ط. $n\mathbb{Z}$ حلقة تامة جزئية من $\mathbb{Z}$.

_____ ي. $\mathbb{Z}$ حقل جزئي من $\mathbb{Q}$.

18. كل منطقة من المناطق الست المرقمة في الشكل 10.19 تمثل نوعًا محددًا من الحلقات. أعط مثالاً على حلقة تقع في كل منطقة من المناطق الست، على سبيل المثال: الحلقة المتوافرة في المنطقة 3 يجب أن تكون إبدالية (لأنها داخل دائرة الإبدالية) ولها عنصر محايد، لكنها ليست حلقة تامة.

19. (خاص بالطلاب الذين درسوا مادة الجبر الخطي). خذ الحقل F، وأعطِ خمس صفات مختلفة لعنصر A في $M_n(F)$، ليكون قاسمًا للصفر.

20. أعد رسم الشكل 10.19 ليحوي المجموعة الجزئية التي تمثل حلقات القسمة.

براهين مختصرة

21. أعطِ جملة مختصرة لإثبات الجزء «إذا» في المبرهنة 5.19.

22. أعطِ جملة مختصرة لإثبات المبرهنة 11.19.

براهين

23. يسمى العنصر a في الحلقة R **متساوي القوى (idempotent)** إذا كان $a = a^2$. بيّن أنّ حلقة القسمة تحتوى فقط على عنصرين متساويي القوى.

24. أثبت أنّ تقاطع حلقات تامة جزئية من حلقة تامة D هو حلقة تامة جزئية في D.

25. أثبت أنّ الحلقة المنتهية R التي فيها عنصر محايد $0 \neq 1$، ولا توجد فيها قواسم لـ 0 هي حلقة قسمة. (في الواقع هي حقل على الرغم من أنّ إثبات الخاصية الإبدالية ليس بالأمر الهين. انظر المبرهنة 10.24).

[ملاحظة: لتبين أن $a \neq 0$ عنصر وحدة، عليك أن تبين أن "المعكوس الضربي من اليسار" لـ $a \neq 0$ في R هو أيضًا «معكوس ضربي من اليمين»].

26. خذ حلقة R فيها عنصران على الأقل، افترض أنه لكل عنصر غير صفري $a \in R$ يوجد عنصر وحيد $b \in R$ بحيث

$$aba = a.$$

أ. أثبت أنّ R ليس فيها قواسم للصفر.

ب. أثبت أنّ $bab = b$.

جـ. أثبت أنّ R فيها عنصر محايد.

د. أثبت أنّ R حلقة قسمة.

27. أثبت أنّ مميز حلقة تامة جزئية من حلقة تامة D هو مميز D.

28. أثبت أنه إذا كانت D حلقة تامة، فإن $\{n.1 \mid n \in \mathbb{Z}\}$ حلقة تامة جزئية من D محتواة في أي حلقة تامة جزئية من D.

29. أثبت أنّ مميز الحلقة التامة D إما 0 أو عددًا أوليًّا p.

[مساعدة: إذا كان مميز D هو mn، فخذ $(n.1)\,(m.1)$ في D].

30. يوضّح هذا التمرين أنّ أي حلقة R يمكن تكبيرها (إذا لزم الأمر) إلى حلقة S فيها عنصر محايد، ولها مميز R نفسه، خذ $S = R \times \mathbb{Z}$ إذا كان مميز R يساوي 0، و $R \times \mathbb{Z}_n$ إذا كان مميز R يساوي n. ليكن الجمع على S هو الجمع الاعتيادي على المركبات، وسنعرِّف الضرب بـ

$$(r_1\,,\, n_1)\,.\,(r_2,\, n_2) = (r_1 r_2 + n_1.\, r_2 + n_2.\, r_1,\, n_1\, n_2)$$

حيث إنّ معنى $n.r$ كما هو مشروح في الفصل 18.

أ. أثبت أنّ S حلقة.

ب. أثبت أنّ S فيها عنصر محايد.

جـ. أثبت أنّ S و R لهما المميز نفسه.

د. أثبت أنّ الدالة $\phi: R \longrightarrow S$ المعطاة بالعلاقة $\phi(r) = (r,0)$ لـ $r \in R$ تربط R تماثليًّا وبصورة غامرة مع حلقة جزئية من S.

الفصل 20 مبرهنتا فيرما وأويلر Fermat's and Euler's Theorems

مبرهنة فيرما

نعلم أنّ الزمرتين الجمعيتين $\mathbb{Z}_n$ و $\mathbb{Z}/n\mathbb{Z}$ بينهما تماثل طبيعي، حيث المجموعة المشاركة $a+n\mathbb{Z}$ تقابل a لكل $a\in\mathbb{Z}_n$، إضافة إلى ذلك فإن، جمع المجموعات المشاركة من $\mathbb{Z}/n\mathbb{Z}$ يمكن تشكيله عن طريق أخذ مجموعة من الممثلين وجمعها في $\mathbb{Z}$، ثم حساب المجموعة المشاركة لناتج الجمع، إذ من السهولة ملاحظة أن $\mathbb{Z}/n\mathbb{Z}$ يمكن تحويلها إلى حلقة عن طريق ضرب المجموعات المشاركة بالأسلوب نفسه، أي بضرب مجموعة من الممثلين المختارين، حيث سنوضّح الحالة العامة لهذا فيما بعد، بينما نوضح الحالة الخاصة الآن. نحتاج إلى أن نثبت فقط، أنّ ضرب المجموعات المشاركة حسن التعريف؛ لأن العملية التجميعية على الضرب وقانوني التوزيع يتبعان مباشرة من خصائص الممثلين المختارين من $\mathbb{Z}$.

لإثبات ذلك، اختر الممثلين $a+rn$ و $b+sn$ بدلاً من a و b من المجموعتين المشاركتين $a+n\mathbb{Z}$ و $b+n\mathbb{Z}$. عندها:

$$(a+rn)(b+sn)=ab+(as+rb+rsn)n$$

وهو أيضًا عنصر في $ab+n\mathbb{Z}$؛ لذلك، فإن الضرب حسن التعريف، وعليه، تشكل المجموعات المشاركة حلقة تماثل الحلقة $\mathbb{Z}_n$.

الآتي هو حالة خاصة من تمرين 37 في الفصل 18.

مجموعة العناصر غير الصفرية في أي حقل تشكل زمرة بالنسبة إلى عملية الضرب المعرفة على الحقل.

بوجه خاص، العناصر من $\mathbb{Z}_p$

$$1,2,3,\ldots,p-1$$

تشكل زمرة من الرتبة $p-1$ بالنسبة إلى عملية الضرب مقياس p؛ لأن رتبة أي عنصر في زمرة يقسم رتبة الزمرة، نرى أنه لـ $b\neq 0$ و $b\in\mathbb{Z}_p$، فإن $b^{p-1}=1$ في $\mathbb{Z}_p$، وباستخدام حقيقة أنّ $\mathbb{Z}_p$ تماثل حلقة المجموعات المشاركة على الصورة $a+p\mathbb{Z}$ الموصوفة في الأعلى، فسنرى من الوهلة الأولى أنّه لأي $a\in\mathbb{Z}$ ليس في المجموعة المشاركة $p\mathbb{Z}+0$ فإن:

$$a^{p-1}\equiv 1 \quad (\text{مقياس } p)$$

هذه العلاقة ستعطينا في الحال ما يُسمّى المبرهنة الصغرى لفيرما.

1.20 المبرهنة (المبرهنة الصغرى لفيرما) (Little theorem of Fermat)

إذا كانت $a\in\mathbb{Z}$ و p عددًا أوليًّا لا يقسم a، فإن p يقسم $a^{p-1}-1$، أي إنّ $a^{p-1}\equiv 1$ (مقياس p) لـ $a\not\equiv 0$ (مقياس p).

2.20 نتيجة إذا كانت $a\in\mathbb{Z}$، فإن $a^p\equiv a$ (مقياس p) لأيّ عدد أولي p.

البرهان هذه النتيجة مشتقة من المبرهنة 1.20 في حالة $a \not\equiv 0$ (مقياس p)، أما إذا كانت $a \equiv 0$ (مقياس p) فإن كلا الجانبين يختصر إلى 0 مقياس p. ♦

نبذة تاريخية

ظهر نص المبرهنة 1.20 من رسالة من بييردي فيرما (Pierre de Fermat 1601- 1665) إلى بيرنارد فيرنيكل دي بيسي (Bernard Frenicle de Bessy) مؤرخة بتاريخ 18 أكتوبر عام 1640م.

حيث نصّت مبرهنة فيرما على أنه لأيّ عدد أولي p ولأيّ متوالية هندسية $a, a^2, ..., a^t, ...,$ يوجد على الأقل عدد a^T من المتوالية، بحيث p يقسم $a^T - 1$، يوجد إضافة إلى ذلك، T يقسم $p-1$ و p وكذلك يقسم كل الأرقام $a^{KT} - 1$.

(إنه لأمر غريب أن يفشل فيرما في ملاحظة شرط عدم قسمة p لـ a، وربما شعر بأنه لأمر واضح أنّ النتيجة تفشل في هذه الحالة).

لم يكتب فيرما إثبات هذه النتيجة في رسالته أو أي مكان آخر، وفي الحقيقة، فإنه لم يذكر هذه المبرهنة مرة أخرى، ولكن اهتمامه بهذه النتيجة جاء من خلال دراسته للأعداد التامة. (العدد التام هو عدد صحيح موجب m بحيث يساوي مجموعة قواسمه الأقل منه، على سبيل المثال: $6=1+2+3$ هو عدد تام)، وقد أوضح إقليدس (Euclid) أن $2^{n-1}(2^n - 1)$ عدد تام إذا كان $2^n - 1$ عددًا أوليًّا، كان السؤال في إيجاد طريقة لتحديد فيما إذا كان $2^n - 1$ عددًا أوليًّا أم لا، إذ لاحظ فيرما أنّ $2^n - 1$ عدد مركب إذا كان n عددًا مركبًا، وبعدها اشتق من المبرهنة النتيجة الآتية: إذا كان n عددًا أوليًّا، فإن القواسم المحتملة لـ $2^n - 1$ تكون على صورة $2kn + 1$، ومن هذه النتيجة استطاع أن يبين على سبيل المثال: أن $2^{37} - 1$ قابل للقسمة على $2.3.37 + 1 = 223$.

3.20 مثال لنحسب باقي قسمة 8^{103} على 13، باستخدام مبرهنة فيرما سيكون عندنا:

$$8^{103} \equiv (8^{12})^8 (8^7) \equiv (1^8)(8^7) \equiv 8^7 \equiv (-5)^7$$
$$\equiv (25)^3(-5) \equiv (-1)^3(-5) \equiv \text{(مقياس 13)}$$

▲

4.20 مثال: وضّح أن $2^{11.213} - 1$ غير قابل للقسمة على 11.

الحل باستخدام مبرهنة فيرما، فإن $2^{10} \equiv 1$ (مقياس 11)، وعليه، فإن

$$2^{11.213} - 1 \equiv \left[(2^{10})^{1.121}.2^3\right] - 1 \equiv \left[1^{1.121}.2^3\right] - 1$$
$$\equiv 2^3 - 1 \equiv 8 - 1 \equiv 7 \text{ (مقياس 11)}$$

أي إنّ باقي قسمة $2^{11,213} - 1$ على 11 يساوي 7 وليس 0، (العدد 11,213 عدد أولي، وقد أثبت أنّ $2^{11,213} - 1$ عدد أولي، وتُعرف الأعداد الأولية $2^p - 1$ حيث p عدد أولي **بأعداد مرسين الأولية (Mersenne Primes).** ▲

5.20 مثال بيّن أنه لأي عدد صحيح n، العدد $n^{33} - n$ قابل للقسمة على15.

الحل تبدو أنها نتيجة غير معقولة، فهي تعني أنّ 15 يقسم $2^{33} - 2$ و $3^{33} - 3$ و $4^{33} - 4$ وهكذا.

الآن،15=3.5، سنستخدم مبرهنة فيرما في إثبات أنّ $n^{33} - n$ قابل للقسمة على كلا العددين 3 و5 لأي عدد n، لاحظ أنّ $n^{33} - n = n(n^{32} - 1)$.

إذا كان 3 يقسم n، فبالتأكيد 3 يقسم $n(n^{32} - 1)$، ولكن إذا كان 3 لا يقسم n، فإنه باستخدام مبرهنة فيرما، $n^2 \equiv 1$ (مقياس 3)، وعليه، فإنّ:

$$n^{32} - 1 \equiv (n^2)^{16} - 1 \equiv 1^{16} - 1 \equiv 0 (\text{mod } 3) \quad \text{(مقياس 3)}$$

وهذا يعني أنّ 3 يقسم $n^{32} - 1$.

إذا كان $n \equiv 0$ (مقياس 5) فإن $n^{33} - n \equiv 0$ (مقياس 5) أما إذا كان

$n \not\equiv 0$ (مقياس 5)، فباستخدام مبرهنة فيرما، $n^4 \equiv 1$ (مقياس 5) وعليه، فإنّ:

$$n^{32} - 1 \equiv (n^4)^8 - 1 \equiv 1^8 - 1 \equiv 0 \quad \text{(مقياس 5)}$$

وهذا يعني أنّ $n^{33} - n \equiv 0$ (مقياس 3) لأيّ عدد n. ▲

تعميم أويلر

قدم أويلر تعميمًا لمبرهنة فيرما، وسيكون تعميمه هذا نتيجة للمبرهنة المقبلة، التي أثبتت عن

6.20 المبرهنة طريق العد (*Counting*)، مستخدمين المبدأ نفسه الذي استخدم في إثبات مبرهنة 11.19.

المجموعة G_n للعناصر غير الصفرية في $\mathbb{Z}_n$، التي هي ليست قواسم للصفر تمثل زمرة تحت الضرب مقياس n.

البرهان يجب علينا أولاً إثبات أنّ G_n مغلقة تحت عملية الضرب مقياس n، خذ $a,b \in G_n$ إذا كان $ab \notin G_n$، فإنه يوجد $c \neq 0$ في $\mathbb{Z}_n$، حيث $(ab)\, c = 0$.

الآن، $(ab)\, c = 0$ يؤدي إلى $a(bc) = 0$، لأن $b \in G_n$ و $c \neq 0$ فإنه باستخدام تعريف المجموعة G_n، $bc \neq 0$، وعليه، فإن $a(bc) = 0$ يؤدي إلى أن $a \notin G_n$، وهذا يناقض الفرض. لاحظ أنّنا بيّنا مسبقًا أنه لأيّ حلقة، تكون مجموعة العناصر التي هي ليست قواسم للصفر مغلقة بالنسبة إلى عملية الضرب؛ ولأن $\mathbb{Z}_n$ حلقة، فإن بنية $\mathbb{Z}_n$ لا تختلف عن بنية أيّ حلقة.

وسنثبت الآن أن G_n زمرة، بالطبع الضرب مقياس n يحقق الخاصية التجميعية و $1 \in G_n$، بقي علينا أن نثبت أنه لأيّ

$a \in G_n$ يوجد $b \in G_n$ حيث $ab = 1$. افترض أنّ:

$$1, a_1, \ldots, a_r$$

هي عناصر G_n، والعناصر

$$a1, aa_1, \ldots, a.a_r$$

هي عناصر مختلفة؛ لأن $aa_i = aa_j$ يؤدي إلى $a(a_i - a_j) = 0$، ولأن $a \in G_n$، أي ليست أحد قواسم الصفر، فإن $a_i - a_j = 0$ أيّ $a_i = a_j$؛ ولهذا وعن طريق العد، سنجد أنه إما $a.1 = 1$ أو aa_j يجب أن يكون 1 لأحد عناصر $a_i \in G_n$؛ لذلك، فإن a له معكوس ضربي. ♦

لاحظ أنّ الخاصية الوحيدة لـ $\mathbb{Z}_n$ المستخدمة في المبرهنة السابقة، عدا أنّها حلقة فيها عنصر محايد، فهي منتهية أيضًا، وقد وظفنا مبدأ العدّ في كلتا المبرهنتين 11.19 و6.20، وهو مبدأ بسيط، ولكنه من بين أقوى الأدوات المستخدمة في الرياضيات.

خذ عددًا صحيحًا موجبًا n، ودعنا نعرّف $\varphi(n)$ بعدد الأرقام الصحيحة الموجبة التي هي أقل من أو تساوي n، والتي هي أولية بالنسبة إلى n، لاحظ أنّ $\varphi(1) = 1$

7.20 مثال لتكن $n = 12$، الأعداد الصحيحة الموجبة التي هي أقل من أو تساوي 12 وأولية بالنسبة إلى 12 هي 1، 5، 7 و11؛ لذلك $\varphi(12) = 4$ ▲

باستخدام المبرهنة 3.19، $\varphi(n)$ هو عدد العناصر غير الصفرية في $\mathbb{Z}_n$، التي هي ليست قواسم للصفر، هذه الدالة $\varphi = \mathbb{Z}^+ \to \mathbb{Z}^+$ تسمى فاي لأويلر **(Euler phi-function)** يمكننا الآن أن نصف تعميم أويلر لمبرهنة فيرما.

8.20 مبرهنة (**مبرهنة أويلر**)، إذا كان a عددًا صحيحًا أوليًا نسبيًّا مع n، فإن $a^{\varphi(n)} - 1$ قابل للقسمة على n، أي إن $a^{\varphi(n)} \equiv 1$. (مقياس n).

البرهان إذا كان a أوليًّا نسبيًّا مع n، فإن المجموعة المشاركة $a + n\mathbb{Z}$ من $n\mathbb{Z}$ التي فيها a، تحوي عددًا صحيحًا $b < n$ وأوليًّا نسبيًّا مع n.

باستخدام حقيقية أنّ الضرب بين المجموعات المشاركة عن طريق الضرب مقياس n لممثلي هذه المجموعات هو حسن التعريف، فإن

$$a^{\varphi(n)} \equiv b^{\varphi(n)} \quad (\text{مقياس } n)$$

باستخدام المبرهنتين 3.19و 6.20، يُنْظَر إلى b على أنه عنصر في المجموعة الضربية G_n من الرتبة $\varphi(n)$، التي تحوي $\varphi(n)$ من العناصر من $\mathbb{Z}_n$ كل منها أولي بالنسبة إلى n، وعليه، فإنّ:

$$b^{\varphi(n)} \equiv 1 \quad (\text{مقياس } n)$$

ما يعني أن مبرهنتنا قد أُثبتت. ◆

9.20 مثال لتكن $n = 12$، رأينا في مثال 7.20 أنّ $\varphi(12) = 4$، أي إنه إذا أخذنا عددًا صحيحًا مثل a أوليًّا بالنسبة إلى 12، فإن $a^4 \equiv 1$ (مقياس 12)، على سبيل المثال: إذا كان $a = 7$، فإن $7^4 = (49)^2 = 2401 = 12(200) + 1$؛ لذلك، فإن $7^4 \equiv 1$ (مقياس 12) وبالطبع، فإن أسهل طريقة لحساب 7^4 (مقياس 12)، دون استخدام مبرهنة أويلر، هي حسابها في $\mathbb{Z}_{12}$، حيث نعلم في $\mathbb{Z}_{12}$ أن $7 = -5$ ؛ لذلك:

$$7^2 = (-5)^2 = 5^2 = 1 \quad \text{و} \quad 7^4 = 1^2 = 1$$ ▲

تطبيق على $ax \equiv b$ (مقياس m)

باستخدام المبرهنة 6.20، نستطيع أن نجد حلول التطابق الخطّي $ax \equiv b$ (مقياس m) كلها، نفضل أن نتعامل مع معادلة في $\mathbb{Z}_m$، ومن ثم نفسر النتائج بوصفها تطابقات.

10.20 مبرهنة ليكن m عددًا موجبًا صحيحًا، وخذ $a \in \mathbb{Z}_m$ أوليًّا نسبيًّا مع m، لأي عدد $b \in \mathbb{Z}_m$ ، المعادلة $ax = b$ لها حل وحيد في $\mathbb{Z}_m$.

البرهان باستخدام المبرهنة 6.20، فإن a عنصر وحدة في $\mathbb{Z}_m$ و $s = a^{-1}b$ هو بالتأكيد حل للمعادلة، وبضرب طرفي المعادلة $ax = b$ من اليسار بـ a^{-1} سنرى أنه الحل الوحيد. ◆

في حالة تفسير هذه المبرهنة بوصفها تطابقات سنخرج بالنتيجة الآتية:

11.20 نتيجة إذا كان a و m عددين صحيحين أوليين نسبيًّا، فإنه لأي عدد صحيح b، الأعداد الصحيحة التي تمثل حلولًا للتطابق $ax \equiv b$ (مقياس m) تقع بالضبط في صف بواقي واحد مقياس m.

المبرهنة 10.20 تخدم بوصفها تمهيدية للحالة العامة.

12.20 مبرهنة ليكن m عددًا صحيحًا موجبًا، وخذ $a,b \in \mathbb{Z}_m$. $gcd\,(a,m) = d$. المعادلة $ax = b$ لها حل في $\mathbb{Z}_m$، إذا وفقط إذا كان d يقسم b. عندما d يقسم b سيكون للمعادلة بالضبط d من الحلول في $\mathbb{Z}_m$.

البرهان أولاً، سنثبت أنه لا يوجد حل للمعالة $ax = b$ في $\mathbb{Z}_m$، إلا إذا كان d يقسم b، افترض أن $s \in \mathbb{Z}_m$ هو حل للمعادلة، فإن $as - b = qm$ في $\mathbb{Z}$؛ لذلك، $b = as - qm$، ولأنّ d يقسم كلًّا من a و m، فإنه يقسم الجانب الأيمن من المعادلة $b = as - qm$؛ ولذلك فهو يقسم b، ما يعني أنّ الحل s متوافر فقط، إذا كان d يقسم b، افترض الآن، أنّ d يقسم b، وخذ

$$a = a_1 d, \qquad b = b_1 d, \qquad m = m_1 d$$

وعليه، فإنّ المعادلة $as - b = qm$ في $\mathbb{Z}$ يمكن إعادة صياغتها على الصورة $d(a_1 s - b_1) = d\,qm_1$، ونرى أنّ $as - b$ من مضاعفات m، إذا وفقط إذا كان $a_1 s - b_1$ من مضاعفات m_1، ما يعني أنّ الحلول s للمعادلة $ax = b$ في $\mathbb{Z}_m$ هي بالضبط العناصر التي تُقرأ مقياس m_1، التي تكون حلولًا للمعادلة $a_1 x = b_1$ في $\mathbb{Z}_{m_1}$، وخذ الآن $s \in \mathbb{Z}_{m_1}$ الذي يمثل الحل الوحيد للمعادلة $a_1 x = b_1$ في $\mathbb{Z}_{m_1}$ كما في المبرهنة 10.20، الأعداد في $\mathbb{Z}_m$ التي تختزل إلى s مقياس m_1 هي بالضبط العناصر التي تُحسب في $\mathbb{Z}_m$ كما يأتي:

$$s, s + m_1, s + 2m_1, s + 3m_1, \ldots, s + (d-1)m_1$$

وهذا يعني أنه يوجد d من الحلول للمعادلة في $\mathbb{Z}_m$. ♦

تقدم لنا المبرهنة 12.20 النتيجة التقليدية الآتية لإيجاد حلول أي تطابق خطي.

13.20 نتيجة ليكن d القاسم المشترك الأكبر للعددين الموجبين a و m، يوجد حل للتطابق (مقياس m) $ax \equiv b$ إذا وفقط إذا كان d يقسم b، في هذه الحالة، تكون حلول المعادلة هي الأعداد الصحيحة التي توجد بالضبط في d من صفوف البواقي المختلفة مقياس m.

في الواقع، وضّح إثباتنا للمبرهنة 12.20 حلول المعادلة (مقياس m) $ax \equiv b$ بصورة أكبر مما نصت عليه النتيجة السابقة، حيث بيّنت المبرهنة أنه إذا وجد أيّ حل s، فإن حلول المعادلة جميعها هي العناصر التي توجد في صفوف البواقي $(s + km_1) + (m\mathbb{Z})$، حيث $m_1 = \dfrac{m}{d}$، و k يأخذ القيم الصحيحة كلها من 0 إلى $d - 1$، إضافة إلى أنها تخبرنا أيضًا بأنه يمكننا إيجاد هذا الحل s عن طريق إيجاد $a_1 = \dfrac{a}{d}$ و $b_1 = \dfrac{b}{d}$، ومن ثم حل المتطابقة $a_1 x \equiv b_1$ (مقياس m_1) ولحل هذه المتطابقة يمكننا استبدال a_1 و b_1 ببواقيهما مقياس m_1، ثمّ حلّ المعادلة $a_1 x = b_1$ في $\mathbb{Z}_{m_1}$.

14.20 مثال أوجد الحلول جميعها للمتطابقة $12x \equiv 27$ (مقياس 18).

الحل القاسم المشترك الأكبر بين 12 و 18 هو 6، إلّا أنّ 6 لا تقسم 27. باستخدام النتيجة السابقة، لا يوجد أي حل. ▲

15.20 مثال أوجد الحلول جميعها للمتطابقة $15x \equiv 27$ (مقياس 18).

الحل القاسم المشترك الأكبر بين 15 و18 هو 3 و3 يقسم 27.

