الوحدة التاسعة

التحليل
Factorization

الفصل 45 حلقات تامة وحيدة التحليل. Unique Factorization Domains

الحلقة التامة $\mathbb{Z}$ هي مثالنا الأساسي لحلقة تامة، حيث يوجد فيها تحليل وحيد إلى أعداد أولية (غير مختزلة)، وكما بَيَّن لنا الفصل 23 بالنسبة إلى الحقل F، فإنّ $F[x]$ أيضًا حلقة تامة فيها تحليل وحيد. وسنقدِّم مجموعة من التعريفات؛ لأجل مناقشة أفكار مشابهة في أيّ حلقة تامة، علمًا بأنّ بعضها إعادة لتعريفات قديمة، ومن الجيد وضعها في مكان واحد للرجوع إليها.

تعريف 1.45 لتكن R حلقة إبدالية فيها عنصر محايد، وليكن $a, b \in R$، فإذا وجد $c \in R$ بحيث $b = ac$، فإنّ a **يقسم (divides)** b (أو a عامل لـ b)، ويرمز لها بالرمز $a|b$، ونقرأ $a \nmid b$ "a لا يقسم b". ■

تعريف 2.45 العنصر u في الحلقة الإبدالية R التي فيها عنصر محايد يسمّى **عنصر وحدة (unit)** في R، إذا كان u يقسم 1، أي إنه إذا كان لـ u معكوس ضربي في R، والعنصران $a. b \in R$ **متشاركان في R (associates)** إذا كان $a = bu$، حيث u عنصر وحدة في R. ■

يطلب منا التمرين 27 أن نوضّح أنَّ خاصية a و b متشاركين هي علاقة تكافؤ على R.

مثال 3.45 عناصر الوحدة في $\mathbb{Z}$ هي 1 و -1 فقط؛ لذلك، الذي يشارك 26 في $\mathbb{Z}$ هما 26 و -26 فقط. ▲

تعريف 4.45 ليكن p عنصرًا غير صفري، وليس وحدة في حلقة تامة D. يقال عن p: إنه **غير مختزل (irreducible)** على D، إذا كان أيّ تحليل $p = ab$ في D يؤدي إلى أنّ a أو b عنصر وحدة. ■

لاحظ أنّ مشارك غير المختزلة p هو أيضًا غير مختزل؛ وذلك لأنه إذا كانت $p = uc$ حيث u عنصر وحدة، فإنّ أيّ تحليل لِـ c هو تحليل لِـ p.

نبذة تاريخية

ظهر السؤال عن التحليل الوحيد في حلقة تامة غير الأعداد الصحيحة بدايةً للعلن في بحث منشور، وكانت له علاقة بمحاولة جبرائيل لامي (Gabriel-Lame 1795–1870) في إثبات مبرهنة فيرما الأخيرة، وهي تخمين أنّ $x^n + y^n = z^n$ ليس لها حلول صحيحة غير صفرية لـ $n > 2$، وليس من الصعب أن نبيّن أنّ هذا التخمين صحيح، إذا أمكن إثباتها للأعداد الأولية الفردية p كلها، وقد أعلن لامي في اللقاء الذي عقد في أكاديمية باريس في واحد مارس عام 1847م، أنه أثبت المبرهنة، وقدّم إثباتًا مختصرًا، فقد كانت فكرته أولًا: أن نحلل $x^p + y^p$ في الأعداد المركبة كالآتي:

$$x^p + y^p =$$
$$(x + y)(x + \alpha y)(x + \alpha^2 y) \cdots (x + \alpha^{p-1} y)$$

حيث α الجذر البدائي من الرتبة p للواحد، ثمّ حاول بعدها أن يبيِّن أنه إذا كانت العوامل في التعبير أولية نسبيًّا، وإذا كان $x^p + y^p = z^p$، فإنّ كلًّا من هذه العوامل p يجب أن تكون من قوى p، بعدها استطاع أن يوضِّح أنّ معادلة فيرما هذه ستكون صحيحة للثلاثي x' , y' , z'، حيث كل عدد أقل من العدد المقابل له في الثلاثي الأصلي، وهذا سيقود إلى متتالية متناقصة لا نهائية من الأعداد الصحيحة الموجبة، واستحالة هذا يثبت المبرهنة.

