الوحدة الخامسة

المثاليات وحلقات العامل
Ideals and Factor Rings

1 الفصل 28 ليس متطلبًا لما بقي من الكتاب.

الفصل 26 التشاكلات وحلقات العامل Homomorphisms and Factor Rings

التشاكلات

عَرَّفنا مفاهيم وللحلقات في الفصل 18؛ لأننا نود الحديث عن تشاكلات تعويض لكثيرات حدود وعن الحلقات المتماثلة، ونعيد بعض التعريفات؛ لتسهيل المراجعة.

تذكر أنّ التشاكل هو دالة تحافظ على التركيب، وتشاكل الحلقات يربط بين البنية الجمعية وبين البنية الضربية لكل منهما.

1.26 تعريف الدالة ϕ من حلقة R إلى حلقة R' هي **تشاكل** (**homomorphism**) إذا كان:

$$\phi(a+b)=\phi(a)+\phi(\mathrm{b})$$

و

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

لكل العناصر a و b في R. ■

عَرَّفنا في المثال 10.18 تشاكلات التعويض، وقد بيّن المثال 11.18 أنّ الدالة $\phi:\mathbb{Z}\to\mathbb{Z}_n$، حيث $\phi(m)$ هو باقي قسمة m على n - هي تشاكل، وهذا مثالٌ آخر بسيط لتشاكل، لكنه أساسي جدًّا.

2.26 مثال (**تشاكلات الإسقاط (projection homomorphisms)**) لتكن R_1 ، R_2 ، ... ، R_n حلقات، ولكل i، الدالة $\pi_i: R_1\times R_2\times\ldots\times R_n \longrightarrow R_i$ المعرفة بـ $\pi_i(r_1, r_2, \cdots, r_n)=r_i$ هي تشاكل إسقاط غامر الى المركبة R_i، فالخاصيتان المطلوبتان متحققتان للتشاكل π_i؛ لأنّ الجمع والضرب في الضرب المباشر يحسب من خلال الجمع والضرب لكل مركبة بصورة منفصلة. ▲

خصائص التشاكلات

سنعمل بطريقتنا خلال الشرح للفصل 13، لكن لتشاكلات حلقات.

3.26 مبرهنة (**رديف المبرهنة 12.13**): ليكن ϕ تشاكلاً من حلقة R إلى R'، فإذا كان 0 هو المحايد الجمعي في R، فإنّ $\phi(0)=0'$ هو المحايد الجمعي في R'، وإذا كان $a\in R$، فإنّ $\phi(-a)=-\phi(a)$، وإذا كانت S حلقة جزئية من R، فإنّ $\phi[S]$ حلقة جزئية من R'، وفي المقابل، إذا كانت S' حلقة جزئية من R'، فإنّ $\phi^{-1}[S']$ حلقة جزئية من R، أخيرًا، إذا كان لـ R عنصر محايد 1، فإنّ $\phi(1)$ عنصر محايد لـ $\phi[R]$ ، باختصار: حلقات جزئية تناظر حلقات جزئية، وحلقات بعنصر محايد تناظر حلقات بعنصر محايد بالنسبة إلى تشاكل حلقات.

البرهان ليكن ϕ تشاكلاً من حلقة R إلى حلقة R'؛ لأن – بوصفها حالة خاصة – ϕ يمكن أن ينظر إليه على أنه تشاكل زمر من $\langle R, +\rangle$ إلى $\langle R', +'\rangle$. تخبرنا المبرهنة 12.13 أنّ $\phi(0) = 0'$ هو العنصر المحايد للجمع لـ R'، وأنّ $\phi(-a) = -\phi(a)$، وتخبرنا أيضًا بأنه إذا كانت S حلقة جزئية من R، فإنه باعتبار زمرة الجمع $\langle S, +\rangle$، فالمجموعة $\langle \phi[S], +'\rangle$ تمثّل زمرة جزئية لـ $\langle R', +'\rangle$. وإذا كان $\phi(s_1)$ و $\phi(s_2)$ عنصرين من $\phi[S]$، فإنّ:

$$\phi(s_1)\,\phi(s_2) = \phi(s_1 s_2)$$

و$\phi(s_1s_2) \in \phi[S]$. وعليه، $\phi(s_1)\phi(s_2) \in \phi[S]$، وهكذا $\phi[S]$ مغلقة بالنسبة إلى الضرب، بناءً على ذلك، $\phi[S]$ حلقة جزئية من R'. في المقابل، تبيِّن المبرهنة 12.13 أيضًا، أنه إذا كانت S' حلقة جزئية من R' ، فإنّ $\langle \phi^{-1}[S'],+\rangle$ حلقة جزئية من $\langle R,+\rangle$. ليكن $a, b \in \phi^{-1}[S']$، وهكذا $\phi(a) \in S'$ و $\phi(b) \in S'$ عندئذ:

$$\phi(ab) = \phi(a)\phi(b).$$

لأنّ $\phi(a)\phi(b) \in S'$، نرى أنّ $ab \in \phi^{-1}[S']$ وهكذا $\phi^{-1}[S']$ مغلقة بالنسبة إلى الضرب، وعليه فإن $\phi[S]$ حلقة جزئية من R.

أخيرًا، إذا كان لـ R عنصر محايد 1، فإنّ لكل $r \in R$ ،

$$\phi(r) = \phi(1r) = \phi(r1) = \phi(1)\phi(r) = \phi(r)\phi(1)،$$

وهكذا $\phi(1)$ عنصر محايد لـ $\phi[R]$. ♦

في المبرهنة 3.26، لاحظ أنّ $\phi(1)$ هو عنصر محايد لـ $\phi[R]$، لكن ليس بالضرورة لـ R'، وسنطلب إليك أن تبيّن ذلك في التمرين 9.

4.26 تعريف لتكن الدالة $\phi : R \to R$ تشاكل حلقات، الحلقة الجزئية

$$\phi^{-1}[0'] = \{r \in R \mid \phi(r) = 0'\}$$

هي **النواة (Kernel)** لـ ϕ، ويرمز لها بالرمز $\text{Ker}(\phi)$. ■

الآن، $\text{Ker}(\phi)$ هي النواة نَفْسُها لتشاكل الزمر من $\langle R, +\rangle$ إلى $\langle R', +\rangle$ المعطاة من خلال ϕ، المبرهنة 15.13 والنتيجة 18.13 لتشاكلات الزمر تعطينا مباشرة نتائج مُنَاظِرة لتشاكلات حلقات.

5.26 مبرهنة (**رديف المبرهنة** 15.13) ليكن $\phi : R \to R'$ تشاكل حلقات، ولتكن $H = \text{Ker}(\phi)$، وليكن $a \in R$. عندئذ $\phi^{-1}[\phi(a)] = a + H = H + a$ ، حيث $a + H = H + a$ هي مجموعة المشاركة التي تحوي a لزمرة الجمع الإبدالية $\langle H, +\rangle$.

6.26 نتيجة (**رديف النتيجة** 18.13) تشاكل حلقات $\phi : R \to R$ هو دالة أحادية إذا وفقط إذا كان $\text{Ker}(\phi) = \{0\}$.

حلقات (خوارج القسمة) العامل

إننا جاهزون الآن لوصف النتائج الرديفة لحلقات الفصل 14، ونبدأ بمناظِرةٍ للمبرهنة 1.14.

7.26 مبرهنة (رديف المبرهنة 1.14) ليكن $\phi : R \to R$ تشاكل حلقات نواته H، عندئذ تُشَكِّلُ مجموعات المشاركة مع الجمع لـ H حلقة R/H، تُعَرَّف عملياتها الثنائية باختيار الممثِّلين، أي إنّ مجموعَ مجموعتي مشاركة مُعرَّف بـ

$$(a + H) + (b + H) = (a + b) + H,$$

وضَرْب مجموعتي مشاركة مُعرَّف بـ

$$(a + H)(b + H) = (ab) + H.$$

أيضًا، الدالة $\mu : R/H \to \phi[R]$، المعرفة بـ $\mu(a + H) = \phi(a)$ هي تماثل.

البرهان مرة أخرى، أنجز جزء الجمع لمبرهنتنا في المبرهنة 1.14، ونكمل بفحص ظواهر الضرب.

يجب أن نبيّن أولاً أنّ ضرب مجموعات المشاركة باختيار الممثلين حسن التعريف، ولعمل ذلك، ليكن $h_1\ h_2 \in H$، وعليه، فإنّ $a + h_1$ مُمَثِّلٌ لـ $a + H$ و $b + h_2$ مُمَثِّلٌ لـ $b + H$. ليكن

$$c = (a+h_1)(b+ h_2) = ab + ah_2 + h_1b + h_1h_2$$

يجب أن نثبت أنّ هذا العنصر c يقع في مجموعة المشاركة $ab +H$ ولأن

$ab+H = \phi^{-1}[\phi(ab)]$ نحتاج فقط إلى إثبات أنّ $\phi(c) = \phi(ab)$. ولأن ϕ تشاكل و $\phi(h) = 0'$

نحصل لـ $h \in H$ على:

$$\begin{aligned}\phi(c) &= \phi(ab + ah_2 + h_1b + h_1h_2)\\ &= \phi(ab) + \phi(ah_2) + \phi(h_1b) + \phi(h_1h_2)\\ &= \phi(ab) + \phi(a)0' + 0'\phi(b) + 0'0'\\ &= \phi(ab) + 0' + 0' + 0' = \phi(ab). \qquad (1)\end{aligned}$$

وعليه، الضرب باختيار الممثلين حسن التعريف.

لإثبات أنّ R / H حلقة، بقي أن نثبت أنّ الخاصية التجميعية للضرب وقانوني التوزيع متحققة في R / H؛ لأنّ الجمع والضرب يحسب باختيار المُمَثلين، وهذه الخصائص تنتج مباشرة من الخصائص المقابلة في R.

تبيّن المبرهنة 1.14 أنّ الدالة μ المعرَّفة في نَصِّ المبرهنة 4.26 حسنة التعريف، وأحادية، وغامرة لـ $\phi[R]$، وتحقق خاصية الجمع للتشاكل، فمن ناحية الضرب، لدينا:

$$\begin{aligned}\mu[(a+H)(b+H)] &= \mu(ab+H) = \phi(ab)\\ &= \phi(a)\,\phi(b) = \mu(a+H)\mu(b+H)\end{aligned}$$

هذه تُكْمِلُ إثبات أنّ μ تماثل. ♦

8.26 مثال المثال 11.18 يبيّن أنّ الدالة $\phi: \mathbb{Z} \to \mathbb{Z}_n$ المُعرَّفة بـ $\phi(m) = r$ هي تشاكل، حيث r هو باقي m عند قسمته على n؛ لأن $\text{Ker}(\phi) = n\mathbb{Z}$، وتبيّن المبرهنة 7.26 أنّ $\mathbb{Z} / n\mathbb{Z}$ حلقة، حيث إنّه يمكن حساب العمليات على صفوف البواقي باختيار الممَثلين، وبعمل العملية المقابلة في $\mathbb{Z}$، وتبيّن المبرهنة أيضًا، أنّ هذه الحلقة $\mathbb{Z} / n\mathbb{Z}$ تماثل $\mathbb{Z}_n$. ▲

بقي فقط أن نَصفَ تلك الحلقات الجزئية H من حلقة R، بحيث إنّ ضرب مجموعات المشاركة مع الجمع لـ H باختيار الممثلين حسن التعريف. وقد أُثْبِتَ ضرب مجموعات المشاركة في المبرهنة 7.26 في المعادلة (1) بأنه حسن التعريف، ويُعزى نجاح المعادلة (1) إلى حقيقة أنّ، $\phi(ah_2) = \phi(h_1b) = \phi(h_1h_2) = 0'$ أي إنه إذا كان $h \in H$، حيث $H = \text{Ker}(\phi)$. فإنّ لكل $a, b \in R$ لدينا $ah \in H$ و $hb \in H$، وهذا تقترحه المبرهنة 9.26 في الأسفل، التي هي مناظرة للمبرهنة 4.14.

9.26 مبرهنة (**رديف المبرهنة** 4.14): لتكن H حلقة جزئية من الحلقة R. ضرب مجموعات المشاركة مع الجمع لـ H حسن التعريف من خلال المعادلة:

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

إذا وفقط إذا كان $ah \in H$ و $hb \in H$ لكل $a,b \in R$ و $h \in H$.

البرهان افترض أولاً أنّ $ah \in H$ و $hb \in H$ لكل $a,b \in R$ ولكل $h \in H$. ليكن $h_1, h_2 \in H$ ؛ ولذلك، $a + h_1$ و $b + h_2$ هما أيضًا مُمَثِّلَانِ لمجموعتي المشاركة $a + H$ و $b + H$ تحويان a و b، عندئذ:

$$(a + h_1)(b + h_2) = ab + ah_2 + h_1b + h_1h_2$$

لأنّنا نرى من المعطيات ah_2 ، h_1b ، و h_1h_2 جميعها في H ، أنّ $(a + h_1)(b + h_2) \in ab + H$.

في المقابل، افترض أنّ ضرب مجموعات المشاركة مع الجمع من خلال الممثلين حسن التعريف، وليكن $a \in R$ وخذ في الحسبان ضرب مجموعات المشاركة $(a + H)\, H$، فباختيار المُمَثِّلَيْن $a \in (a + H)$ و $0 \in H$، نرى أنّ $(a + H)\, H = a0 + H = 0 + H = H$؛ ولأنه يمكننا أيضًا حساب $(a+H)\, H$، باختيار $a \in (a + H)$ وأي $h \in H$ نرى أنّ $ah \in H$ لأي $h \in H$، ويبيّن برهانٌ مشابه يبدأ مع الضرب $H(b + H)$ أنّ $hb \in H$ لأي $h \in H$. ♦

الزمر الجزئية الناظمية في مبرهنة الزمر هي بالتحديد نوع البنية الجزئية للزمر المطلوبة لتشكيل زمرة عامل مع عملية حسنة التعريف على مجموعات مشاركة معطاة بالتعامل مع ممثلين مختارين، حيث تُبَيِّن المبرهنة 9.26 أنّ البنية الجزئية المناظرة في مبرهنة الحلقات، يجب أن تكون حلقة جزئية H من حلقة R بحيث إنّ: $aH \subseteq H$ و $Hb \subseteq H$ لكل $a, b, \in R$، حيث $aH = \{ah \mid h \in H\}$ و $Hb = \{hb \mid h \in H\}$، من الآن فصاعدًا سنرمز عادة لبنية جزئية كهذه بـ N بدل H، وتذكر أننا في الفصل 15 بدأنا باستخدام N لنعني زمرة جزئية ناظمية.