استكمالاً لما هو مشروح قبل مثال 14.20، سنقسم كل شيء على 3، ونحصل على المتطابقة $5x \equiv 9$ (مقياس 6)، التي تعادل إيجاد حلول المعادلة $5x = 3$ في $\mathbb{Z}_6$، حيث إنّ العناصر التي تمثل عناصر وحدة في $\mathbb{Z}_6$ هي 1 و 5، والمعكوس الضربي لـ 5 هو 5 في هذه الزمرة. ما يعني أنّ حلّ المعادلة في $\mathbb{Z}_6$ هو $x = (5^{-1})(3) = (5)(3) = 3$، وعليه، فإن حلول المتطابقة $15x \equiv 27$ (مقياس 18) هي الأعداد الصحيحة المتوافرة في صفوف البواقي:

$$3+18\mathbb{Z} = \{\ldots, -33, -15, 3, 21, 39, \ldots\},$$
$$9+18\mathbb{Z} = \{\ldots, -27, -9, 9, 27, 45, \ldots\}.$$
$$15+18\mathbb{Z} = \{\ldots, -21, -3, 15, 33, 51, \ldots\},$$

كما هو موضح في النتيجة 13.20، لاحظ أنّ $d = 3$ الحلول الثلاثة 3، 9، 15 تقع في $\mathbb{Z}_{18}$، والحلول كافة في صفوف البواقي الثلاثة مقياس 18 المكتوبة في الأعلى، يمكن جمعها في صف الباقي $3+6\mathbb{Z}$ مقياس 6؛ لأنها جاءت من الحل $x = 3$ للمعادلة $5x = 3$ في $\mathbb{Z}_6$. ▲

تمارين 20

حسابات

سنرى لاحقًا أنّ الزمرة الضربية للعناصر غير الصفرية لحقل منتهٍ هي زمرة دورية، وضّح هذا بإيجاد المولِّد لهذه الزمرة للحقل المنتهي المعطى

1. $\mathbb{Z}_7$ **2.** $\mathbb{Z}_{11}$ **3.** $\mathbb{Z}_{17}$

باستخدام مبرهنة فيرما، أوجد باقي قسمة 3^{47} على23.

5. باستخدام مبرهنة فيرما، أوجد باقي قسمة 37^{49} على 7.

6. احسب باقي قسمة $2^{(2^{17})}+1$ على 19. [مساعدة: ستحتاج إلى أن تحسب باقي قسمة 2^{17} مقياس 18].

7. اصنع جدولاً للقيم $\varphi(n)$ لـ $n \le 30$.

8. احسب $\varphi(p^2)$، حيث p عدد أولي.

9. احسب $\varphi(pq)$، حيث p و q عددان أوليان.

10. استخدم تعميم أويلر لمبرهنة فيرما في إيجاد باقي قسمة 7^{1000} على 24.

في التمارين 11 إلى 18، صف الحلول جميعها للمتطابقة المعطاة كما فعلنا في المثالين 14.20، و15.20.

11. $2x \equiv 6$ (مقياس 4) **12.** $22x \equiv 5$ (مقياس 15)

13. $36x \equiv 15$ (مقياس 24) **14.** $45x \equiv 15$ (مقياس 24)

15. $39x \equiv 125$ (مقياس 9) **16.** $41x \equiv 125$ (مقياس 9)

17. $155x \equiv 75$ (مقياس 65) **18.** $39x \equiv 52$ (مقياس 130)

19. ليكن p عددًا أوليًّا ≥ 3، استخدم تمرين 28 في إيجاد باقي قسمة $(p-2)!$ مقياس p.

20. استخدم تمرين 28 في إيجاد باقي قسمة 34! مقياس 37.

21. استخدم تمرين 28 في إيجاد باقي قسمة 49! مقياس 53.

22. استخدم تمرين 28 في إيجاد باقي قسمة 24! مقياس 29.

مفاهيم

23. ضع إشارة صح أو إشارة خطأ:

_____ أ. $a^{p-1} \equiv 1$ (مقياس p) لكل الأعداد الصحيحة a والأولية p.

_____ ب. $a^{p-1} \equiv 1$ (مقياس p) لكل الأعداد الصحيحة a، حيث $a \not\equiv 0$ (مقياس p) و p عدد أولي.

_____ جـ. $\varphi(n) \leq n$ لكل $n \in \mathbb{Z}^+$.

_____ د. $\varphi(n) \leq n-1$ لكل $n \in \mathbb{Z}^+$

_____ هـ. عناصر الوحدة في $\mathbb{Z}_n$ هي الأعداد الصحيحة الموجبة الأقل من n والأولية بالنسبة إلى n.

_____ و. حاصل ضرب عنصري وحدة في $\mathbb{Z}_n$ يكون دائمًا عنصر وحدة.

_____ ز. حاصل ضرب عددين كل منهما ليس عنصر وحدة في $\mathbb{Z}_n$، يمكن أن يكون عنصر وحدة.

_____ ح. حاصل ضرب عنصر وحدة وآخر ليس عنصر وحدة من $\mathbb{Z}_n$ ليس عنصر وحدة أبدًا.

_____ ط. كل تطابق $ax \equiv b$ (مقياس p)، حيث p عدد أولي لها حل.

_____ ي. افترض أنّ d هو القاسم المشترك الأكبر للعددين الموجبين a و m. إذا كان d يقسم b، فإن التطابق $ax \equiv b$ (مقياس m)، له بالضبط d من الحلول غير المتطابقة.

24. اكتب جدول الضرب للزمرة الضربية لعناصر الوحدة في $\mathbb{Z}_{12}$. أيُّ زمرةٍ من الرتبة 4 تماثل هذه الزمرة؟

براهين مختصرة

25. أعطِ جملة واحدة موجزة لإثبات المبرهنة 1.20.

26. أعطِ جملة واحدة موجزة لإثبات المبرهنة 8.20.

براهين

27. بيّن أنّ 1 و $p-1$ هما العنصران الوحيدان في الحقل $\mathbb{Z}_p$، اللّذان لكل منهما المعكوس الضربي نفسه. [مساعدة: حلّ المعادلة $x^2 - 1 = 0$].

28. باستخدام تمرين 27، أثبت مبرهنة ويلسون (*Wilsons Theorem*)، التي تنص على أنه إذا كان p عددًا أوليًّا، فإن $(p-1)! \equiv -1$ (مقياس p). [النصف الآخر من المبرهنة ينص على أنه إذا كان n عددًا صحيحًا أكبر من 1 بحيث $(n-1)! \equiv -1$ (مقياس n) فإنّ n عدد أولي. فقط فكّر: ماذا سيكون باقي قسمة $(n-1)!$ مقياس n إذا كان n ليس عددًا أوليًّا].

29 . استخدم مبرهنة فيرما في إثبات أنه لأيّ عدد صحيح موجب n، العدد الصحيح

$n^{37} - n$ قابل للقسمة على383838. [مساعدة: (37)(19)(13)(7)(3)(2) = 383838].

30 . بالعودة إلى تمرين 29، أوجد عددًا أكبر من 383838 يقسم $n^{37} - n$ لأيّ عدد صحيح موجب n.

الفصل 21 حقل خوارج القسمة للحلقة التامة
The Field of Qutients of an Integral Domain

إذا توافرت حلقة تامة، بحيث كل عنصر غير صفري فيها له معكوس ضربي، فهي إذن حقل، مع ذلك، هناك الكثير من الحلقات التامة، مثل $\mathbb{Z}$ لا تشكل حقلًا، لكن هذه ليست مشكلة كبيرة؛ لأن الغرض من الفصل هو إثبات أنّ أيّ حلقة تامة يمكن جعلها محتواة في حقل محدد، يطلق عليه اسم **حقل خوارج القسمة لحلقة تامة (a field of quotients of the integral domain)**، هذا الحقل سيكون أصغر حقل يحتوي الحلقة التامة، كما سوف نبين، على سبيل المثال: الأعداد الصحيحة محتواة في الحقل $\mathbb{Q}$، الذي يمكن التعبير عن عناصره على أنها خوارج القسمة للأعداد الصحيحة، حيث إنّ بنيتنا لحقل خوارج القسمة لحلقة تامة تشابه تمامًا بنيتنا للأعداد النسبية من الأعداد الصحيحة، وهذه البنية موجودة في أيّ كتاب لمبادئ الرياضيات أو تفاضل وتكامل متقدم، ويعدّ إتمام هذا البناء أفضل تمرين في استخدام تعريفات ومفهوم التماثل، التي سنناقشها بشيء من التفصيل على الرغم من أنه ممل، غير أنه من الممكن أن نجعل الدراسة ممتعة بأن نتحرك في كل خطوة بالطريقة نفسها التي نتحرك بها لبناء $\mathbb{Q}$ من $\mathbb{Z}$.

البناء

خذ الحلقة التامة D، التي سنحاول أن نوسعها إلى حقل خوارج القسمة F. الخطوات المختصرة المباشرة التي سنقوم بها هي على النحو الآتي:

1. نعرف عناصر F كيف تكون.
2. نعرف العمليتين الثنائيتين؛ الجمع والضرب على F.
3. تحقق من شروط الحقل كافة؛ لإثبات أنّ F هو حقل بالنسبة إلى هاتين العمليتين الثنائيتين.
4. أثبت أنّ F يحتوي D بوصفها حلقة تامة جزئية منه.

الخطوات 1، 2، 4 ممتعة جدًا، ولكن الخطوة 3 هي عمل روتيني طويل، سنبدأ الآن بالبناء.

الخطوة (1): افترض أنّ D حلقة تامة معطاة، وشكِّل حاصل الضرب الديكارتي

$$D \times D = \{(a, b) \mid a, b \in D\}$$

سننظر إلى الزوج المرتب (a, b) على أنه يمثل شكليًّا خارج القسمة (formal quotient a/b)، أي إنه إذا كان $D = \mathbb{Z}$، فإنّ الزوج المرتب $(2, 3)$ سيمثل لنا العدد $\frac{2}{3}$، أما الزوج المرتّب $(2, 0)$ فلا يمثل أيّ عنصر في $\mathbb{Q}$؛ ولذلك سنقترح أن نقلص $D \times D$ قليلًا، افترض أنّ S هي مجموعة جزئية من $D \times D$ معطاة بالعلاقة:

$$S = \{(a, b) \mid a, b \in D, b \neq 0\}.$$

ما زالت S ليست هي حقلنا المنشود؛ لأنه في الحقيقة عندما $D = \mathbb{Z}$، فإن **الأزواج المرتبة المختلفة (different)** من الأعداد الصحيحة، مثل $(2, 3)$ و$(4, 6)$ يمكن أن تمثل العدد النسبي نفسه (لاحقًا سوف نعرف متى يمثل عنصران مختلفان في S فعليًّا العنصر نفسه في F، أو كما سوف نرى، سنعرف متى يكون عنصران في S متكافئين).

1.21 تعريف العنصران (a, b) و (c, d) **متكافئان في** S (***equivalent***)، ويعبر عن ذلك بـ $(a, b) \sim (c, d)$، إذا وفقط إذا كان $ad = bc$. ■

لاحظ أنّ هذا التعريف معقول؛ لأنّ الخاصية $(a, b) \sim (c, d)$ هي المعادلة $ad = bc$، التي تحوي عناصر من D، وتشمل عملية الضرب المعلومة على D، لاحظ أيضًا في حالة $D = \mathbb{Z}$، أنّ هذه الخاصية تعطينا التعريف الطبيعي للمساواة بين $\frac{a}{b}$ و $\frac{c}{d}$ فمثلاً $\frac{4}{6} = \frac{2}{3}$؛ لأن $(4)(3) = (6)(2)$، ويمكن أن ينظر إلى العدد النسبي الذي سوف نعبر عنه بـ $\frac{2}{3}$ على أنه يمثل خوارج القسمة كلها للأعداد الصحيحة، التي تختصر إلى أو تكافئ $\frac{2}{3}$.

2.21 تمهيدية العلاقة $\sim$ بين عناصر من المجموعة S كما وصفت في الأعلى، هي علاقة تكافؤ.

البرهان يجب علينا أن نفحص الخصائص الثلاثة لعلاقة التكافؤ.

منعكسة (Reflexive) $(a, b) \sim (a, b)$ لأن $ab = ba$، لاحظ أنّ الضرب على D إبدالي.

متناظرة (Symmetric) إذا كان $(a, b) \sim (c, d)$، فإنّ $ad = bc$؛ ولأنّ الضرب على D إبدالي، نجد أنّ $cb = da$، وعليه، فإنّ $(c, d) \sim (a, b)$.

متعدية (Transitive) إذا كان $(a, b) \sim (c, d)$ و $(c, d) \sim (r, s)$، فإن $ad = bc$ و $cs = dr$. باستخدام هذه العلاقات وحقيقة أنّ الضرب على D إبدالي نجد أنّ:

$$asd = sad = sbc = bcs = bdr = brd$$

والآن لأنّ $d \neq 0$ و D حلقة تامة، فيمكننا استخدام قانون الحذف، وهذه هي الخطوة الأهم، وعليه، فإن العلاقة $asd = brd$ ستؤول إلى العلاقة $as = br$؛ لذلك، فإن $(a, b) \sim (r, s)$. ♦

باستعراض المبرهنة 22.0 نعلم الآن أنّ $\sim$ تجزِّئ المجموعة S إلى صفوف تكافؤ، ولتجنب وضع خطوط عرضية طويلة فوق تعبيرات ممتدة، سوف نستخدم $[(a, b)]$ بدلاً من $\overline{(a, b)}$ للتعبير عن صف التكافؤ لـ (a, b) في S تحت العلاقة $\sim$، وسننهي الخطوة 1 الآن بتعريف المجموعة F على أنها المجموعة التي تحوي صفوف التكافؤ كلها $[(a, b)]$ لـ $(a, b) \in S$

الخطوة (2): التمهيدية المقبلة ستخدمنا بتعريف الجمع والضرب على F، لاحظ أنه إذا كان $D = \mathbb{Z}$ و $[(a, b)]$ هو $(a/b) \in \mathbb{Q}$، فإن التعريف المقبل يقدم لنا عمليات الجمع والضرب العادية على $\mathbb{Q}$.

3.21 تمهيدية إذا كان $[(a, b)]$ و $[(c, d)]$ في F، فإنّ المعادلات:

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

و

$$[(a, b)][(c, d)] = [(ac, bd)]$$

تعطي عمليات حسنة التعريف للجمع والضرب على F.

البرهان لاحظ أولاً أنه إذا كان $[(a, b)]$ و $[(c, d)]$ في F، فإن (a, b) و (c, d) في S، ما يعني $b \neq 0$ و$d \neq 0$؛ لأنّ D حلقة تامة، فإن $bd \neq 0$، ما يعني أنّ كلاً من $(ad + bc , bd)$ و (ac, bd) في S. (لاحظ أنّ أهم حقيقة استخدمناها هي: أنّ D ليس فيها قواسم للصفر)، وهذا يعني أنّ الجانب الأيمن – على الأقل – في كلتا المعادلتين يقع في F.

بقي علينا أن نبيّن أنّ الجمع والضرب المعرف على F حسن التعريف، وهذا يعني أنه يجب علينا أن نبين أنه إذا تمّ اختيار ممثلين آخرين من S، فإن النتيجة نفسها ستظهر في F. لإنهاء هذا الأمر، افترض أن $(a_1, b_1) \in [(a, b)]$ و$(c_1, d_1) \in [(c, d)]$، علينا أن نثبت أن

$$(a_1d_1 + b_1c_1, b_1d_1) \in [(ad + bc, bd)]$$

و

$$(a_1c_1, b_1d_1) \in [(ac, bd)]$$

الآن، $(a_1, b_1) \in [(a, b)]$، ما يعني أنّ $(a_1, b_1) \sim (a, b)$، وهذا يؤدي إلى

$$a_1b = b_1a.$$

بالأسلوب نفسه $(c_1, d_1) \in [(c, d)]$ يؤدي إلى

$$c_1d = d_1c.$$

للحصول على «مقام مشترك» للأزواج المرتبة الأربعة $(a, b), (a_1, b_1), (c, d), (c_1, d_1)$، ونضرب المعادلة الأولى بـ d_1d والمعادلة الثانية بـ b_1b، ثم بإضافة المعادلتين الناتجتين إلى بعضهما نحصل على المعادلة الآتية في D:

$$a_1bd_1d + c_1db_1b = b_1ad_1d + d_1cb_1b$$

ثم باستخدام المسلمات المختلفة على الحلقة التامة نرى أنه:

$$(a_1d_1 + b_1c_1)bd = b_1d_1(ad + bc),$$

لذلك، فإنّ:

$$(a_1d_1 + b_1c_1, b_1d_1) \sim (ad + bc, bd),$$

ما يؤدي إلى أنّ $(a_1d_1 + b_1c_1, b_1d_1) \in [(ad + bc, bd)]$، وبهذا ننتهي من الجمع على F، أمّا بالنسبة إلى الضرب على F، فبضرب المعادلتين $a_1b = b_1a$ و $c_1d = d_1c$ ببعضهما نحصل على:

$$a_1bc_1d = b_1ad_1c$$

وهذا يؤدي إلى:

$$(a_1c_1, b_1d_1) \sim (ac, bd)$$

أي إنّ $(a_1c_1, b_1d_1) \in [(ac, bd)]$، وهكذا يكتمل الإثبات. ♦

من المهم أن نفهم معنى التمهيدية السابقة وأهمية إثباتها، وعندها تكتمل الخطوة (2).

الخطوة (3): تعدّ الخطوة 3 خطوة روتينية، ولكن من الجيد لنا أن نقوم بهذه الخطوة بشيء من التفصيل، إذ لا نستطيع أن نقوم بها إلا إذا كنا قد فهمنا ما قمنا به سابقًا؛ ولذلك، فإنّ قيامنا بهذه الخطوة سيعزز فهمنا لهذا البناء، سنضع قائمة بالأشياء التي يجب أن نثبتها، حيث سنثبت بعضها، ونترك البقية للتمارين.

البرهان

1. الجمع في F إبدالي.

باستخدام تعريف الجمع $[(a, b)] + [(c, d)]$ هو $[(ad + bc, bd)]$، أيضًا باستخدام تعريف الجمع $[(c, d)] + [(a, b)]$ هو $[(cb + da, db)]$. نحتاج إلى أن نبيّن أنّ $(ad + bc, bd) \sim (cb + da, db)$، ولكنه صحيح، لأنه باستخدام المسلمات على D، فإنّ $ad + bc = cb + da$ و $bd = db$. ♦

2. الجمع عملية تجميعية.

3. $[(0, 1)]$ هو العنصر المحايد لعملية الجمع على F.

4. $[(-a, b)]$ هو المعكوس الجمعي لـ $[(a, b)]$ في F.

5. الضرب على F عملية تجميعية.

6. الضرب على F إبدالي.

7. قانونا التوزيع متحققان في F.

8. $[(1, 1)]$ هو العنصر المحايد لعملية الضرب على F.

9. إذا كان $[(a,b)] \in F$ ليس العنصر المحايد في عملية الجمع، فإن $a \neq 0$ في D و $[(b,a)]$ هو المعكوس الضربي لـ $[(a,b)]$.

البرهان لتكن $[(a,b)] \in F$. إذا كان $a = 0$، فإنّ:

$$a1 = b0 = 0$$

لذلك،

$$(a,b) \sim (0,1)$$

وهذا يعني أنّ $[(a,b)] = [(0,1)]$، ولكن باستخدام الفقرة الثالثة، فإن $[(0,1)]$ هو العنصر المحايد لعملية الجمع، ما يعني أنه إذا كان $[(a,b)]$ ليس العنصر المحايد لعملية الجمع في F، فإنّ $a \neq 0$، وبهذا، فإنه من المعقول الحديث عن $[(b,a)]$ في F.

والآن، $[(a,b)][(b,a)] = [(ab,ba)]$، ولكن $ab = ba$ في D، وهذا يعني

$$(ab)\,1 = (ba)\,1$$

و

$$(ab,ba) \sim (1,1)$$

لذلك،

$$[(a,b)][(b,a)] = [(1,1)]$$

و $[(1,1)]$ هو العنصر المحايد لعملية الضرب كما في الفقرة الثامنة. ♦

وهذا ينهي الخطوة 3

الخطوة (4): بقي علينا أن نبيّن أنّ F تحوي D، ولكي نبين هذا الأمر، علينا أن نوضح أنه يوجد تماثل i بين D وحلقة تامة جزئية من F، فإذا أعدنا تسمية صورة D بالنسبة إلى i باستخدام أسماء العناصر في D، فنكون قد انتهينا، التمهيدية المقبلة ستقدم لنا هذا التماثل، حيث سنستخدم الحرف i في هذا التماثل إشارة إلى دالة الواحد لواحد (انظر إلى الهامش صفحة 4)؛ سنحقن D داخل F.

4.21 تمهيدية الدالة $i : D \to F$ المعطاة بالعلاقة $i(a) = [(a,1)]$، تماثل بين D وحلقة جزئية من F.

البرهان لـ a و b في D فإن:

$$i(a+b) = [(a+b, 1)].$$

كذلك:

$$i(a) + i(b) = [(a, 1)] + [(b, 1)] = [(a1 + 1b, 1)] = [(a+b, 1)].$$

لذلك، فإن: $i(a+b) = i(a) + i(b)$. إضافة إلى ذلك،

$$i(ab) = [(ab, 1)],$$

بينما

$$i(a)i(b) = [(a, 1)][(b, 1)] = [(ab, 1)],$$

لذلك، $i(ab) = i(a)i(b)$.
بقي علينا أن نثبت فقط أن i هو واحد لواحد، فإذا كان $i(a) = i(b)$، فإن

$$[(a, 1)] = [(b, 1)],$$

لذلك، $(a, 1) \sim (b, 1)$ يعني أنّ $a1 = 1b$؛ ما يعني أنّ

$$a = b$$

أي إنّ i تماثل من D إلى $i[D]$، وبالطبع، $i[D]$ حلقة تامة جزئية من F. ♦

لأن $[(a, b)] = [(a, 1)][(1, b)] = [(a, 1)]/[(b, 1)] = i(a)/i(b)$ متحقق بصورة واضحة في F، فإننا نكون قد أثبتنا المبرهنة المقبلة.

5.21 مبرهنة أي حلقة تامة D يمكن توسيعها إلى (أو طمرها في) حقل F، بحيث كل عنصر في F يمكن التعبير عنه بوصفه خارج قسمة عنصرين في D. (هذا الحقل F يسمى **حقل خارج القسمة على *D***).

الوحدانية (Uniqueness)

قلنا في البداية إنّ F يمكن أن يعدّ إلى حد ما أصغر حقل يحتوي D، وهذا الأمر محسوس؛ لأن كل حقل يحوي D، فلا بدّ أن يحوي العناصر a/b لكل $a, b \in D$، حيث $b \neq 0$، تثبت لنا المبرهنة المقبلة أنّ كل حقل يحوي D يحوي حقل جزئيًّا، بوصفه حقلًا خارج القسمة على D، وتثبت أيضًا، أنّ أيّ حقلي خارج قسمة على D متماثلان.

6.21 مبرهنة ليكن F حقلًا خارج قسمة على D، وليكن L أيّ حقل يحوي D، فتوجد دالة $\psi : F \to L$ تعطي تماثلًا لـ F مع حقل جزئي من L، حيث $\psi(a) = a$ لكل $a \in D$.

البرهان الحقل الجزئي والرسم التخطيطي في شكل 7.21 قد يساعدك على تصور الوضع لهذه المبرهنة.

صورة أيّ عنصر في F هي: $a/_F\ b$، حيث $/_F$ تعني خارج قسمة $a \in D$ على $b \in D$، على أن تعدّ أنها عناصر في F، ونريد بالطبع أن نربط $a/_F\ b$ بصورة غامرة مع $a/_L\ b$، حيث إنّ $/_L$ يعني خارج قسمة عناصر من L، إذ سيكون العمل الرئيس إثبات أنّ مثل هذه الدالة حسنة التعريف.

علينا أن نعرف $\psi: F \longrightarrow L$، وسنبدأ بتعريف

$$a \in D \text{ لـ } \psi(a) \longrightarrow a$$

كل عنصر $x \in F$ هو خارج قسمة $a/_F\ b$ للعنصرين a و $b \neq 0$، من D، لنحاول أن نعرف ψ بـ $\psi(a\ /_F\ b) = \psi(a)\ /_L\ \psi(b)$:

يجب أن نبيّن أنّ هذه الدالة ψ منطقية وحسنة التعريف؛ ولأن ψ محايد على D، لـ $b \neq 0$، فإن $\psi(b) \neq 0$؛ لذلك، فإنّ: تعريفنا لـ $\psi(a\ /_F\ b)$ بـ $\psi(a)\ /_L\ \psi(b)$ منطقي. إذا كان $a\ /_F\ b = c\ /_F\ d$ في F، فإن $ad = bc$ في D؛ لذلك، $\psi(ad) = \psi(bc)$، لكن لأن ψ محايد على D،

$$\psi(ad) = \psi(a)\psi(d) \text{ و } \psi(bc) = \psi(b)\psi(c)$$

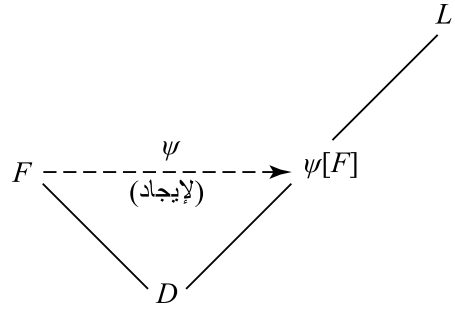
لذلك،

$$\psi(a)\ /_L\ \psi(b) = \psi(c)\ /_L\ \psi(d)$$

في L، ما يعني أنّ ψ حسن التعريف.

المعادلتان

$$\psi(xy) = \psi(x)\psi(y)$$



الشكل 7.21

و

$$\psi(x+y)=\psi(x)+\psi(y)$$

متحققتان بسهولة من خلال تعريف ψ على F، ومن خلال حقيقة أنّ ψ محايدة على D.

إذا كان $\psi(a\ /_F\ b)=\psi(c\ /_F\ d)$، فإن:

$$\psi(a)\ /_L\ \psi(b)=\psi(c)\ /_L\ \psi(d)$$

لذلك،

$$\psi(a)\psi(d)=\psi(b)\psi(c)$$

لأن ψ محايدة على D، نستنتج أنّ $ad=bc$، لذلك $a\ /_F\ b=c\ /_F\ d$ وهذا يعني أن ψ واحد لواحد.