أنهى لامي إعلانه، ومع ذلك، قدّم جوزيف ليوفيل (Joseph Liouville 1809-1882) شكوكًا مهمّة على خُلاصة الإثبات، مشيرًا إلى استنتاج أنَّ كلًّا من العوامل الأولية النسبية هي من قوى p؛ لأن حاصل ضربها من قوى p اعتمدت على النتيجة أنَّ إيّ عدد صحيح يمكن تحليله بصورة وحيدة إلى حاصل ضرب أعداد أولية. أصبح واضحًا لا محالة أنَّ "الأعداد الصحيحة" من النوع $x+\alpha^k y$ لها خاصية هذا التحليل الوحيد، وعلى الرغم من أنَّ لامي حاول أن يتجاوز اعتراضات ليوفيل، فقد تمّت تسوية الموضوع في 24 مايو، عندما أظهر ليوفيل رسالة من إيرنست كمر (Ernst Kummer) يشير إلى أنه قد أثبت بالفعل عام 1844م، أنَّ التحليل الوحيد فشل في الحلقة التامة $\mathbb{Z}[\alpha]$، حيث α هي الجذر الثالث والعشرون للواحد.

لم تثبت مبرهنة فيرما حتى عام 1994م، وباستخدام تقنيات الهندسة الجبرية، وهي غير معروفة عند لامي وكمر، في أواخر الخمسينيات لاحظ يوتاكا تانياما (Taniyama Yutaha)– وجوروشيمورا (Goro shimura) علاقة قوية بين حقلين في الرياضيات يبدوان مختلفين، المنحنيات الناقصية والأشكال المقي اسية.

بعد سنوات من الوفاة المأساوية لتانياما عن عمر 31 عامًا، أوضح شيمورا هذه الفكرة، وكوَّن ما أصبح يعرف الآن بمخمنة تانياما– شيمورا. عام 1984، أكد جرهارد فري (Gerhard Fery)، وعام 1986م أثبت كن ريبت (Ken Ribet) أنّ تخمين تانياما– شيمورا سيؤدي إلى صحّة مبرهنة فيرما الأخيرة.

أخيرًا، أعطى أندرو وايلز (Andrew Wiles) من جامعة برينستون، وبعد عمل مضنٍ على هذه المعضلة استمر سبع سنوات، سلسلة محاضرات في جامعة كامبريدج في حزيران 1993م، التي أعلن من خلالها إثبات كفاية تخمين تانياما– شيمورا لإثبات مبرهنة فيرما الأخيرة، ولسوء الطالع اكتشف سريعًا فجوة في الإثبات، ورجع وايلز إلى العمل، واستغرق منه العمل أكثر من عام، ولكنه تمكن أخيرًا من ملء الفجوة، وذلك بمساعدة طالبه ريتشارد تايلور (Taylor Richard)، وقد نُشرت النتيجة في (Annals of Mathematics) في مايو عام 1995م، فحُلّت المعضلة التي عمرها 350 عامًا.

5.45 تعريف نقول: إن الحلقة التامة D **حلقة تامة وحيدة التحليل (Unique factorization domain)** (باختصار UFD) إذا تحققت الشروط الآتية:

1. كل عنصر في D ليس 0 ، وليس عنصر وحدة يمكن تحليله إلى حاصل ضرب عدد منتهٍ من غير المختزلات.