10.26 تعريف نقول: إن زمرة الجمع الجزئية N من حلقة R **مثالي (ideal)** إذا حققت الخصائص:

$aN \subseteq N$ و $Nb \subseteq N$ لكل $a,b \in R$ ■

مثال 11.26 نرى أنّ $n\mathbb{Z}$ مثالي من الحلقة $\mathbb{Z}$ ؛ لأننا نعلم أنها حلقة جزئية و $s(nm) = (nm)s = n(ms) \in n\mathbb{Z}$ لكل $s \in \mathbb{Z}$. ▲

مثال 12.26 لتكن F حلقة الدوال جميعها من $\mathbb{R}$ إلى $\mathbb{R}$، ولتكن C الحلقة الجزئية من F المتكوّنة من جميع الدوال الثابتة في F. هل C مثالي من F؟ لماذا؟

الحل ليس صحيحًا أنّ الضرب لدالة ثابتة مع كل دالة هو مرة أخرى دالة ثابتة، فمثلاً: الضرب لـ $\sin x$ و 2 هو الدالة $2\sin x$، وعليه، C ليست مثاليًّا من F. ▲

نبذة تاريخية

قَدَّم إرنست إدوارد كُمر (Ernst Eduard Kummer 1810 – 1893) عام 1847م مفهوم "عدد مركب مثالي" حتى يحافظ على مفهوم التحليل الوحيد في حلقات معينة لأعداد صحيحة جبرية، وبوجه خاص، أراد كُمر أن يكون قادرًا على أن يحلل إلى أعداد أولية على الشكل $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{p-1}\alpha^{p-1}$، حيث α جذر مركب لـ $x^p = 1$ (p أولي)، و a_i أعداد صحيحة عادية، وقد لاحظ كُمر أنّ التعريف البسيط للأعداد الأولية "بوصفها أعدادًا غير قابلة للتحليل" لا يقود إلى النتائج المرجوَّة؛ فالضرب لاثنين من مثل هذه الأعداد "غير القابلة للتحليل" يمكن بحق أن يكون قابلاً للقسمة على أعداد أخرى "غير قابلة للتحليل"، عَرَّف كُمر "العوامل الأولية المثالية" و "الأعداد المثالية" بدلالة علاقات تطابق معينة؛ وهذه "العوامل المثالية" استخدمت بعد ذلك على أنها القواسم الضرورية للحفاظ على التحليل الوحيد، وباستخدامها، كان كُمر في الحقيقة قادرًا على إثبات حالات معينة من المبرهنة الأخيرة لفيرما، التي تنصّ على أنّ $x^n + y^n = z^n$ ليس لها حلول $x, y, z \in \mathbb{Z}^+$ إذا كان $n > 2$.

أثبت في النهاية أنّ "عددًا مثاليًّا" – الذي هو بوجه عام ليس "عددًا" – حُدِّدَ بصورة حديدة عن طريق مجموعة الأعداد الصحيحة التي "يقسمها"، أمّا ريتشارد ديديكيند (Richard Dedekind)، فقد أخذ فائدة من هذه الحقيقة ليطابق العامل المثالي مع هذه المجموعة؛ لذلك سمّى المجموعة نفسها مثاليًّا، وواصل لإثبات أنه يحقق التعريف المعطى في هذا الكتاب، أصبح ديديكيند بعد ذلك قادرًا على تعريف مفهومي المثالي الأولي وضرب مثاليين، وبيَّن أنّ أيّ مثالي في حلقة الأعداد الصحيحة لأيّ حقل أعداد جبري، يمكن كتابته على نحو وحيد على صورة ضرب مثاليات أولية.

مثال 13.26 لتكن F كما في المثال السابق، ولتكن N الحلقة الجزئية للدوال f جميعها، بحيث إنّ $f(2) = 0$. هل N مثالي من F؟ لماذا أو لماذا لا؟

الحل ليكن $f \in N$، وليكن $g \in F$. عندئذ $(fg)(2) = f(2)g(2) = 0g(2) = 0$، وهكذا $fg \in N$؛ بالمثل نجد أنّ $gf \in N$؛ لهذا السبب N مثالي من F. يمكننا أيضًا إثباتها فقط بملاحظة أنّ N هي النواة لتشاكل التعويض $\phi_2 : F \rightarrow \mathbb{R}$. ▲

علمنا أنّ الضرب باختيار الممثلين حسن التعريف على مجموعات المشاركة مع الجمع لحلقة جزئية N من R، القانون التجميعي للضرب وقانونا التوزيع لمجموعات المشاركة هذه تنتج مباشرة عن الخصائص نفسها في R، فلدينا مباشرة هذه النتيجة للمبرهنة 9.26.

14.26 نتيجة (**رديف النتيجة 5.14**) ليكن N مثاليًّا من حلقة R، عندئذٍ: مجموعات المشاركة مع الجمع لـِ N تُشَكِّل حلقة R/N مع عمليات ثنائية معرَّفة بـِ

$$(a+N)+(b+N)=(a+b)+N$$

و

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

15.26 تعريف الحلقة R/N في النتيجة السابقة هي **حلقة العامل (factor ring)** (**أو الحلقة الخارجة (quotient ring)**) **لـ R عن طريق** N. ■

إذا استخدمت مصطلح الحلقة الخارجة، فتأكد من عدم خلطك له مع مفهوم الحقل لخوارج القسمة لحلقة تامة، الذي نوقش في الفصل 21.

مبرهنة التشاكل الأساسية (Fundamental Homomorphism Theorem)

لإكمال مُناظرتنا مع الفصلين 13 و 14 نعطي مناظِرَتين للمبرهنتين 9.14 و 11.14.

16.26 مبرهنة (**رديف المبرهنة 9.14**) ليكن N مثاليًّا من حلقة R. عندئذ $\gamma: R \to R/N$ المعطى بـِ $\gamma(x)=x+N$ هو تشاكل حلقاتٍ نواته N.

البرهان جزء الجمع أُنجز في المبرهنة 9.14، وبالعودة إلى مسألة الضرب، نرى أنّ:

$$\gamma(xy)=(xy)+N=(x+N)(y+N)=\gamma(x)\gamma(y).$$ ♦

17.26 مبرهنة (**مبرهنة التشاكل الأساسية؛ رديف المبرهنة 11.14**) ليكن $\phi: R \to R'$ تشاكل حلقات نواته N. عندئذ: $\phi[R]$ حلقة، والدالة $\mu: R/N \to \phi[R]$ المعطاة بـ $\mu(x+N)=\phi(x)$ هي تماثل. إذا كان $\gamma: R \to R/N$ هو التشاكل المعطى بـِ $\gamma(x)=x+N$، فلكل $x \in R$، لدينا $\phi(x)=\mu\gamma(x)$.

البرهان تنتج هذه مباشرة عن المبرهنتين 7.26 و 16.26، والشكل 18.26 مناظر للشكل 10.14. ♦

$$\begin{tikzcd} R \arrow[rr, "\phi"] \arrow[dr, "\gamma"'] & & \phi[R] \arrow[dl, "\mu"] \\ & R/N & \end{tikzcd}$$

الشكل 18.26

19.26 مثال يبيّن المثال 11.26 أنّ $n\mathbb{Z}$ مثالي من $\mathbb{Z}$، وهكذا يمكننا تشكيل حلقة العامل $\mathbb{Z}/n\mathbb{Z}$، ويبيّن المثال 11.18 أن $\phi: \mathbb{Z} \to \mathbb{Z}_n$ حيث $\phi(m)$ باقي m مقياس n، هو تشاكل، ونرى أن $\mathrm{Ker}(\phi) = n\mathbb{Z}$. بعد ذلك، تبيّن المبرهنة 17.26 أنّ الدالة $\mu : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ – حيث $\mu(m + n\mathbb{Z})$ باقي m مقياس n، هي تماثل وحسنة التعريف. ▲

بوجه عام، كل تشاكل حلقات مجاله R ينشئ حلقة عامل R / N ، وكل حلقة عامل R / N تنشيء دالة تشاكل من R إلى R / N. والمثالي في مبرهنة الحلقات يناظر الزمرة الجزئية الناظمية وكلاهما هو نوع البنية الجزئية الضروري لتشكيل بنية العامل.

يجب علينا الآن أن نضيف إضافة للمبرهنة 3.26 على خصائص التشاكلات. ليكن $\phi: R \longrightarrow R'$ تشاكلاً، وليكن N مثاليًّا من R، عندئذ: $\phi[N]$ مثالي من $\phi[R]$، مع أنه ليس بالضرورة مثاليًّا من R' أيضًا، إذا كان N' مثاليًّا من $\phi[R]$ أو من R'، فإنّ $\phi^{-1}[N']$ مثالي من R. نترك برهانها إلى التمرين 22.

تمارين 26

حسابات

1. صِفْ جميع تشاكلات الحلقات من $\mathbb{Z} \times \mathbb{Z}$ إلى $\mathbb{Z} \times \mathbb{Z}$ [لاحظ: أنه إذا كان ϕ تشاكلاً، فإنّ $\phi((1,0))=\phi((1,0))\phi((1,0))$ و$\phi((0,1))=\phi((0,1))\phi((0,1))$. خذ في الحسبان أيضًا $\phi((1,0)(0,1))$].
2. أوجد الأعداد الصحيحة الموجبة n جميعها، بحيث إنّ $\mathbb{Z}_n$ تحوي حلقة جزئية تماثل $\mathbb{Z}_2$.
3. أوجد المثاليات Nمن $\mathbb{Z}_{12}$ جميعها، واحسب في كل حالة $\mathbb{Z}_{12}/N$ ؛ أي أوجد حلقة معروفة تماثلها الحلقة الخارجة.
4. أعطِ جداول الجمع والضرب لـِ $2\mathbb{Z}/8\mathbb{Z}$. هل $2\mathbb{Z}/8\mathbb{Z}$ و $\mathbb{Z}_4$ حلقات متماثلة؟

مفاهيم

في التمارين من 5 إلى 7، صحِّح تعريف الحدّ المكتوب بخط مائل دون الرجوع إلى الكتاب –إن كانت هناك حاجة للتصحيح – بحيث يكون بصيغة قابلة للنشر.

5. **التماثل** من حلقة R إلى حلقة R' هو تشاكلٌ $\phi : R \to R'$ ، بحيث إنّ $\mathrm{Ker}(\phi) = \{0\}$.
6. **المثالي** N من حلقة R هو زمرة جمع جزئية من $\langle R, +\rangle$، بحيث إنه لكل $r \in R$ ولكل $n \in N$ لدينا $rn \in N$ و $nr \in N$.

7. النواة لتشاكل ϕ يربط الحلقة R بالحلقة R' هي $\{\phi(r) = 0' \mid r \in R\}$

8. لتكن F حلقة الدوال كلها من $\mathbb{R}$ إلى $\mathbb{R}$ ولها مشتقات من الرتب كلها، والاشتقاق يعطي دالة $\delta: F \to F$، حيث $\delta(f(x))=f'(x)$. هل δ تشاكل؟ لماذا؟ اربط بين هذا التمرين والمثال 12.26.

9. أعْطِ مثالاً لتشاكل حلقات $\phi: R \to R'$، حيث R لها عنصر محايد 1 و $\phi(1) \neq 0'$، لكن $\phi(1)$ ليس عنصرًا محايدًا لـ R'.

10. ضع إشارة صح أو إشارة خطأ:

_______ أ. مفهوم تشاكل الحلقات مرتبط إلى حدٍّ بعيد بفكرة حلقة العامل.

_______ ب. تشاكل الحلقات $\phi: R \to R'$ يحمل المثاليات من R إلى مثاليات من R'.

_______ جـ. تشاكل الحلقات أحادي إذا وفقط إذا كانت النواة هي $\{0\}$.

_______ د. $\mathbb{Q}$ مثالي من $\mathbb{R}$.

_______ هـ. كل مثالي من حلقة هو حلقة جزئية من الحلقة.

_______ و. كل حلقة جزئية من كل حلقة هي مثالي من الحلقة.

_______ ز. كل حلقة خارجة من كل حلقة إبدالية هي مرة أخرى حلقة إبدالية.

_______ ح. الحلقات $\mathbb{Z}/4\mathbb{Z}$ و $\mathbb{Z}_4$ متماثلة.

_______ ط. مثالي N من حلقة R مع عنصر محايد 1 هو R جميعها إذا وفقط إذا كان $1 \in N$.

_______ ي. مفهوم المثالي لمفهوم الحلقة مثل مفهوم الزمرة الجزئية الناظمية لمفهوم الزمرة.

11. لتكن R حلقة. لاحظ أنّ $\{0\}$ و R كلايهما مثاليان من R. هل حلقتا العامل R/R و $R/\{0\}$ لهما أهمية حقيقية؟ لماذا؟

12. أعط مثالاً يبيّن أنّ حلقة عامل من حلقة تامة يمكن أن تكون حقلاً.

13. أعط مثالاً يبيّن أنّ حلقة عامل من حلقة تامة يمكن أن يكون لها قواسم لـ 0.

14. أعط مثالاً يبيّن أنّ حلقة عامل من حلقة مع قواسم لـ 0 يمكن أن تكون حلقة تامة.

15. أوجد حلقة جزئية من الحلقة $\mathbb{Z} \times \mathbb{Z}$ لا تكون مثاليًا من $\mathbb{Z} \times \mathbb{Z}$.

16. سُئل طالب ليثبت أنّ الحلقة الخارجة من حلقة R مقياس مثالي N هي إبدالية إذا وفقط إذا كان $(rs - sr) \in N$ لكل $r, s \in R$. بدأ الطالب بـ:

افترض أنّ R/N إبدالية، عندئذ: $rs = sr$ لكل $r, s \in R/N$.

أ. لماذا كانت قراءة المدرس لذلك تجعله يتوقع عدم المنطقية لما بعدها؟

ب. ماذا كان يجب على الطالب أن يكتب؟

جـ. أثبت الادعاء. (لاحظ "إذا وفقط إذا").

براهين

17. لتكن $R = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$، ولتكن R' تتكوّن من المصفوفات كلها من الدرجة 2×2 على الشكل $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ لـ $a, b \in \mathbb{Z}$. أثبت أنّ R حلقة جزئية من $\mathbb{R}$، وأنّ R' حلقة جزئية من $M_2(\mathbb{Z})$. بعد ذلك أثبت أن $\phi : R \to R'$، حيث $\phi(a + b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ هو تماثل.

18. أثبت أنّ كل تشاكل من حقل إلى حلقة إما أحاديًا أو يرسل كل شيء بصورة غامرة إلى 0.

19. أثبت أنه إذا كانت R ، و R' ، و R'' حلقات، وإذا كان $\phi : R \to R'$ و $\psi : R' \to R''$ تشاكلين، فإن دالة التركيب $\psi\phi : R \to R''$ هي تشاكل. (استخدم التمرين 49 للفصل 13).

20. لتكن R حلقة إبدالية مع عنصر محايد بمميز أولي p. أثبت أنّ الدالة $\phi_p : R \to R$ المعطاة بـ $\phi_p(a) = a^p$ هي تشاكل (**تشاكل فروبينس** (**Frobenius homomorphism**).

21. لتكن R و R' حلقتين، وليكن $\phi : R \to R'$ تشاكل حلقات، بحيث إنّ $\phi[R] \neq \{0'\}$. أثبت أنه إذا كان لـ R عنصر محايد 1، و R' ليس لها قواسم لـ 0، فإنّ $\phi(1)$ عنصر محايد لـ R'.

22. ليكن $\phi : R \to R'$ تشاكل حلقات، وليكن N مثاليًا من R.

أ. أثبت أنّ $\phi[N]$ مثالي من $\phi[R]$.

ب. أعْطِ مثالاً يُثبت أنّ $\phi[N]$ ليس بالضرورة مثاليًا من R'.

جـ. ليكن N' مثاليًا إما من $\phi[R]$ أو من R'. أثبت أن $\phi^{-1}[N']$ مثاليًا من R.