من التعريف، $\psi(a)=a$ لكل $a\in D$. ♦

8.21 نتيجة كل حقل L يحوي الحلقة التامة D، فإنه يحوي حقل خارج القسمة على D.

البرهان في إثبات المبرهنة 6.21 كل عنصر في الحقل الجزئي $\psi[F]$ من L، هو خارج القسمة في L لعناصر D. ♦

9.21 نتيجة أيّ حقلي خارج قسمة للحلقة التامة D متماثلان.

البرهان افترض –كما في المبرهنة 6.21– أنّ L هو حقل خارج القسمة لـ D؛ لذلك، فإن كل عنصر x في L يمكن أن يُعبَّر عنه على صورة $a/_L\ b$، حيث $a,b\in D$، فإن L هو الحقل $\psi[F]$ كما في برهان المبرهنة 6.21، وهو بهذا يماثل F. ♦

■ تمارين 21

حسابات

1. صف حقل خارج القسمة F للحلقة التامة الجزئية:

$$D = \{n + mi \mid n, m \in \mathbb{Z}\}$$

من $\mathbb{C}$. "صف" تعني اكتب عناصر $\mathbb{C}$ التي تصنع حقل خارج القسمة D في $\mathbb{C}$. (عناصر D تسمى الأعداد الصحيحة لجاوس).

2. صف (كما في التمرين 1) حقل خارج القسمة F للحلقة الجزئية التامة:

$D = \{n + m\sqrt{2} \mid n, m \in \mathbb{Z}\}$ في $\mathbb{R}$.

مفاهيم

3. صحّح تعريف المصطلح المكتوب بخط مائل دون الرجوع إلى الكتاب– إذا احتاج إلى تصحيح– بحيث يكون قابلًا للنشر.

حقل خارج القسمة للحلقة التامة D هو الحقل F، الذي يمكن إدخال D فيه، بحيث كل عنصر غير صفري من D هو عنصر وحدة في F.

4. ضع إشارة صح أو إشارة خطأ:

_____ أ. $\mathbb{Q}$ حقل خارج القسمة لـ $\mathbb{Z}$.

_____ ب. $\mathbb{R}$ حقل خارج القسمة لـ $\mathbb{Z}$.

_____ جـ. $\mathbb{R}$ حقل خارج القسمة لـ $\mathbb{R}$.

_____ د. $\mathbb{C}$ حقل خارج القسمة لـ $\mathbb{R}$.

_____ هـ. إذا كان D حقلاً، فإن أيّ حقل خارج قسمة على D يماثل D.

_____ و. حقيقة أنّ D لا يوجد فيه قواسم للصفر استخدمت بقوة مرات عدة في بناء حقل خارج القسمة F للحلقة التامة D.

_____ ز. كل عنصر في الحلقة التامة D، هو عنصر وحدة في حقل خارج القسمة F على D.

_____ ح. كل عنصر غير صفري في الحلقة التامة D، هو عنصر وحدة في حقل خارج القسمة F على D.

_____ ط. حقل خارج القسمة F' للحلقة التامة الجزئية D' من الحلقة التامة D يمكن أن يعدّ حقلًا جزئيًّا لحقل خارج القسمة على D.

ـــــــــــــــ ي. كل حقل خارج قسمة على $\mathbb{Z}$ يماثل $\mathbb{Q}$.

5. وضِّح بمثال أنّ حقل خارج القسمة F' على حلقة تامة جزئية فعليًّا D' من حلقة تامة D. يمكن أن يكون أيضًا حقل خارج القسمة على D.

براهين

6. أثبت الفرع الثاني للخطوة 3. يمكنك استخدام أيّ فرع سابق في الخطوة 3.

7. أثبت الفرع الثالث للخطوة 3. يمكنك استخدام أيّ فرع سابق في الخطوة 3.

8. أثبت الفرع الرابع للخطوة 3. يمكنك استخدام أيّ فرع سابق في الخطوة 3.

9. أثبت الفرع الخامس للخطوة 3. يمكنك استخدام أيّ فرع سابق في الخطوة 3.

10. أثبت الفرع السادس للخطوة 3. يمكنك استخدام أيّ فرع سابق في الخطوة 3.

11. أثبت الفرع السابع للخطوة 3. يمكنك استخدام أيّ فرع سابق في الخطوة 3

12. لتكن R حلقة إبدالية غير صفرية، ولتكن T مجموعة جزئية غير خالية من R مغلقة بالنسبة إلى الضرب، ولا تحوي الصفر ولا قواسم له. ابدأ بـ $T \times R$، وإلا اتبع بالضبط طريقة البناء في هذا الفصل، يمكننا أن نبين أنّ الحلقة R يمكن توسيعها إلى حلقة جزئية لخوارج القسمة (*Partial ring of quotients*) $Q(R, T)$، فكر في هذا مدة 15 دقيقة، أو راجع البناء؛ لترى أنّ الأمور ما زالت تعمل. بوجه خاص، وضح ما يأتي:

أ. $Q(R, T)$ يملك العنصر المحايد حتى لو أنّ R لا تملك.

ب. في $Q(R, T)$، كل عنصر غير صفري في T عنصر وحدة.

13. أثبت باستخدام تمرين **12** أنّ كلّ حلقة إبدالية غير صفرية تحوي عنصر a ليس من قواسم الصفر، يمكن توسيعها إلى حلقة إبدالية تحوي العنصر المحايد. قارنه بتمرين **30** في الفصل 19.

14. بالرجوع إلى تمرين **12**، ما عدد عناصر الحلقة $Q(\mathbb{Z}_4, \{1, 3\})$؟

15. بالرجوع إلى تمرين **12**، صف الحلقة $Q(\mathbb{Z}, \{2^n \mid n \in \mathbb{Z}^+\})$، عن طريق وصف حلقة جزئية من $\mathbb{R}$ تماثلها.

16. بالرجوع إلى تمرين **12**، صف الحلقة $Q(3\mathbb{Z}, \{6^n \mid n \in \mathbb{Z}^+\})$، عن طريق وصف حلقة جزئية من $\mathbb{R}$ تماثلها.

17. بالرجوع إلى تمرين **12**، افترض أننا أسقطنا شرط أنّ T لا توجد فيها قواسم للصفر، وأبقينا فقط على أن T ليست خالية، ولا تحوي 0، ومغلقة بالنسبة إلى الضرب، إذ إن محاولة توسيع R إلى حلقة إبدالية تحوي العنصر المحايد، بحيث كل عنصر غير صفري في T هو عنصروحدة، يجب أن تفشل إذا حوت T عنصرًا من قواسم الصفر؛ لأن قاسمًا للصفر لا يمكن أن يكون عنصر وحدة، حاول أن تكتشف أنه إذا بدأت بـ $T \times R$، فأين أول مشكلة ستقع لهذا البناء الموازي للبناء الذي في هذا الكتاب؟ بوجه خاص، لـ $R = \mathbb{Z}_6$ و$T = \{1, 2, 4\}$، وضّح أول صعوبة تظهر. [مساعدة: إنها في الخطوة 1].

الفصل 22 حلقات كثيرات الحدود Rings of Polynomials

كثيرات الحدود في غير معين

الكل يملك فكرة عملية عما تعنيه كثيرة حدود في x، حيث المعاملات من الحلقة R، ونستطيع أن نخمِّن كيف نجمع ونضرب كثيرات حدود، إضافة إلى أننا نعلم ما تعنيه درجة كثيرة حدود، ونتوقع أنّ المجموعة من كثيرات الحدود، حيث المعاملات من الحلقة R نفسها هي حلقة تحت عمليات الجمع والضرب الاعتيادية على كثيرات الحدود، و R حلقة جزئية من $R[x]$، وعلى الرغم من ذلك، سنتعامل مع كثيرات الحدود بطريقة مختلفة عن الأسلوب المتبع في الجبر في مرحلة الدراسة الثانوية أو في التفاضل والتكامل، إذ إنّ هناك أشياء قليلة نريد أن نقولها.

في المقام الأول، سنسمي x **غير معين** (***indeterminate***) بدلاً من متغير، افترض– على سبيل المثال– أنّ حلقة المعاملات $\mathbb{Z}$، وإحدى كثيرات الحدود في الحلقة $\mathbb{Z}[x]$ هي $1x$، التي سنكتبها ببساطة x، والآن، فإنّ x ليست 1 أو 2 أو أيّ عنصر آخر من $\mathbb{Z}[x]$؛ لذلك، من الآن فصاعدًا لن نكتب أشياء مثل "$x= 1$" أو "$x= 2$" كما كنا نفعل في مقررات دراسية أخرى، وسنسمي x غير معين بدلاً من متغير، كي نؤكد على هذا التغيير، كذلك لن نكتب تعبيرًا مثل "$x^2 -4= 0$"؛ لأنه ببساطة: $x^2 - 4$ ليس كثيرة الحدود الصفرية في حلقتنا $\mathbb{Z}[x]$، فنحن معتادون في الحديث عن "حلّ معادلة كثيرة حدود"، وسنمضي الكثير من الوقت فيما تبقى من كتابنا للحديث عن هذا الأمر، إلّا أننا سنشير إليه بـ "إيجاد صفر كثيرة الحدود".

نحاول باختصار أن نكون حريصين في مناقشتنا للتركيبات الجبرية، على ألا نقول في سياق ما: إن هناك أشياء متساوية، وفي سياق آخر: إنها غير متساوية.

■ **نبذة تاريخية**

كان استخدام x وحروف أخرى من نهاية الأحرف الهجائية لتمثل غير المعين من خلال رينيه ديكارت **(Rene'Descartes 1596- 1650)**، وقبل ذلك استخدم فرانشيوس فايت **(Francios Viete 1540- 1603)** أحرف العلَّة لغير المعينات والأحرف الساكنة للكميات المعلومة، فقد كان ديكارت مسؤولاً عن أول ظهور لمبرهنة العامل (نتيجة 3.23) في بحثه "الهندسة" **(The Geometry)**، الذي نشر بوصفه ملحقًا في كتابه **(Discourse on Method) (1637)**، وقد حوى هذا العمل أيضًا أول ظهور لمفاهيم الهندسة التحليلية؛ حيث أوضح ديكارت كيف يمكن وصف المنحنيات الهندسية جبريًّا.

ولد ديكارت لعائلة غنية في لاهاي في فرنسا؛ ولأن صحّته كانت دائمًا غير مستقرة، أصبحت عنده عادة أن يمضي نهاره في السرير، في هذه الأوقات أنهى معظم عمله الخصب .**(Discourse on Method)** وهي محاولة منه لإظهار الإجراءات المميزة لـ "البحث عن الحقيقة في العلوم"، كانت الخطوة الأولى في هذا العمل، رفض كل شيء فيه قليل من الشك وعدّه خطأً مطلقًا، ولكن لأنه من الضروري أنَّ من يفكِّر هو "شيء"، فقد وضع المبدأ الأول في الفلسفة: "أنا أفكر إذن أنا موجود"، وأهم الأجزاء التي تمّ تسليط الضوء عليها في كتابه **(Discourse on Method)** كانت ثلاثة ملاحق، هي : البصريات، والهندسة، وعلم الأحوال الجوية، وفي الواقع قدّم ديكارت في هذه الملاحق أمثلة على كيفية تطبيقه لطريقته.

ومن أهم الأفكار التي اكتشفها ديكارت في عمله ونشرها: قانون الجيب لانعكاس الضوء، وأسس مبرهنة المعادلات، والتفسير الهندسي لقوس المطر.

دُعيَ ديكارت إلى ستوكهولم عام 1649م من قبل كرستينا ملكة السويد؛ لتعليمها، ولسوء الطالع، طلبت منه الملكة أن يصحو في ساعات الصباح الباكر، وذلك عكس عادته القديمة المتأصلة معه، ثمّ أُصيب بعدها بوقت قصير بمرض ذات الرئة، وتوفي عام 1650م.

إذا كان هناك شخص لا يعلم شيئًا عن كثيرات الحدود، فليس بالأمر السهل وصف طبيعة كثيرة حدود في x بدقة، حيث المعاملات من الحلقة R، فإذا عرّفنا كثيرة حدود بالمجموع الشكلي المنتهي (*Finite Formal Sum*)

$$\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$$

حيث $a_i \in R$، فإننا نضع أنفسنا في مشكلة بسيطة، بالتأكيد $a_1 x + 0$ و$0 + a_1 x + 0\, x^2$ مختلفان بالمجموع الشكلي، ولكننا سنعدّهما كثيرة الحدود نفسها. الحل العملي لهذه المشكلة يكمن في تعريف كثيرة الحدود بالمجموع الشكلي اللانهائي (*infinite formal Sum*)

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + \ldots,$$

حيث كل $a_i = 0$ عدا عدد منتهٍ من قيم i، لا مشكلة الآن بوجود أكثر من مجموع شكلي يمثل كثيرة حدود واحدة.

1.22 تعريف لتكن R حلقة، تُعرّف كثيرة الحدود **(polynomial)** $f(x)$ حيث المعاملات من R على أنها المجموع الشكلي اللانهائي

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + \ldots,$$

حيث $a_i \in R$، وكل $a_i = 0$ عدا عدد منته من قيم i. a_i هي **معاملات (coefficients)** $f(x)$، فإذا كان لبعض $i \geq 0$ صحيح أنه $a_i \neq 0$، فإنّ أكبر قيمة i لها هذه الخاصية تسمى درجة **(degree)** $f(x)$، وإذا كان كل $a_i = 0$، فإن درجة $f(x)$ غير معرفة[1]. ■

ولتبسيط العمل مع كثيرات الحدود، نفترض أنه إذا كانت $f(x)=a_0+a_1x+\ldots+a_nx^n+\ldots$ فيها $a_i=0$ لـ $i > n$، فيمكننا أن نرمز لـ $f(x)$ بـ $a_0 + a_1 x + \ldots + a_n x^n$، كذلك إذا وجد في R عنصر محايد $1 \neq 0$، فسنكتب الحدّ $1x^K$ في أيّ مجموع على الشكل x^K، على سبيل المثال: في $\mathbb{Z}[x]$ سنكتب كثيرة الحدود $1x + 2$ بـ $x+2$. أخيرًا، سنوافق على أنه يمكننا حذف $0x^i$ أو a_0 إذا كان $a_0 = 0$ من المجموع الشكلي، ولكن ليس كل $a_i = 0$؛ لذلك، 0، 2، x و x^2+2 هي كثيرات حدود معاملاتها من $\mathbb{Z}$. أي عنصر في R هو كثيرة حدود ثابتة.

الجمع والضرب على كثيرات الحدود التي معاملاتها من الحلقة R معرفة بطريقة مألوفة لدينا، إذا كان:

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$$

و

$$g(x) = b_0 + b_1 x + \ldots + b_n x^n + \ldots,$$

فإن جمع كثيرات الحدود هو:

[1] تعرف درجة كثيرة الحدود الصفرية في بعض الأحيان بـ -1، وهو أول عدد صحيح أقل من 0، أو تعرف بـ $-\infty$ لذلك، فإن درجة $f(x)$ و $g(x)$ ستكون مجموع رتب $f(x)$ و $g(x)$ إذا كان أحدهما صفرًا.

$f(x)+g(x)=c_0+c_1x+\ldots+c_nx^n+\ldots$، حيث $c_n=a_n+b_n$،

وضرب كثيرات الحدود هو:

$f(x)g(x)=d_0+d_1x+\ldots+d_nx^n+\ldots$، حيث $d_n=\sum_{i=0}^{n}a_ib_{n-i}$.

لاحظ أنَّ c_i و d_i كلاهما صفر، إلا لعدد منتهٍ من قيم i؛ لذلك، فإن كلا التعريفين لهما معنى، ولاحظ أن $\sum_{i=0}^{n}a_ib_{n-i}$ ممكن ألا يساوي $\sum_{i=0}^{n}b_ia_{n-i}$ ، إذا كانت R غير إبدالية،

وباستخدام تعريفي الجمع والضرب سيكون عندنا المبرهنة الآتية:

2.22 مبرهنة المجموعة $R[x]$ من كثيرات الحدود في غير المعين x، والمعاملات من الحلقة R هي حلقة تحت جمع وضرب كثيرات الحدود، إذا كانت R إبدالية، فإن $R[x]$ كذلك، وإذا كانت R تحوي العنصر المحايد $1\neq 0$، فإن 1 هو العنصر المحايد في $R[x]$.

البرهان من الواضح أنّ $\langle R[x],+\rangle$ زمرة إبدالية، وكذلك فإن قانون التجميع على عملية الضرب وقانوني التوزيع مباشران، ولكن الحسابات مرهقة بعض الشيء، حيث سنوضح بتقديم برهان قانون التجميع.

بتطبيق مسلمات الحلقة على $a_i,b_j,c_k\in R$ نحصل على:

$$\begin{aligned}
\left[\left(\sum_{i=0}^{\infty}a_ix^i\right)\left(\sum_{j=0}^{\infty}b_jx^j\right)\right]\left(\sum_{k=0}^{\infty}c_kx^k\right)&=\left[\sum_{n=0}^{\infty}\left(\sum_{i=0}^{n}a_ib_{n-i}\right)x^n\right]\left(\sum_{k=0}^{\infty}c_kx^k\right)\\
&=\sum_{s=0}^{\infty}\left[\sum_{n=0}^{s}\left(\sum_{i=0}^{n}a_ib_{n-i}\right)c_{s-n}\right]x^s\\
&=\sum_{s=0}^{\infty}\left(\sum_{i+j+k=s}a_ib_jc_k\right)x^s\\
&=\sum_{s=0}^{\infty}\left[\sum_{m=0}^{s}a_{s-m}\left(\sum_{j=0}^{m}b_jc_{m-j}\right)\right]x^s\\
&=\left(\sum_{i=0}^{\infty}a_ix^i\right)\left[\sum_{m=0}^{\infty}\left(\sum_{j=0}^{m}b_jc_{m-j}\right)x^m\right]\\
&=\left(\sum_{i=0}^{\infty}a_ix^i\right)\left[\left(\sum_{j=0}^{\infty}b_jx^j\right)\left(\sum_{k=0}^{\infty}c_kx^k\right)\right]
\end{aligned}$$

التعبير الرابع له علامتا جمع، ويجب أن يرمز لقيمة حاصل الضرب الثلاثي $f(x)g(x)h(x)$ لكثيرات الحدود هذه مع الضرب التجميعي. (بالأسلوب نفسه نرمز لـ $f(g(h(x)))$ بقيمة التركيب التجميعي $(f \circ g \circ h)(x)$ للدوال الثلاث f، g وh).

يمكن إثبات قانوني التوزيع بصورة مشابهة (انظر تمرين 26).

أوضحت الملاحظات التي سبقت نص المبرهنة أنّ $R[x]$ حلقة إبدالية إذا كانت R إبدالية، والعنصر المحايد $1 \neq 0$ في R هو العنصر المحايد لـ $R[x]$، من خلال تعريف الضرب على $R[x]$. ♦

لذلك، فإن $\mathbb{Z}[x]$ هي حلقة كثيرات الحدود لغير المعين x، حيث المعاملات صحيحة، $\mathbb{Q}[x]$ هي حلقة كثيرات الحدود في x، حيث المعاملات نسبية، وهكذا.

مثال 3.22 في $\mathbb{Z}_2[x]$ لدينا:

$$(x+1)^2 = (x+1)(x+1) = x^2 + (1+1)x + 1 = x^2 + 1$$

ما زلنا نعمل في $\mathbb{Z}_2[x]$، نجد أن:

$$(x+1)+(x+1) = (1+1)x + (1+1) = 0x + 0 = 0. \quad \blacktriangle$$

إذا كانت R حلقة وx وy غير معينين، فإنه يمكن تشكيل الحلقة $(R[x])[y]$، وهي حلقة كثيرات الحدود في y والمعاملات كثيرات الحدود في x، وكل كثيرة حدود في y حيث معاملاتها كثيرات حدود في x، يمكن إعادة كتابتها بطريقة طبيعية لتكون كثيرة حدود في x، حيث معاملاتها كثيرات حدود في y كما يوضح تمرين 20، هذا يؤدي إلى أنّ $(R[x])[y]$ تماثل طبيعي $(R[y])[x]$ على الرغم من أنّ الإثبات الدقيق ممل.

سوف نعرف هاتين الحلقتين باستخدام التماثل الطبيعي بينهما، وسوف نعبر عن الحلقة $R[x, y]$ بحلقة كثيرات الحدود بغير المعنيين x وy والمعاملات من R.

الحلقة $R[x_1, \cdots, x_n]$ لكثيرات الحدود في n من غير المعينات x_i والمعاملات من R تعرف بصورة مشابهة.

سنترك لتمرين 24 إثبات أنه إذا كانت D حلقة تامة، فإن $D[x]$ حلقة تامة، وبوجه خاص، إذا كان F حقلاً، فإن $F[x]$ حلقة تامة، لاحظ أنّ $F[x]$ ليس حقلاً؛ لأن x ليس عنصر وحدة في $F[x]$، أي إنه لا توجد كثيرة حدود $f(x) \in F[x]$، حيث $xf(x) = 1$، وباستخدام المبرهنة 21.5 يمكن تركيب حقل خارج القسمة $F(x)$ لـ $F[x]$ فأي عنصر في $F[x]$ يمكن أن يُعبّر عنه بخارج القسمة $f(x)/g(x)$ لكثيرتي حدود في $F[x]$، حيث $g(x) \neq 0$، وبصورة مشابهة نعرف $F(x_1, \ldots, x_n)$ ليكون حقل خارج القسمة لـ $F[x_1, \ldots, x_n]$، هذا الحقل $F(x_1, \ldots, x_n)$ هو حقل الدوال النسبية في n من غير المعينات على F. ولهذه الحقول وظيفة مهمة في الهندسة الجبرية.

تشاكلات التعويض

نحن الآن مستعدون لمواصلة توضيح كيفية استخدام التشاكلات في دراسة ما نشير إليها دائمًا باسم (معادلة كثيرة حدود)، لتكن E وF حقولاً، حيث F حقل جزئي من E، أي إن $F \leq E$، وتؤكد المبرهنة المقبلة توافر تشاكلات مهمة من $F[x]$ إلى E، التي ستكون أدوات أساسية لأكثر ما تبقى من هذا العمل.

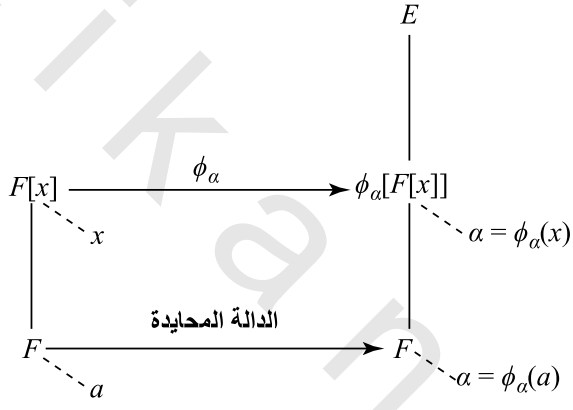
4.22 مبرهنة (**التشاكلات التعويضية لمبرهنة الحقول**): ليكن F حقلًا جزئيًّا من E، وليكن α عنصرًا في E، وx غير معين. الدالة $\phi_\alpha : F[x] \to E$ معرفة بـ

$$\phi_\alpha\left(a_0 + a_1x + \cdots + a_nx^n\right) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

حيث $(a_0 + a_1x + \cdots + a_nx^n) \in F[x]$ هي تشاكل من $F[x]$ إلى E. كذلك $\phi_\alpha(a) = a$ و ϕ_α ينقل F تماثليًّا بالدالة المحايدة، أي إنّ $\phi_\alpha(a) = a$ لكل $a \in F$. التشاكل ϕ_α هو تعويض لـ α.

البرهان الحقل الجزئي والمخطط الدالي في شكل5.22 قد يساعدنا على استيضاح هذا الوضع.

الخطوط المتقطعة التي تشير إلى عنصر في المجموعة المبرهنة هي استنتاج مباشر



الشكل 5.22

لتعريفاتنا للجمع والضرب على $F[x]$، والدالة ϕ_α حسنة التعريف، أي إنها لا تعتمد على تمثيلنا لـ $f(x) \in F[x]$ بالمجموع المنتهي

$$a_0 + a_1x + \ldots + a_nx^n$$

لأن المجموع المنتهي الذي يمثل $f(x)$ يمكن تغييره فقط بإضافة الحدود $0x^i$ أو إلغائها، التي تؤثر في قيمة $\phi_\alpha(f(x))$.

إذا: $f(x) = a_0 + a_1x + \ldots + a_nx^n, g(x) = b_0 + b_1x + \ldots + b_mx^m$،

و $h(x) = f(x) + g(x) = c_0 + c_1x + \cdots + c_rx^r$،

فإن:

$$\phi_\alpha(f(x)+g(x)) = \phi_\alpha(h(x)) = c_0 + c_1\alpha + \cdots + c_r\alpha^r$$

بينما:

$$\phi_\alpha(f(x)) + \phi_\alpha(g(x)) = \left(a_0 + a_1\alpha + \cdots + a_n\alpha^n\right) + \left(b_0 + b_1\alpha + \cdots + b_m\alpha^m\right).$$

باستخدام تعريف الجمع على كثيرات الحدود فإن $c_i = a_i + b_i$، نرى أنَّ:

$$\phi_\alpha(f(x)+g(x)) = \phi_\alpha(f(x)) + \phi_\alpha(g(x))$$

وبالرجوع إلى الضرب نرى أنه إذا

$$f(x)g(x) = d_0 + d_1x + \cdots + d_sx^s,$$

فإن:

$$\phi_\alpha(f(x)g(x)) = d_0 + d_1\alpha + \cdots + d_s\alpha^s,$$

بينما:

$$[\phi_\alpha(f(x))][\phi_\alpha(g(x))] = \left(a_0 + a_1\alpha + \cdots + \alpha_n\alpha^n\right)\left(b_0 + b_1\alpha + \cdots + b_m\alpha^m\right).$$

وباستخدام تعريف الضرب على كثيرات الحدود $d_j = \sum_{i=0}^{j} a_i b_{j-i}$، نرى أنَّ:

$$\phi_\alpha(f(x)g(x)) = [\phi_\alpha(f(x))][\phi_\alpha(g(x))].$$

لذلك ϕ_α تشاكل.