2. إذا كان $q_1 \ldots q_s$ ،$p_1 \ldots p_r$ هما تحليلان للعنصر نفسه في D إلى غير مختزلات، فإنّ $r = s$ و q_j يمكن إعادة ترقيمها، بحيث p_i و q_i متشاركان. ■

6.45 مثال توضّح المبرهنة 20.23 بالنسبة إلى الحقل F، أنّ $F[x]$ هو UFD، ونعلم كذلك أنّ $\mathbb{Z}$ هو UFD، وقد استخدمنا هذه الحقيقة مرارًا على الرغم من أننا لم نثبتها قطّ، على سبيل المثال: في $\mathbb{Z}$ عندنا:

$$24 = (2)(2)(3)(2) = (-2)(-3)(2)(2).$$

هنا 2 و 2− متشاركان وكذلك 3 و 3−؛ لذلك، باستثناء الترتيب والمشاركات، العوامل غير المختزلة في كلا التحليلين لِـ 24 متشابهة. ▲

تذكر أنّ المثالي الرئيس $\langle a \rangle$ في D يحوي مضاعفات العنصر a.

بعد تعريف إضافي واحد فقط يمكننا وصف ما نتمنى أن نصل إليه في هذا الفصل.

7.45 تعريف الحلقة التامة D هي **حلقة المثاليات الرئيسة التامة** (**Principal ideal domain**) (باختصار PID)، إذا كانت كل مثالية في D مثالية رئيسة. ■

نعلم أنّ $\mathbb{Z}$ هو PID ؛ لأن كل مثالية على صورة $n\mathbb{Z}$، مولّدة بالعدد الصحيح n، وتوضّح المبرهنة 24.27 أنَّه إذا كان F حقلًا، فإنّ $F[x]$ هو PID.

هدفنا في هذا الفصل أن نثبت مبرهنتين مهمّتين إلى حدّ بعيد:

1. كل PID يكون UFD. (المبرهنة 17.45).

2. إذا كانت D هي UFD، فإنّ $D[x]$ هي UFD (المبرهنة 29.45).

توضِّح حقيقة أنّ $F[x]$ تكون UFD حيث F حقل (باستخدام المبرهنة 20.23)، كلتا المبرهنتين؛ لأنه باستخدام المبرهنة 24.27، $F[x]$ PID كذلك لأنه لا يوجد في F عنصر غير صفري ليس عنصر وحدة، حيث إنّ F تحقق شروط UFD؛ لذلك، ستقدم المبرهنة 29.45 إثباتًا آخر على أنَّ $F[x]$ UFD عدا حقيقة أننا سنستخدم المبرهنة 20.23 في إثبات المبرهنة 29.45. في الفصل المقبل سندرس خصائص صنف خاص ومحدد من UFD، الحلقات التامة الإقليدية. لنواصل إثبات المبرهنتين.

كل PID يكون UFD

الخطوات التي قادتنا إلى المبرهنة 20.23 وإثباتها تحدد طريق إثباتنا للمبرهنة 17.45، حيث إنّ معظم هذه المادة سيكون مكررًا، وقد تعاملنا بصورة محدودة ومنفصلة مع الحالة الخاصة $F[x]$ في المبرهنة 20.23؛ لأنها سهلة، وكانت الحالة الوحيدة التي نحتاج إليها في مبرهنة الحقول بوجه عام.

لإثبات أنّ الحلقة التامة D هي UFD، من الضروري أن نبيّن أنّ كلا الشرطين 1 و 2 لتعريف UFD متحققان، وبالنسبة إلى حالتنا الخاصة $F[x]$ في المبرهنة 20.23، كان الشرط الأول سهلًا، ونتج عن المفهوم القائل: إنه في تحليل كثيرة حدود من الرتبة >0 إلى حاصل ضرب كثيرتي حدود غير ثابتتين، بحيث إنّ رتبة كل عامل أقل من رتبة كثيرة الحدود الأصلية، وبذلك لا يمكننا أن نستمر في التحليل بصورة غير محددة من غير الاصطدام بعوامل وحدة، أي كثيرات حدود من الرتبة 0، أمّا بالنسبة إلى الحالة العامة لـ PID، فمن الصعب أن نبيِّن ذلك.