23. ليكن F حقلاً، ولتكن S أي مجموعة جزئية من $F \times F \times \ldots \times F$ لـ n عامل. أثبت أنّ المجموعة N_S لكل $f(x_1, \cdot \cdot \cdot, x_n) \in F[x_1, \cdot \cdot \cdot, x_n]$ التي لها كل عنصر $(a_1, \ldots, a_n)$ في S بوصفه صفرًا (انظر التمرين 28 للفصل 22) هي مثالي من $F[x_1,\ldots, x_n]$. هذه ذات أهمية في علم الهندسة الجبرية.

24. أثبت أنّ حلقة العامل من حقل إما حلقة تافهة (صفر) من عنصر واحد أو تماثل الحقل.

25. أثبت أنه إذا كانت R حلقة مع عنصر محايد و N مثالي من R، بحيث إنّ $N \neq R$، فإنّ R / N حلقة مع عنصر محايد.

26. لتكن R حلقة إبدالية، وليكن $a \in R$. أثبت أن $I_a = \{x \in R \mid ax = 0\}$ مثالي من R.

27. أثبت أنّ تقاطع مثاليات من حلقة R هو أيضًا مثالي من R.

28. لتكن R و R' حلقتين، وليكن N و N' مثاليين من R و R' على الترتيب. ليكن ϕ تشاكلاً من R إلى R'. أثبت أنّ ϕ ينشئ تشاكلاً طبيعيًا $\phi_*: R/N \to R'/N'$ إذا كانت $\phi[N] \subseteq N'$ (استخدم التمرين 39 للفصل 14) .

29. ليكن ϕ تشاكلاً من حلقة R مع عنصر محايد وبصورة غامرة إلى حلقة غير صفرية R'. ليكن u عنصر وحدة في R. أثبت أنّ $\phi(u)$ عنصر وحدة في R'.

30. يسمى العنصر a من حلقة R **متلاشي القوى (nilpotent)**، إذا كان $a^n = 0$ لعنصر ما $n \in \mathbb{Z}^+$. أثبت أنّ مجموعة جميع العناصر متلاشية القوى من حلقة إبدالية R هي مثالي – **متلاشي الجذر لـ (nilradical of)** R.

31. بالرجوع إلى التعريف المعطى في التمرين 30، أوجد متلاشي الجذر للحلقة $\mathbb{Z}_{12}$، ولاحظ أنه إحدى المثاليات من $\mathbb{Z}_{12}$ التي تم إيجادها في التمرين 3. ما متلاشي الجذر لـ $\mathbb{Z}$؟ لـ $\mathbb{Z}_{32}$؟

32. بالرجوع إلى التمرين 30، أثبت أنه إذا كان N هو متلاشي الجذر لحلقة إبدالية R، فإنّ متلاشي الجذر لـ R/N هو المثالي التافه $\{0 + N\}$.

33. لتكن R حلقة إبدالية وليكن N مثاليًا من R. بالرجوع إلى التمرين 30، أثبت أنه إذا كان كل عنصر في N متلاشي القوى، وكان متلاشي الجذر لـ R/N هو R/N، فإن متلاشي الجذر لـ R هو R.

34. لتكن R حلقة إبدالية وليكن N مثاليًا من R. أثبت أنّ المجموعة $\sqrt{N}$ لكل $a \in R$، بحيث إنّ $a^n \in N$ لعنصر ما $n \in \mathbb{Z}^+$، هي مثالي من R، **الجذر لـ (radical of)** N.

35. بالرجوع إلى التمرين 34، أثبت بأمثلة أنه لمثاليات فعلية N من حلقة إبدالية R

أ. $\sqrt{N}$ ليست بالضرورة أن تساوي N.

ب. $\sqrt{N}$ ممكن أن تساوي N.

36. ما علاقة المثالي $\sqrt{N}$ – من التمرين 34– بمتلاشي الجذر لـ R/N (انظر التمرين 30)؟ صغ كلمات إجابتك بحذر.

37. أثبت أنّ $\phi : \mathbb{C} \longrightarrow M_2(\mathbb{R})$ المعطى بـ:

$$\phi(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

لـ $a, b \in \mathbb{R}$ يعطي تماثلاً لـ $\mathbb{C}$ مع الحلقة الجزئية $\phi[\mathbb{C}]$ من $M_2(\mathbb{R})$.

38. لتكن R حلقة مع عنصر محايد، ولتكن $\text{End}(\langle R, +\rangle)$ حلقة التشاكلات الداخلية الموصوفة في الفصل 24. ليكن $a \in R$، وليكن $\lambda_a : R \longrightarrow R$ معطًى بـ

$$\lambda_a(x) = ax$$

لـ $x \in R$

أ. أثبت أنّ λ_a تشاكل داخلي لـ $\langle R, +\rangle$.

ب. أثبت أنّ $R' = \{\lambda_a \mid a \in R\}$ حلقة جزئية من $\text{End}(\langle R, +\rangle)$.

جـ. أثبت المناظرة لمبرهنة كايلي (Cayley's theorem) لـ R بإثبات أنّ R' للفرع (ب) تماثل R.

الفصل 27 المثاليات الأولية والأعظمية Prime and Maximal Ideals

طلبت التمارين من 12 إلى 14 في الفصل السابق، أن نزوّد بأمثلة لحلقات العامل R/N، حيث R و R/N لهما خصائص بنائية مختلفة جدًا، وسنبدأ مع أمثلة لهذا الوضع، وسنزوّد بحلول لتلك التمارين في أثناء تقدمنا.

1.27 مثال كما أُثبت في النتيجة 12.19 لعدد أولي p الحلقة $\mathbb{Z}_p$ – التي تماثل $\mathbb{Z}/p\mathbb{Z}$– هي حقل. ▲

2.27 مثال الحلقة $\mathbb{Z} \times \mathbb{Z}$ ليست حلقة تامة؛ لأن:

$$(0, 1)(1, 0) = (0, 0),$$

تبيّن أنّ $(0,1)$ و $(1,0)$ قواسم لـ 0، لتكن $N = \{(0,n) \mid n \in \mathbb{Z}\}$. الآن، N مثالي من $\mathbb{Z} \times \mathbb{Z}$ و $(\mathbb{Z} \times \mathbb{Z})/N$ يماثل $\mathbb{Z}$ بالنسبة إلى التقابل $m \leftrightarrow [(m,0)+N]$، حيث $m \in \mathbb{Z}$. وعليه، حلقة العامل من حلقة يمكن أن تكون حلقة تامة على الرغم من أنّ الحلقة الأصلية ليست كذلك. ▲

3.27 مثال من السهل رؤية أن المجموعة الجزئية $N = \{0,3\}$ من $\mathbb{Z}_6$ تمثّل مثاليًا من $\mathbb{Z}_6$ و $\mathbb{Z}_6/N$ لها ثلاثة عناصر، $0 + N$، $1 + N$، و $2 + N$، حيث تجمع، وتضرب بنمطٍ مُعَيَّنٍ كأنك تبيّن أنّ: $\mathbb{Z}_6/N \simeq \mathbb{Z}_3$ بالنسبة إلى التقابل

$$(0+N) \leftrightarrow 0, \quad \text{و} \quad (1+N) \leftrightarrow 1, \quad (2 + N) \leftrightarrow 2.$$

وتبين هذه أنه إذا كانت R ليست حتى حلقة تامة – أي إذا كانت R تحوي قواسم للصفر – فما زال محتملاً لـ R/N أن تكون حقلًا. ▲

4.27 مثال لاحظ أنّ $\mathbb{Z}$ حلقة تامة، لكن $\mathbb{Z}/6N \simeq \mathbb{Z}_6$ ليست كذلك، وقد بيّنت الأمثلة السابقة أنّ حلقة العامل يمكن أن تكون لها بنية تبدو أفضل من تلك التي للحلقة الأصلية، ويشير هذا المثال إلى أنّ بنية حلقة العامل قد تبدو أكثر سوءًا من تلك التي للحلقة الأصلية. ▲

كل حلقة غير صفرية R لها على الأقل مثاليان: **المثالي غير الفعلي (improper ideal)** R و**المثالي التافه (trivial ideal)** $\{0\}$، ولهذين المثاليين حلقتا العامل، هما: R/R – التي لها عنصر واحد فقط – و $R/\{0\}$ – والتي تماثل R، وهاتان الحالتان غير مشوقتين، كما هو للزمرة الجزئية من زمرة، **ومثالي غير تافه فعلي (proper nontrivial ideal)** من حلقة R هو مثالي N من R، بحيث إنّ $N \neq \{0\}$ و $N \neq R$.

بينما حلقات العامل لحلقات ولحلقات تامة يمكن أن تكون ذات فائدة كبيرة، كما أشارت إليه الأمثلة في الأعلى، فالنتيجة 6.27 التي تعقب مبرهنتنا الآتية تبين أنّ حلقة العامل لحقل في الحقيقة ليست مفيدة لنا.

5.27 مبرهنة إذا كانت R حلقة مع عنصر محايد، وكان N مثاليًا من R يحوي عنصر وحدة، فإنّ $N = R$.

البرهان ليكن N مثاليًّا من R، وافترض أنَّ $u \in N$ عنصر وحدة في R، عندئذ: الشرط $rN \subseteq N$ لكل $r \in R$ يتضمن - إذا أخذنا $r = u^{-1}$ و $u \in N$، أنّ $1 = u^{-1}u$ في N، لكن $rN \subseteq N$ لكل $r \in R$ تؤدي إلى أنّ $r1 = r$ هو في N لكل $r \in R$، وهكذا $N = R$. ♦

6.27 نتيجة لا يحوي الحقل فعليًّا مثاليات غير تافهة.

البرهان لأنّ كل عنصر غير صفري في حقل هو عنصر وحدة، فينتج مباشرة عن المبرهنة 5.27 أنّ المثالي من حقل F، هو إما $\{0\}$ أو F كلها. ♦

المثاليات الأوّلية والأعظمية

نطرح السؤال: متى تكون حلقة العامل حقلاً؟ ومتى تكون حلقة تامة؟

يمكن أن يوسع التناظر مع الفصل 15 بقدر بسيط ليغطي هذه الحالة، حيث حلقة العامل هي حقل.

7.27 تعريف **المثالي الأعظمي من حلقة (maximal ideal of a ring)** R هو مثالي M يختلف عن R، بحيث إنه لا يوجد مثالي فعلي N من R يحوي M فعليًّا. ■

8.27 مثال ليكن p عددًا صحيحًا موجبًا أوليًّا، ونعلم أنّ $\mathbb{Z}/p\mathbb{Z}$ تماثل $\mathbb{Z}_p$، وبالتغاضي عن الضرب لحظة وأن نعدّ $\mathbb{Z}/p\mathbb{Z}$ و $\mathbb{Z}_p$ زمر جمع، نعلم أنّ $p\mathbb{Z}$ زمرة بسيطة، بناءً على ذلك ومن خلال المبرهنة 18.15، $p\mathbb{Z}$ يجب أن تكون زمرة جزئية ناظمية أعظمية من $\mathbb{Z}$؛ ولأنّ $\mathbb{Z}$ زمرة إبدالية وكل زمرة جزئية هي زمرة جزئية ناظمية، نرى أنَّ $p\mathbb{Z}$ هي زمرة جزئية فعلية أعظمية من $\mathbb{Z}$؛ ولأنّ $p\mathbb{Z}$ مثالي من الحلقة $\mathbb{Z}$، فينتج أنّ $p\mathbb{Z}$ مثالي أعظمي من $\mathbb{Z}$، ونعلم أنّ $\mathbb{Z}/p\mathbb{Z}$ تماثل الحلقة $\mathbb{Z}_p$ ، وأنّ $\mathbb{Z}_p$ في الحقيقة حقلاً، وعليه، تكون $\mathbb{Z}/p\mathbb{Z}$ حقلاً. وهذه توضح المبرهنة الآتية. ▲

9.27 مبرهنة (**رديف المبرهنة** 15.18): لتكن R حلقة إبدالية مع عنصر محايد، عندئذٍ: M مثالي أعظمي من R إذا وفقط إذا كان R/M حقلاً.

البرهان افترض أنّ M مثالي أعظمي من R. لاحظ أنه إذا كانت R حلقة إبدالية مع عنصر محايد، فإنَّ R/M أيضًا حلقة إبدالية غير صفرية مع عنصر محايد، ولأن $M \neq R$، والتي هي الحالة إذا كان M أعظميًّا. ليكن $(a + M) \in R/M$ مع $a \notin M$، حيث إنّ $a + M$ ليس العنصر المحايد للجمع لـ R/M. افترض أنّ $a + M$ ليس له معكوسٌ ضربي في R/M، عندئذ: المجموعة $(R/M)(a + M) = \{(r + M)(a + M) \mid (r + M) \in R/M\}$ لا تحوي $1 + M$. نرى بسهولة أن $(R/M)(a+M)$ مثالي غير تافه من R/M؛ لأنّ $a \notin M$، وهو أيضاً مثالي فعلي؛ لأنه لا يحوي $1 + M$. من خلال الفقرة الأخيرة للفصل 26، إذا كان $\gamma : R \to R/M$ هو التشاكل القانوني، فإن $\gamma^{-1}[(R/M)(a + M)]$ مثالي فعلي من R يحوي فعليًّا M ، لكنّ هذه تناقض فرضنا أنّ M مثالي أعظمي، وهكذا $a + M$ يجب أن يكون له معكوس ضربي في R/M.

في المقابل، افترض أنّ R/M حقل، ومن خلال الفقرة الأخيرة للفصل 26، إذا كان N أي مثالي من R، بحيث إنّ $M \subset N \subset R$ و γ هو التشاكل القانوني من R وبصورة غامرة إلى R/M ، فإن $\gamma[N]$ مثالي من R/M مع $\{(0+M)\} \subset \gamma[N] \subset R/M$؛ لكن هذه تناقض النتيجة 6.27 – التي تنصّ على أنّ الحقل R/M لا يحوي مثاليات غير تافهة فعلية، وعليه، إذا كان R/M حقلاً، فإنّ M أعظمي. ♦

10.27 مثال لأنّ $\mathbb{Z}/n\mathbb{Z}$ تماثل $\mathbb{Z}_n$ و $\mathbb{Z}_n$ حقل إذا وفقط إذا كان n أوليًّا، نرى أنّ المثاليات الأعظمية من $\mathbb{Z}$ هي بالضبط المثاليات $p\mathbb{Z}$ للأعداد الصحيحة الموجبة الأولية p. ▲

11.27 نتيجة الحلقة الإبدالية مع عنصر محايد هي حقل إذا وفقط إذا كان ليس لها مثاليات غير تافهة فعلية.

البرهان النتيجة 6.27 تبيّن أنّ الحقل ليس له مثاليات غير تافهة فعلية.

في المقابل، إذا كانت R حلقة إبدالية مع عنصر محايد، وليس لها مثاليات غير تافهة فعلية، فإنّ $\{0\}$ مثالي أعظمي و $R/\{0\}$ – الذي يماثل R – هو حقل من خلال المبرهنة 9.27. ♦

نعود الآن إلى سؤال الوَصْف – لحلقة إبدالية R مع عنصر محايد – للمثاليات $N \neq R$، بحيث إنّ R/N حلقة تامة، في الواقع الإجابة هنا واضحة، فحلقة العامل R/N ستكون حلقة تامة، إذا وفقط إذا كان $(a+N)(b+N)=N$ تضمن إما

$$a+N=N \quad \text{أو} \quad b+N=N.$$

هذه بالضبط هي العبارة: R/N ليس لها قواسم لـ 0؛ لأنّ مجموعة المشاركة N تؤدي دَوْرَ الـ 0 في R/N ، وبالنظر إلى الممثلين، نرى أنّ هذا الشرط يكافئ القول: إنّ $ab \in N$ إما أن يؤدي إلى $a \in N$ أو $b \in N$.