بتطبيق ϕ_α وكما هي معرفة على كثيرة الحدود الثابتة $a \in F[x]$ حيث $a \in F$، يعطي $\phi_\alpha(a) = a$؛ لذلك، ϕ_α تنقل F تماثليًّا بوصفها دالة محايدة، ومرة أخرى باستخدام تعريف ϕ_α، فإنّ:

$$\phi_\alpha(x) = \phi_\alpha(1x) = 1\alpha = \alpha.$$ ♦

نشير إلى أنّ هذه المبرهنة متحققة، وبالإثبات نفسه إذا كانت F و E فقط حلقتين إبداليتين مع توافر العنصر المحايد بدلاً من حقلين، ومع ذلك، سنهتم بصورة رئيسة في حالة أنهما حقلان.

من الصعب تأكيد أهمية هذه المبرهنة، فهي أساسية للأعمال المقبلة كلها في مبرهنة الحقول، وهي بسيطة جدًّا، بحيث يمكن تبرير تسميتها بملاحظة بدلاً من مبرهنة، وربما كان من الخطأ كتابة الإثبات؛ لأن صورة كثيرة الحدود تجعلها تبدو معقدة جدًّا، بحيث يمكن أن نعتقد بحماقة أنها مبرهنة صعبة.

6.22 مثال لتكن F هي $\mathbb{Q}$، و E هي $\mathbb{R}$ في المبرهنة 4.22، وليكن تشاكل التعويض

$\phi_0 : \mathbb{Q}[x] \to \mathbb{R}$ معرفًا بالقاعدة:

$$\phi_0(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_10 + \cdots + a_n0^n = a_0.$$

لذلك، كل كثيرة حدود تنتقل بصورة غامرة إلى الحد الثابت. ▲

7.22 مثال لتكن F هي $\mathbb{Q}$، و E هي $\mathbb{R}$ في المبرهنة 4.22، وليكن تشاكل التعويض $\phi_2 : \mathbb{Q}[x] \to \mathbb{R}$ معرفًا بالقاعدة:

$$\phi_2(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_12 + \cdots + a_n2^n.$$

لاحظ أن:

$$\phi_2(x^2 + x - 6) = 2^2 + 2 - 6 = 0.$$

لذلك، $x^2 + x - 6$ تقع في النواة N لـ ϕ_2، بالطبع:

$$x^2 + x - 6 = (x - 2)(x + 3)$$

وسبب أنّ $\phi_2(x^2 + x - 6) = 0$ هو $\phi_2(x - 2) = 2 - 2 = 0$ ▲

8.22 مثال لتكن F هي $\mathbb{Q}$، و E هي $\mathbb{C}$ في المبرهنة 4.22، وليكن تشاكل التعويض

$\phi_i : \mathbb{Q}[x] \to \mathbb{C}$. معرفًا بالقاعدة:

$$\phi_i(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1i + \cdots + a_ni^n$$

و $\phi_i(x) = i$، لاحظ أن:

$$\phi_i(x^2 + 1) = i^2 + 1 = 0,$$

لذلك، $x^2 + 1$ تقع في النواة N لـ ϕ_i. ▲

9.22 مثال لتكن F هي $\mathbb{Q}$ و E هي $\mathbb{R}$ في المبرهنة 4.22، وليكن تشاكل التعويض

$\phi_\pi : \mathbb{Q}[x] \to \mathbb{R}$ معرفًا بالقاعدة:

$$\phi_\pi(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\pi + \cdots + a_n\pi^n.$$

يمكن إثبات أنّ $a_0 + a_1\pi + \cdots + a_n\pi^n = 0$ إذا وفقط إذا كان $a_i = 0$ لـ $i = 0,1,\ldots,n$:

لذلك، فإن نواة ϕ_π هي $\{0\}$، و ϕ_π دالة واحد لواحد، وهذا يبين أن كثيرات الحدود كلها في π، ذات المعاملات النسبية تماثل حلقات إلى $\mathbb{Q}[x]$ بطريقة طبيعية، حيث $\phi_\pi(x) = \pi$. ▲

الطريقة الجديدة

نكمل العلاقة بين أفكارنا الجديدة والمفهوم الأساسي لحل معادلة كثيرة حدود، فبدلاً من الحديث عن حل معادلة كثيرة حدود، نستخدم التعبير "إيجاد صفر لكثيرة حدود".

10.22 تعريف ليكن F حقلًا جزئيًّا من الحقل E، و α عنصرًا في E، لتكن $\phi_\alpha : F[x] \to E$ تشاكل تعويض، كما في المبرهنة 4.22، ولتكن $f(\alpha)$ ترمز إلى:

$$\phi_\alpha(f(x)) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

إذا كان $f(\alpha) = 0$، فإن α **صفر (zero)** لـ $f(x)$ ■

باستخدام هذا التعريف، يمكننا أن نفسر المشكلة التقليدية لإيجاد الأعداد الحقيقية r كلها، حيث $r^2 + r - 6 = 0$ عن طريق فرض $F = \mathbb{Q}$ و $E = \mathbb{R}$، ثم إيجاد كل $\alpha \in \mathbb{R}$ حيث:

$$\phi_\alpha(x^2 + x - 6) = 0,$$

أي إنّ إيجاد أصفار $x^2 + x - 6$ كلها في $\mathbb{R}$، فكلتا المشكلتين لهما الجواب نفسه؛ لأن

$$\{\alpha \in \mathbb{R} \mid \phi_\alpha(x^2 + x - 6) = 0\} = \{r \in \mathbb{R} \mid r^2 + r - 6 = 0\} = \{2, -3\}.$$

يبدو أننا نجحنا فقط في جعل مشكلة بسيطة تبدو معقدة، وفي الحقيقة، فإنّ ما فعلناه هو أن نعبِّر عن المشكلة بلغة التحويلات، ويمكننا الآن استخدام ميكانيكية التحويل كلها التي طوّرناها، ثم نستمر في تطوير حلها.

هدفنا الأساس

سنواصل المحاولة لوضع عملنا المستقبلي في منظور معين، فالفصلان 26 و27 مترابطان في موضوعات حول مبرهنة الحلقات، ومشابهة للمادة عن زمر العامل والتشاكلات في مبرهنة الزمر، ومع ذلك، فإنّ هدفنا في تطوير هذه المفاهيم المشابهة للحلقات سيكون مختلفًا تمامًا عن هدفنا في مبرهنة الزمر، إذ استخدمنا في مبرهنة الزمر مفاهيم العامل والتشاكلات في دراسة بنية زمرة معطاة، وفي تحديد أنواع بنى الزمر ذات الرتبة المحددة التي يمكن توافرها، حيث سنتحدث عن التشاكلات وحلقات العامل في الفصل 26 وعيننا على إيجاد أصفار كثيرات الحدود، التي هي واحدة من أقدم المسائل وأكثرها جوهرية في الجبر، لنتحدث عن هذا الهدف في ضوء تاريخ الرياضيات، باستخدام لغة "حل معادلات كثيرة حدود" التي تعوّدنا عليها، سنبدأ بمدرسة فيثاغورس للرياضيات قرابة 525 قبل الميلاد، فقد اشتغل الفيثاغوريون على افتراض أنّ المسافات جميعها **قابلة للقياس**؛ أي إنه إذا أُعطينا مسافتين a و b، فتوجد وحدة مسافة u وعددان صحيحان n و m، بحيث $a = (n)(u)$ و $b = (m)(u)$، فقد ذكروا بمفهوم الأعداد وفي اعتقادهم، أنَّ الأعداد كلها أرقام صحيحة؛ لأنَّ u وحدة مسافة واحدة.

فكرة أنّ كل شيء قابل للقياس يمكن إرجاعها إلى فكرتنا، وهي تنص على أنّ الأعداد كلها أعداد نسبية، فمثلاً: إذا كان a و b عددين نسبيين، فإن كلًّا منهما هو مضاعف صحيح لمقلوب المضاعف المشترك الأصغر لمقاميهما، على سبيل المثال: $a = \frac{7}{12}$ و $b = \frac{19}{15}$، فإن $a = (35)(\frac{1}{60})$ و $b = (76)(\frac{1}{60})$.

عرف الفيثاغوريون، بالطبع، ما يسمى الآن مبرهنة فيثاغورس، أي إنَّه لأيّ مثلث قائم، حيث ضلعاه أطوالهما a و b والوتر طوله c، فإن

$$a^2 + b^2 = c^2.$$

هم أيضًا مَن امتلك حق إيجاد قيمة الوتر لمثلث قائم الزاوية فيه ضلعان متساويان في الطول، لنقل: كلٌّ منهما طوله وحدة واحدة، سيكون طول الوتر لهذا المثلث كما نعلم $\sqrt{2}$، فتخيل بعدها رعبهم وفزعهم عندما يأتي واحد من مجتمعهم – طبقًا لبعض القصص هو فيثاغورس نفسه – بالحقيقة المدهشة التي نصّها طبقًا لمصطلحنا في المبرهنة الآتية:

11.22 مبرهنة كثيرة الحدود $x^2 - 2$ ليس لها أصفار في مجموعة الأعداد النسبية، أي إنَّ $\sqrt{2}$ ليس عددًا نسبيًّا.

البرهان افترض أنّ $\frac{m}{n}$ حيث $m, n \in \mathbb{Z}$ عدد نسبي بأبسط صورة، وأن $\left(\frac{m}{n}\right)^2 = 2$، عندئذ،

$$m^2 = 2n^2،$$

حيث m^2 و $2n^2$ عددان صحيحان؛ فلأن m^2 و $2n^2$ هما العدد الصحيح نفسه؛ ولأنّ 2 هو عامل لـ n^2 2، نرى أنّ 2 يجب أن يكون أحد عوامل m^2، لكن بوصفه مربعًا كاملًا، فإنّ عوامل m^2 هي عوامل m مكررة مرتين؛ لذلك، m^2 يجب أن تملك مرتين العامل 2، إذن $2n^2$ لها العامل 2 مرتين؛ ولذلك، n^2 تملك العامل 2، وعليه، فإنّ n لها العامل 2. استنتجنا من $m^2 = 2n^2$ أن كلاً من m و n قابل للقسمة على 2، وهذا يناقض الحقيقة أنّ الكسر $\frac{m}{n}$ في أبسط صورة؛ لذلك، فإنّ

$$\left(\frac{m}{n}\right)^2 \neq 2 \text{ لأيّ } m, n \in \mathbb{Z}.$$

♦

لذلك سار الفيثاغوريون في الطريق الصحيح نحو السؤال عن حل معادلة كثيرة الحدود $x^2 - 2 = 0$. نحيل الطالب إلى (Shanks) [36، وحدة 3] لأخذ المحبوب والمبهج في معضلة فيثاغوريس وأهميتها في الرياضيات.

■ **نبذة تاريخية**

حلّ معادلات كثيرة حدود كان هدف علماء الرياضيات منذ قرابة 4000 عام، فقد طوّر البابليون نماذج من التركيبات التربيعية لحلّ معادلات تربيعية، على سبيل المثال: لحلّ المعادلة $x^2 - x = 870$، شجع المؤلف البابلي طلابه على أخذ نصف $1\left(\frac{1}{2}\right)$ وتربيعه $\left(\frac{1}{4}\right)$ وإضافته إلى 870، فالجذر التربيعي لـ $870\frac{1}{4}$ الذي هو $29\frac{1}{2}$، يضاف إلى $\frac{1}{2}$ للحصول على 30 بوصفه جوابًا، ما لم يناقشه المؤلف كان: ماذا نفعل إذا كان الجذر التربيعي في هذه العملية ليس عددًا نسبيًّا؟

اكتشف علماء الرياضيات الصينيون، منذ قرابة 200 قبل الميلاد، طريقة مشابهة لما تسمى الآن طريقة هورنر في حل المعادلات التربيعية بالطرق العددية؛ لأنهم استخدموا النظام العشري، فقد كان بإمكانهم باستخدام هذا المبدأ أن يصلوا بالحساب إلى أبعد ما يكون، متجاهلين التفريق بين الحلول النسبية وغير النسبية.

في الواقع وسّع الصينيون تقنيتهم العددية هذه لحلّ معادلات كثيرة حدود من رتب أعلى.

وفي العالم العربي، طوّر الشاعر الإيراني – عالم الرياضيات – عمر الخيام (1048 – 1131) طرقًا لحلّ معادلات تكعيبية هندسيًّا، عن طريق إيجاد نقاط التقاطع التقريبية للقطوع المخروطية المختارة، بينما استخدم شرف الدين الطوسي (توفي عام 1213م) تقنيات الحسبان؛ ليحدِّد ما إذا كان للمعادلة التكعيبية جذر حقيقي موجب أم لا، وقد كان الإيطالي جيرولامو كاردانو (Girolamo Cardano 1501 – 1576) أول من نشر إجراءً لحل معادلة تكعيبية جبريًّا.

من خلال **تعريفنا الممتع للزمرة**، علّقنا على أهمية توافر الأعداد السالبة، ما يعني أنّ المعادلات مثل $x + 2 = 0$ يمكن أن يكون لها حل، وقد سبّب تعريف الأعداد السالبة نوعًا محددًا من الرعب في الدوائر الفلسفية، إذ يمكننا تخيل تفاحة واحدة، وتفاحتين وحتى $\frac{13}{11}$ تفاحة، ولكن كيف نشير إلى شيء، ونقول: هذا 17- تفاحة؟

وأخيرًا، قادتنا المعادلة $x^2 + 1 = 0$ إلى تعريف العدد i، وأظهر الاسم "العدد التخيلي" الذي أُعطيَ لـ i كيف كانت النظرة لهذا العدد، فكثير من الطلاب حتى يومنا هذا يقودهم الاسم للنظر إلى i مع بعض من الشك، بينما قُدِّمت لنا الأعداد السالبة في مرحلة مبكرة من تطور الرياضيات، حيث قبلناها من غير سؤال.

أول ما تعرفنا كثيرات الحدود في جبر المرحلة الثانوية للمبتدئين، كان السؤال الأول وقتها: كيف نتعلم الجمع، والضرب والتحليل إلى عوامل كثيرات حدود؟ وبعدها في الجبر للمبتدئين والكتاب الثاني في الجبر للمرحلة الثانوية، فقد ركز بشدة على حلّ معادلات كثيرة حدود، وهذه الموضوعات بالضبط التي ستكون موضع اهتمامنا، إذ إنّ الفرق في أنّنا ركزنا في المرحلة الثانوية على كثيرات الحدود التي معاملاتها أعداد حقيقية، وسنعمل على كثيرات الحدود التي معاملاتها من أيّ حقل.

وحيث إننا طوّرنا آلية التشاكلات وحلقات العامل في الفصل 26، فسوف نوظفها مع هدفنا الأساسي؛ لنبين أنه لأيّ كثيرة حدود معطاة من الدرجة ≤ 1، حيث معاملاتها من أيّ حقل، يمكن إيجاد صفر لكثيرة الحدود هذه في حقل ما يحوي الحقل المعطى، وبعد تطوير هذه الآلية في الفصلين 26 و 27، فسيكون إنجاز هذا الهدف سهلاً جدًّا، وفي الحقيقة سيكون تحفة رائعة من الرياضيات، وإذا عدنا بتفكيرنا إلى التاريخ، فسنجد أنه ذروة أكثر من 2000 عام من المساعي الرياضية للعمل على معادلات كثيرات الحدود.

بعد إنجاز هدفنا الأساسي، سنقضي ما تبقى من وقتنا في دراسة طبيعة هذه الحلول لمعادلات كثيرات الحدود، إذ لا يجب علينا الخوف من الخوض في هذا الأمر، فقد تعاملنا مع موضوعات مشابهة في الجبر للمرحلة الثانوية، وهذا العمل سيكون طبيعيًّا أكثر من مبرهنة الزمر.

ختامًا، نشير إلى أنّ آلية حلقات العامل والتشاكلات الحلقية ليست ضرورية لنا لإنجاز هدفنا الأساسي، وللإثبات المباشر انظر Artin [27, p.29]. مع ذلك، حلقات العامل والتشاكلات الحلقية هي أفكار أساسية يجب أن نتمسك بها، ثم سيتبعها هدفنا الأساسي بسهولة عند دراستها.

■ تمارين 22

حسابات

في التمارين 1 إلى 4، أوجد حاصل جمع وضرب كثيرات الحدود المعطاة في حلقة كثيرة الحدود المعطاة:

1. $f(x) = 4x - 5$، $g(x) = 2x^2 - 4x + 2$ في $\mathbb{Z}_8[x]$.

2. $f(x) = x + 1$، $g(x) = x + 1$ في $\mathbb{Z}_2[x]$.

3. $f(x) = 2x^2 + 3x + 4$، $g(x) = 3x^2 + 2x + 3$ في $\mathbb{Z}_6[x]$.

4. $f(x) = 2x^3 + 4x^2 + 3x + 2$، $g(x) = 3x^4 + 2x + 4$ في $\mathbb{Z}_5[x]$.

5. ما عدد كثيرات الحدود من الدرجة ≥ 3 في $\mathbb{Z}_2[x]$؟ (يشمل 0).

6. ما عدد كثيرات الحدود من الدرجة ≥ 2 في $\mathbb{Z}_5[x]$؟ (يشمل 0).

في التمرينين 7 و 8، $F = E = \mathbb{C}$ في المبرهنة 4.22. احسب تشاكل التعويض الآتي:

7. $\phi_2(x^2 + 3)$

8. $\phi_i(2x^3 - x^2 + 3x + 2)$

في التمارين 9 إلى 11، $F = E = \mathbb{Z}_7$ في المبرهنة 4.22. احسب تشاكل التعويض الآتي:

9. $\phi_3[(x^4 + 2x)(x^3 - 3x^2 + 3)]$

10. $\phi_5[(x^3 + 2)(4x^2 + 3)(x^7 + 3x^2 + 1)]$

11. $\phi_4(3x^{106} + 5x^{99} + 2x^{53})$ [مساعدة: استخدم مبرهنة فيرما].

في التمارين 12 إلى 15، أوجد الأصفار جميعها في الحقل المنتهي المعطى لكثيرة الحدود المعطاة، التي معاملاتها تنتمي إلى ذلك الحقل. [مساعدة: إحدى الطرق هي ببساطة تجربة جميع القيم الممكنة!].

12. $x^2 + 1$ في $\mathbb{Z}_2$ **13.** $x^3 + 2x + 2$ في $\mathbb{Z}_7$

14. $x^5 + 3x^3 + x^2 + 2x$ في $\mathbb{Z}_5$

15. $f(x)\,g(x)$ حيث $f(x) = x^3 + 2x^2 + 5$ و $g(x) = 3x^2 + 2x$ في $\mathbb{Z}_7$

16. لتكن $\phi_a : \mathbb{Z}_5[x] \to \mathbb{Z}_5$ تشاكل تعويض كما في المبرهنة 4.22. استخدم مبرهنة فيرما لحساب $\phi_3(x^{231} + 3x^{117} - 2x^{53} + 1)$

17. استخدم مبرهنة فيرما لحساب الأصفار جميعها لكثيرة الحدود في الحقل $\mathbb{Z}_5$:

$$2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}$$

مفاهيم

في التمرينين 18 و19، صحّح تعريف الحدّ المكتوب بخط مائل دون الرجوع إلى الكتاب –إن كانت هناك حاجة للتصحيح – بحيث يكون بصيغة قابلة للنشر.

18. كثيرة الحدود التي معاملاتها من الحلقة R هو المجموع الشكلي اللانهائي:

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

حيث $a_i \in R$ لـ $i = 0,1,2,\ldots$.

19. ليكن F حقلًا، ولتكن $f(x) \in F[x]$، وصفر $f(x)$ هو $\alpha \in F$ بحيث $\phi_\alpha(f(x)) = 0$، و $\phi_\alpha : F(x) \to F$ تشاكل التعويض الذي ينقل x إلى α.

20. ليكن العنصر

$$f(x, y) = (3x^3 + 2x)y^3 + (x^2 - 6x + 1)y^2 + (x^4 - 2x)y + (x^4 - 3x^2 + 2)$$

في $(\mathbb{Q}[x])[y]$. اكتب $f(x,y)$، بوصفه عنصرًا في $(\mathbb{Q}[y])[x]$.

21. ليكن تشاكل التعويض $\phi_5 : \mathbb{Q}[x] \to \mathbb{R}$. أوجد ستة عناصر في نواة التشاكل ϕ_5

22. أوجد كثيرة حدود من درجة > 0 في $\mathbb{Z}_4[x]$، بحيث تكون عنصر وحدة.

23. ضع إشارة صح أو إشارة خطأ:

_____ أ. كثيرة الحدود $(a_n x^n + \cdots + a_1 x + a_0) \in R[x]$ هي 0، إذا وفقط إذا كان $a_i = 0$ لـ $i = 0,1,..,n$.

ب. إذا كانت R حلقة إبدالية، فإنّ $R[x]$ إبدالية.

جـ. إذا كانت D حلقة تامة، فإنّ $D[x]$ حلقة تامة.

د. إذا كانت R حلقة تحوي قواسم للصفر، فإنّ $R[x]$ تحوي قواسم للصفر.

هـ. إذا كانت R حلقة و $f(x)$ و $g(x)$ في $R[x]$ من الدرجتين 3 و 4 على الترتيب، فإنّ $f(x)\,g(x)$ يمكن أن تكون من الرتبة 8 في $R[x]$.

و. إذا كانت R أيّ حلقة و $f(x)$ و $g(x)$ في $R[x]$ من الدرجتين 3 و 4 على الترتيب، فإنّ $f(x)\,g(x)$ دائمًا من الدرجة 7.

ز. إذا كان F حقلًا جزئيًّا من E و $\alpha \in E$ هو صفر لـ $f(x) \in F[x]$، فإنّ α صفر لـ $h(x) = f(x)\,g(x)$ لكل $g(x) \in F[x]$.

ح. إذا كان F حقلاً، فإنّ عناصر الوحدة في $F[x]$ هي بالضبط عناصر الوحدة في F.

ط. إذا كانت R حلقة، فإنّ x ليس قاسمًا للصفر في $R[x]$.

ي. إذا كانت R حلقة، فإن قواسم الصفر في $R[x]$ هي بالضبط قواسم الصفر في R.

براهين

24. أثبت أنه إذا كانت D حلقة تامة، فإنّ $D[x]$ حلقة تامة.

25. لتكن D حلقة تامة و x غير معين.

أ. صف عناصر الوحدة في $D[x]$.

ب. أوجد عناصر الوحدة في $\mathbb{Z}[x]$.

جـ. أوجد عناصر الوحدة في $\mathbb{Z}_7[x]$.

26. أثبت قانون التوزيع من اليسار لـ $R[x]$، حيث R حلقة و x غير معين.

27. ليكن F حقلًا مميزه صفر، ولتكن D دالة الاشتقاق لكثيرة الحدود المكونة، حيث:

$$D(a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) = a_1 + 2.a_2x + \ldots + n.a_nx^{n-1}$$

أ. بيّن أنّ $D : F[x] \to F[x]$ هي تشاكل زمر من $\langle F[x], + \rangle$ إلى نفسها. هل D تشاكل حلقات؟

ب. أوجد نواة D.

جـ. أوجد صورة $F[x]$ تحت D.

28. ليكن F حقلًا جزئيًّا من الحقل E.

أ. عرّف تشاكل التعويض

$\phi_{a_1,\ldots a_n} : F[x_1,\ldots,x_n] \to E$ حيث $\alpha_1 \in E$

طبقًا لما ورد في مبرهنة 4.22.

ب. إذا كان $E = F = \mathbb{Q}$. احسب $\phi_{-3,2}(x_1^2 x_2^3 + 3x_1^4 x_2)$

جـ. عرّف المفهوم صفر كثيرة الحدود $f(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$ بطريقة مشابهة للتعريف في الكتاب لـ صفر $f(x)$.

29. لتكن R حلقة، وR^R هي مجموعة الدوال كلها التي تنقل R إلى R.

لـ $\phi, \psi \in R^R$، عرّف الجمع $\phi + \psi$ بـ

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

والضرب $\phi.\psi$ بـ

$$(\phi.\psi)(r) = \phi(r)\psi(r)$$

لـ $r \in R$، لاحظ أنّ (.) ليست التركيب الدالي. بيِّن أنّ $\langle R^R, +, . \rangle$ حلقة.

30. بالرجوع إلى تمرين 29، ليكن F حقلًا، والعنصر ϕ في F^F هو **دالة كثيرة الحدود على** F، فإذا وجد $f(x) \in F[x]$، حيث $\phi(a) = f(a)$ لكل $a \in F$.

أ. بيّن أنّ المجموعة P_F لدوال كثيرة الحدود على F تشكل حلقة جزئية من F^F.

ب. بيّن أنّ الحلقة P_F لا تماثل بالضرورة $F[x]$. [مساعدة: بيّن أنه إذا كان F حقلًا منتهيًا، P_F و $F[x]$ ليس لهما العدد نفسه من العناصر].

31. ارجع إلى التمرينين 29 و 30 لإجابة الأسئلة الآتية:

أ. ما عدد العناصر في $\mathbb{Z}_2^{\mathbb{Z}_2}$ ؟ $\mathbb{Z}_3^{\mathbb{Z}_3}$ ؟

ب. صنّف $\langle +, \mathbb{Z}_2^{\mathbb{Z}_2} \rangle$ و$\langle +, \mathbb{Z}_3^{\mathbb{Z}_3} \rangle$ باستخدام المبرهنة 12.11، المبرهنة الأساسية للزمر الإبدالية منتهية التوليد.

جـ. بيّن أنه إذا كان F حقلًا منتهيًا، فإن $F^F = P_F$. [مساعدة: بالطبع $P_F \subseteq F^F$.