ونعود الآن إلى هذه المسألة، سنحتاج زيادة على ذلك إلى مفهوم من مبرهنة المجموعات.

8.45 تعريف إذا كانت $\{A_i \mid i \in I\}$ مجموعة من المجموعات، فإنّ **الاتحاد للمجموعات** A_i $\cup_{i\in I} A_i$ (***union of the sets***) هو مجموعة كل x، بحيث $x \in A_i$ على الأقل لـ $i \in I$ واحدة. ■

9.45 تمهيدية لتكن R حلقة إبدالية، ولتكن $N_1 \subseteq N_2 \subseteq \cdots$ سلسلة تصاعدية من المثاليات N_i في R، فإنّ $N = \cup_i N_i$ مثالية في R.

البرهان ليكن $a, b \in N$، فتوجد مثاليتان N_i و N_j في السلسلة، بحيث $a \in N_i$ و $b \in N_j$، والآن إما $N_i \subseteq N_j$ أو $N_j \subseteq N_i$؛ لنفترض أنّ $N_i \subseteq N_j$؛ لذلك، كلا a و b في N_j، وهذا يؤدي إلى أنَّ $a \pm b$ و ab في N_j ؛ إذن، $a \pm b$ و ab في N، وبأخذ $a = 0$، نرى أنَّ $b \in N$ تؤدي إلى أن $-b \in N$ و $0 \in N$ ؛ لأن $0 \in N_i$، وبذلك N حلقة جزئية من D، ولـ $a \in N$ و $d \in D$، يجب علينا أن نأخذ $a \in N_i$ لبعض N_i؛ ولأن N_i مثالية، $da = ad$ في N_i؛ لذلك، $da \in \cup_i N_i$ أي إنّ $da \in N$؛ إذن، N مثالية. ◆

10.45 تمهيدية (شرط السلسلة التصاعدية لـ PID) (**Ascending chain condition for a PID**): لتكن D PID، فإذا كانت $N_1 \subseteq N_2 \subseteq \cdots$ سلسلة تصاعدية من المثاليات N_i، فيوجد عدد صحيح موجب r، بحيث $N_r = N_s$ لكل $s \geq r$، وهذا يكافئ أنّ كل سلسلة تصاعدية فعليًّا من المثاليات (الاحتواءات كلها فعلية) في PID، تكون ذات طول منتهٍ، ونعبِّر عن ذلك بقولنا: **شرط السلسلة التصاعدية (ascending chain condition (ACC))** تتحقق للمثاليات في PID.

البرهان عن طريق التمهيدية 9.45، نعلم أنّ $N = \cup_i N_i$ مثالية في D. الآن بوصفها ماثلية في D التي هي PID، $N = \langle c \rangle$، حيث $c \in D$؛ ولأن $N = \cup_i N_i$، فيجب أن يكون عندنا $c \in N_r$، حيث $r \in \mathbb{Z}^+$. لِـ $s \geq r$، عندنا

$$\langle c \rangle \subseteq N_r \subseteq N_s \subseteq N = \langle c \rangle$$

لذلك، $N_r = N_s$ لكل $s \geq r$. ◆

العبارة المتكافئة مع ACC مباشِرَة.

سيكون من المفيد فيما تبقى أن نتذكر أنه للعنصرين a و b في الحلقة التامة D،

$\langle a \rangle \subseteq \langle b \rangle$، إذا وفقط إذا كان b ويقسم a،

و $\langle a \rangle = \langle b \rangle$، إذا وفقط إذا كان a و b متشاركين.