12.27 مثال جميع المثاليات من $\mathbb{Z}$ هي على الصورة $n\mathbb{Z}$. لـ $n=0$، لدينا $n\mathbb{Z}=\{0\}$ و $\mathbb{Z}/\{0\}\simeq\mathbb{Z}$ التي هي حلقة تامة، ولـ $n>0$، لدينا $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ و $\mathbb{Z}_n$ حلقة تامة، إذا وفقط إذا كان n أوليًّا، وعليه، المثاليات غير الصفرية $n\mathbb{Z}$، حيث إنّ $\mathbb{Z}/n\mathbb{Z}$ حلقة تامة هي على الصورة $p\mathbb{Z}$، حيث p أولي، وبالتأكيد $\mathbb{Z}/p\mathbb{Z}$ في الواقع حقل؛ لذلك، $p\mathbb{Z}$ مثالي أعظمي من $\mathbb{Z}$. لاحظ أنه ليكون ضرب أعداد صحيحة rs في $p\mathbb{Z}$، فإنّ العدد الأولي p يجب أن يقسم إما r أو s. دور الأعداد الأولية في هذا المثال يجعل استخدام كلمة أولي في التعريف الآتي ذا معنى. ▲

13.27 تعريف المثالي $N \neq R$ من حلقة إبدالية R هو **مثالي أولي (prime ideal)** إذا كان $ab \in N$ تضمن أنه إما $a \in N$ أو $b \in N$ لـ $a,b \in R$. ■

لاحظ أنّ $\{0\}$ مثالي أولي من $\mathbb{Z}$، وفي الواقع من أيّ حلقة تامة.

14.27 مثال لاحظ أنّ $\mathbb{Z} \times \{0\}$ مثالي أولي من $\mathbb{Z} \times \mathbb{Z}$؛ لأنه إذا كان $(a,b)(c,d) \in \mathbb{Z} \times \{0\}$، فيجب أن نحصل على $bd = 0$ في $\mathbb{Z}$. هذا يضمن أنه إما $b = 0$ وهكذا $(a,b) \in \mathbb{Z} \times \{0\}$ أو $d = 0$ وهكذا $(c,d) \in \mathbb{Z} \times \{0\}$. لاحظ أنّ $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\})$ تماثل $\mathbb{Z}$، الذي هو حلقة تامة. ▲

تتضمن الملحوظات قبل المثال 12.27 برهانًا للمبرهنة الآتية، التي وُضِّحَتْ من خلال المثال 14.27.

15.27 مبرهنة لتكن R حلقة إبدالية مع عنصر محايد، وليكن $N \neq R$ مثاليًا من R، عندئذٍ: R/N حلقة تامة إذا وفقط إذا كان N مثاليًا أوليًا من R.

16.27 نتيجة كل مثالي أعظمي من حلقة إبدالية R مع عنصر محايد هو مثالي أولي.

البرهان إذا كان M أعظميًا من R، فإنّ R/M حقل، ومن ثَمَّ حلقة تامة، ولهذا السبب M مثالي أولي من خلال المبرهنة 15.27. ♦

المادة التي عرضت توًّا المتعلقة بالمثاليات الأولية والأعظمية مهمّة جدًّا، وسوف نستخدمها بكثرة، ويجب علينا أن نحفظ الأفكار الرئيسة جيدًا في أذهاننا، ويجب أيضًا أن نَعْرِفَ تعريفات المثاليات الأولية والأعظمية، ونفهمها، ويجب كذلك تذكر الحقائق الآتية التي أثبتناها.

لحلقة إبدالية R مع عنصر محايد: 1. المثالي M من R أعظمي إذا وفقط إذا كان R/M حقلًا. 2. المثالي N من R هو أولي إذا وفقط إذا كانت R/N حلقة تامة. 3. كل مثالي أعظمي من R هو مثالي أولي.

الحقول الأولية

سنكمل لبيان أنّ الحلقتين $\mathbb{Z}$ و $\mathbb{Z}_n$ تشكلان أساسًا تبنى عليه جميع الحلقات مع عنصر محايد، وأنّ $\mathbb{Q}$ و $\mathbb{Z}_p$ تؤديان دورًا مشابهًا للحقول كلها. لتكن R أي حلقة مع عنصر محايد 1، تذكر أنه لـ $n.1$ نعني $1+ \ldots +1+1$ لـ n حد لـ $n > 0$، و $(-1)+\ldots+(-1)+(-1)$ لـ $|n|$ حد لـ $n < 0$، بينما $n.1 = 0$ لـ $n = 0$.

17.27 مبرهنة إذا كانت R حلقة مع عنصر محايد 1، فإنّ الدالة $\phi : \mathbb{Z} \longrightarrow R$ المعطاة بـ:

$$\phi(n) = n \cdot 1$$

لـ $n \in \mathbb{Z}$ هي تشاكل من $\mathbb{Z}$ إلى R.

البرهان لاحظ أنّ

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

قانونا التوزيع في R يبيّنان أنّ:

$$\underbrace{(1+1+\cdots+1)}_{n\text{ حد}}\underbrace{(1+1+\cdots+1)}_{m\text{ حد}} = \underbrace{(1+1+\cdots+1)}_{nm\text{ حد}}.$$

وعليه، $(n.1)(m.1) = (nm).1$ لـ $n,m > 0$. وبصورة مشابهة مع قانوني التوزيع نرى أنه لكل $n,m \in \mathbb{Z}$، لدينا:

$$(n \cdot 1)(m \cdot 1) = (nm) \cdot 1.$$

وعليه،

$$\phi(nm) = (nm) \cdot 1 = (n \cdot 1)(m \cdot 1) = \phi(n)\phi(m)$$ ♦

18.27 نتيجة إذا كانت R حلقة مع عنصر محايد وبمميز $n > 1$، فإنّ R تحوي حلقة جزئية تماثل $\mathbb{Z}_n$، وإذا كانت R لها مميز 0، فإنّ R تحوي حلقة جزئية تماثل $\mathbb{Z}$.

البرهان من خلال المبرهنة 17.27 يتبين أن الدالة $\phi:\mathbb{Z} \longrightarrow R$ المعطاة بـ $\phi(m) = m.1$ لـ $m \in \mathbb{Z}$ تمثل تشاكلًا ويجب أن تكون النواة مثاليّة من $\mathbb{Z}$، والمثاليات جميعها من $\mathbb{Z}$ هي على الصورة $s\mathbb{Z}$ لعنصر ما $s \in \mathbb{Z}$، ومن خلال المبرهنة 15.19 نرى أنه إذا كانت R لها مميز $n > 0$، فإنّ النواة لـ ϕ هي $n\mathbb{Z}$، عندئذ: الصورة $\phi[\mathbb{Z}] \le R$ تماثل $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. أما إذا كان المميز لـ R هو 0، فإنّ $m.1 \neq 0$ لكل $m \neq 0$، وهكذا النواة لـ ϕ هي $\{0\}$. وعليه، الصورة $\phi[\mathbb{Z}] \le R$ تماثل $\mathbb{Z}$. ♦

19.27 مبرهنة الحقل F إما بمميز أولي p ويحوي حقلًا جزئيًّا يماثل $\mathbb{Z}_p$ أو بمميز 0 ويحوي حقلًا جزئيًّا يماثل $\mathbb{Q}$.

البرهان إذا كان المميز لـ F ليس 0، فالنتيجة في الأعلى تبيّن أنّ F يحوي حلقة جزئية تماثل $\mathbb{Z}_n$ وعندئذ n يجب أن يكون أوليًّا p، وإلا فإن F يكون له قواسم لـ 0. إذا كان F بمميز 0، فإن F يجب أن يحوي حلقة جزئية تماثل $\mathbb{Z}$، وفي هذه الحالة النتيجتان 8.21 و 9.29 تُبيِّنان أنّ F يجب أن يحوي حقلاً للخوارج من هذه الحلقة الجزئية، وأنّ هذا الحقل يجب أن يماثل $\mathbb{Q}$. ♦

20.27 تعريف الحقلان $\mathbb{Z}_p$ و $\mathbb{Q}$ حقلان أوّليّان **(prime fields)**. ■

بنية المثالي من $F[x]$

خلال ما بقي من هذا الفصل، نفترض أنّ F حقل، ونعطي التعريف الآتي لحلقة إبدالية عامة R مع عنصر محايد، على الرغم من اهتمامنا فقط بالحالة $R= F[x]$. لاحظ أنه لحلقة إبدالية R مع عنصر محايد و $a \in R$، المجموعة $\{ ra \mid r \in R\}$ هي مثالي من R يحوي العنصر a.

21.27 تعريف إذا كانت R حلقة إبدالية مع عنصر محايد و $a \in R$، فالمثالي $\{ ra \mid r \in R\}$ لكل مضاعفات a هو **المثالي الرئيس المولّد بـ (principal ideal generated by)** العنصر a، ويرمز له بالرمز $\langle a \rangle$، ومثالي N من R هو مثالي رئيس، إذا كان $N = \langle a \rangle$ لعنصر ما $a \in R$. ■

22.27 مثال كل مثالي من الحلقة $\mathbb{Z}$ هو على الصورة $n\mathbb{Z}$، وهو مولّد بالعنصر n، وهكذا كل مثالي من $\mathbb{Z}$ هو مثالي رئيس. ▲

23.27 مثال المثالي $\langle x \rangle$ من $F[x]$ يتكون من جميع كثيرات الحدود في $F[x]$، التي حدّها الثابت صفر. ▲

المبرهنة الآتية هي تطبيق بسيط؛ لكنه مهم جدًّا لخوارزمية القسمة في $F[x]$ (انظر المبرهنة 1.23)، ومقام إثبات هذه المبرهنة بالنسبة إلى خوارزمية القسمة في $F[x]$ كإثبات أنّ زمرة جزئية من زمرة دورية هي دورية بالنسبة إلى خوارزمية القسمة في $\mathbb{Z}$.

24.27 مبرهنة إذا كان F حقلاً، فكل مثالي من $F[x]$ هو مثالي رئيس.

البرهان ليكن N مثاليًّا من $F[x]$، فإذا كان $N=\{0\}$، فإنّ $N=\langle 0\rangle$. افترض أنّ $N\neq\{0\}$، وليكن $g(x)$ عنصرًا غير صفري في N ذا درجة صغرى، فإذا كانت درجة $g(x)$ هي 0، فإنّ $g(x)\in F$ وهو عنصر وحدة، وهكذا من خلال المبرهنة 5.27، $N=F[x]=\langle 1\rangle$، وعليه، فإنّ N رئيس. إذا كانت الدرجة لـ $g(x)$ أكبر أو تساوي 1، وكان $f(x)$ أي عنصر في N، فعندئذ: ومن خلال المبرهنة 1.23 $f(x)=g(x)\,q(x)+r(x)$، حيث $r(x)=0$ أو (درجة $r(x)$) < (درجة $g(x)$). الآن، $f(x)\in N$ و$g(x)\in N$ تؤديان إلى أنّ $f(x)-g(x)\,q(x)=r(x)$ في N من خلال تعريف المثالي؛ ولأن $g(x)$ عنصر غير صفري في N ذو درجة صغرى، فيجب أن يكون لدينا $r(x)=0$. وعليه، $f(x)=g(x)q(x)$ و $N=\langle g(x)\rangle$. ♦

يمكننا الآن وصف المثاليات الأعظمية من $F[x]$. هذه خطوة حاسمة في إنجاز هدفنا الأساسي: لإثبات أنّ أيّ كثيرة حدود غير ثابتة $f(x)$ في $F[x]$ لها صفر في حقل ما E يحوي F.

25.27 مبرهنة المثالي $\langle p(x)\rangle\neq\{0\}$ من $F[x]$ هو أعظمي إذا وفقط إذا كان $p(x)$ غير مختزل على F.

البرهان افترض أنّ $\langle p(x)\rangle\neq\{0\}$ مثالي أعظمي من $F[x]$، عندئذ: $\langle p(x)\rangle\neq F[x]$، وهكذا $p(x)\notin F$. ليكن $p(x)=f(x)g(x)$ تحليلاً لـ $p(x)$ في $F[x]$؛ لأنّ $\langle p(x)\rangle$ مثالي أعظمي، فهو أيضًا مثالي أولي، وعليه $(f(x)g(x))\in\langle p(x)\rangle$ تؤدي إلى أنّ $f(x)\in\langle p(x)\rangle$ أو $g(x)\in\langle p(x)\rangle$؛ أي إن $p(x)$ إما عاملاً لـ $f(x)$ أو عاملاً لـ $g(x)$؛ لكن لا يمكن عندئذ أن يكون لدينا درجتا $f(x)$ و$g(x)$ أقل من درجة $p(x)$، وهذه تثبت أنّ $p(x)$ غير مختزل على F.

في المقابل، إذا كان $p(x)$ غير مختزل على F، افترض أنّ N مثالي، حيث إنّ $\langle p(x)\rangle\subseteq N\subseteq F[x]$، ومن خلال المبرهنة 24.27، N هو مثالي رئيس، وهكذا $N=\langle g(x)\rangle$ لعنصر ما $g(x)\in N$، عندئذ: $p(x)\in N$ تؤدي إلى أنّ $p(x)=g(x)q(x)$ لعنصر ما $q(x)\in F[x]$؛ لكن $p(x)$ غير مختزل، التي تؤدي إلى أنه إما $g(x)$ أو $q(x)$ درجته 0، فإذا كان $g(x)$ درجته 0 – أي إنه ثابت غير صفري في F – فإنّ $g(x)$ عنصر وحدة في $F[x]$، وهكذا $\langle g(x)\rangle=N=F[x]$، وإذا كان $q(x)$ درجته 0، فإنّ $q(x)=c$، حيث $c\in F$ و$g(x)=(1/c)p(x)$ في $\langle p(x)\rangle$، وهكذا $N=\langle p(x)\rangle$. وعليه، فمن المستحيل أنّ $\langle p(x)\rangle\subset N\subset F[x]$، وهكذا $\langle p(x)\rangle$ أعظمي. ♦

26.27 مثال يبين المثال 9.23 أنّ x^3+3x+2 غير مختزل في $\mathbb{Z}_5[x]$، وهكذا $\mathbb{Z}_5[x]/\langle x^3+3x+2\rangle$ حقل، وبالمثل، المبرهنة 11.22 تُبَيِّنُ أنّ x^2-2 غير مختزل في $\mathbb{Q}[x]$، وهكذا $\mathbb{Q}[x]/\langle x^2-2\rangle$ حقل. سوف نفحص لاحقًا مثل هذه الحقول بتفصيل أكثر. ▲

تطبيق على وحدانية التحليل في $F[x]$

في الفصل 23 ذكرنا المبرهنة 27.27 الآتية من غير برهان. (انظر المبرهنة 18.23) . بافتراض صحة هذه المبرهنة، وأثبتنا في الفصل 23 أنّ تحليل كثيرات الحدود في $F[x]$ إلى كثيرات حدود غير مختزلة هو وحيد، باستثناء ترتيب العوامل وعناصر الوحدة في F، وقد أَخَّرْنَا إثبات المبرهنة 27.27 لغاية الآن؛ لأنّ الآلية التي طورناها تُمَكِّنُنَا من إعطاء برهان بسيط من أربعة أسطر، ويملأ الفجوة في برهان وحدانية التحليل في $F[x]$.