افترض أنّ عناصر F هي $a_1, \ldots, a_n$. لاحظ أنه إذا كان:

$$f_i(x) = c(x-a_1)\ldots(x-a_{i-1})(x-a_{i+1})\ldots(x-a_n),$$

فإنّ $f_i(a_j) = 0$ لـ $j \neq i$، وقيمة $f_i(a_i)$ يُتَحكَّمْ فيها باختيار $c \in F$. استخدم هذا لتبين أن كل دالة على F هي دالة كثيرة الحدود].

الفصل 23 تحليل كثيرات الحدود على حقل Factorization of Polynominls over a Field

تذكر أننا مهتمون في إيجاد أصفار كثيرات الحدود، ليكن F و E حقلين بحيث $F \leq E$، وافترض أنّ $f(x) \in F[x]$ تتحلل في $F[x]$، بحيث $f(x) = g(x)\ h(x)$ لـ $g(x),\ h(x) \in F[x]$، ولتكن $a \in E$. والآن، بالنسبة إلى تشاكل التعويض ϕ_a، فإنّ:

$$f(\alpha) = \phi_\alpha(f(x)) = \phi_\alpha(g(x)h(x)) = \phi_\alpha(g(x))\phi_\alpha(h(x)) = g(\alpha)h(\alpha).$$

لذلك، إذا كان $a \in E$، فإنّ $f(a) = 0$، إذا وفقط إذا $g(a) = 0$ أو $h(a) = 0$. محاولة إيجاد صفر $f(x)$ تختصر إلى مسألة إيجاد صفر لأحد عوامل $f(x)$. هذا أحد أسباب أهمية دراسة تحليل كثيرات الحدود.

خوارزمية القسمة داخل $F[x]$

المبرهنة الآتية أداة أساسية لعملنا في هذا الفصل، لاحظ التشابه مع خوارزمية القسمة لـ $\mathbb{Z}$ المعطاة في المبرهنة 3.6، التي تمّ تفصيل أهميتها بإسهاب.

1.23 مبرهنة (**خوارزمية القسمة لـ $F[x]$**): لتكن

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

و

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0$$

كثيرتي حدود في $F[x]$، حيث a_n و b_m عنصران غير صفرين في F و $m > 0$.

عندئذ، توجد كثيرتا حدود وحيدتان $q(x)$ و $r(x)$ في $F[x]$، تحققان $f(x) = g(x)\ q(x) + r(x)$؛ حيث إما $r(x) = 0$ أو درجة $r(x)$ أقل من الدرجة m لـ $g(x)$.

البرهان لتكن المجموعة $S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$ إذا كانت $0 \in S$، فإنه يوجد $s(x) \in F[x]$، بحيث $f(x) - g(x)s(x) = 0$؛ لذلك، $f(x) = g(x)s(x)$؛ وبأخذ $q(x) = s(x)$ و $r(x) = 0$، نكون قد انتهينا، وإلاّ لتكن $r(x)$ عنصر ذو أصغر درجة في S. فإن

$$f(x) = g(x)q(x) + r(x)$$

لبعض $q(x) \in F[x]$. يجب علينا أن نبين أنّ درجة $r(x)$ أقل من m. افترض أنَّ:

$$r(x) = c_t x^t + c_{t-1}x^{t-1} + \ldots + c_0$$

حيث $c_j \in F$ و $c_t \neq 0$. إذا كانت $t \geq m$، فإنّ:

(1)

$$f(x) - q(x)g(x) - (c_t / b_m)x^{t-m} g(x) = r(x) - (c_t / b_m)x^{t-m} g(x)$$

وهذه الأخيرة ستكون على الصورة

$r(x)$- (حدود من درجة أقل + $c_t x^t$)

التي هي كثيرة حدود من درجة أقل من t، درجة $r(x)$، بينما كثيرة الحدود في المعادلة (1) يمكن كتابتها على صورة

$$f(x) - g(x)\left[q(x) + (c_t / b_m)x^{t-m} \right]$$

لذلك، هي في S وهذا يناقض حقيقة أنّ $r(x)$ اختيرت لتكون صاحبة أصغر درجة في S؛ ولذلك، فإنّ درجة $r(x)$ أقل من الدرجة m لـ $g(x)$. لإثبات الوحدانية، إذا كان:

$$f(x) = g(x)q_1(x) + r_1(x)$$

و

$$f(x) = g(x)q_2(x) + r_2(x),$$

فإنه بالطرح يكون لدينا:

$$g(x)\left[q_1(x) - q_2(x)\right] = r_2(x) - r_1(x)$$

لأنه إما $r_2(x)$- $r_1(x)$ =0 أو درجة $r_2(x) - r_1(x)$ أقل من درجة $g(x)$، فإنها تتحقق فقط إذا كان $q_1(x)$- $q_2(x)$= 0 ؛ لذلك $q_1(x) = q_2(x)$. وعليه، يجب أن يكون عندنا $r_2(x)$- $r_1(x)$= 0، أي $r_1(x) = r_2(x)$. ♦

يمكننا حساب كثيرات الحدود $q(x)$ و$r(x)$ في المبرهنة 1.23 باستخدام القسمة الطويلة، كما كنا نقسم كثيرات حدود في $\mathbb{R}[x]$ في المرحلة الثانوية.

2.23 مثال لنعمل على كثيرات حدود في $\mathbb{Z}_5[x]$، ونقسم

$$f(x) = x^4 - 3x^3 + 2x^3 + 4x - 1$$

على $g(x)$= x^2- 2x +3 ؛ لإيجاد $q(x)$ و $r(x)$ في المبرهنة 1.23، القسمة المطوَّلة سهلة المتابعة، ولكن تذكر أننا في $\mathbb{Z}_5[x]$، حيث على سبيل المثال: $4x - (-3x) = 2x$

$$
\begin{array}{r|l}
 & x^2 - x - 3 \\
\hline
x^2 - 2x + 3 & x^4 - 3x^3 + 2x^2 + 4x - 1 \\
 & \underline{x^4 - 2x^3 + 3x^2} \\
 & \quad - x^3 - x^2 + 4x \\
 & \quad \underline{- x^3 + 2x^2 - 3x} \\
 & \qquad - 3x^2 + 2x - 1 \\
 & \qquad \underline{- 3x^2 + x - 4} \\
 & \qquad\quad x + 3
\end{array}
$$

لذلك:

$$q(x) = x^2 - x - 3 \quad \text{و} \quad r(x) = x + 3$$ ▲

3.23 نتيجة (**مبرهنة العامل**): العنصر $a \in F$ هو صفر $f(x) \in F[x]$، إذا وفقط إذا كان $x - a$ عاملًا لـ $f(x)$ في $F[x]$.

البرهان افترض أن $a \in F$ و $f(a) = 0$، باستخدام المبرهنة 1.23 يوجد $q(x), r(x) \in F[x]$، حيث:

$$f(x) = (x - a)q(x) + r(x)$$

إذ إما $r(x) = 0$ أو درجة $r(x)$ أقل من 1؛ لذلك، يجب أن يكون عندنا $r(x) = c$ لـ $c \in F$، وعليه، فإنّ:

$$f(x) = (x - a)q(x) + c$$

بتطبيق تشاكلنا التعويضي $\phi_a : F[x] \to F$ للمبرهنة 4.22 نجد:

$$0 = f(a) = 0q(a) + c$$

لذلك، يجب أن تكون $c = 0$. وعليه، فإنّ $f(x) = (x - a)\, q(x)$؛ ولذلك $x - a$ عامل لـ $f(x)$. وبالعكس، إذا كان $x - a$ عاملًا لـ $f(x)$ في $F[x]$، حيث $a \in F$، فإنّ تطبيق تشاكلنا التعويضي ϕ_a على $f(x) = (x-a)q(x)$ وبهذا نحصل على $f(a) = 0q(a) = 0$ ♦

4.23 مثال بالعمل مرة أخرى في $\mathbb{Z}_5[x]$، لاحظ أنّ 1 هو صفر لـ

$$(x^4 + 3x^3 + 2x + 4) \in \mathbb{Z}_5[x].$$

لذلك، باستخدام نتيجة 3.23 سنكون قادرين على تحليل $x^4 + 3x^3 + 2x + 4$ إلى

$(x\text{-}1)q(x)$ في $\mathbb{Z}_5[x]$. لنجد ناتج التحليل باستخدام القسمة المطولة.

$$\begin{array}{r|l} & x^3 + 4x^2 + 4x + 1 \\ \hline x - 1 & x^4 + 3x^3 + \quad 2x + 4 \\ & \underline{x^4 - x^3} \\ & \quad 4x^3 \\ & \quad \underline{4x^3 - 4x^2} \\ & \quad\quad 4x^2 + 2x \\ & \quad\quad \underline{4x^2 - 4x} \\ & \quad\quad\quad x + 4 \\ & \quad\quad\quad \underline{x - 1} \\ & \quad\quad\quad\quad 0 \end{array}$$

لذلك: $x^4+3x^3+2x+4=(x-1)(x^3+4x^2+4x+1)$ في $\mathbb{Z}_5[x]$ لأنه يمكن مشاهدة أنّ 1 صفر لـ x^3+4x^2+4x+1؛ لذلك، نستطيع أن نقسم كثيرة الحدود هذه على $x-1$ ونحصل على:

$$\begin{array}{r|l} & x^2 + 4 \\ \hline x - 1 & x^3 + 4x^2 + 4x + 1 \\ & \underline{x^3 - x^2} \\ & \quad 0 + 4x + 1 \\ & \quad\quad \underline{4x - 4} \\ & \quad\quad\quad 0 \end{array}$$

لأن 1 ما زال صفرًا لـ x^2+4، نستطيع أن نقسم مرة أخرى على $x-1$ ونحصل على:

$$\begin{array}{r|l} & x + 1 \\ \hline x - 1 & x^2 \quad + 4 \\ & \underline{x^2 - x} \\ & \quad\quad x + 4 \\ & \quad\quad \underline{x - 1} \\ & \quad\quad\quad 0 \end{array}$$

لذلك: $x^4+3x^3+2x+4=(x-1)^3(x+1)$ في $\mathbb{Z}_5[x]$. ▲

النتيجة المقبلة تبدو مشهورة.

5.23 نتيجة عدد أصفار كثيرة الحدود غير الصفرية $f(x) \in F[x]$ من الدرجة n، لا يزيد على n في الحقل F.

البرهان تبيّن النتيجة السابقة أنه إذا كان $a_1 \in F$ صفرًا لـ $f(x)$، فإنَّ:

$$f(x) = (x - a_1)q_1(x)$$

حيث بالطبع، درجة $q_1(x)$ هي n- 1، والصفر $a_2 \in F$ لـ $q_1(x)$ يؤدي إلى التحليل

$$f(x) = (x - a_1)(x - a_2)q_2(x).$$

بالاستمرار في هذه الطريقة، نصل إلى:

$$f(x) = (x - a_1)...(x - a_r)q_r(x)$$

حيث لم يبقَ لـ $q_r(x)$ أصفار في F؛ ولأن درجة $f(x)$ هي n، فإنه على الأكثر n من العوامل $(x - a_i)$ يمكن أن تظهر على الجانب الأيمن من المعادلة الأخيرة؛ لذلك $r \leq n$. أيضًا، إذا كان $b \neq a_i$ لـ i=1, …, r و $b \in F$، فإنّ:

$$f(b) = (b - a_1)...(b - a_r)q_r(b) \neq 0$$

لأن F ليس لها قواسم لـ 0 وليس أيّ من b - a_i أو $q_r(b)$ صفرًا تبعًا لبنائهم؛ لذلك، a_i لـ i=1,…, $r \leq n$ هي الأصفار كلها في F لـ $f(x)$. ♦

تركز نتيجتنا الأخيرة على بناء الزمرة الضربية F^* للعناصر غير الصفرية للحقل F، بدلاً من التحليل في $F[x]$، ربما يبدو مدهشًا من الوهلة الأولى أنّ مثل هذه النتيجة تنتج عن خوارزمية القسمة على $F[x]$، ولكن تذكر النتيجة التي تقول: الزمرة الجزئية من زمرة دورية هي دورية، تنتج من خوارزمية القسمة على $\mathbb{Z}$.

6.23 نتيجة إذا كانت G زمرة جزئية منتهية من الزمرة الضربية $\langle F^*, . \rangle$ للحقل F، فإن G دورية. بوجه خاص، الزمرة الضربية للعناصر غير الصفرية للحقل المنتهي هي دورية.

البرهان باستخدام المبرهنة 12.11، بوصفها زمرة إبدالية منتهية، تماثل G الضرب المباشر

$\mathbb{Z}_{d1} \times \mathbb{Z}_{d2} \times ... \mathbb{Z}_{dr}$ حيث كل d_i هو قوة لعدد أولي، لنفكر في كل $\mathbb{Z}_{d_i}$ على أنها زمرة دورية من الرتبة d_i في المفهوم الضربي، لتكن m المضاعف المشترك الأصغر لكل d_i لـ i = 1, …, r، لاحظ أنّ $m \leq d_1 d_2 \ldots d_r$. إذا كان $a_i \in \mathbb{Z}_{d_i}$، فإن $a_i^{di} = 1$؛ لذلك، $a_i^m = 1$؛ لأن d_i يقسم m؛ لذلك لكل $a \in G$، عندنا $\alpha^m = 1$، وعليه، فإن كلّ عنصر في G هو صفر لـ x^m- 1. لكن G يملك $d_1 d_2 \ldots d_r$ من العناصر، بينما يمكن أن يكون لـ x^m- 1 على الأكثر m من الأصفار في الحقل F كما في النتيجة 5.23؛ لذلك $m \geq d_1 d_2 \ldots d_r$؛ وبهذا $m = d_1 d_2 \ldots d_r$، وعليه، فإنّ الأعداد الأولية المشمولة في قوى الأعداد الأولية $d_1, d_2, \ldots, d_r$ مختلفة، والزمرة G تماثل الزمرة الدورية $\mathbb{Z}_m$. ♦

تطلب منا التمارين 5 إلى 8 إيجاد المولدات كلها للزمر الدورية لعناصر الوحدة لبعض الحقول المنتهية، وحقيقة أنَّ الزمرة الضربية لعناصر الوحدة لحقل منتهٍ دورية تمّ تطبيقها في التشفير الجبري.

كثيرات الحدود غير المختزلة

تعريفنا القادم يشير إلى نوع من كثيرات الحدود في $F[x]$ التي ستكون لها أهمية كبرى لنا، وربما يبدو المفهوم معروفًا تقريبًا، فنحن فعليًّا نفعل ما نفعله في المرحلة الثانوية، ولكن بوضع أكثر عمومًا.

7.23 تعريف تسمى كثيرة الحدود غير الثابتة $f(x) \in F[x]$ **غير مختزلة على** F، أو **كثيرة حدود غير مختزلة في** $F[x]$ **(irreducible)**، إذا كان من غير الممكن التعبير عن $f(x)$ بوصفه حاصل ضرب $g(x)$ $h(x)$ لكثيرتي حدود $g(x)$ و $h(x)$ في $F[x]$، حيث كلتا درجتيهما أقل من درجة $f(x)$، فإذا كانت $f(x) \in F[x]$ كثيرة حدود غير ثابتة، وليست غير مختزلة على F، فإن $f(x)$ **مختزلة على** F **(reducible)**. ■

لاحظ أنّ التعريف السابق ركز على المفهوم غير مختزلة على F وليس فقط المفهوم غير مختزلة، إذ إنّ كثيرة الحدود $f(x)$ ربما تكون غير مختزلة على F، لكنها ربما تكون مختزلة إذا عُرِضت داخل حقل أكبر E يحوي F. سنوضح هذا.

8.23 مثال توضّح المبرهنة 11.22 أنّ $x^2 - 2$ الموجودة في $\mathbb{Q}[x]$ ليس لها أصفار في $\mathbb{Q}$، هذا يبين أنّ $x^2 - 2$ غير مختزلة على $\mathbb{Q}$؛ لأنّ أي تحليل $x^2 - 2 = (ax + b)(cx + d)$ لـ $a,b,c,d \in \mathbb{Q}$ سيؤدي إلى توافر أصفار لـ $x^2 - 2$ في $\mathbb{Q}$، بينما $x^2 - 2$ الموجودة في $\mathbb{R}[x]$ مختزلة على $\mathbb{R}$؛ لأنّ $x^2 - 2$ تتحلل في $\mathbb{R}[x]$ إلى $\left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$. ▲

إنه لأمر جدير بالاهتمام أن نتذكر أنّ عناصر الوحدة في $F[x]$، هي بالضبط العناصر غير الصفرية في F؛ لذلك، يمكننا تعريف كثيرة الحدود غير المختزلة $f(x)$ على أنها كثيرة حدود غير ثابتة، بحيث لأي تحليل $f(x) = g(x)h(x)$ في $F[x]$ إما $g(x)$ أو $h(x)$ عنصر وحدة.

9.23 مثال لنبين أنّ $f(x) = x^3 + 3x + 2$ الموجودة في $\mathbb{Z}_5[x]$ غير مختزلة على $\mathbb{Z}_5$، إذا كانت $x^3 + 3x + 2$ تتحلل في $\mathbb{Z}_5[x]$ إلى كثيرتي حدود ذوات درجة أقل، فإنه يوجد على الأقل عامل خطي واحد لـ $f(x)$ على صورة $x - a$ لبعض $a \in \mathbb{Z}_5$. لكن $f(a)$ سيكون 0 باستخدام النتيجة 3.23، إلّا أنّ $f(0) = 2$، $f(1) = 1$، $f(-1) = -2$، $f(2) = 1$ و$f(2) = -2$ يبيِّن أنّ $f(x)$ ليس لها أصفار في $\mathbb{Z}_5$؛ لذلك، $f(x)$ غير مختزلة على $\mathbb{Z}_5$، هذا الاختبار لغير الاختزال عن طريق إيجاد الأصفار، يعمل بصورة جيدة بالنسبة إلى كثيرات الحدود التربيعية والتكعيبية على حقل منتهٍ فيه عدد قليل من العناصر. ▲

كثيرات الحدود غير مختزلة ستؤدي دورًا مهمًّا في عملنا من الآن فصاعدًا، ومشكلة تحديد هل كثيرة حدود معطاة $f(x) \in F[x]$ هي غير مختزلة على F ربما تكون صعبة.

نقدم الآن بعض الاختبارات لعدم قابلية الاختزال ذات الأهمية لبعض الحالات الخاصة، وقد قُدِّمت تقنية واحدة لتحديد عدم القابلية للاختزال لكثيرة حدود تربيعية أو تكعيبية في المثالين 8.23 و9.23، وسنصوغها في مبرهنة.

10.23 مبرهنة لتكن $f(x) \in F[x]$، ولتكن $f(x)$ من الدرجة 2 أو 3، فإنّ $f(x)$ مختزلة على F، إذا وفقط إذا توافرت لها أصفار في F.

البرهان إذا كانت $f(x)$ مختزلة، حيث $f(x) = g(x)h(x)$، بحيث كل من درجة $g(x)$ ودرجة $h(x)$ أقل من رتبة $f(x)$، إذن؛ لأنَّ $f(x)$ إما تربيعية أو تكعيبية، إما $g(x)$ أو $h(x)$ من الدرجة 1. إذا- فرضًا- $g(x)$ من الدرجة 1، فإنه باستثناء العامل المحتمل من F، $g(x)$ على صورة $x - a$ إذن، $g(a) = 0$ الذي يؤدي إلى أنّ $f(a) = 0$؛ لذلك، $f(x)$ لها صفر في F.

في المقابل، توضح النتيجة 3.23 أنه إذا كان $f(a) = 0$ لـ $a \in F$، فإنّ $x - a$ هو أحد عوامل $f(x)$؛ لذلك، $f(x)$ مختزلة. ♦

سنتحول إلى بعض شروط اللااختزال على $\mathbb{Q}$ لكثيرات الحدود في $\mathbb{Q}[x]$. أهم شرط سنقدّمه موجود في المبرهنة القادمة، ولن نثبت هذه المبرهنة هنا؛ فهي تشمل إلغاء المقام، وتؤدي إلى قليل من الفوضى.

11.23 مبرهنة إذا كانت $f(x) \in \mathbb{Z}[x]$، فإن $f(x)$ تتحلل إلى حاصل ضرب كثيرتي حدود ذوات درجات أقل r وs في $\mathbb{Q}[x]$، إذا وفقط إذا كان لها تحليل لكثيرات حدود من الدرجة r وs نفسها في $\mathbb{Z}[x]$.

البرهان البرهان محذوف هنا. ♦

12.23 نتيجة إذا كان $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ في $\mathbb{Z}[x]$، حيث $a_0 \neq 0$، وإذا $f(x)$ لها صفر في $\mathbb{Q}$، فإنّ لها صفر m في $\mathbb{Z}$ وm يقسم a_0.

البرهان إذا كانت $f(x)$ لها صفر a في $\mathbb{Q}$، فإن $f(x)$ لها عامل خطي $x-a$ في $\mathbb{Q}[x]$ باستخدام النتيجة 3.23، وباستخدام المبرهنة 11.23، فإنّ $f(x)$ تتحلل، بحيث يكون لها عامل خطي في $\mathbb{Z}[x]$؛ لذلك، يجب أن تكون لبعض $m \in \mathbb{Z}$:

$$f(x) = (x-m)(x^{n-1} + \ldots - a_0/m)$$

ولذلك، a_0/m في $\mathbb{Z}$، وعليه، فإنّ m تقسم a_0. ♦

13.23 مثال تعطينا النتيجة 12.23 برهانًا آخر لعدم اختزال x^2-2 على $\mathbb{Q}$، حيث x^2-2 تتحلل بصورة غير بدهية في $\mathbb{Q}[x]$، إذا وفقط إذا كان لها صفر في $\mathbb{Q}$ باستخدام المبرهنة 10.23، وباستخدام النتيجة 12.23، لها صفر في $\mathbb{Q}$، إذا وفقط إذا كان لها صفر في $\mathbb{Z}$، إضافة إلى ذلك، الاحتمالات هي فقط القواسم ± 1 و ± 2 لـ 2، ويبين الفحص أنَّه ليس أيّ من هذه الأعداد صفرًا لـ x^2-2. ▲

14.23 مثال لنستخدم المبرهنة 11.23 لنبين أنّ:

$$f(x) = x^4 - 2x^2 + 8x + 1$$

الموجودة في $\mathbb{Q}[x]$ غير مختزلة على $\mathbb{Q}$، فإذا كانت $f(x)$ لها عامل خطي في $\mathbb{Q}[x]$، فإن لها صفرًا في $\mathbb{Z}$، وباستخدام النتيجة 12.23 هذا الصفر سيكون قاسمًا في $\mathbb{Z}$ لـِ 1، أي إنَّه إما ± 1. لكن $f(1) = 8$ و $f(-1) = 8$؛ لذلك، هذا التحليل مستحيل.

إذا كانت $f(x)$ تتحلل إلى عاملين تربيعيين في $\mathbb{Q}[x]$، فباستخدام المبرهنة 11.23 يكون لها التحليل:

$$(x^2 + ax + b)(x^2 + cx + d)$$

في $\mathbb{Z}[x]$. بمساواة المعاملات لقوى x، نجد أنَّ:

$$a + c = 0 \text{ و } bd = 1,\ ad + bc = 8,\ ac + b + d = -2$$

للأعداد الصحيحة $a,b,c,d \in \mathbb{Z}$. من $bd = 1$ نرى أنه إما $b = d = 1$ أو $b = d = -1$. في الأحوال جميعها، $b = d$ ومن $ad + bc = 8$، نستنتج أنَّ $d(a + c) = 8$، لكن هذا مستحيل؛ لأنّ $a + c = 0$؛ لذلك، التحليل إلى كثيرتي حدود تربيعتين أيضًا مستحيل، و $f(x)$ غير مختزلة على $\mathbb{Q}$. ▲

ننهي خاصيتنا اللااختزالية بخاصية أيزنستاين المشهورة عن اللااختزال.

خاصية أخرى مفيدة جدًّا مقدمة في التمرين 37.

15.23 مبرهنة (**خاصية أيزنستاين**): لتكن $p \in \mathbb{Z}$ عددًا أوليًّا، افترض أنَّ:

$f(x) = a_n x^n + \ldots + a_0$ (مقياس p^2) في $\mathbb{Z}[x]$ و $a_n \not\equiv 0$ (مقياس p) لكن $a_i = 0$ (مقياس p) لكل $i < n$، حيث $a_0 \not\equiv 0$ (مقياس p^2)، فإنّ $f(x)$ غير مختزلة على $\mathbb{Q}$.

البرهان باستخدام المبرهنة 11.23 نحتاج فقط إلى إثبات أنّ $f(x)$ لا تتحلل إلى كثيرات حدود ذوات درجات أقل في $\mathbb{Z}[x]$. إذا كان:

$$f(x) = (b_r x^r + \ldots + b_0)(c_s x^s + \ldots + c_0)$$

هو تحليلها في $\mathbb{Z}[x]$، حيث $b_r \neq 0$ و $c_s \neq 0$ و $r, s < n$، فإن $a_0 \not\equiv 0$ (مقياس p^2) تؤدي إلى أنّ كلًّا من c_0 و b_0 لا يطابقان 0 (مقياس p)، افترض أن $b_0 \not\equiv 0$ (مقياس p) و $c_0 \equiv 0$ (مقياس p) الآن، $a_0 \not\equiv 0$ (مقياس p) يؤدي إلى $b_r, c_s \not\equiv 0$ (مقياس p) لأنّ: $a_n = b_r c_s$.

لتكن m أصغر قيمة لـ k، بحيث $c_k \not\equiv 0$ (مقياس p). فإنّ:

$$a_m = b_0 c_m + b_1 c_{m-1} + \ldots + \begin{cases} b_m c_0 & \text{عندما } r \geq m, \\ b_r c_{m-r} & \text{عندما } r < m \end{cases}$$

حقيقة أنَّ لا b_0 ولا c_m يطابق 0 (مقياس p)، بينما $c_0, \ldots, c_{m-1}$ كلها تطابق 0 (مقياس p) تؤدي إلى أنَّ $a_m \not\equiv 0$ (مقياس p)؛ لذلك، $m = n$، وبناءً على ذلك، $s = n$ مناقض لافتراضنا أنّ $s < n$؛ أي إنّ تحليلنا ليس تافهًا. ♦

لاحظ أنه إذا أخذنا $p = 2$، فإن خاصية أيزنستاين تعطينا أيضًا إثباتًا آخر على أنّ $x^2 - 2$ غير مختزلة على $\mathbb{Q}$.

16.23 مثال بأخذ $p = 3$، من مبرهنة 15.23 نرى أنّ:

$$25x^5 - 9x^4 - 3x^2 - 12$$

غير مختزلة على $\mathbb{Q}$. ▲

17.23 نتيجة كثيرة الحدود

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

غير مختزلة على $\mathbb{Q}$ لأي عدد أولي p.

البرهان مرة أخرى باستخدام المبرهنة 11.23 نريد فقط أن نعدّ التحليلات في $\mathbb{Z}[x]$، فقد أشرنا بعد مبرهنة 5.22، إلى أنَّ إثباتها حقيقةً يبيّن أنّ تشاكلات التعويض يمكن استخدامها فقط في الحلقات الإبدالية، ونريد هنا أن نستخدم التشاكل التعويضي $\phi_{x+1}:\mathbb{Q}[x]\to\mathbb{Q}[x]$. من الطبيعي لنا أن نرمز لـ $\phi_{x+1}(f(x))$ بـ $f(x+1)$ لـ $f(x)\in\mathbb{Q}[x]$ ليكن

$$g(x)=\Phi_p(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=\frac{x^p+\binom{p}{1}x^{p-1}+\ldots+px}{x}$$

معامل x^{p-r} لـ $0<r<p$ هو المعامل الثنائي الحد $p!/[r!(p\text{-}r)!]$، وهو قابل للقسمة على p؛ لأن p يقسم $p!$، بينما لا يقسم $r!$ أو $(p\text{-}r)!$ عندما $0<r<p$؛ لذلك:

$$g(x)=x^{p-1}+\binom{p}{1}x^{p-2}+\ldots+p$$

تحقق خاصية أيزنستاين للعدد الأولي p، وبهذا فهي غير مختزلة على $\mathbb{Q}$، لكن إذا كان:

$\Phi_p(x)=h(x)r(x)$ هو تحليل غير بدهي لـ $\Phi_p(x)$ في $\mathbb{Z}[x]$، فإنّ:

$$\Phi_P(x+1)=g(x)=h(x+1)r(x+1)$$

سيعطي تحليلًا غير بدهي لـ $g(x)$ في $\mathbb{Z}[x]$؛ لذلك $\Phi_p(x)$ يجب أن تكون غير مختزلة على $\mathbb{Q}$. ♦

كثيرة الحدود $\Phi_p(x)$ في النتيجة 17.23 تسمى **كثيرة الحدود الدورية من الرتبة *p***.

وحدانية التحليل في *F*[x].

كثيرات الحدود في $F[x]$ يمكن أن تتحلل إلى حاصل ضرب كثيرات حدود غير مختزلة في $F[x]$ بطريقة جوهرية فريدة. لـ $f(x), g(x)\in F[x]$ نقول: إنّ $g(x)$ **يقسم** $f(x)$ **في** $F[x]$، إذا وجد $q(x)\in F[x]$، بحيث $f(x)=g(x)q(x)$.

لاحظ التشابه بين المبرهنة الآتية والخاصية (1) لـ $\mathbb{Z}$ المؤطرة، التي جاءت بعد مثال9.6.

18.23 مبرهنة لتكن $p(x)$ كثيرة حدود غير مختزلة في $F[x]$، إذا كان $p(x)$ يقسم $r(x)s(x)$ لـ $r(x), s(x)\in F[x]$، فإنه إما $p(x)$ يقسم $r(x)$ أو $p(x)$ يقسم $s(x)$.

البرهان سنرجئ برهان هذه المبرهنة إلى الفصل 27 (انظر المبرهنة 27.27). ♦

19.23 نتيجة إذا كانت $p(x)$ غير مختزلة في $F[x]$ و$p(x)$ يقسم حاصل الضرب $r_1(x)\cdots r_n(x)$ لـ $r_i(x)\in F[x]$، فإنّ $p(x)$ يقسم $r_i(x)$ على الأقل لـ i واحدة.

البرهان نصل إلى النتيجة باستخدام الاستقراء الرياضي، ومن المبرهنة 18.23. ♦

20.23 مبرهنة إذا كان F حقلًا، فإنّ كل كثيرة حدود غير ثابتة $f(x) \in F[x]$ يمكنها أن تتحلل في $F[x]$ إلى حاصل ضرب كثيرات حدود غير مختزلة، إذ إنّ كثيرات الحدود غير المختزلة هذه وحيدة، عدا الترتيب والضرب بعناصر وحدة (أي ثابت غير صفري) في F.

البرهان لتكن $f(x) \in F[x]$ كثيرة حدود غير ثابتة، فإذا كانت $f(x)$ اختزالية، فإنّ $f(x) = g(x)h(x)$، حيث رتبة $g(x)$ ورتبة $h(x)$ كلتاهما أقل من رتبة $f(x)$.

إذا كان كلا $g(x)$ و$h(x)$ غير مختزلة، نتوقف هنا، وإلاّ، على الأقل أحدهما يتحلل إلى كثيرات حدود من درجات أقل، وبالاستمرار في العمل نصل إلى التحليل:

$$f(x) = p_1(x)p_2(x)...p_r(x)،$$

حيث $p_i(x)$ غير مختزلة لـ $i = 1, 2, \ldots, r$.

بقي علينا أن نثبت الوحدانية، افترض أنّ:

$$f(x) = p_1(x)p_2(x)...p_r(x) = q_1(x)q_2(x)....q_s(x)$$

هما تحليلان لـ $f(x)$ إلى كثيرات حدود غير مختزلة، فإنه باستخدام النتيجة 19.23، $p_1(x)$ يقسم بعض $q_j(x)$، ولنفترض أنه $q_1(x)$؛ لأنّ $q_1(x)$ غير مختزلة، فإنّ

$$q_1(x) = u_1p_1(x)$$

حيث $u_1 \neq 0$، لكن u_1 في F، ولهذا هو عنصر وحدة، وبتعويض $u_1p_1(x)$ بدلاً من $q_1(x)$ وبالحذف، نحصل على:

$$p_2(x)...p_r(x) = u_1q_2(x)....q_s(x)$$

بأسلوب مشابه، قل: $q_2(x) = u_2p_2(x)$؛ لذلك،

$$p_3(x)...p_r(x) = u_1u_2q_3(x)..q_s(x).$$

وبالاستمرار بهذا النمط نصل فعليًّا إلى:

$$1 = u_1u_2..u_rq_{r+1}(x)..q_s(x).$$

هذا فقط ممكن إذا كان $s = r$؛ لذلك، المعادلة هي فعليًّا $u_1u_2 \dots u_r = 1$.

وهكذا، فإنّ العوامل غير المختزلة $p_i(x)$ و $q_j(x)$ هي نفسها، عدا احتمالية الترتيب وعوامل عناصر وحدة من F. ♦

21.23 مثال في المثال 4.23 تحليل لـ $x^4 + 3x^3 + 2x + 4$ إلى عواملها في $\mathbb{Z}_5[x]$ هو $(x - 1)^3(x+1)$، إذ إنّ هذه العوامل غير المختزلة في $\mathbb{Z}_5[x]$ وحيدة فقط لعناصر الوحدة في $\mathbb{Z}_5[x]$، أي للثوابت غير الصفرية في $\mathbb{Z}_5$. على سبيل المثال: $(x-1)^3(x+1) = (x-1)^2(2x-2)(3x+3)$ ▲

■ تمارين 23

حسابات

في التمارين 1 إلى 4، أوجد $q(x)$ و $r(x)$ كما وُصفتا في خوارزمية القسمة، بحيث:

$f(x) = g(x)q(x) + r(x)$، حيث $r(x) = 0$، أو درجتها أقل من درجة $g(x)$.

1. $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ و $g(x) = x^2 + 2x - 3$ في $\mathbb{Z}_7[x]$.

2. $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ و $g(x) = 3x^2 + 2x - 3$ في $\mathbb{Z}_7[x]$.

3. $f(x) = x^5 - 2x^4 + 3x - 5$ و $g(x) = 2x + 1$ في $\mathbb{Z}_{11}[x]$.

4. $f(x) = x^4 + 5x^3 - 3x^2$ و $g(x) = 5x^2 - x + 2$ في $\mathbb{Z}_{11}[x]$.

في التمارين 5 إلى 8، أوجد مولدات الزمرة الضربية الدورية جميعها لعناصر الوحدة في الحقل المنتهي المعطى (راجع النتيجة 16.6).

5. $\mathbb{Z}_5$ **6.** $\mathbb{Z}_7$ **7.** $\mathbb{Z}_{17}$ **8.** $\mathbb{Z}_{23}$

9. كثيرة الحدود $x^4 + 4$ يمكن تحليلها إلى عوامل غير مختزلة في $\mathbb{Z}_5[x]$. أوجد هذا التحليل.

10. كثيرة الحدود $x^3 + 2x^2 + 2x + 1$ يمكن تحليلها إلى عوامل غير مختزلة في $\mathbb{Z}_7[x]$. أوجد هذا التحليل.

11. كثيرة الحدود $2x^3 + 3x^2 - 7x - 5$ يمكن تحليلها إلى عوامل غير مختزلة في $\mathbb{Z}_{11}[x]$. أوجد هذا التحليل.

12. هل $x^3 + 2x + 3$ كثيرة حدود غير مختزلة في $\mathbb{Z}_5[x]$؟ لماذا؟ عبِّر عنها بوصفها حاصل ضرب كثيرات حدود غير مختزلة في $\mathbb{Z}_5[x]$.

13. هل $2x^3 + x^2 + 2x + 2$ كثيرة حدود غير مختزلة في $\mathbb{Z}_5[x]$؟ لماذا؟ عبِّر عنها بوصفها حاصل ضرب كثيرات حدود غير مختزلة في $\mathbb{Z}_5[x]$.

14. بيّن أنّ $f(x) = x^2 + 8x - 2$ غير مختزلة على $\mathbb{Q}$. هل $f(x)$ غير مختزلة على $\mathbb{R}$؟ على $\mathbb{C}$؟

15. أعد تمرين 14 لـ $g(x) = x^2 + 6x + 12$ بدلاً من $f(x)$.

16. تحقق من أنّ $x^3 + 3x^2 - 8$ غير مختزلة على $\mathbb{Q}$.

17. تحقق من أنّ $x^4 - 22x^2 + 1$ غير مختزلة على $\mathbb{Q}$.

في التمارين 18 إلى 21، حدّد فيما إذا كثيرة الحدود في $\mathbb{Z}[x]$ تحقق خاصية أيزنستاين للاختزالية على $\mathbb{Q}$.

18. $x^2 - 12$

19. $8x^3 + 6x^2 - 9x + 24$

20. $4x^{10} - 9x^3 + 24x - 18$

21. $2x^{10} - 25x^3 + 10x^2 - 30$

22. أوجد أصفار $6x^4 + 17x^3 + 7x^2 + x - 10$ في $\mathbb{Q}$ جميعها. (هذه مسألة جبرية مملّة للمرحلة الثانوية، ويمكن أن تستخدم القليل من الهندسة التحليلية وعلم التفاضل والتكامل لرسم الدالة، أو استخدم طريقة نيوتن لترى أفضل المرشحين ليكونوا أصفارًا).

مفاهيم

في التمرينين 23 و24، صحّح تعريف الحدّ المكتوب بخط مائل دون الرجوع إلى الكتاب –إذا كانت هناك حاجة للتصحيح– بحيث يكون بصيغة قابلة للنشر.

23. كثيرة الحدود $f(x) \in F[x]$ غير مختزلة على الحقل F، إذا وفقط إذا كان $f(x) \neq g(x)h(x)$ لأي كثيرتي حدود $g(x), h(x) \in F[x]$.

24. كثيرة الحدود غير الثابتة $f(x) \in F[x]$ غير مختزلة على الحقل F، إذا وفقط إذا كان أي تحليل لها في $F[x]$، أحد العوامل في F.

25. ضع إشارة صح أو إشارة خطأ:

_____ أ. $x-2$ غير مختزلة على $\mathbb{Q}$.

_____ ب. $3x - 6$ غير مختزلة على $\mathbb{Q}$.

_____ جـ. $x^2 - 3$ غير مختزلة على $\mathbb{Q}$.

_____ د. $x^2 + 3$ غير مختزلة على $\mathbb{Z}_7$.

_____ هـ. إذا كان F حقل، فإن عناصر الوحدة في $F[x]$ هي بالضبط العناصر غير الصفرية في $F[x]$.

_____ و. اذا كان F حقل، فإن عناصر الوحدة في $F[x]$ هي بالضبط العناصر غير الصفرية في F.

_____ ز. كثيرة الحدود $f(x)$ من الدرجة n، بحيث معاملاتها من الحقل F، يمكن أن يكون لها على الأكثر n من الأصفار في أي حقل E، حيث $F \leq E$.

_____ حـ. كل كثيرة حدود من الدرجة 1 في $F[x]$ لها على الأقل صفر واحد في الحقل F.

_____ ط. كل كثيرة حدود في $F[x]$ يمكن أن يكون لها على الأكثر عدد منتهٍ من الأصفار في الحقل F.

26. أوجد الأعداد الأولية p كلها، بحيث $x + 2$ أحد عومل $x^4 + x^3 + x^2 - x + 1$ في $\mathbb{Z}_p[x]$.

في التمارين 27 إلى 30، أوجد كثيرات الحدود غير المختزلة كلها من الدرجة المبينة في الحقل المعطى.

27. درجة 2 في $\mathbb{Z}_2[x]$.

28. درجة 3 في $\mathbb{Z}_2[x]$.

29. درجة 2 في $\mathbb{Z}_3[x]$.

30. درجة 3 في $\mathbb{Z}_3[x]$.

31. أوجد عدد كثيرات الحدود التربيعية غير المختزلة في $\mathbb{Z}_p[x]$، حيث p عدد أولي. [مساعدة: أوجد عدد كثيرات الحدود المختزلة التي صيغتها $x^2 + ax + b$، ثمّ عدد التربيعيات المختزلة، ثم اطرح هذا من العدد الكلي للتربيعيات].

براهين مختصرة

32. أعطِ برهانًا مختصرًا للنتيجة 5.23.

33. أعطِ برهانًا مختصرًا للنتيجة 6.23.

براهين

34. بيّن أنه لأيّ عدد أولي p، كثيرة الحدود $x^p + a$ في $\mathbb{Z}_p[x]$ مختزلة، لأي $a \in \mathbb{Z}_p$.

35. إذا كان F حقلًا، و$a \neq 0$ صفر لـ $f(x) = a_0 + a_1x + \ldots + a_nx^n$ في $F[x]$، فبيِّن أنّ $1/a$ صفر لـ $a_n + a_{n-1}x + \ldots + a_0x^n$.

36. (مبرهنة الباقي): لتكن $f(x) \in F[x]$، حيث F حقل، ولتكن $a \in F$. بيَّن أنّ الباقي $r(x)$ عندما تقسم $f(x)$ على $x - \alpha$، طبقًا لخوارزمية القسمة، هو $f(a)$.

37. لتكن $\sigma_m : \mathbb{Z} \to \mathbb{Z}_m$ التشاكل الطبيعي المعطى بـ (a باقي قسمة على m) $= \sigma_m(a)$ لـ $a \in \mathbb{Z}$.

أ. بيّن أنّ $\overline{\sigma_m} : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ المعطى بـ

$$\overline{\sigma_m}(a_0 + a_1x + \ldots + a_nx^n) = \sigma(a_0) + \sigma_m(a_1)x + \ldots + \sigma_m(a_n)x^n$$

هو تشاكل غامر من $\mathbb{Z}[x]$ إلى $\mathbb{Z}_m[x]$.

ب. بيّن أنّه إذا كانت $f(x) \in \mathbb{Z}[x]$ و $\overline{\sigma_m}(f(x))$، كلتاهما من الدرجة n و $\overline{\sigma_m}(f(x))$ لا يتحلل في $\mathbb{Z}_m[x]$ إلى حاصل ضرب كثيرتي حدود من درجات أقل من n، فإن $f(x)$ غير مختزلة في $\mathbb{Q}[x]$.

جـ. استخدم الجزء (ب) لتبين أنّ $x^3 + 17x + 36$ غير مختزلة في $\mathbb{Q}[x]$. [مساعدة: جرب عددًا أوليًّا m الذي يبسط المعاملات].

الفصل 24 أمثلة غير إبدالية [1] Noncommutative Examples

المثال الوحيد الذي قدّمناه سابقًا على حلقة غير إبدالية، هو: الحلقة $M_n(F)$ وتحوي المصفوفات كلها من الدرجة $n \times n$، بحيث المدخلات من الحقل F، وعلى الأغلب لن نفعل شيئًا للحلقات غير الإبدالية وحقول القسمة؛ لنبين أنه توجد حلقات غير إبدالية أخرى مهمّة وبصورة طبيعية جدًّا في الجبر، سنقدم أمثلة مختلفة على هذه الحلقات.

حلقات التشاكل الداخلية

لتكن A أيّ زمرة إبدالية، حيث يسمّى التشاكل من A إلى نفسها **تشاكلًا داخليًّا (endomorphism) على** A، ولتكن مجموعة التشاكلات الداخلية على A كلها $\mathrm{End}(A)$؛ لأنّ تركيب تشاكلين من A إلى نفسها هو مرة أخرى تشاكل، ونعرّف الضرب على $\mathrm{End}(A)$ باستخدام دالة التركيب، وبهذا يكون الضرب تجميعيًّا.

لتعريف الجمع، خذ $\phi, \psi \in \mathrm{End}(A)$، علينا أن نصف القيمة لـ $(\phi + \psi)$ على كل $a \in A$. عرّف

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

لأن:

$$\begin{aligned}(\phi+\psi)(a+b)&=\phi(a+b)+\psi(a+b)\\&=[\phi(a)+\phi(b)]+[\psi(a)+\psi(b)]\\&=[\phi(a)+\psi(a)]+[\phi(b)+\psi(b)]\\&=(\phi+\psi)(a)+(\phi+\psi)(b)\end{aligned}$$

نرى أنّ $\phi + \psi$ هي مرة أخرى موجودة في $\mathrm{End}(A)$.

لأنّ A إبدالية، عندنا:

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

لكل $a \in A$؛ لذلك، $\phi + \psi = \psi + \phi$ والجمع على $\mathrm{End}(A)$ إبدالي، ونحصل على الخاصية التجميعية على الجمع من:

[1] لن يستخدم هذا الفصل في بقية الكتاب.

$$\begin{aligned}[\phi+(\psi+\theta)](a) &= \phi(a)+[\psi+\theta(a)]\\ &= \phi(a)+\big[\psi(a)+\theta(a)\big]\\ &= [\phi(a)+\psi(a)]+\theta(a)\\ &= (\phi+\psi)(a)+\theta(a)\\ &= \big[(\phi+\psi)+\theta\big](a).\end{aligned}$$

إذا كان e العنصر المحايد لعملية الجمع على A، فإن التشاكل 0 المعرف بـ

$$0(a) = e$$

لكل $a \in A$ يكون العنصر المحايد لعملية الجمع في End(A). أخيرًا، لـ

$$\phi \in \text{End(A)},$$

$-\phi$ معرف بـ

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

موجود في $\text{End}(A)$؛ لأنّ:

$$\begin{aligned}(-\phi)(a+b) &= -\phi(a+b) = -\big[\phi(a)+\phi(b)\big]\\ &= -\phi(a)-\phi(b) = (-\phi)(a)+(-\phi)(b)\end{aligned}$$

و$0 =(-\phi)+\phi$ ؛ لذلك: $\langle \text{End}(A), + \rangle$ زمرة إبدالية.

لاحظ أنّنا لم نستخدم حقيقة أنَّ دوالنا هي تشاكلات إلّا لنبيِّن أنَّ $\psi + \phi$ و $-\phi$ هي أيضًا تشاكلات؛ لذلك، المجموعة A^A المكونة من الدوال جميعها من A إلى A هي زمرة إبدالية تحت تعريف الجمع نفسه بالضبط، وبالطبع، التركيب الدالي يعطى أيضًا عملية تجميعية جميلة على A^A، ومع ذلك، نحتاج حقيقة إلى أن هذه الدوال في $\text{End}(A)$ هي تشاكلات الآن؛ لإثبات قانون التوزيع من اليسار على $\text{End}(A)$، فباستثناء قانون التوزيع من اليسار هذا، فإن $\left\langle A^A, +, \cdot \right\rangle$ تحقق مسلمات الحلقة جميعها، لتكن ψ و ϕ و θ في $\text{End}(A)$، ولتكن $a \in A$، فإنّ:

$$(\theta(\phi+\psi))(a) = \theta((\phi+\psi)(a)) = \theta(\phi(a)+\psi(a))$$

لأنّ θ تشاكل

$$\begin{aligned}\theta(\phi(a)+\psi(a)) &= \theta(\phi(a))+\theta(\psi(a))\\ &= (\theta\phi)(a)+(\theta\psi)(a)\\ &= (\theta\phi+\theta\psi)(a).\end{aligned}$$

لذلك: $\theta\psi + \theta\phi = \theta(\phi+ \psi)$، أمّا قانون التوزيع من اليمين، فلا يمثل أي مشكلة، حتى في A^A، ويأتي من:

$$\begin{aligned}((\psi + \theta)\phi)(a) &= (\psi + \theta)(\phi(a)) = \psi(\phi(a)) + \theta(\phi(a)) \\ &= (\psi\phi)(a) + (\theta\phi)(a) = (\psi\phi + \theta\phi)(a).\end{aligned}$$

وبذلك نكون قد أثبتنا المبرهنة الآتية:

1.24 مبرهنة المجموعة $\mathrm{End}(A)$ من التشاكلات الداخلية على الزمرة الإبدالية A تشكل حلقة بالنسبة إلى جمع التشاكلات وضربها (التركيب الدالي).

مرة أخرى، لنبين الصلة الوثيقة في هذا الفصل، علينا أن نقدم مثالاً موضحًا على أن $End\ (A)$ ليست بالضرورة إبدالية؛ لأنّ التركيب الدالي ليس على العموم إبداليًّا، وهذا من الممكن توقعه، لكن $End\ (A)$ ربما تكون إبدالية في بعض الحالات، بالفعل، فتمرين 15 يُقرّ بأنّ $\mathrm{End}\left(\langle\mathbb{Z},+\rangle\right)$ إبدالية.

2.24 مثال لتكن الزمرة الإبدالية $\langle\mathbb{Z}\times\mathbb{Z},+\rangle$ التي نوقشت في الفصل 11. من البدهي أن تتحقق من أنّ φ وψ عنصران في $\mathrm{End}\ \langle\mathbb{Z}\times\mathbb{Z},+\rangle$، والمعرفان بـ

$$\psi\left((m,\ n)\right) = (0,\ n) \text{ و } \phi\left((m,\ n)\right) = (m+n, 0)$$

لاحظ أنّ ϕ ترسل كل شيء بصورة غامرة إلى العامل الأول لـ $\mathbb{Z}\times\mathbb{Z}$، و$\psi$ تسحق العامل الأول؛ لذلك:

$$(\psi\phi)(m,n) = \psi(m+n,0) = (0,0)$$

بينما:

$$(\phi\psi)(m,n) = \phi(0,n) = (n,0)$$

لذلك، $\phi\psi \neq \psi\phi$. ▲

3.24 مثال ليكن F حقلًا مميزه صفر، ولتكن $\langle F[x],+\rangle$ الزمرة الجمعية للحلقة $F[x]$ من كثيرات الحدود التي معاملاتها من F، ولهذا المثال دعنا نرمز للزمرة الجمعية بـ $F[x]$ لتبسيط المفهوم، إذ يمكننا أن نعدّ $\mathrm{End}\ (F[x])$. أحد عناصر $\mathrm{End}\ (F[x])$ يؤثر في أي كثيرة حدود في $F[x]$، عن طريق ضربها بـ x، وليكن هذا التشاكل الداخلي هو X؛ لذلك،

$$X\ (a_0 + a_1x\ + a_2x^{\ 2} + \cdots + a_nx^{\ n}) = a_0x\ + a_1x^{\ 2} + a_2x^{\ 3} + \cdots + a_nx^{\ n+1}$$

عنصر آخر من End $(F[x])$ هو الاشتقاق الشكلي بالنسبة إلى x. (الصيغة المشهورة "مشتقة حاصل الجمع هو حاصل جمع المشتقات" تضمن أنَّ الاشتقاق تشاكل داخلي على $F[x]$) ليكن Y هذا التشاكل، وبهذا

$$Y\ (a_0 + a_1x\ + a_2x^{\,2} + \cdots + a_nx^{\,n}) = a_1 + 2a_2x\ + \cdots + na_nx^{\,n-1}$$

يطلب منا تمرين 17 أن نبين أنّ $YX - XY = 1$، حيث 1 العنصر المحايد (الدالة المحايدة) في $End\ (F[x])$؛ لذلك، $YX \neq XY$، ضرب كثيرات الحدود في $F[x]$ في أي عنصر من F يعطينا أيضًا عنصرًا في $End\ (F[x])$، الحلقة الجزئية من $End\ (F[x])$ المولَّدة من X و Y والضرب بعناصر من F هي **جبر وايل (Weyl algebra)**، وهي مهمة في ميكانيكا الكم. ▲

حلقات وجبريات الزمر

لتكن $G = \{g_i \mid i \in I\}$ زمرة ضربية، ولتكن R حلقة إبدالية فيها العنصر المحايد غير الصفري، ولتكن RG مجموعة أشكال الجمع

$$\sum_{i \in I} a_i g_i$$

لـ $g_i \in G\ ,\ a_i \in R$، حيث a_i كلها عدا عدد منتهٍ منها صفر. عرِّف حاصل جمع عنصرين من RG بـ

$$\left(\sum_{i \in I} a_i g_i\right) + \left(\sum_{i \in I} b_i g_i\right) = \sum_{i \in I} (a_i + b_i) g_i$$

تحقق من أنّ $(a_i + b_i) = 0$ عدا عدد منتهٍ من المؤشرات i؛ لذلك، $\sum_{i \in I} (a_i + b_i) g_i$ في RG، ومن البدهي أنّ $\langle RG, + \rangle$ زمرة إبدالية، حيث العنصر المحايد للجمع $\sum_{i \in I} 0 g_i$.