27.27 مبرهنة لتكن $p(x)$ كثيرة حدود غير مختزلة في $F[x]$، فإذا كانت $p(x)$ تقسم $r(x)s(x)$ لـ $r(x), s(x) \in F[x]$، فإما $p(x)$ تقسم $r(x)$ أو $p(x)$ تقسم $s(x)$.

البرهان افترض أنّ $p(x)$ تقسم $r(x)s(x)$، عندئذ: $r(x)s(x) \in \langle p(x)\rangle$، الذي هو أعظمي من خلال المبرهنة 25.27، لهذا السبب $\langle p(x)\rangle$ مثالي أولي من خلال النتيجة 16.27، إذن، $r(x)s(x) \in \langle p(x)\rangle$ تؤدي إما إلى $r(x) \in \langle p(x)\rangle$ وهي تعطي أنّ $p(x)$ تقسم $r(x)$ – أو أن $s(x) \in \langle p(x)\rangle$ وهي تعطي أنّ $p(x)$ تقسم $s(x)$. ◆

عرض أولي لهدفنا الأساسي

نختم هذا الفصل بمخطط لإثبات هدفنا الأساسي في الفصل 29. لدينا الأفكار جميعها للبرهان، وربما بإمكانك أن تكملَ التفاصيل من هذا المخطط.

الهدف الأساسي: ليكن F حقلاً، ولتكن $f(x)$ كثيرة حدود غير ثابتة في $F[x]$. أثبت أنه يوجد حقل E يحوي F، ويحوي صفرًا α لـ $f(x)$.

مخطط البرهان

1– ليكن $p(x)$ عاملاً غير مختزل لـ $f(x)$ في $F[x]$.

2– ليكن E $F[x] / \langle p(x)\rangle$. (انظر المبرهنتين 5.27 و 9.27).

3– أثبت أنه لا يوجد عنصران مختلفان من F في مجموعة المشاركة نفسها في $F[x]/\langle p(x)\rangle$، واستنتج أنه يمكننا أن نَعدّ F (تبعاً للتماثل) حقلاً جزئيًّا من E.

4– لتكن α مجموعة المشاركة $x + \langle p(x)\rangle$ في E. أثبت أنه لتشاكل التعويض $\phi_\alpha : F[x] \to E$، لدينا $\phi_\alpha(f(x)) = 0$. أي إنّ: α صفر لـ $f(x)$ في E.

سيعطى مثال لحقل يبنى وفق هذا المخطط في الفصل 29، وسنعطي جدولي الجمع والضرب للحقل $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ ، ونثبت أنّ هذا الحقل له أربعة عناصر، مجموعات المشاركة

$$0 + \langle x^2 + x + 1\rangle \text{ ، } 1 + \langle x^2 + x + 1\rangle \text{ ، } x + \langle x^2 + x + 1\rangle$$

و

$$(x + 1) + \langle x^2 + x + 1\rangle$$

نعيد تسمية مجموعات المشاركة هذه لتصبح 0، 1، α و $\alpha + 1$ على الترتيب، ولنحصل على الجدولين 20.29 و 21.29 للجمع والضرب في هذا الحقل ذي العناصر الأربعة، لنرى كيف بُني هذان الجدولان، تذكر أننا في حقل مميزه 2؛ ولذلك، $\alpha + \alpha = \alpha(1+1) = \alpha 0 = 0$، وتذكر أيضًا، أنّ α هي صفر لـ $x^2 + x + 1$ ؛ ولذلك، $\alpha^2+\alpha+1=0$، وبناءً على ذلك، $\alpha^2 = -\alpha - 1 = \alpha + 1$.

■ تمارين 27

حسابات

1. أوجد جميع المثاليات الأوّلية وجميع المثاليات الأعظمية من $\mathbb{Z}_6$.

2. أوجد جميع المثاليات الأوّلية وجميع المثاليات الأعظمية من $\mathbb{Z}_{12}$.

3. أوجد جميع المثاليات الأوّلية وجميع المثاليات الأعظمية من $\mathbb{Z}_2 \times \mathbb{Z}_2$.

4. أوجد جميع المثاليات الأوّلية وجميع المثاليات الأعظمية من $\mathbb{Z}_2 \times \mathbb{Z}_4$.

5. أوجد جميع العناصر $c \in \mathbb{Z}_3$، حيث إنّ $\mathbb{Z}_3[x] / \langle x^2 + c \rangle$ حقل.

6. أوجد جميع العناصر $c \in \mathbb{Z}_3$، حيث إنّ $\mathbb{Z}_3[x] / \langle x^3 + x^2 + c \rangle$ حقل.

7. أوجد جميع العناصر $c \in \mathbb{Z}_3$، حيث إنّ $\mathbb{Z}_3[x] / \langle x^3 + cx^2 + 1 \rangle$ حقل.

8. أوجد جميع العناصر $c \in \mathbb{Z}_5$، حيث إنّ $\mathbb{Z}_5[x] / \langle x^2 + x + c \rangle$ حقل.

9. أوجد جميع العناصر $c \in \mathbb{Z}_5$، حيث إنّ $\mathbb{Z}_5[x] / \langle x^2 + cx + 1 \rangle$ حقل.

مفاهيم

في التمارين من 10 إلى 13 صَحِّح الحدّ المكتوب بخط مائل، دون الرجوع إلى الكتاب– إن كانت هناك حاجة للتصحيح– بحيث يكون بصيغة قابلة للنشر.

10. المثالي الأعظمي من حلقة R هو مثالي غير مُحْتَوًى في أيّ مثالي آخر من R.

11. المثالي الأولي من حلقة إبدالية R هو مثالي على الصورة $pR = \{pr \mid r \in R\}$ لعنصر ما أولي p.

12. المثالي الأولي هو حقل ليس له حقل جزئي فعلي.

13. المثالي الرئيس من حلقة إبدالية مع عنصر محايد هو مثالي N، مع الخاصية أنه يوجد $a \in N$، بحيث إنّ N هو المثالي الأصغر الذي يحوي a.

14. ضع إشارة صح أو إشارة خطأ:

_____ أ. كل مثالي أولي من كل حلقة إبدالية مع عنصر محايد هو مثالي أعظمي.

_____ ب. كل مثالي أعظمي من كل حلقة إبدالية مع عنصر محايد هو مثالي أولي.

_____ جـ. $\mathbb{Q}$ هي الحقل الجزئي الأولي من ذاتها.

_____ د. الحقل الجزئي الأولي من $\mathbb{C}$ هو $\mathbb{R}$.

_____ هـ. كل حقل يحوي حقلاً جزئيًّا يماثل حقلاً أوليًّا.

_____ و. الحلقة مع قواسم للصفر يمكن أن تحوي أحد الحقول الأولية بوصفها حلقة جزئية.

ـــــــ ز. كل حقل مميزه صفر يحوي حقلاً جزئيًا يماثل $\mathbb{Q}$.

ـــــــ ح. ليكن F حقلاً، ولأن $F[x]$ ليس له قواسم لـ 0، فكل مثالي من $F[x]$ هو مثالي أولي.

ـــــــ ط. ليكن F حقلاً. كل مثالي من $F[x]$ هو مثالي رئيس.

ـــــــ ي. ليكن F حقلاً. كل مثالي رئيس من $F[x]$ هو مثالي أعظمي.

15. أوجد مثاليًّا أعظميًّا من $\mathbb{Z} \times \mathbb{Z}$.

16. أوجد مثاليًّا أوليًّا من $\mathbb{Z} \times \mathbb{Z}$ لا يكون أعظميًّا.

17. أوجد مثاليًّا فعليًّا غير تافه من $\mathbb{Z} \times \mathbb{Z}$ لا يكون أوليًّا.

18. هل $\mathbb{Q}[x]/\langle x^2 - 5x + 6\rangle$ حقل؟ لماذا؟

19. هل $\mathbb{Q}[x]/\langle x^2 - 6x + 6\rangle$ حقل؟ لماذا؟

براهين مختصرة

20. أعطِ اختصارًا بجملة أو جملتين لجزء "فقط إذا" للمبرهنة 9.27.

21. أعطِ اختصارًا بجملة أو جملتين لجزء "إذا" للمبرهنة 9.27.

22. أعطِ اختصارًا بجملة أو جملتين للمبرهنة 24.27.

23. أعطِ اختصارًا بجملة أو جملتين لجزء "فقط إذا" للمبرهنة 25.27.

براهين

24. لتكن R حلقة إبدالية منتهية مع عنصر محايد. أثبت أنّ كل مثالي أولي من R هو مثالي أعظمي.

25. تخبرنا النتيجة 18.27 بأنّ كلّ حلقة مع عنصر محايد تحوي حلقة جزئية تماثل إما $\mathbb{Z}$ أو $\mathbb{Z}_n$ لعنصر ما n. فهل من الممكن أنّ حلقة مع عنصر محايد تحوي في آنٍ واحد حلقتين جزئيتين تماثلان $\mathbb{Z}_n$ و $\mathbb{Z}_m$ لـ $n \neq m$؟ إذا كانت ممكنة، فأعطِ مثالاً. وإذا كانت مستحيلة فأثبتها.

26. بإكمال التمرين 25، هل من الممكن أنّ حلقة مع عنصر محايد تحوي في آن واحد حلقتين جزئيتين تماثلان الحلقين $\mathbb{Z}_p$ و $\mathbb{Z}_q$ لأوليين مختلفين p و q. أعطِ مثالاً أو أثبت أنها مستحيلة.

27. باتباع الفكرة في التمرين 26، هل من الممكن أنّ حلقة تامّة تحوي حلقتين جزئيتين تماثلان $\mathbb{Z}_p$ و $\mathbb{Z}_q$ لـ $p \neq q$ و p و q كلاهما أولي؟ أعطِ سببًا أو توضيحًا.

28. أثبت مباشرة من تعريفي المثاليات الأولية والأعظمية أنّ كل مثالي أعظمي من حلقة إبدالية R مع عنصر محايد هو مثالي أولي. [افترض أنّ: M أعظمي من R، $ab \in M$ و $a \notin M$. ناقش الآتي: أصغر مثالي $\{ra + m \mid r \in R, m \in M\}$ يحوي a و M يجب أن يحوي 1، عبّر عن 1 على الصورة $ra+m$، واضرب بـ b].

29. أثبت أنّ N مثالي أعظمي من حلقة R إذا وفقط إذا كانت R/N **حلقة بسيطة (simple ring)** – أي إنه غير تافه، وليس له مثاليات غير تافهة فعلية (قارن بالمبرهنة 18.15).

30. أثبت أنه إذا كان F حقلاً، فإنّ كل مثالي أولي غير تافهٍ فعلي من $F[x]$ هو أعظمي.

31. ليكن F حقلاً و $f(x), g(x) \in F[x]$. أثبت أنّ $f(x)$ يقسم $g(x)$ إذا وفقط إذا كان $g(x) \in \langle f(x) \rangle$.

32. ليكن F حقلاً، وليكن $f(x), g(x) \in F[x]$. أثبت أنّ:

$$N = \{r(x)f(x) + s(x)g(x) \mid r(x), s(x) \in F[x]\}$$

مثالي من $F[x]$. أثبت أنه إذا كان $f(x)$ و $g(x)$ لهما درجتان مختلفتان و $N \neq F[x]$، فإنّ $f(x)$ و $g(x)$ ليس كلاهما غير مختزل على F.

33. استخدم المبرهنة 24.27 في إثبات تكافؤ هاتين المبرهنتين:

المبرهنة الأساسية في الجبر (Fundamental Theorem of Algebra): كل كثيرة حدود غير ثابتة في $\mathbb{C}[x]$ لها صفر في $\mathbb{C}$.

مبرهنة المواقع الصفرية لـ $\mathbb{C}[x]$ (Nullstellensatz for $\mathbb{C}[x]$): ليكن $f_1(x),\ldots,f_r(x)\in\mathbb{C}[x]$، وافترض أنّ كل صفر $\alpha \in \mathbb{C}$ لكثيرات الحدود هذه جميعها هو أيضًا صفر لكثيرة حدود $g(x)$ في $\mathbb{C}[x]$. عندئذ، قوة ما لـ $g(x)$ هي في المثالي الأصغر من $\mathbb{C}[x]$، الذي يحوي كثيرات الحدود $f_1(x), \ldots, f_r(x)$

هناك نوع من الحساب للمثاليات في الحلقة. التمارين الثلاثة الآتية تُعَرِّفُ جمع، وضرب، وخارج قسمة مثاليات.

34. إذا كان A و B مثاليين من حلقة R، **الجمع (sum)** $A + B$ لـ A و B مُعَرَّف بـ:

$$A + B = \{a + b \mid a \in A, b \in B\}$$

أ. أثبت أنّ $A + B$ مثالي. **ب.** أثبت أنّ $A \subseteq A + B$ و $B \subseteq A + B$.

35. ليكن A و B مثاليين من حلقة R. **الضرب (product)** AB لـ A و B مُعَرَّف بـ:

$$AB = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in A, b_i \in B, n \in Z^+ \right\}.$$

أ. أثبت أنّ AB مثالي من R. **ب.** أثبت أنّ $AB \subseteq (A \cap B)$.

36. ليكن A و B مثاليين من حلقة R. **خارج القسمة (quotient)** $A : B$ لـ A **على** B مُعَرَّف بـ:

$$A:B = \{r \in R \mid rb \in A \text{ لكل } b \in B\}$$

أثبت أنّ $A : B$ مثالي من R.

37. أثبت أنّ لحقل F، المجموعة S للمصفوفات على الصورة

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$$

لـ $a, b \in F$ **هي مثالي أيمن (right ideal)** لكن ليست **مثاليًا أيسر (left ideal)** من $M_2(F)$. أيْ أنْ تثبت أنَّ S حلقة جزئية مغلقة بالنسبة إلى الضرب من اليمين بأيّ عنصر من $M_2(F)$، ولكن ليست مغلقة بالنسبة إلى الضرب من اليسار.

38. أثبت أنّ حلقة المصفوفات $M_2(\mathbb{Z}_2)$ هي حلقة بسيطة – أي إنّ $M_2(\mathbb{Z}_2)$ ليس لها مثاليات غير تافهة فعلية.

الفصل 28 أساسيات جروبنر للمثاليات[1] Gröbner Bases for Ideals

يعطي هذا الفصل مقدّمة مختصرة في علم الهندسة، وبوصفها حالة خاصة، نحن مهتمون بمسألة إيجاد وصف بأبسط ما نستطيع لمجموعة الأصفار المشتركة لعدد منته من كثيرات الحدود، وحتى نكمل هدفنا في فصل واحد من هذا الكتاب، سنبدأ بسرد بعض المبرهنات من غير برهان، وللدراسة الإضافية والبراهين ننصح بكتاب (Adams and Loustaunau [23]).

المتنوعات الجبرية والمثاليات

ليكن F حقلاً، تذكر أنّ $F[x_1, x_2, \ldots, x_n]$ هي حلقة كثيرات الحدود لـ n من غير المعينات x_1، x_2، ...، x_n بمعاملات في F، لنجعل F^n هو الضرب الديكارتي $F \times F \times \ldots \times F$ لـ n عامل؛ ولنسهِّل الكتابة، سنرمز للعنصر $(a_1, a_2, \ldots, a_n)$ من F^n بـ $\mathbf{a}$، بحرف غامق. باستخدام تنظيم مشابه، لنجعل $F[\mathbf{x}] = F[x_1, x_2, \ldots, x_n]$، لكل $\mathbf{a} \in F^n$، لدينا تشاكل تعويض $\phi_{\mathbf{a}}: F[\mathbf{x}] \longrightarrow F$ كما هو في المبرهنة 4.22، أي إنه لـ $f(\mathbf{x}) = f(x_1, x_2, \ldots, x_n) \in F[\mathbf{x}]$ نُعَرِّف $\phi_{\mathbf{a}}(f(\mathbf{x})) = f(\mathbf{a}) = f(a_1, a_2, \ldots, a_n)$، برهان أنَّ $\phi_{\mathbf{a}}$ تشاكل ينتج من الخصائص التجميعية، والإبدالية، والتوزيعية للعمليات في $F[\mathbf{x}]$ وF، وكما في حالة غير المعين الواحد، العنصر $\mathbf{a}$ من F^n هو صفر لـ $f(\mathbf{x}) \in F[\mathbf{x}]$ **(zero of)** إذا كان $f(\mathbf{a}) = 0$، إضافة إلى ذلك، سنختصر فيما سيأتي كثيرة الحدود $f(\mathbf{x})$ بـ "f".

في هذا الفصل نناقش مسألة إيجاد أصفار مشتركة في F^n لعدد منته من كثيرات الحدود $f_1, f_2, \ldots, f_r$ في $F[\mathbf{x}]$، إذ إنَّ إيجاد الخصائص الهندسية لمجموعة هذه الأصفار المشتركة جميعها ودراستها هما موضوع الهندسة الجبرية.

1.28 تعريف لتكن S مجموعة جزئية منتهية من $F[\mathbf{x}]$. **المتنوعة الجبرية (algebraic variety)** $V(S)$ في F^n، هي مجموعة جميع الأصفار المشتركة في F^n لكثيرات الحدود في S. ■

في أمثلتنا التوضيحية – التي عادة تتضمن على الأكثر ثلاثة غير معينات – نستخدم x، y، z بدلاً من x_1، x_2 و x_3.

2.28 مثال لتكن $S = \{2x + y - 2\} \subset \mathbb{R}[x,y]$. المتنوعة الجبرية $V(S)$ في $\mathbb{R}^2$ هي خط مستقيم مقطعه السيني 1 ومقطعه الصادي 2. ▲

نترك للتمرين 29 البرهان المباشر بأنه لـ r عنصر $f_1, f_2, \ldots, f_r$ من حلقة إبدالية R مع عنصر محايد، المجموعة:

$$I = \{c_1 f_1 + c_2 f_2 + \ldots + c_r f_r \mid c_i \in R, i = 1, \ldots, r\}$$

هي مثالي من R، نرمز لهذا المثالي بـ $\langle f_1, f_2, \ldots, f_r \rangle$. نحن مهتمون بالحالة $R = F[\mathbf{x}]$ حيث c_i و f_i جميعها كثيرات حدود في $F[\mathbf{x}]$. نعدّ الـ c_i "بوصفها معاملات كثيرات حدود". فمن خلال بنيته، هذا المثالي I هو أصغر مثالي يحوي كثيرات الحدود $f_1, f_2, \ldots, f_r$ يمكن أيضًا أن يوصف بأنه تقاطع جميع المثاليات التي تحوي كثيرات الحدود هذه.

---

[1] لن يستخدم هذا الفصل في بقية الكتاب

3.28 تعريف ليكن I مثاليًا من حلقة إبدالية R مع عنصر محايد. مجموعة جزئية $\{b_1, b_2, \ldots , b_r\}$ من I هي أساس (**basis**) لـ I، إذا كان $I = \langle b_1, b_2, \cdots , b_r\rangle$. ■

بخلاف الوضع في الجبر الخطي، ليس هناك حاجة لاستقلالية العناصر في الأساس، أو وحدانية التمثيل لعنصر من المثالي بدلالة الأساس.

4.28 مبرهنة ليكن $f_1, f_2, \ldots f_r \in F[\mathbf{x}]$. مجموعة الأصفار المشتركة في F^n لكثيرات الحدود f_i لـ $i = 1, 2, \ldots, r$ هي مجموعة الأصفار نفسها المشتركة في F^n لكل كثيرات الحدود في كامل المثالي $I = \langle f_1, f_2, \cdots , f_r\rangle$.

البرهان ليكن:

$$f = c_1 f_1 + c_2 f_2 + \ldots + c_r f_r \tag{1}$$

أي عنصر في I. وليكن $\mathbf{a} \in F^n$ صفرًا مشتركًا لـ $f_1, f_2, \ldots, f_r$ بتطبيق تشاكل التعويض $\phi_{\mathbf{a}}$ على المعادلة (1) نحصل على:

$$\begin{aligned} f(\boldsymbol{a}) &= c_1(\boldsymbol{a})f_1(\boldsymbol{a}) + c_2(\boldsymbol{a})f_2(\boldsymbol{a}) + \cdots + c_r(\boldsymbol{a})f_r(\boldsymbol{a}) \\ &= c_1(\boldsymbol{a})0 + c_2(\boldsymbol{a})0 + \cdots + c_r(\boldsymbol{a})0 = 0, \end{aligned}$$

وهذه تُبيّن أنّ $\mathbf{a}$ أيضًا صفر لكل كثيرة حدود f في I، وبالطبع، صفر لكل كثيرة حدود في I سيكون صفرًا لكل f_i؛ لأنّ كل $f_i \in I$. ♦

لمثالي I من $F[\mathbf{x}]$ جعلنا $V(I)$ مجموعة الأصفار المشتركة لكل العناصر في I. يمكننا أن نجمل المبرهنة 4.28 على النحو:

$$V(\{f_1, f_2, \cdots, f_r\}) = V(\langle f_1, f_2, \cdots, f_r\rangle)$$

نذكر مبرهنة أساس هلبرت من غير برهان. (انظر [23] Adams and Loustaunau)

5.28 مبرهنة (مبرهنة أساس هلبرت (**Hilbert Basis Theorem**)) كل مثالي من $F[x_1, x_2, \cdots , x_n]$ له أساس منتهٍ.

هدفنا: إذا أعطيت أساس لمثالي I من $F[\mathbf{x}]$، عَدِّله إن أمكن ليصبح أساسًا يُظْهِرُ بصورة أفضل تركيب I وهندسة المتنوعة الجبرية المرافقة $V(I)$.

تزوّد المبرهنة الآتية بأداة لهذه الغاية، عليك ملاحظة أنّ المبرهنة تعطي معلومات عن خوارزمية القسمة التي لم نذكرها في المبرهنة 1.23، وهنا قد استخدمنا الرمز نفسه كما في المبرهنة 1.23، لكن استخدمنا $\mathbf{x}$ بدلاً من x. إذا كان: $f(\mathbf{x}) = g(\mathbf{x})\, h(\mathbf{x})$ في $F(\mathbf{x})$، فإنّ $g(\mathbf{x})$ و $h(\mathbf{x})$ يسميان "**قواسم (divisors)**" أو "**عوامل (factors)**" لـ $f(\mathbf{x})$.

6.28 مبرهنة (خاصية خوارزمية القسمة) لتكن $f(\mathbf{x})$؛ $g(\mathbf{x})$، $q(\mathbf{x})$ و$r(\mathbf{x})$ وكثيرات حدود في $F[\mathbf{x}]$، بحيث إنّ $f(\mathbf{x}) = g(\mathbf{x})\ q(\mathbf{x}) + r(\mathbf{x})$. الأصفار المشتركة في F^n لـ $g(\mathbf{x})$ و $f(\mathbf{x})$ هي نفسها الأصفار المشتركة لـ $r(\mathbf{x})$ و $g(\mathbf{x})$، أيضًا القواسم المشتركة في $F[\mathbf{x}]$ لـ $f(\mathbf{x})$ و $g(\mathbf{x})$ هي نفسها القواسم المشتركة لـ $g(\mathbf{x})$ و $r(\mathbf{x})$.

إذا كان $f(\mathbf{x})$ و $g(\mathbf{x})$ عنصرين في أساسٍ لمثالي I من $F[\mathbf{x}]$، فإن استبدال $f(\mathbf{x})$ بـ $r(\mathbf{x})$ في الأساس سيبقى يعطي أساسًا لـ I.

البرهان إذا كان $\mathbf{a} \in F^n$ صفرًا مشتركًا لـ $g(\mathbf{x})$ و $r(\mathbf{x})$، فإنه بتطبيق $\phi_{\mathbf{a}}$ لطرفي المعادلة $f(\mathbf{x}) = g(\mathbf{x})\ q(\mathbf{x}) + r(\mathbf{x})$، نحصل على: $f(\mathbf{a}) = g(\mathbf{a})\ q(\mathbf{a}) + r(\mathbf{a}) = 0q(\mathbf{a}) + 0 = 0$، وهكذا $\mathbf{a}$ صفر مشترك لـ $g(\mathbf{x})$ و $f(\mathbf{x})$. إذا كان $\mathbf{b} \in F[\mathbf{x}]$ صفرًا مشتركًا لـ $f(\mathbf{x})$ و $g(\mathbf{x})$، فإنّ تطبيق $\phi_{\mathbf{b}}$ يعطي $f(\mathbf{b}) = g(\mathbf{b})\ q(\mathbf{b}) + r(\mathbf{b})$، وهكذا $0 = 0q(\mathbf{b}) + r(\mathbf{b})$ ونرى أنّ $r(\mathbf{b}) = 0$، إضافة إلى أنّ $g(\mathbf{b}) = 0$.

البرهان المتعلق بالقواسم المشتركة هو بصورة جوهرية البرهان في الأعلى نفسه، ويترك للتمرين 30.

أخيرًا، ليكن B أساسًا لمثالي I، وليكن $f(\mathbf{x}), g(\mathbf{x}) \in B$، وليكن، $f(\mathbf{x}) = g(\mathbf{x})q(\mathbf{x}) + r(\mathbf{x})$، ولتكن B' المجموعة الناتجة عن B باستبدال $f(\mathbf{x})$ بـ $r(\mathbf{x})$، وليكن I' المثالي الذي أساسه هو B'. ولتكن S المجموعة الناتجة عن B بضم $r(\mathbf{x})$ إلى B، لاحظ أيضًا أنّ S يمكن الحصول عليها بضم $f(\mathbf{x})$ إلى B'. المعادلة $f(\mathbf{x}) = g(\mathbf{x})\ q(\mathbf{x}) + r(\mathbf{x})$ تبيّن أنّ $f(\mathbf{x}) \in I'$، وهكذا لدينا $B' \subseteq S \subseteq I'$. وعليه، S أساس لـ المعادلة $r(\mathbf{x}) = f(\mathbf{x}) - q(\mathbf{x})\ g(\mathbf{x})$ تبيّن أنّ $r(\mathbf{x}) \in I$، وهكذا لدينا $B \subseteq S \subseteq I$. وعليه، S أساس لـ I؛ لهذا السبب $I' = I$ و B' أساس لـ I. ♦

توضيح خطي مألوف

الأسلوب الأساسي لحل مسألة في الجبر الخطي هو إيجاد جميع الحلول المشتركة لعدد منتهٍ من المعادلات الخطية، سنتخلى في هذه اللحظة عن عادتنا في عدم كتابة "$f(\mathbf{x}) = 0$" لكثيرة حدود غير صفرية، وسنحل مسألة نموذجية، كما نفعل في مقرر دراسي للجبر الخطي.

7.28 مثال **(الحل كما في مقرر دراسي للجبر الخطي)** أوجد جميع الحلول في $\mathbb{R}^3$ للنظام الخطي

$$x + y - 3z = 8$$

$$2x + y + z = -5.$$

الحل نضرب المعادلة الأولى بـ 2-، ونضيفها للمعادلة الثانية، فنحصل على النظام الجديد:

$$x + y - 3z = 8$$

$$-y + 7z = -21$$

الذي له مجموعة الحل نفسها في $\mathbb{R}^3$ كما للنظام السابق. ولأيّ قيمة z، نستطيع أن نجد قيمة y المقابلة، وذلك من المعادلة الثانية، ومن ثم نحدد x من المعادلة الأولى، بإبقاء z غير مُعَين نحصل على $\{-4z - 13, 7z + 21, z) \mid z \in \mathbb{R}\}$ بوصفها مجموعة حل، التي هي خط مستقيم يمرّ من خلال النقطة (0, 21, 13-) في فضاء إقليدس ثلاثي الأبعاد. ▲

باستخدام رموز هذا الفصل، المسألة في المثال السابق يمكن أن يعبر عنها على النحو الآتي:

صِفْ $V(\langle x + y - 3z - 8, 2x + y + z + 5\rangle)$ في $\mathbb{R}^3$

وقد حللناها بإيجاد أساس أكثر نفعًا، نعني:

$$\{x + y - 3z - 8, -y + 7z + 21\}$$

لاحظ أنّ العنصر الثاني $-y + 7z + 21$ من هذا الأساس الجديد يمكن الحصول عليه من كثيرتي الحدود في الأساس الأصلي بوصفه باقي $r(x, y, z)$ لعملية القسمة، أي إنّ:

$$\begin{array}{r|l} & \quad 2 \\ \hline x + y - 3z - 8 & 2x + y + z + 5 \\ & \underline{2x + 2y - 6z - 16} \\ & \quad -y + 7z + 21 \end{array}$$

وعليه، $2x + y + z + 5 = (x + y - 3z - 8)(2) + (-y + 7z + 21)$ هو تعبيرٌ على الصورة $f(x, y, z) = g(x, y, z)\, q(x, y, z) + r(x, y, z)$. نستبدل كثيرة الحدود f بكثيرة الحدود r كما في المبرهنة 6.28، التي تضمن لنا أنّ $V(\langle f, g\rangle) = V(\langle g, r\rangle)$ وأن $\langle f, g\rangle = \langle g, r\rangle$، وقد اخترنا في المثال 7.28 مسألة بسيطة جدًّا من خطوة واحدة، على أيّ حال، من الواضح أنَّ الطريقة المقدمة في مقرر دراسي للجبر الخطي لحل نظام خطي، يمكن أن يُعَبَّر عنها بدلالة تطبيق عملية متكررة لخوارزمية القسمة، لتغيير أساس مثالي معطى إلى أساس يوضح الهندسة للمتنوعة الجبرية المرافقة بصورة أفضل.