ضرب عنصر في RG معرف باستخدام الضرب في G و R على النحو الآتي:

$$\left(\sum_{i \in I} a_i g_i\right)\left(\sum_{i \in I} b_i g_i\right) = \sum_{i \in I}\left(\sum_{g_j g_k = g_i} a_j b_k\right) g_i$$

ببساطة نوزّع شكليًّا المجموع $\sum_{i \in I} a_i g_i$ على المجموع $\sum_{i \in I} b_i g_i$، ونعيد تسمية الحدّ $a_j g_j b_k g_k$ بـ $a_j b_k g_i$ حيث $g_j g_k = g_i$ في G؛ لأن a_i و b_i كلها 0 عدا عدد منتهٍ من i،

المجموع $\sum_{gjg_k=g_i} a_j b_k$ يحوي فقط عددًا منتهيًا لمجاميع غير صفرية

$a_j b_k \in R$، وبذلك يمكن رؤيتها بوصفها عنصرًا في R، ومرة أخرة عدد منتهٍ من المجاميع

$\sum_{gjg_k=g_i} a_j b_k$ غير صفرية،

بهذا يكون الجمع مغلقًا على RG.

قانونا التوزيع يأتيان مباشرة من تعريف الجمع والطريقة الاعتيادية، التي نستخدم بها العملية التوزيعية لتعريف الضرب، بالنسبة إلى العملية التجميعية على الضرب:

$$\left(\sum_{i\in I} a_i g_i\right)+\left[\left(\sum_{i\in I} b_i g_i\right)\left(\sum_{i\in I} c_i g_i\right)\right]=\left(\sum_{i\in I} a_i g_i\right)\left[\sum_{i\in I}\left(\sum_{gjgk=gi} b_j c_k\right) g_i\right]$$

$$=\sum_{i\in I}\left(\sum_{g_h g_j g_k=g_i} a_h b_j c_k\right) g_i$$

$$=\left[\sum_{i\in I}\left(\sum_{g_h g_j=g_i} a_h b_j\right) g_i\right]\left(\sum_{i\in I} c_i g_i\right)$$

$$=\left[\left(\sum_{i\in I} a_i g_i\right)\left(\sum_{i\in I} b_i g_i\right)\right]\left(\sum_{i\in I} c_i g_i\right)$$

بهذا نكون قد أثبتنا المبرهنة الآتية:

4.24 مبرهنة إذا كانت G أيّ زمرة ضربية، وR حلقة إبدالية فيها العنصر المحايد غير الصفري، فإنّ $\langle RG, +, . \rangle$ حلقة.

بالنسبة إلى أيّ $g \in G$، عندنا العنصر $1g$ في RG، وإذا عرّفنا (أعدنا تسمية) $1g$ بـ g، نرى أنّ $\langle RG, . \rangle$ يمكن أن نعدّها تحوي G بصورة طبيعية بوصفها نظامًا جزئيًّا ضربيًّا؛ لذلك، إذا كانت G ليست إبدالية، فإن RG حلقة غير إبدالية.

5.24 تعريف الحلقة RG المعرفة في الأعلى هي **حلقة الزمرة (group ring)** لـ G **على** R. إذا كان F حقلًا، فإن FG **جبر الزمرة (group algebra)** لـG **على** F. ■

6.24 مثال لنقدم جداول الجمع والضرب لجبر الزمرة $G\mathbb{Z}_2$، حيث $G = \{e, a\}$ دورية من الرتبة 2، فعناصر Z_2G هي:

$$1e + 1a \text{ و } 1e + 0a \text{ ،} 0e + 1a \text{ ،} 0e + 0a$$

إذا رمزنا لهذه العناصر بطريقة طبيعية واضحة بـ

$$0 \text{، } a \text{، } e \text{، و } e + a \text{،}$$

+	0	a	e	$e + a$
0	0	a	e	$e + a$
a	a	0	$e + a$	e
e	e	$e + a$	0	a
$e + a$	$e + a$	e	a	0

الجدول 7.24

	0	a	e	$e + a$
0	0	0	0	0
a	0	e	a	$e + a$
e	0	a	e	$e + a$
$e + a$	0	$e + a$	$e + a$	0

الجدول 8.24

على الترتيب، نحصل على الجدولين24. 7 و 8.24، على سبيل المثال: لترى أنّ

$(e + a)(e + a) = 0$، لدينا:

$$(1e + 1a)(1e + 1a) = (1 + 1)e + (1 + 1)a = 0e + 0a$$

هذا المثال يبين أنّ جبر الزمرة ربما فيه قواسم لـ 0، وبصورة فعلية، فإنّ هذه هي الحالة دائمًا. ▲

المرباعيات

لم نقدم مثالًا على حلقة قسمة غير إبدالية لغاية الآن، والمرباعيات لهاميلتون (Hamilton) مثال قياسي على حقل تخالفي قطعي.

■ **نبذة تاريخية**

اكتشف السيرويليام روان هاملتون (William Rowan Hamilton 1805–1865) المرباعيات عام 1843م، عندما كان يبحث عن طريقة لضرب ثلاثيات العدد (متجهات في $\mathbb{R}^3$).

قبل ست سنوات طوّر الأعداد المركبة بصورة مجردة بوصفها أزواجًا مرتبة (a, b) من الأعداد الحقيقية، حيث الجمع $(a, b) + (a', b') = (a + a', b + b')$، والضرب $(a, b) \cdot (a', b') = (aa' - bb', ab' + a'b)$؛ بعدها بحث عن ضرب مشابه لثلاثة متجهات، بحيث يكون تجميعيًّا، ويكون طول المتجه الناتج عن حاصل الضرب هو حاصل ضرب أطوال العوامل، وبعد محاولات فاشلة عدة لضرب متجهات من الشكل $a + bi + cj$ (حيث $1, i, j$ متعامدة بصورة تبادلية)، وبينما كان يسير على طول القنال الملكي في دبلن، أدرك في 16 أكتوبر عام 1843م أنه محتاج إلى "رمز تخيلي" جديد k يكون عموديًّا على بقية العناصر الثلاث، فلم يستطع "أن يقاوم الاندفاع... ليكتب بسكين على حجر من جسر بروغام" الصيغ الأساسية المعرفة في صفحة 225 لضرب هذه المرباعيات.

كانت المرباعيات أول مثال معلوم عن حقل تخالفي قطعي، بعدها اكتُشفت أمثلة أخرى بصورة تتابعية، وقد لوحظ أنه ليس أي منها منتهيًّا، وعام 1909م قدّم جوزف هنري ماكلاجان ويدربيرن Joseph Henry (MaclaganWedderburn 1882–1948) ومن بعده قدم مدرس في جامعة برينستون، أول إثبات للمبرهنة 10.24.

لتكن المجموعة $\mathbb{H}$ لهاميلتون هي $\mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}$. الآن، $\langle \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}, + \rangle$ هي زمرة بالنسبة إلى عملية الجمع على المركبات؛ الضرب المباشر لـ $\mathbb{R}$ بالنسبة إلى الجمع مع نفسها أربع مرات، وهذا يعطي عملية الجمع على $\mathbb{H}$، لنعيد تسمية عناصر محددة من $\mathbb{H}$.

سنجعل:

$$1 = (1, 0, 0, 0), \quad i = (0, 1, 0, 0)$$

$$j = (0, 0, 1, 0), \quad k = (0, 0, 0, 1)$$

إضافة إلى ذلك، نوافق على أن نجعل:

$$a_1 = (a_1, 0, 0, 0), \quad a_2 i = (0, a_2, 0, 0).$$

$$a_3 j = (0, 0, a_3, 0), \quad a_4 k = (0, 0, 0, a_4)$$

من خلال تعريفنا للجمع، عندنا:

$$(a_1, a_2, a_3, a_4) = a_1 + a_2 i + a_3 j + a_4 k$$

لذلك:

$$(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k)$$
$$= (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3) j + (a_4 + b_4)k$$

ولتعريف الضرب على $\mathbb{H}$، نبدأ بتعريف

$$1a = a1 = a \text{ لـ } a \in \mathbb{H} ،$$

$$i^2 = j^2 = k^2 = -1 ،$$

$$ik = -j \text{ و } ،kj = -i ،ji = -k ،ki = j ،jk = i ،ij = k$$

لاحظ التشابه مع ما يُسمّى الضرب التصالبي على المتجهات، فهذه الصيغ سهلة التذكر إذا فكرنا في المتتالية :

$$.i, j, k, i, j, k$$

الضرب من اليسار إلى اليمين لعنصرين متتاليين هو العنصر الآتي من اليمين، والضرب من اليمين إلى اليسار لعنصرين متاليين هو سالب العنصر الآتي من اليسار، بعدها نعرّف الضرب كما يجب ليحقق قانوني التوزيع، وهو:

$$(a_1 + a_2 i + a_3 j + a_4 k)(b_1 + b_2 i + b_3 j + b_4 k)$$
$$= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3)i$$
$$+ (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2) j$$
$$+ (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1)k.$$

يبين تمرين 19 أنّ المرباعيات تماثل حلقة جزئية من $M_2(\mathbb{C})$ ؛ لذلك، فالضرب تجميعي.

لأن $ij = k$ و $ji = -k$، نرى أنّ الضرب ليس إبداليًّا؛ ولذلك، $\mathbb{H}$ بالتأكيد ليس حقلاً، وبالعودة إلى توافر المعكوس الضربي، ليكن $a = a_1 + a_2 i + a_3 j + a_4 k$، حيث ليس كل $a_i = 0$، فالحساب يبين أنّ

$$(a_1 + a_2 i + a_3 j + a_4 k)(a_1 - a_2 i - a_3 j - a_4 k) = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

إذا افترضنا

$$\bar{a} = a_1 - a_2 i - a_3 j - a_4 \mathrm{k} \text{ و } |a|^2 = a_1^{\,2} + a_2^{\,2} + a_3^{\,2} + a_4^{\,2}$$

نرى أنَّ

$$\frac{\bar{a}}{|a|^2} = \frac{a_1}{|a|^2} - \left(\frac{a_2}{|a|^2}\right) i - \left(\frac{a_3}{|a|^2}\right) j - \left(\frac{a_4}{|a|^2}\right) k$$

المعكوس الضربي لـ a. وبذلك نعدّ أنفسنا قد وضّحنا المبرهنة الآتية:

9.24 مبرهنة المرباعيات $\mathbb{H}$ تشكل حقلًا تخالفيًّا قطعيًّا بالنسبة إلى الجمع والضرب.

لاحظ أنّ $G = \{\pm 1, \pm i, \pm j, \pm k\}$ هي زمرة من الرتبة 8 تحت الضرب الرباعي.

هذه الزمرة تتولد من i و j، حيث :

$$ji = i^3 j \text{ ،} j^2 = i^2 \text{ ،} i^4 = 1$$

ووجد حقول تخالفية منتهية قطعًا، وهذا هو محتوى المبرهنة الشهيرة لويبدربيرن (Wedder-burn) التي سنذكرها من غير برهان.

10.24 مبرهنة (مبرهنة ويدربيرن) كل حلقة قسمة منتهية حقل.

البرهان انظر آرتن، نيسبت وثرال [24] لإثبات مبرهنة ويدربيرن. ◆

■ تمارين 24

حسابات

في التمارين 1 إلى 3، لتكن $G = \{e, a, b\}$ زمرة دورية من الرتبة 3، حيث العنصر المحايد e. اكتب العنصر في جبر الزمرة $\mathbb{Z}_5 G$ على صورة:

$$r, s, t \in \mathbb{Z}_5 \text{ لـ } re + sa + tb$$

1. $(2e + 3a + 0b) + (4e + 2a + 3b)$

2. $(2e + 3a + 0b)(4e + 2a + 3b)$

3. $(3e + 3a + 3b)^4$

في التمارين 4 إلى 7، اكتب العنصر في $\mathbb{H}$ على صورة $a_1 + a_2 i + a_3 j + a_4 k$ لـ $a_i \in \mathbb{R}$.

4. $(i + 3j)(4 + 2j - k)$

5. $i^2 j^3 k j i^5$

6. $(i + j)^{-1}$

7. $[(1 + 3i)(4j + 3k)]^{-1}$

8. بالرجوع إلى الزمرة S_3، المعطاة في مثال 7.8 احسب حاصل ضرب:

$$(0\rho_0 + 1\rho_1 + 0\rho_2 + 0\mu_1 + 1\mu_2 + 1\mu_3)(1\rho_0 + 1\rho_1 + 0\rho_2 + 1\mu_1 + 0\mu_2 + 1\mu_3)$$

في جبر الزمرة $\mathbb{Z}_2 S_3$.

9. أوجد مركز الزمرة $\langle \mathbb{H}^*, . \rangle$، حيث $\mathbb{H}^*$ هي مجموعة المرباعيات غير الصفرية.

مفاهيم

10. أوجد مجموعتين جزئيتين من $\mathbb{H}$ مختلفتين عن $\mathbb{C}$ وعن بعضهما، كل منهما حقل مماثل لـ $\mathbb{C}$ بالنسبة إلى الجمع والضرب المشتقين من $\mathbb{H}$.

11. ضع إشارة صح أو إشارة خطأ:

_____ أ. لا يوجد قواسم لـ 0 في $M_n(F)$ لأيّ n ولأيّ حقل F.

_____ ب. كل عنصر غير صفري في $M_2(\mathbb{Z}_2)$ عنصر وحدة.

_____ جـ. $\text{End}(A)$ دائمًا حلقة فيها العنصر المحايد $\neq 0$ لأي زمر إبدالية A.

_____ د. $\text{End}(A)$ ليست أبدًا حلقة فيها العنصر المحايد $\neq 0$ لأي زمرة إبدالية A.

_____ هـ. المجموعة الجزئية Iso (A) من End (A) ـ تحوي التماثلات الغامرة من A إلى Aـ تشكل حلقة جزئية من End (A) لأيّ زمرة إبدالية A.

_____ و. $R \langle \mathbb{Z}, +, . \rangle$ تماثل $\langle \mathbb{Z}, +, . \rangle$ لأيّ حلقة إبدالية R فيها العنصر المحايد.

_____ ز. حلقة الزمرة RG للزمرة الإبدالية G، هي حلقة إبدالية لأي حلقة إبدالية R فيها العنصر المحايد.

_____ ح. تشكل المرباعيات حقلًا.

_____ ط. $\langle \mathbb{H}^*, . \rangle$ زمرة، حيث $\mathbb{H}^*$ مجموعة المرباعيات غير الصفرية.

_____ ي. ليست أي حلقة جزئية من $\mathbb{H}$ حقلًا.

12. وضّح كلاً مما يأتي بمثال:

أ. كثيرة حدود من الدرجة n، حيث معاملاتها من حقل تخالفي قطعي، يمكن أن يكون لها أكثر من n من الأصفار في الحقل التخالفي.

ب. زمرة جزئية ضربية منتهية من حقل تخالفي قطعي، ممكن ألا تكون دورية.

براهين

13. لتكن ϕ العنصر في $\text{End}\left(\langle \mathbb{Z}\times\mathbb{Z}, + \rangle\right)$ المعطى في المثال 2.24، الذي بيَّن أنّ ϕ قاسم لـ 0 من اليمين. بيِّن أنّ ϕ أيضًا قاسم لـ 0 من اليسار.

14. بيِّن أنّ $M_2(F)$ فيها على الأقل ستة عناصر وحدة لأي حقل F. أوجد عناصر الوحدة هذه. [مساعدة: في F على الأقل عنصران: 0 و 1].

15. بيِّن أنّ $\text{End}\left(\langle \mathbb{Z}, + \rangle\right)$ تماثل طبيعي (قانوني) $\langle \mathbb{Z}, +, . \rangle$ و $\text{End}(\langle \mathbb{Z}_n, + \rangle)$ تماثل طبيعي $(\langle \mathbb{Z}_n, +, . \rangle)$.

16. بيِّن أنّ $\text{End}(\langle \mathbb{Z}_2 \times \mathbb{Z}_2, + \rangle)$ لا تماثل $\langle \mathbb{Z}_2 \times \mathbb{Z}_2, +, . \rangle$.

17. بالعودة إلى مثال 3.24، بيِّن أنّ $YX - XY = 1$.

18. إذا كانت $G = \{e\}$ زمرة من عنصر واحد، بيِّن أنّ RG تُماثل R لأي حلقة R.

19. توجد مصفوفة $K \in M_2(\mathbb{C})$، بحيث $\phi : \mathbb{H} \to M_2(\mathbb{C})$ المعرفة بـ

$$\phi(a + bi + ci + dk) = a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + c\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} + dk$$

لكل $a, b, c, d \in \mathbb{R}$، تعطي تماثلًا من $\mathbb{H}$ إلى $\phi[\mathbb{H}]$.

أ. أوجد المصفوفة K.

ب. ما المرباعيات الثمانية التي يجب فحصها، لنرى أنّ ϕ هي حقيقةً تشاكل؟

جـ. ما الشيء الآخر الذي يجب فحصه، لنبيِّن أنّ ϕ تعطي تماثلًا من $\mathbb{H}$ إلى $\phi[\mathbb{H}]$؟

الفصل 25 الحلقات والحقول المرتبة[3] Orderd Rings and Fields

نحن خبراء بعلاقة التباين $>$ على المجموعة $\mathbb{R}$ وعلى أي مجموعة جزئية من $\mathbb{R}$.

(نذكرك بأنّ العلاقات نوقشت في الفصل 0، انظر تعريف 7.0). نلاحظ أنّ $>$ تعطينا ترتيبًا على الأعداد الحقيقية، وفي هذا الفصل، سندرس الترتيبات على الحلقات والحقول، حيث سنفترض خلاله أنّ الحلقات التي سنناقشها فيها العنصر المحايد غير الصفري 1.

في الأعداد الحقيقية، $a < b$ إذا وفقط إذا كان $b - a$ موجبًا؛ لذلك، فإنّ علاقة الترتيب $>$ على $\mathbb{R}$ مفهومة تمامًا، إذا علمنا ما الأعداد الموجبة.

سنستخدم فكرة وصف عناصر محددة بالموجبة لتعريف مفهوم الحلقة المرتبة.

1.25 تعريف **الحلقة المرتبة (ordered ring)** هي حلقة R مع مجموعة جزئية ليست خالية P من R وتحقق الخاصيتين الآتيتين:

إغلاق (closure) لكل $a, b \in P$، كلا $a + b$ و ab في P.

تثليث (trichotomy) لأي $a \in R$، واحد وفقط واحد من هذه الأمور يتحقق:

$$a \in P,\ a = 0,\ -a \in P.$$

تسمّى عناصر P "**موجبة**" **(positive)**. ■

من السهولة أن ترى أنه إذا كانت R حلقة مرتبة، حيث المجموعة P هي العناصر الموجبة، و S حلقة جزئية من R، فإن $P \cap S$ تحقق متطلبات مجموعة العناصر الموجبة في الحلقة S، وهذا يعطي ترتيبًا على S. (انظر تمرين 26). هذا هو **الترتيب المحدث (induced ordering)** من الترتيب المعطى على R.

نلاحظ من الوهلة الأولى أنّ للحلقات $\mathbb{Z}$، و $\mathbb{Q}$ و $\mathbb{R}$ مجموعة العناصر التي نعدّها دائمًا موجبة، يتحقق فيها شرطا الإغلاق والتثليث، سنشير إلى هذا الترتيب المألوف لهذه الحلقات والترتيب المحدث للحلقات الجزئية منها **بالترتيب الطبيعي**، وسنقدم الآن مفهومًا غير مألوف.

2.25 مثال لتكن R حلقة مرتبة والمجموعة P من العناصر الموجبة، هناك طريقان طبيعيان لتعريف الترتيب على حلقة كثيرة الحدود $R[x]$، حيث سنصف مجموعتين محتملتين، P_{low} و P_{high} من العناصر الموجبة، وكثيرة الحدود غير الصفرية في $R[x]$ تكتب على صورة:

[3] هذا الفصل لا يستخدم في باقي الكتاب.

$$f(x) = a_r x^r + a_{r+1} x^{r+1} + \ldots + a_n x^n$$

حيث $a_r \neq 0$ و $a_n \neq 0$ لذلك، $a_r x^r$ و $a_n x^n$ هما الحدّان غير الصفريين لأقل وأعلى رتبة على الترتيب، لتكن P_{low} هي مجموعة $f(x)$ كلها، حيث $a_r \in P$، و لتكن P_{high} هي مجموعة $f(x)$ كلها، حيث $a_n \in P$. إن متطلبات الإغلاق والتثليث التي يجب على P_{low} و P_{high} تحقيقها لتعطي ترتيبًا على $\mathrm{R}[x]$، تنبع من الوهلة الأولى من الخصائص نفسها على P وتعريف الجمع والضرب في $R[x]$، وبالتطبيق على $\mathbb{Z}[x]$، حيث الترتيب معطًى بـ P_{low} فكثيرة الحدود

$f(x) = -2x + 3x^4$ ليست موجبة؛ لأن -2 ليس موجبًا في $\mathbb{Z}$، وباستخدام الترتيب المعطى بـ P_{high} كثيرة الحدود نفسها، ستكون موجبة؛ لأن 3 موجب في $\mathbb{Z}$. ▲

افترض أنّ P هي مجموعة العناصر الموجبة في الحلقة المرتبة R، وليكن a عنصرًا غير صفري من R، فإنه إما a أو $-a$ في P؛ لذلك، باستخدام الإغلاق $a^2 = (-a)^2$ أيضًا في P ؛ ولذلك، مربعات العناصر غير الصفرية من R موجبة. بوجه خاص، $1=1^2$ موجب، باستخدام الإغلاق، نرى أنّ $1+1+\cdots+1+1$ لأي عدد منته من الجمع دائمًا في P؛ لذلك، ليس صفرًا أبدًا، وعليه، فإنّ الحلقة المرتبة مميزها صفر؛ ولأنّ مربعات العناصر غير الصفرية يجب أن تكون موجبة، نرى أنّ الترتيب الطبيعي على $\mathbb{R}$ هو الترتيب الوحيد الممكن، والأعداد الحقيقية الموجبة هي بالضبط مربعات الأعداد الحقيقية غير الصفرية، وهذه المجموعة لا يمكن توسيعها دون تدمير التثليث؛ ولأن $1+1+\ldots+1+1$ يجب أن تكون موجبة، فإنّ الترتيب الممكن على $\mathbb{Z}$ هو الترتيب الطبيعي أيضًا، فالحلقات المرتبة كلها مميزها صفر؛ لذلك، يمكننا عن طريق إعادة التعريف (التسمية)، أن نعدّ كل حلقة مرتبة تحوي $\mathbb{Z}$ بوصفها حلقة جزئية مرتبة.

إذا كانت a و b عناصر غير صفرية من P، فإنه إما $-a$ أو a في P وإما $-b$ أو b في P، وبوصفها نتيجة منطقية من الإغلاق، فإنه إما ab أو $-ab$ في P، إذ لا يمكن أن يكون ab صفرًا باستخدام التثليث، وعليه، فإنّ الحلقة المرتبة ليست لها قواسم للصفر.

نلخص هذه الاستنتاجات في مبرهنة ونتيجة.

3.25 مبرهنة لتكن R حلقة مرتبة. مربعات العناصر جميعها غير الصفرية في R موجبة، R مميزها 0، ولا توجد فيها قواسم للصفر.

4.25 نتيجة يمكننا أن نعدّ $\mathbb{Z}$ مدخلة في أي حلقة مرتبة R، والترتيب المحدث على $\mathbb{Z}$ من R هو الترتيب الطبيعي على $\mathbb{Z}$، الترتيب الوحيد الممكن على $\mathbb{R}$ هو الترتيب الطبيعي.

توضّح المبرهنة 3.25 أنّ الحقل $\mathbb{C}$ من الأعداد المركبة لا يمكن أن يكون مرتبًا؛ لأن كلًّا من $1=1^2$ و $-1=i^2$ مربعان، وتوضح أيضًا، أنه لا توجد حلقة منتهية يمكن أن تكون مرتبة؛ لأن مميز أي حلقة مرتبة صفر.

المبرهنة القادمة تعرّف العلاقة $<$ في حلقة مرتبة، وتقدم خصائصها .

تعريف $<$ مشتقة من المفهوم الذي ينصّ على أنه في الأعداد الحقيقية، $a<b$ إذا وفقط إذا كان $b-a$ موجبًا، توضّح المبرهنة أيضًا، أنّ الترتيب يمكن تعريفه بدلالة علاقة $<$ ذات الخصائص المذكورة أدناه.

5.25 مبرهنة لتكن R حلقة مرتبة، حيث P مجموعة العناصر الموجبة، لتكن $<$، وتقرأ "أقلّ من"، علاقة على R معرفة بـ $a < b$ إذا وفقط إذا كان $(b - a) \in P$ (1)

لـ $a, b \in R$. العلاقة $<$ لها الخصائص الآتية لكل $a, b, c \in R$.

التثليث (Trichotomy) واحد وفقط واحد من هذ الأمور تتحقق:

$$a < b,\ a = b,\ b < a$$

التعدي (Transitivity) إذا كانت $a<b$ و $b<c$، فإن $a<c$.