توضيح غير معين مفرد

افترض أننا نريد إيجاد المتنوعة $V(I)$ في F ، المرافقة لمثالي I من $F[x]$، حلقة كثيرات الحدود لغير معين مفرد x من خلال المبرهنة 24.27، كل مثالي من $F[x]$ هو رئيس، وهكذا يوجد $f(x) \in F[x]$، حيث إنّ $I = \langle f(x) \rangle$، وعليه، $V(I)$ يتكوّن من أصفار كثيرة حدود مفردة، و$\{f(x)\}$ من المحتمل أنه أساس لـ I بوصفه أبسط ما يمكننا أن نطلب، ونعطي مثالاً يوضّح الحساب لمثل هذا المولِّد المفرد $f(x)$ لـ I، في حالة كان الأساس المعطى لـ I يحوي أكثر من كثيرة حدود واحدة، فلأن كثيرة الحدود في $\mathbb{R}[x]$ لها فقط عدد منته من الأصفار في $\mathbb{R}$، نتوقع ألا يكون هناك أصفار مشتركة لكثيرتي حدود أو أكثر اختيرت بصورة عشوائية في $\mathbb{R}[x]$؛ لكننا بنينا الأساس في مثالنا بحذر!

8.28 مثال لِنَصِفَ المتنوعة الجبرية V من $\mathbb{R}$ المتكوّنة من الأصفار المشتركة لـ:

$$f(x) = x^4 + x^3 - 3x^2 - 5x - 2 \text{ و } g(x) = x^3 + 3x^2 - 6x - 8.$$

نريد إيجاد أساس جديد لـ $\langle f, g \rangle$ يحتوي على كثيرات حدود درجتها أصغر ما أمكن؛ لذلك، نستخدم خوارزمية القسمة $f(x) = g(x)\, q(x) + r(x)$ في المبرهنة 1.23، حيث $r(x)$ ستكون درجتها على الأكثر 2، عندئذٍ: نستبدل الأساس $\{f, g\}$ بالأساس $\{g, r\}$

$$\begin{array}{r|l}
 & x - 2 \\
\hline
x^3 + 3x^2 - 6x - 8 & x^4 + x^3 - 3x^2 - 5x - 2 \\
 & \underline{x^4 + 3x^3 - 6x^2 - 8x} \\
 & \quad -2x^3 + 3x^2 + 3x - 2 \\
 & \quad \underline{-2x^3 - 6x^2 + 12x + 16} \\
 & \qquad\quad 9x^2 - 9x - 18
\end{array}$$

لأن أصفار $9x^2 - 9x - 18$ هي نفسها أصفار $x^2 - x - 2$ ، جعلنا $r(x) = x^2 - x - 2$، وأخذنا الأساس الجديد

$$\{g, r\} = (x^3 + 3x^2 - 6x - 8, x^2 - x - 2)$$

بقسمة $g(x)$ على $r(x)$ نحصل على الباقي $r_1(x)$، سنكون الآن قادرين على إيجاد أساس $\{r(x), r_1(x)\}$ يتألف من كثيرتي حدود درجتاهما على الأكثر 2.

$$\begin{array}{r|l}
 & x + 4 \\
\hline
x^2 - x - 2 & x^3 + 3x^2 - 6x - 8 \\
 & \underline{x^3 - x^2 - 2x} \\
 & \quad 4x^2 - 4x - 8 \\
 & \quad \underline{4x^2 - 4x - 8} \\
 & \qquad\qquad 0
\end{array}$$

أساسُنا الجديد $\{r(x), r_1(x)\}$ أصبح الآن $\{x^2 - x - 2\}$، وعليه:

$I = \langle f(x), g(x) \rangle = \langle x^2 - x - 2 \rangle = \langle (x-2)(x+1) \rangle$ ونرى أنّ $V = \{-1, 2\}$.

تخبرنا المبرهنة 6.28 بأنّ القواسم المشتركة لـ $f(x)$ و $g(x)$ في المثال السابق هي نفسها القواسم المشتركة لـ $r(x)$ و $r_1(x)$؛ ولأن $r(x)\ (0) = 0$ ، فنرى أنّ $r(x)$ يقسم 0، وهكذا القواسم المشتركة لـ $f(x)$ و $g(x)$ هي فقط تلك القواسم لـ $r(x)$، التي بالطبع تشمل $r(x)$ نفسها. وعليه، $r(x)$ يسمى "قاسمًا مشتركًا أكبر" (اختُصِرَ gcd) لـ $f(x)$ و $g(x)$.

أساسات جروبنر

سنعالج مسألة إيجاد أساس متقن لمثالي I من $F[\mathbf{x}] = F[x_1, x_2, \cdots, x_n]$. بالنظر إلى توضيحنا لحالات غير معين واحد خطي، إنه يبدو من المعقول محاولة استبدال كثيرات حدود في الأساس بكثيرات حدود درجاتها أقل، أو تحوي غير معينات أقل. إنه من الحاسم أن يكون لدينا طريقة نظامية لإتمام ذلك. كل مدرس للجبر الخطي يصادف أحيانًا طالبًا غير قادر على إتقان اختزال المصفوفات، حيث يصنع مدخلات صفرية في أعمدة المصفوفة بنمط عشوائي تقريبًا، بدلًا من إنهاء العمود الأول ثم الانتقال إلى العمود الثاني، وهكذا كخطوة أولى في إتجاه هدفنا سنعالج مسألة تحديد ترتيب لكثيرات الحدود.

كثيرات الحدود في $F[\mathbf{x}]$ حدودها على الشكل $ax_1^{m_1}x_2^{m_2}\ldots x_n^{m_n}$، حيث $a \in F$.

خصائص الترتيب لضروب القوى
1. $1 < P$ لكل ضروب القوى $P \neq 1$.
2. لضربي قوى P_i و P_j تتحقق واحدة فقط من الآتية: $P_i < P_j$, $P_i = P_j$, $P_j < P_i$.
3. إذا كان $P_i < P_j$ و $P_j < P_k$، فإنّ $P_i < P_k$.
4. إذا كان $P_i < P_j$، فإنّ $PP_i < PP_j$ لأيّ ضرب قوى P.

لنَعدّ **ضرب القوى في** $F[\mathbf{x}]$ بوصفه مقدارًا جبريًّا على الصورة:

$P = x_1^{m_1}x_2^{m_2}\ldots x_n^{m_n}$ حيث $0 \leq m_i$ في $\mathbb{Z}$ لكل i.

لاحظ تمثيل جميع x_i ومن المحتمل أن يكون بعضها لأُسٍ صفري. ومن ثم في $F[x,y,z]$، يجب أن تكتب xz^2 بوصفه ضرب قِوى على النحو xy^0z^2. نرغب بوصف ترتيب كلي $<$ على مجموعة جميع ضروب القوى، وذلك حتى نعلم فقط معنى أن نقول $P_i < P_j$، وليزوّدنا برمز الحجم النسبي لضروب القوى، بعد ذلك يمكننا محاولة تغيير أساس لمثالي بطريقة نظامية لصنع أساس كثيرات حدود فيه، ذوات حدود على الصورة a_iP_i تكون فيه ضروب القوى P_i أصغر ما يمكن. سنرمز لضرب القوى الذي فيه جميع الأُسُس صفرية بالرمز 1، وسنشترط تحقيق الترتيب لضروب القوى الخصائص المذكورة في الصندوق، افترض أنّ ترتيب كهذا قد وُصِفَ، وأنّ $P_i \neq P_j$ وP_i تقسم P_j؛ بحيث $P_j = PP_i$، حيث $1 < P$. الخاصية 4 في الصندوق، تؤدي إلى أن $1P_i < PP_i = P_j$، وهكذا $P_i < P_j$. إذا P_i تقسم P_j فإنها تؤدي إلى أن $P_i < P_j$، في التمرين 28 نطلب أن تُثبت بمثال مضاد أنّ $P_i < P_j$ لا تؤدي إلى أنَّ P_i تقسم P_j.

من الممكن إثبات أنّ هذه الخصائص تضمن أنّ أي عملية تدريجية لتعديل أساس منته لمثالي، التي لا تزيد الحجم لأيِ ضرب قوّى أكبر في عنصر الأساس، وفي كل خطوة تستبدلُ واحدًا بشيء أصغر، سوف تنتهي بعدد محدود من الخطوات.

في $F[x]$ مع غير المعين الوحيد x، يتوافر ترتيب ضرب قوّى واحد فقط؛ لأنه من خلال الخاصية 1، يجب أن يكون لدينا $x>1$، وبالضرب بصورة متكررة بـ x وباستخدام الخاصية 4، لدينا $x<x^2, x^2<x^3$ ، ... إلخ، بعدئذ تبيّن الخاصية 3 أنّ $1<x<x^2<x^3<\cdots$ هو الترتيب الممكن الوحيد، لاحظ أنّنا عَدَّلنا الأساس في المثال 8.28، باستبدال كثيرات حدود الأساس بكثيرات حدود تحوي ضروب قوّى أصغر.

هناك عدد من الترتيبات المحتملة لضروب القوى في $F[\mathbf{x}]$ مع n غير معين، وسنقدم واحدًا فقط، (*lexicographical order*) (يرمز له بـ "lex"). في lex، حيث نُعرِّف:

$$x_1^{s_1} x_2^{s_2} \cdots x_n^{s_n} < x_1^{t_0} x_2^{t_2} \cdots x_n^{t_n} \tag{2}$$

إذا وفقط إذا كان $s_i < t_i$ لأول رمز دليلي i – بالقراءة من اليسار إلى اليمين– بحيث إنّ $s_i \neq t_i$. وعليه، إذا كتبنا في $F[x,y]$ ضرب قوّى بترتيب $x^n y^m$، فلدينا $x = x^1 y^0 > x^0 y^1 = y$ و $xy < xy^2$ ، وباستخدام lex، فإنّ الترتيب لـ n غير معيّن يكون $x_1 > x_2 > \ldots > x_{n-1} > x_n > 1$ ، اختزالنا في المثال 7.28 حيث تخلصنا أولاً قدر استطاعتنا من كل x "كبيرة" ، وبعدئذ y "الأصغر" المقابلة للترتيب lex: $x > y > z$، أي لتكتب ضروب القوى جميعها على الترتيب $x^m y^n z^s$ لحالة غير معينين مع $x > y$ ، مخطط ترتيب حدود lex الكلي هو:

$$1 < y < y^2 < y^3 \cdots < x < xy < xy^2 < xy^3 < \cdots < x^2 < x^2 y < x^2 y^2 < \cdots$$

يُحدثُ ترتيبٌ لضروب قوى P ترتيبًا واضحًا لحدود كثيرة حدود في $F[\mathbf{x}]$ حدودها aP، الذي سنشير إليه بوصفه ترتيب حدود (**term order**)، ومن الآن فصاعدًا، إذا أُعطينا ترتيبًا لضروب قوّى، فسنعُدّ أنّ كل كثيرة حدود f في $F[\mathbf{x}]$ كُتبَت بترتيب حدود متناقص؛ ولذلك، الحدّ القائد (الأول) درجته الأعلى، حيث نرمز بـ $\mathrm{lt}(f)$ للحدّ القائد لـ f ، ونرمز بـ $\mathrm{lp}(f)$ لضرب القوى للحد القائد، فإذا كانت f و g كثيرتي حدود في $F[\mathbf{x}]$ ، حيث إنّ $\mathrm{lp}(g)$ يقسم $\mathrm{lp}(f)$، فإنه يمكننا أن نجري قسمة f على g، كما وُضحت في الحالتين الخطية وغير معين واحد – لنحصل على $f(\mathbf{x}) = g(\mathbf{x})\, q(\mathbf{x}) + r(\mathbf{x})$، حيث $\mathrm{lp}(r) < \mathrm{lp}(f)$. لاحظ لم نقل: $\mathrm{lp}(r) < \mathrm{lp}(g)$. المثال الآتي يوضّح ذلك.

9.28 مثال من خلال القسمة، اختزل الأساس $\{xy^2, y^2 - y\}$ للمثالي $I = \langle xy^2, y^2 - y\rangle$ من $\mathbb{R}[x,y]$ إلى أساس ذي أصغر حجم لأكبر حدّ، بافتراض الترتيب lex مع $x > y$.

الحل

نرى أنّ y^2 يقسم xy^2 ، ونحسب:

$$\begin{array}{r|l} & x \\ \hline y^2 - y & xy^2 \\ & \underline{xy^2 - xy} \\ & \quad xy \end{array}$$

لأنّ y^2 لا يقسم xy لا نستطيع الاستمرار في القسمة، لاحظ أنّ $\mathrm{lp}\ (xy) = xy$ ليس أقلّ من $\mathrm{lp}(y^2 - y) = y^2$. على أي حال، لدينا $\mathrm{lp}(xy) < \mathrm{lp}(xy^2)$، أساسنا الجديد لـ I هو $\{xy, y^2 - y\}$. ▲

عند التعامل مع أكثر من غير معين واحد، فإنه سيكون أكثر سهولة عمل اختزال أساس بضرب كثيرة حدود $g(\mathbf{x})$ للأساس بكثيرة حدود $-q\ (\mathbf{x})$ وإضافتها لكثيرة حدود $f(\mathbf{x})$؛ للحصول على $r(\mathbf{x})$، إضافة إلى أننا نعمل اختزال المصفوفات في الجبر الخطي، بدل كتابة القسمة بصورتها الظاهرة كما عملنا في المثال السابق، فالبدء بكثيرتي حدود xy^2 و $y^2{-}y$ في أساس، يمكننا اختزال xy^2 بضرب $y^2{-}y$ بـ $-x$ وإضافة الناتج $-xy^2 + xy$ إلى xy^2، نحصل على البديل xy لـ xy^2. يمكننا عمل ذلك في أذهاننا وكتابة النتيجة مباشرة.

بالرجوع مرة أخرى إلى المثال 9.28، سينتج مما ذكرناه آنفًا أنه لأيّ كثيرة حدود معطاة $f\,(x, y) = c_1(x, y)(xy) + c_2(x, y)(y^2 - y)$ في $\langle xy, y^2 - y\rangle$، إما xy أو y^2 سيقسم $\mathrm{lp}(f)$. (انظر التمرين 31)، هذه توضح الخاصية المُعَرِّفَة لأساس جروبنر

10.28 تعريف المجموعة $\{g_1, g_2, \dots , g_r\}$ لكثيرات حدود غير صفرية في $F[x_1, x_2, \dots , x_n]$، مع ترتيب حدود $<$، هي **أساس جروبنر (Gröbner basis)** للمثالي $I = \langle g_1, g_2, \cdots , g_r\rangle$ إذا وفقط إذا كان لكل $f \in I$ غير صفري يوجد i، $1 \le i \le r$ ، حيث إنّ $\mathrm{lp}\ (g_i)$ يقسم $\mathrm{lp}\ (f)$. ■

بينما وضّحنا الحساب لأساس جروبنر من أساس معطًى لمثالي، وذلك في الأمثلة 7.28، 8.28، و 9.28 لم نعطِ خوارزمية محددة. نرجع القارئ إلى (Admas and Loustaunau [23])، حيث تتألف الطريقة من ضرب كثيرة حدود ما في الأساس بأيّ كثيرة حدود في $F[\mathbf{x}]$، وإضافة الناتج إلى كثيرة حدود أخرى في الأساس بطريقة تقلل الحجم لضروب القوى، وقد عالجنا في توضيحنا الحالة المتضمنة لقسمة $f\,(\mathbf{x})$ على $g\ (\mathbf{x})$، حيث $\mathrm{lp}(g)$ يقسم $\mathrm{lp}\ (f)$، لكننا نستطيع أيضًا استخدام العملية إذا كان $\mathrm{lp}\ (g)$ يقسم فقط ضرب قوًى آخر في f على سبيل المثال: إذا كان أساس فيه العنصران $xy - y^3$ و $y^2 - 1$، يمكننا ضرب $y^2 - 1$ بـ y ، وإضافة الناتج إلى $xy - y^3$، مختزلين $xy - y^3$ إلى $xy - y$، وتبيّن المبرهنة 6.28 أنّ هذا حساب صحيح.