التواتر (Isotonicity) إذا كانت $b < c$، فإن $a + b < a + c$

وإذا كانت $b < c$ و$a > 0$، فإنّ $ab < ac$ و $ba < ca$.

وبالعكس، إذا أُعْطيت علاقة $<$ على حلقة غير صفرية R تحقق هذه الشروط الثلاثة، فإنّ المجموعة $P = \{x \in R \mid 0 < x\}$ تحقق خاصيتين لمجموعة العناصر الموجبة في تعريف 1.25، والعلاقة $<_P$ المعرفة في الشرط (1) بالنسبة إلى P هي العلاقة $<$ المعطاة.

البرهان لتكن R حلقة مرتبة، حيث P مجموعة العناصر الموجبة، ولتكن $a < b$ تعني $(b - a) \in P$). سنثبت الخصائص الثلاث لـ $<$.

التثليث: لتكن $a,b \in R$، باستخدام خاصية التثليث على P في تعريف 1.25 ومطبقةً على $b-a$، بالضبط واحد من:

$$(b - a) \in P,\ b - a = 0,\ (a - b) \in P$$

متحقق: تترجم هذه بدلالة $<$ إلى

$$a < b,\ a = b,\ b < a$$

على الترتيب.

التعدي: لتكن $a < b$ و $b < c$، فإنّ $(b - a) \in P$ و $(c - b) \in P$)، وباستخدام الإغلاق على P تحت الجمع، يكون لدينا:

$$(b - a) + (c - b) = (c - a) \in P$$

لذلك، $a < c$.

التواتر: لتكن $b < c$، إذن $(c - b) \in P$)، وهكذا، فإنّ $(a + c) - (a + b) = (c - b) \in P$ إذن $a + b < a + c$. كذلك، إذا كان $a > 0$، فباستخدام الإغلاق على P، كلّ من $a(c - b) = ac - ab$ و $(c - b)a = ca - ba$ في P، إذن، $ab < ac$ و $ba < ca$.

سنترك الجزء "وبالعكس" من المبرهنة بوصفه تمرينًا سهلًا ومماثلًا. (انظر تمرين 27).◆

باستعراض المبرهنة 5.25، سنشعر الآن بحرية لاستخدام < لترمز إلى الحلقة مرتبة الرموز >، ≤ و≥ معرّفة عادة بدلالة < و= . أي إنّ

$a > b$ تعني $a < b$، $a \leq b$ تعني إما $a=b$ أو $a < b$،

$a \geq b$ تعني إما $b < a$ أو $b=a$.

6.25 مثال لتكن R حلقة مرتبة، إنَّه لأمر توضيحي بأن نفكر فيما تعنيه الترتيبات على $R[x]$ المعطاة بـ P_{low} و P_{high} في المثال 2.25 بدلالة العلاقة < في المبرهنة 5.25.

بأخذ P_{low} في الحسبان، نلاحظ أنَّه لأي $a > 0$ في R، $a - x$ موجب إذن، $a > 0$، كذلك، $x = x - 0$ موجبة، إذن، $x > 0$ ؛ لذلك $0 < x < a$ لكل a في R، ولدينا $(x^i - x^j) \in P_{low}$ عندما $i < j$، إذن، $x^j < x^i$ إذ كان $i < j$. وحيدات الحدّ لها الترتيب:

$$0 < \ldots x^6 < x^5 < x^4 < x^3 < x^2 < x < a$$

لأي عدد موجب $a \in R$. بأخذ $R = \mathbb{R}$، نرى أنه في هذا الترتيب على $\mathbb{R}[x]$ يوجد عدد لا نهائي من العناصر الموجبة، التي هي أقل من أي عدد حقيقي موجب!

سنترك النقاش المشابه لـ < بالنسبة إلى الترتيب على $R[x]$ المعطى بـ P_{high} إلى تمرين 1. ▲

7.25 تعريف المثال السابق مهم؛ لأنه يقدم ترتيبًا غير أرخميدي، وسنقدم تعريفًا يوضّح هذا المفهوم، تذكر أنه يمكننا أن نعدّ $\mathbb{Z}$ حلقة جزئية من أيّ حلقة مرتبة.

الترتيب على الحلقة R الذي له هذه الخاصية:

لأي عنصرين موجبين a و b في R، يوجد عدد صحيح موجب n، بحيث $na > b$ هو **ترتيب أرخميدي (Archimedian ordering)**. ■

الترتيب الطبيعي على $\mathbb{R}$ أرخميدي، بينما الترتيب على $\mathbb{R}[x]$ المعطى بـ P_{low} الذي نوقش في مثال6.25 ليس أرخميديًّا؛ لأنه لأي عدد صحيح موجب n لدينا $(17 - nx) \in P_{low}$، إذن $nx < 17$ لكل $n \in \mathbb{Z}^+$.

سنقدم مثالين نصف بهما أنواع الحلقات المرتبة والحقول، التي تهمنا في عملٍ أكثر تطورًا.

مثال 8.25 (**حلقات متسلسلة القوى الشكلية**): لتكن R حلقة، وقد عرّفنا كثيرة الحدود في الفصل 22 في $R[x]$ على أنها المجموع الشكلي، $\sum_{i=0}^{\infty} a_i x^i$ حيث كل a_i أصفار عدا عدد منته من a_i ليس صفرًا، وإذا لم نشترط أيًّا من a_i صفرًا، فسنحصل على **متسلسلة القوى الشكلية** في x، حيث المعاملات من الحلقة R. (الصفة شكلي، تستخدم بصورة عرفية؛ لأننا لا نتعامل مع المتسلسلات المتقاربة). بالضبط الصيغ نفسها التي سنستخدمها لتعريف الجمع والضرب على هذه المتسلسلات، هي المستخدمة على كثيرات الحدود في الفصل 22. مارس معظمنا جمع المتسلسلات وضربها عند دراسة التفاضل والتكامل، فهذه المتسلسلات تمثل حلقة يرمز لها بـ $R[[x]]$، التي تحوي $R[x]$ بوصفها حلقة جزئية.

إذا كانت R حلقة مرتبة، فيمكننا توسيع الترتيب على $R[[x]]$، بالضبط كما وسّعنا الترتيب على $R[x]$ مستخدمين المجموعة P_{low} للعناصر الموجبة. (لا يمكننا أن نستخدم P_{high}. لم لا؟) ووحيدات الحدّ لها الترتيب نفسه الذي عرضناه في المثال 6.25. ▲

مثال 9.25 (**حقول متسلسلات لورنت الشكلية Formal Laurent Series Fields**): بالاستمرار في فكرة مثال 8.25، نفترض F حقلًا، ولتكن المتسلسلة الشكلية $\sum_{i=N}^{\infty} a_i x^i$، حيث N أي عدد صحيح موجب، صفر أو سالب، و$a_i \in F$. (بالتماثل، يمكننا أن نعدّ $\sum_{i=-\infty}^{\infty} a_i x^i$ حيث a_i كلها – عدا عدد نهائي من a_i– صفر للقيم السالبة من i، إذ إننا خلال دراسة التفاضل والتكامل لدوال المتغيرات التخيلية، نواجه متسلسلات من هذا النوع المسماة "متسلسلات لورنت")، وبالجمع والضرب الطبيعي على هذه المتسلسلات نحصل فعليًّا على حقل يرمز له بـ $F((x))$. معكوس x هي المتسلسلة $x^{-1} + 0 + 0x + 0x^2 + \cdots$ معكوسات العناصر والكسور يمكن حسابها باستخدام قسمة المتسلسلات، وسنحسب أول ثلاثة حدود لـ $(x^{-1} - 1 + x - x^2 + x^3 + \cdots)/(x^3 + 2x^4 + 3x^5 + \cdots)$ في $\mathbb{R}((x))$ للتوضيح.

$$
\begin{array}{r|l}
x^3 + 2x^4 + 3x^5 + \cdots & x^{-1} - 1 + x - x^2 + x^3 + \cdots \\
\hline
 & x^{-4} - 3x^{-3} + 4x^{-2} + \cdots \\
 & \underline{x^{-1} + 2 + 3x + \cdots} \\
 & \quad -3 - 2x + \cdots \\
 & \quad \underline{-3 - 6x - 9x^2 + \cdots} \\
 & \qquad 4x + \cdots
\end{array}
$$

إذا كان F حقـلا مرتبًـا، فيمكننـا أن نستخـدم التناظـر الموضـح لـ P_{low} في $R[[x]]$ لنعـرف الترتيـب علـى $F((x))$. وسنطلـب منـك في تمريـن 2 رمزيًّـا ترتيـب وحيـدات الحـد $\cdots x^{-3}, x^{-2}, x^{-1}, x^0 = 1, x, x^2, x^3, \cdots$ كما فعلنا لـ $R[x]$ في مثال 6.25.

لاحظ أنّ $F((x))$ تحوي– بوصفه حقلًا جزئيًّا– حقل خوارج القسمة على $F[x]$، وبذلك نشتق ترتيبًا على حقل خوارج القسمة هذا. ▲

لتكن R حلقة مرتبة، ولتكن $\phi: R \to R'$ تماثل حلقات. إنه لأمر واضح بصورة بدهية مع إعادة التعريف (إعادة التسمية)، أنّه يمكن استخدام الدالة ϕ لحمل الترتيب على R إلى الترتيب على R' . نلخص ذلك على صورة مبرهنة، ويجب إثباتها لمنع الشك، حيث نترك الإثبات إلى التمرين 25.

10.25 مبرهنة لتكن R حلقة مرتبة، حيث P هي مجموعة العناصر الموجبة، وليكن $\phi: R \to R'$ تماثل حلقات، حيث تحقق المجموعة الجزئية $P'=\phi[P]$ متطلبات تعريف 1.25 لمجموعة العناصر الموجبة لـ R'، إضافة إلى ذلك، في الترتيب على R' المعطى من P'، عندنا $\phi(a) <' \phi(b)$ في R'، إذا وفقط إذا كان $a < b$ في R.

لنُسَمِّ الترتيب على R' الموصوف في المبرهنة السابقة "**الترتيب المحدث عن طريق**" ϕ من الترتيب على R.

11.25 مثال نصَّ مثال 9.22 على أنّ تشاكل التعويض $\phi_\pi: \mathbb{Q}[x] \to \mathbb{R}$، حيث:

$$\phi(a_0 + a_1 x + \ldots + a_n x^n) = a_0 + a_1 \pi + \ldots + a_n \pi^n$$

هو واحد لواحد، وبذلك، فهو يزوّدنا بتماثل من $\mathbb{Q}[x]$ إلى $\phi[\mathbb{Q}[x]]$. نرمز إلى هذه الحلقة المصورة بـ $\mathbb{Q}[\pi]$. إذا زودنا $\mathbb{Q}[x]$ بترتيب مستخدمين المجموعة P_{low} للمثالين 2.25 و6.25، فإنّ الترتيب على $\mathbb{Q}[\pi]$ المشتق من φ_π مختلف تمامًا عن الترتيب الطبيعي (الوحيد) على $\mathbb{R}$، ففي الترتيب P_{low}، π أقل من أي عنصر في $\mathbb{Q}$! ▲

أي تماثل من حلقة R على نفسها يسمى **تماثلًا ذاتيًّا** (**automorphism**) على R، حيث يمكن استخدام المبرهنة 10.25 لتقديم ترتيبات مختلفة على حلقة مرتبة R، إذا توافر تماثل ذاتي على R لا ينقل المجموعة P من العناصر الموجبة إلى نفسها. نقدم هذا المثال:

12.25 مثال يبيّن تمرين 11 في الفصل 18 أنّ: $\{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ حلقة.

لنرمز لهذه الحلقة بـ $\mathbb{Z}[\sqrt{2}]$، إذ إنّ لها ترتيبًا طبيعيًّا مشتقًّا من $\mathbb{R}$ ، حيث $\sqrt{2}$ موجب، لكن، ندَّعي أنّ $\mathbb{Z}[\sqrt{2}]$ هي $\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ ، معرّفة بـ $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$ تماثل ذاتي، ومن الواضح أنها واحد لواحد وغامر على $\mathbb{Z}[\sqrt{2}]$، سنترك التحقق من خاصية التشاكل إلى تمرين 17؛ ولأن $\phi(\sqrt{2}) = -\sqrt{2}$ ، نرى أنّ الترتيب المحدث من ϕ سيكون واحدًا، حيث $-\sqrt{2}$ موجب! في الترتيب الطبيعي على $\mathbb{Z}[\sqrt{2}]$، العنصر $m + n\sqrt{2}$ موجب، إذا كان m و n كلاهما موجبًا، أو إذا كان m موجب و $2n^2 < m^2$، أو إذا كان m موجبًا و $m^2 < 2n^2$. سنطلب إليك في تمرين 3 أن تعطينا الصفات المناظرة للعناصر الموجبة في الترتيب على $\mathbb{Z}[\sqrt{2}]$ المحدث من ϕ. ▲

باستعراض المثالين 11.25 و 12.25؛ اللذين قدّما ترتيبين على حلقتين جزئيتين من $\mathbb{R}$ ليس هما الترتيبين المحدثين، نتساءل فيما إذا كانت $\mathbb{Q}$ تقبل ترتيبًا آخر غير الترتيب الطبيعي، مبرهنتنا الأخيرة توضِّح أنَّ هذا مستحيل.

13.25 مبرهنة لتكن D حلقة تامة مرتبة، حيث P مجموعة العناصر الموجبة، وليكن F حقل خوارج القسمة على D. المجموعة

$$P' = \{x \in F \mid x = a/b \text{ حيث } a, b \in D \text{ و } ab \in P\}$$

حسنة التعريف، وتقدِّم ترتيبًا على F المشتق من الترتيب المعطى على D، إضافة إلى ذلك، P' هي المجموعة الجزئية الوحيدة من F التي لها هذه الخاصية.

البرهان لتوضيح أنّ P' حسنة التعريف، افترض أنّ $x = a/b = a'/b'$ لـ $a, b, a', b' \in D$

و $ab \in P$، علينا أن نوضّح $a'b' \in P$. من $a/b = a'/b'$، نحصل على $ab' = a'b$، وبالضرب في b، نحصل على $(ab)\, b' = a'\, b^2$ الآن $b^2 \in P$، وبافتراض $ab \in P$.

باستخدام التثليث والخصائص $a\,(-b) = (-a)b = -\,(ab)$ للحلقة، نرى أنَّه إما a' و b' كلاهما في P أو كلاهما ليس في P، وفي كل حالة، نحصل على $a'\, b' \in P$. نبدأ بالإغلاق على P'، لتكن $x = a/b$ و $y = c/d$ عنصرين من P'، إذن، $ab \in P$ و $cd \in P$. الآن، $x + y = (ad + bc)/bd$ و $(ad + bc)bd = (ab)d^2 + b^2(cd)$ في P؛ لأنَّ المربعات أيضًا في P و P مغلقة على الجمع والضرب؛ لذلك، $(x + y) \in P'$. أيضًا $xy = ac/bd$ في P'؛ لأنّ $acbd = (ab)(cd)$ هي حاصل ضرب عنصرين من P، وبهذا هي في P.

بالنسبة إلى التثليث، نريد فقط أن نلاحظ أنَّه لـ $x = a/b$، حاصل الضرب ab يحقق فقط واحدًا من

$$ab \in P,\ ab = 0,\ ab \notin P$$

باستخدام التثليث على P. بالنسبة إلى P' تترجم هذه إلى $x \in P'$، $x=0$، و$x \notin P'$ على الترتيب.

أوضحنا أنّ P' تقدم ترتيبًا على F. بالنسبة إلى $a \in D$، نرى أنَّ $a = a/1$ في P'، إذا وفقط إذا كان $a1=a$ في P؛ لذلك، الترتيب المعطى على D هو بالفعل الترتيب المحدث من F عن طريق P'.

أخيرًا، افترض أنّ P'' هي مجموعة العناصر الموجبة من F، التي تحقق شروط التعريف 1.25، بحيث P'' $\cap D = P$.، لتكن $x = a/b \in P''$، حيث $a, b \in D$، فإن $xb^2 = ab$ يجب أن يكون في P''؛ لذلك،

$ab \in (P'' \cap D) = P$. إذن $x \in P'$، ولذلك $P'' \subseteq P'$.

يوضح قانون التثليث أنَّه يجب أن يكون عندنا بعدها $P'' = P'$؛ لذلك، تعطينا P' الترتيب الوحيد على F الذي يحافظ على الترتيب الأصلي لعناصر D. ♦

■ تمارين 25

حسابات

1. لتكن R حلقة مرتبة. صف ترتيب عنصر موجب في R ووحيدات الحدّ $x, x^2, x^3, \cdots, x^n, \cdots$ في $R[x]$، كما فعلنا في مثال 6.25، باستخدام المجموعة P_{high} للمثال 25. 6 على أنها مجموعة العناصر الموجبة في $R[x]$.

2. ليكن F حقلًا مرتبًا، وليكن $F((x))$ حقل متسلسلات لورنت الشكلية، حيث المعاملات من F، التي نوقشت في المثال 9.25. صف ترتيب وحيدات الحدّ $\cdots x^{-3}, x^{-2}, x^{-1}, x^0 = 1, x, x^2, x^3, \cdots$ باستخدام الترتيب على $F((x))$ الموصوف في ذلك المثال.

3. وصف مثال 12.25 الترتيب على $\mathbb{Z}\left[\sqrt{2}\right] = \left\{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\right\}$، بحيث $-\sqrt{2}$ موجب. صف بدلالة m وn، العناصر الموجبة جميعها في $\mathbb{Z}\left[\sqrt{2}\right]$ باستخدام ذلك الترتيب.

في التمارين 4 إلى 9، لتكن $\mathbb{R}[x]$ عليها الترتيب المعطى بـ

i. P_{low} ii. P_{high}

الموصوف في المثال 2.25 في كل حالة (i) و (ii)، رتّب الرموز أ، ب، ج، د، هـ لكثيرات الحدود المعطاة بترتيب يتبع الترتيب التصاعدي لكثيرات الحدود، كما وصف بالعلاقة $<$ للمبرهنة 25.5.

4. أ. $-5 + 3x$ ب. $5 - 3x$ ج. $-x + 7x^2$ د. $x - 7x^2$ هـ. $2 + 4x^2$

5. أ. -1 ب. $3x - 8x^3$ جـ. $-5x + 7x^2 - 11x^4$ د. $8x^2 + x^5$ هـ. $-3x^3 - 4x^5$

6. أ. $-3 + 5x^2$ ب. $-2x + 5x^2 + x^3$ جـ. -5 د. $6x^3 + 8x^4$ هـ. $8x^4 - 5x^5$

7. أ. $-2x^2 + 5x^3$ ب. $x^3 + 4x^4$ جـ. $2x - 3x^2$ د. $-3x - 4x^2$ هـ. $2x - 2x^2$

8. أ. $4x - 3x^2$ ب. $4x + 2x^2$ جـ. $4x - 6x^3$ د. $5x - 6x^3$ هـ. $3x - 2x^2$

9. أ. $x - 3x^2 + 5x^3$ ب. $2 - 3x^2 + 5x^3$ جـ. $x - 3x^2 + 4x^3$ د. $x + 3x^2 + 4x^4$ هـ. $x + 3x^2 - 4x^3$

في التمارين 10 إلى 13، لتكن $\mathbb{Q}((x))$ لها الترتيب الموصوف في المثال 9.25 رتّب الرموز أ، ب، جـ، د، هـ للعناصر المعطاة بترتيب يتبع الترتيب التصاعدي لتلك العناصر، كما هو موصوف بالعلاقة $<$ للمبرهنة 5.25.

10. أ. $\frac{1}{x}$ ب. $\frac{-5}{x^2}$ جـ. $\frac{2}{x}$ د. $\frac{-3}{x^2}$ هـ. $4x$

11. أ. $\frac{1}{1-x}$ ب. $\frac{x^2}{1+x}$ جـ. $\frac{1}{x-x^2}$ د. $\frac{-x}{1+x^2}$ هـ. $\frac{3-2x}{x^3+4x}$

12. أ. $\frac{5-7x}{x^2+3x^3}$ ب. $\frac{-2+4x}{4-3x}$ جـ. $\frac{7+2x}{4-3x}$ د. $\frac{9-3x^2}{2+6x}$ هـ. $\frac{3-5x}{-6+2x}$

13. أ. $\frac{1-x}{1+x}$ ب. $\frac{3-5x}{3+5x}$ جـ. $\frac{1}{4x+x^2}$ د. $\frac{1}{-3x+x^2}$ هـ. $\frac{4x+x^2}{1-x}$

مفاهيم

14. يمكن إثبات أنَّ أصغر حقل جزئي من $\mathbb{R}$ يحوي $\sqrt[3]{2}$، يماثل أصغر حقل جزئي من $\mathbb{C}$ يحوي $\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right)$. وضّح لمَ يُبين لنا ـ على الرغم من أنه لا يوجد ترتيب على $\mathbb{C}$ ـ أنّه يمكن إيجاد ترتيب على حقل جزئي من $\mathbb{C}$ يحوي عناصر لَيست أعدادًا حقيقية؟

15. ضع إشارة صح أو إشارة خطأ:

_____ أ. هناك ترتيب وحيد ممكن على الحلقة $\mathbb{Z}$.

_____ ب. يمكن ترتيب الحقل $\mathbb{R}$ فقط بطريقة وحيدة.

_____ جـ. أي حقل جزئي من $\mathbb{R}$ يمكن ترتيبه فقط بطريقة وحيدة.

_____ د. يمكن ترتيب الحقل $\mathbb{Q}$ فقط بطريقة وحيدة.

_____ هـ. إذا كانت R حلقة مرتبة، فإنه يمكن ترتيب $R[x]$ بطريقة مشتقة من الترتيب على R.

_____ و. الترتيب على الحلقة R أرخميدي، إذا كان لكل $a, b \in R$ يوجد $n \in \mathbb{Z}^+$، بحيث $b < na$.

_____ ز. الترتيب على الحلقة R أرخميدي، إذا كان لكل $a, b \in R$، بحيث $0 < a$ يوجد $n \in \mathbb{Z}+$، وبحيث $b < na$.

_____ ح. إذا كانت R حلقة مرتبة و $a \in R$، فإن $-a$ لا يمكن أن تكون موجبة.

_____ ط. إذا كانت R حلقة مرتبة و $a \in R$، فإنه إمّا a أو $-a$ موجبة.

_____ ي. كل حلقة مرتبة فيها عدد لا نهائي من العناصر.

16. صف الترتيب على الحلقة $\mathbb{Q}[\pi]$ الموصوفة في المثال 11.25 بحيث π أكبر من كل عدد نسبي.

براهين

17. بالعودة إلى المثال 12.25، وضِّح أنَّ الدالة $\phi : \mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{R}$، حيث $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$، تشاكل.

في التمارين 18 إلى 24، لتكن R حلقة مرتبة، حيث المجموعة P مجموعة العناصر الموجبة، ولتكن $<$ العلاقة على R المعرفة في المبرهنة 25.5، أثبت العبارة المعطاة.

(الإثباتات جميعها يجب أن تكون بدلالة تعريف 1.25 والمبرهنة 5.25، على سبيل المثال: يجب عليك ألا تقل: "نعلم أنَّ سالب ضرب موجب هو سالب؛ لذلك، إذا كان $a < 0$ و $b < 0$، فإن $ab < 0$").

18. إذا كان $a \in P$، فإن $0 < a$.

19. إذا كان $a, b \in P$ و $ac = bd$، فإنه إما $c = d = 0$ أو $cd \in P$.

20. إذا كان $a < b$، فإنّ $-b < -a$.

21. إذا كان $a < 0$ و $b < 0$، فإنّ $ab > 0$.

22. إذا كان R حقلًا و a, b موجبين، فإنّ a/b موجب.

23. إذا كان R حقلًا و $0 < a < 1$، فإنّ $1/a > 1$.

24. إذا كان R حقلًا و $-1 < a < 0$، فإنّ $1/a < -1$.

25. أثبت المبرهنة 10.25 في الكتاب.

26. بيِّن أنه إذا كانت R حلقة مرتبة والمجموعة P مجموعة العناصر الموجبة وS حلقة جزئية من R، فإن $P \cap S$ تحقق متطلبات العناصر الموجبة في الحلقة S، وبذلك تعطينا ترتيبًا على S.

27. بيِّن أنه إذا كانت العلاقة $<$ على الحلقة R تحقق خصائص التثليث، والتعدي والتواتر المنصوص عليها في المبرهنة 5.25، فإنه توجد مجموعة جزئية P من R، تحقق شروط مجموعة العناصر الموجبة في التعريف 1.25 بحيث إن العلاقة $<_P$، والمعرفة بـ $a <_P b$ إذا وفقط إذا كانت $b - a \in P$ هي نفسها العلاقة $<$.

28. لتكن R حلقة تامة مرتبة. بيِّن أنه إذا كان $a^{2n+1} = b^{2n+1}$، حيث $a, b \in R$ و n عدد صحيح موجب، فإنّ $a=b$.

29. لتكن R حلقة مرتبة، ولتكن الحلقة $R[x, y]$ من كثيرات الحدود في متغيرين، حيث المعاملات من R. يصف المثال 2.25 طريقتين لترتيب $R[x]$، وفي كل واحد منها، يمكننا الاستمرار وترتيب $(R[x])[y]$ بطريقتين متناظرتين بإعطاء أربع طرق للوصول إلى ترتيب $R[x, y]$. توجد هناك أربع طرق أخرى للوصول إلى ترتيب على $R[x, y]$ إذا رتّبنا $R[y]$ بدايةً، وبعدها $(R[y])[x]$. بيَّن أنَّ الترتيبات الثمانية على $R[x, y]$ كلها مختلفة. [مساعدة: يمكن لك أن تبدأ بأن تعدّ إما $x < y$ أو $y < x$ في كلّ من هذه الترتيبات، واستمر في هذا الأسلوب].