من الممكن أن تتعجب كيف أنّ أيّ أساس $\{g_1, g_2, \dots , g_r\}$ يمكن أن يفشل ليصبح أساس جروبنر لـ $I = \langle g_1, g_2, \dots , g_r\rangle$؛ لأننا عندما نشكل عنصرًا $c_1g_1 + c_2g_2 + \cdots + c_r\, g_r$ في I، نرى أنّ $\mathrm{lp}\ (g_i)$ قاسم لـ $\mathrm{lp}\ (c_ig_i)$ لـ $i = 1,2, \dots , r$. على أيّ حال، الحذف لضروب القوى يمكن أن يحدث في الجمع. وإليك توضيح ذلك بمثال.

11.28 مثال ليكن المثالي $I = \langle x^2y - 2, xy^2 - y \rangle$ من $\mathbb{R}[x,y]$ ، فكثيرتا الحدود في الأساس المُبَيَّن لا يمكن اختزالهما أكثر، على أيّ حال، المثالي I يحوي $y\,(x^2y-2) - x\,(xy^2 - y) = xy - 2y$، الذي ضرب قواه القائد xy غير قابل للقسمة على أي من ضربي القوى القائدين x^2y أو xy^2 للأساس المعطى. وعليه، $\{x^2y - 2, xy^2 - y\}$ ليس أسَاس جروبنر لـ I، وفقًا للتعريف 10.28. ▲

عندما بلغنا وضعًا يشبه ذلك في المثال 11.28، أدركنا أنّ أساس جروبنر يجب أن يحوي كثيرة حدود ما لها ضرب قوًى قائد أصغر من ضروب القوى القائدة لكثيرات الحدود الأخرى في الأساس المعطى، لتكن f و g كثيرتي حدود في الأساس المعطى، وكما عملنا في المثال 11.28، يمكننا ضرب f و g بضربي قوى أصغرين قدر الإمكان، حيث إنّ ضربي القوى القائدين الناتجين سيكونان الشيء نفسه، المضاعف المشترك الأصغر (lcm) لـ $\mathrm{lp}\,(f)$ و $\mathrm{lp}\,(g)$، وبعد ذلك اجمع أو اطرح مع معاملات مناسبة من F ، حيث إنّ الحذف يعطي النتيجة، إذ نرمز لكثيرة حدود شكلت بهذا الأسلوب بـ $S\,(f\,,g\,)$، ونذكر من غير برهان مبرهنة يمكن استخدامها بوصفها اختبارًا فيما إذا كان أساس ما مُعطى هو أساس جروبنر.

12.28 مبرهنة الأساس $G = \{g_1, g_2, \cdots, g_r\}$ هو أساس جروبنر للمثالي $\langle g_1, g_2, \cdots, g_r \rangle$ إذا وفقط إذا كان – لكل $i \neq j$ – كثيرة الحدود $S\,(g_i, g_j)$ ، يمكن اختزالها إلى صفر من خلال قسمة متكررة للبواقي على عناصر من G كما في خوارزمية القسمة.

كما ذكرنا سابقًا، من الممكن أن نفضل التفكير في اختزال $S\,(g_i, g_j)$، من خلال متتالية من العمليات المؤلفة من جمع (أو طرح) مضاعفات لكثيرات حدود في G، بدلاً من كتابة القسمة.

يمكننا الآن أن نُبَيِّن كيف يمكننا الحصول على أساس جروبنر من أساس معطًى. بدايةً، اختزل كثيرات الحدود في الأساس فيما بينها قدر الإمكان، اختر بعد ذلك كثيرتي حدود g_i و g_j في الأساس، وشكِّل كثيرة الحدود $S\,(g_i\,, g_j)$، وانظر فيما إذا كانت $S\,(g_i\,, g_j\,)$ يمكن اختزالها إلى صفر كما وُصِفَ توًّا، فإذا كان ذلك بالإمكان، فاختر زوجين مختلفين من كثيرات الحدود، وأعد الإجراءات معهما، أمّا إذا كانت $S\,(g_i\,,\, g_j)$ لا يمكن اختزالها إلى صفر كما وُصِفَ في الأعلى، فزد الأساس المعطى بهذا العنصر $S(g_i\,,\, g_j)$، وابدأ من جديد اختزال هذا الأساس قدر الإمكان، ومن خلال المبرهنة 12.28، عندما تكون كثيرات الحدود جميعها $S\,(g_i\,, g_j\,)$ لكل $i \neq j$ يمكن اختزالها إلى الصفر، وذلك باستخدام كثيرات حدود من الأساس الأخير، نكون وصلنا إلى أساس جروبنر، ونختم بإكمال المثال 11.28:

13.28 مثال بإكمال المثال 11.28، ليكن $g_1 = x^2y - 2$، $g_2 = xy^2 - y$، $I = \langle g_1\,,\, g_2 \rangle$ في $\mathbb{R}^2$، حصلنا في المثال 11.28 على كثيرة الحدود $S(g_1\,,\, g_2) = xy - 2y$ ، التي لا يمكن اختزالها إلى الصفر باستخدام g_1 و g_2، وسنختزل الآن الأساس $\{x^2y - 2, xy^2 - y, xy - 2y\}$ بتوضيح كل خطوة.

$\{x^2\,y - 2,\, xy^2 - y,\, xy - 2y\}$	أساسٌ مَزِيْد
$\{2xy - 2,\, xy^2 - y,\, xy - 2y\}$	بإضافة $(-x)$ (الثالث) إلى الأول
$\{2xy - 2,\, 2y^2 - y,\, xy - 2y\}$	بإضافة $(-y)$ (الثالث) إلى الثاني
$\{4y - 2,\, 2y^2 - y,\, xy - 2y\}$	بإضافة (-2) (الثالث) إلى الأول

$\{4y-2, 0, xy-2y\}$ بإضافة $\left(-\frac{y}{2}\right)$ (الأول) إلى الثاني

$\{4y-2, 0, \frac{1}{2}x-2y\}$ بإضافة $\left(-\frac{x}{4}\right)$ (الأول) إلى الثالث

$\{4y-2, 0, \frac{1}{2}x-1\}$ بإضافة $\left(\frac{1}{2}\right)$ (الأول) إلى الثالث

من الواضح أنّ $\left\{y-\frac{1}{2}, x-2\right\}$ هو أساس جروبنر، لاحظ أنه إذا كان $f=y-\frac{1}{2}$ و $g=x-2$، فإنّ $S(f,g)=xf-yg=\left(xy-\frac{x}{2}\right)-(xy-2y)=-\frac{x}{2}+2y$، التي يمكن بسهولة اختزالها إلى الصفر بجمع $\frac{1}{2}(x-2)$ و $-2\left(y-\frac{1}{2}\right)$.

من أساس جروبنر نرى أنّ المتنوّعة الجبرية $V(I)$ تحوي نقطة واحدة فقط $\left(2,\frac{1}{2}\right)$ في $\mathbb{R}^2$. ▲

تأتي أهمية أساسات جروبنر في التطبيقات من الحقيقة أنها قابلة للحساب بصورة روتينية. وهذه الأساسات لها تطبيقات في الهندسة وعلم الحاسوب إضافة إلى الرياضيات.

تمارين 28

في التمارين من 1 إلى 4، اكتب كثيرات الحدود في $\mathbb{R}[x,y,z]$ بترتيب حدود متناقص باستخدام ترتيب lex لضروب القوى $x^m y^n z^s$ ، حيث $z<y<x$.

1. $2xy^3z^5-5x^2yz^3+7x^2y^2z-3x^3$

2. $3y^2z^5-4x+5y^3z^3-8z^7$

3. $3y-7x+10z^3-2xy^2z^2+2x^2yz^2$

4. $38-4xz+2yz-8xy+3yz^3$

في التمارين من 5 إلى 8، اكتب كثيرات الحدود في $\mathbb{R}[x,y,z]$ بترتيب حدود متناقص باستخدام ترتيب lex لضروب القوى $z^m y^n x^s$، حيث $x<y<z$.

5. كثيرة الحدود في التمرين 1.

6. كثيرة الحدود في التمرين 2.

7. كثيرة الحدود في التمرين 3.

8. كثيرة الحدود في التمرين 4.

ترتيب آخر – deglex– لضروب القوى في $F[x]$ مُعَرَّف كما يأتي:

$$x_1^{s_1}x_2^{s_2}\cdots x_n^{s_n} < x_1^{t_1}x_2^{t_2}\cdots x_n^{t_n}$$

إذا وفقط إذا كان إما $\sum_{i=1}^{n} s_i < \sum_{i=1}^{n} t_i$ أو هذان المجموعان متساويان و $s_i < t_i$ لأصغر قيمة لـ i ، حيث إنّ $s_i \neq t_i$.

التمارين من 9 إلى 13، تهتم بالترتيب deglex.

9. اسرد – بترتيب تصاعدي – أصغر 20 ضرب قوى في $\mathbb{R}[x,y,z]$ لترتيب deglex مع ضروب قوى $x^m y^n z^s$ حيث $z < y < x$.

في التمارين من 10 إلى 13، اكتب كثيرات الحدود بترتيبات حدود متناقص باستخدام الترتيب deglex مع ضروب قوى $x^m y^n z^s$ حيث $z < y < x$

10– كثيرة الحدود في التمرين 1. **11**– كثيرة الحدود في التمرين 2.

12– كثيرة الحدود في التمرين 3. **13**– كثيرة الحدود في التمرين 4.

في التمارين من 14 إلى 17، لتكن ضروب القوى في $\mathbb{R}[x,y,z]$ لها ترتيب lex، حيث $z < y < x$. اعمل – إن أمكن– اختزالاً بخوارزمية القسمة من خطوة واحدة لتغيِّر أساس المثالي المعطى إلى أساس ترتيب حدّه الأكبر أصغر.

14– $\langle xy^2 - 2x, x^2y + 4xy, xy - y^2\rangle$ **15**– $\langle xy + y^3, y^3 + z, x - y^4\rangle$

16– $\langle xyz - 3z^2, x^3 + y^2z^3, x^2yz^3 + 4\rangle$ **17**– $\langle y^2z^3 + 3, y^3z^2 - 2z, y^2z^2 + 3\rangle$

في التمرينين 18 و 19، ليكن ترتيب ضروب القوى في $\mathbb{R}[w, x, y, z]$ هو lex مع $z < y < x < w$. أوجد أساس جروبنر للمثالي المعطى.

18– $\langle w + x - y + 4z - 3, 2w + x + y - 2z + 4, w + 3x - 3y + z - 5\rangle$

19– $\langle w - 4x + 3y - z + 2, 2w - 2x + y - 2z + 5, w - 10x + 8y - z - 1\rangle$

في التمارين من 20 إلى 22 أوجد أساس جروبنر للمثالي المعطى من $\mathbb{R}[x]$.

20– $\langle x^4 + x^3 - 3x^2 - 4x - 4, x^3 + x^2 - 4x - 4\rangle$

21– $\langle x^4 - 4x^3 + 5x^2 - 2x, x^3 - x^2 - 4x + 4, x^3 - 3x + 2\rangle$

22– $\langle x^5 + x^2 + 2x - 5, x^3 - x^2 + x - 1\rangle$

في التمارين من 23 إلى 26، أوجد أساس جروبنر للمثالي المعطى من $\mathbb{R}[x, y]$ ليكن الترتيب لضروب القوى هو lex مع $y < x$. إذا أمكنك، صِف المتنوعة الجبرية المقابلة في $\mathbb{R}[x, y]$.

.23 $\langle x^2y - x - 2, xy + 2y - 9\rangle$ **24**– $\langle x^2y + x, xy^2 - y\rangle$

.25 $\langle x^2y + x + 1, xy^2 + y - 1\rangle$ **.26** $\langle x^2y + xy^2, xy - x\rangle$

مفاهيم

27. ليكن F حقلاً. ضع إشارة صح أو إشارة خطأ:

________ أ. كل مثالي من $F[x]$ له أساس منتهٍ.

________ **ب.** كل مجموعة جزئية من $\mathbb{R}^2$ متنوعة جبرية.

________ **جـ.** المجموعة الخالية من $\mathbb{R}^2$ متنوعة جبرية.

________ د. كل مجموعة جزئية منتهية من $\mathbb{R}^2$ متنوعة جبرية.

________ هـ. كل خط في $\mathbb{R}^2$ متنوعة جبرية.

________ و. كل مجموعة منتهية من الخطوط المستقيمة في $\mathbb{R}^2$ متنوعة جبرية.

________ ز. القاسم المشترك الأكبر لعددٍ منتهٍ من كثيرات حدود في $\mathbb{R}[x]$ (غير معين واحد). يمكن أن يحسب باستخدامٍ خوارزمية القسمة بصورة متكررة.

________ ح. حَسَبْتُ أساسات جروبنر قبل أن أعرف ما هي.

________ **ط.** أي مثالي من $F[x]$ له أساس جروبنر وحيد.

________ **ي.** المثاليان $\langle x,y\rangle$ و $\langle x^2, y^2\rangle$ متساويان؛ لأن كليهما يُنْتِجُ المتنوعة الجبرية نفسها أي $\{(0,0)\}$ في $\mathbb{R}^2$.

28. لتكن $\mathbb{R}[x,y]$ رتبت من خلال lex. أعطِ مثالاً يُبيّن أنّ $P_i < P_j$ لا تؤدي إلى أنّ P_i تقسم P_j.

براهين

29. أثبت أنه إذا كان f_1، f_2، ...، f_r عناصر حلقة إبدالية R مع عنصر محايد، فإنّ $I = \{c_1f_1 + c_2f_2 + \cdots + c_rf_r \mid c_i \in I,\ i = 1, \cdots, r\}$، هو مثالي من R.

30. أثبت أنه إذا كان $f(x) = g(x)\,q(x) + r(x)$ في $F[x]$، فإنّ القواسم المشتركة في $F[x]$ لـ $g(x)$ و $f(x)$ هي نفسها القواسم المشتركة في $F[x]$ لـ $g(x)$ و $r(x)$.

31. أثبت أنّ $\{xy, y^2 - y\}$ هو أساس جروبنر لـ $\langle xy, y^2 - y\rangle$ كما اُدعي بعد المثال 9.28.

32. ليكن F حقلاً. أثبت أنه إذا كانت S مجموعة جزئية غير خالية من F^n، فإنّ

$$I(S) = \{f(x) \in F[x] \mid f(\mathbf{s}) = 0,\} \text{ لكل } \mathbf{s} \in S$$

مثالي من $F[x]$.

33. بالرجوع إلى التمرين 32، أثبت أن $S \subseteq V(I(S))$.

34. بالرجوع إلى التمرين 32، أعطِ مثالاً لمجموعة جزئية S من $\mathbb{R}^2$، بحيث إن $V(I(S)) \neq S$.

35. بالرجوع إلى التمرين 32، أثبت أنه إذا كان N مثاليًا من $F[x]$، فإن $N \subseteq I(V(N))$.

36. بالرجوع إلى التمرين 32، أعطِ مثالاً لمثالي N من $\mathbb{R}[x,y]$، بحيث إن $I(V(N)) \neq N$.