بالنسبة إلى الخاصية الأولى، لاحظ أنّ $\langle b\rangle \subseteq \langle a\rangle$، إذا وفقط إذا كان $a \in \langle b\rangle$، وهو صحيح إذا وفقط إذا كان $a = bd$ ، حيث $d \in D$، أي إنّ b يقسم a، وباستخدام الخاصية الأولى هذه، نرى أنّ $\langle a\rangle = \langle b\rangle$، إذا وفقط إذا كان $a = bc$ و $b = ad$ ، حيث $c, d \in D$، لكنّ $a = adc$ وبالحذف، نجد أنّ $1=dc$؛ إذن، c وd عناصر وحدة؛ ولذلك a و b متشاركان.

يمكننا الآن أن نثبت الشرط 1 من تعريف UFD لحلقة تامة PID.

11.45 مبرهنة لتكن D PID، فكل عنصر ليس 0 وليس عنصر وحدة، هو حاصل ضرب غير مختزلات.

البرهان لتكن $a \in D$، حيث a ليس 0 وليس عنصر وحدة، سنبيِّن أولًا أنَّ a لها على الأقل عامل غير مختزل واحد، إذا كان a غير مختزل، انتهينا، أمّا إذا كان a مختزلًا، فإنّ $a = a_1 b_1$، حيث a_1 وb_1 ليسا عنصري وحدة، الآن:

$$\langle a\rangle \subset \langle a_1\rangle$$

بالنسبة إلى $a \subseteq \langle a_1\rangle$ جاءت من $a = a_1b_1$، إذا كان $\langle a_1\rangle = \langle a\rangle$، فإنّ a و a_1 سيكونان متشاركين، و b_1 سيكون عنصر وحدة، وهذا يناقض الفرض، وبالاستمرار في هذا الإجراء، مبتدئين مع a_1، نصل إلى السلسلة التصاعدية فعليًّا من المثاليات:

$$\langle a\rangle \subset \langle a_1\rangle \subset \langle a_2\rangle \subset \ldots$$

باستخدام ACC في التمهيدية 10.45، تتوقف هذه السلسلة عند $\langle a_r\rangle$، و a_r يجب عندها أن تكون غير مختزلة؛ إذن، لـ a عامل غير مختزل a_r. ◆

باستخدام ما أثبتناه، لأيّ عنصر a ليس 0 وليس عنصر وحدة في D، تكون إما a غير مختزل أو $a = p_1c_1$ ، حيث p_1 غير مختزلة وc_1 ليس عنصر وحدة.

باستخدام مفهوم مشابه لما استخدمناه توًّا، في الحالة الأخيرة نستنتج أنَّ $\langle a\rangle \subset \langle c_1\rangle$، فإذا كانت c_1 مختزلة، فإن$c_1 = p_2 c_2$، حيث p_2 غير مختزلة و c_2 ليس عنصر وحدة.

بالاستمرار، نحصل على السلسلة المتصاعدة فعليًّا من المثالثات

$$\langle a\rangle \subset \langle c_1\rangle \subset \langle c_2\rangle \subset \cdots$$

هذه السلسلة يجب أن تتوقف، باستخدام ACC في التمهيدية 10.45 عند $c_r = q_r$ ، أي إنها غير مختزلة؛ إذن، $a = p_1 p_2 \cdots p_r q_r$.

هذا يكمل بحثنا عن الشرط الأول لتعريف UFD. لنعد إلى الشرط الثاني، إجراءاتنا هنا موازية لتلك التي قادتنا إلى المبرهنة 20.23، والنتائج التي سنحصل عليها على طول الطريق ممتعة بذاتها.

12.45 تمهيدية (تعميم للمبرهنة **25.27**) يكون المثالي $\langle p\rangle$ في PID أعظميًّا، إذا وفقط إذا كان p غير مختزل.

البرهان ليكن $\langle p\rangle$ مثاليًّا أعظميًّا في D، PID، وافترض أنّ $p = ab$ في D ، إذن $\langle p\rangle \subseteq \langle a\rangle$، وإذا كان $\langle a\rangle = \langle p\rangle$، فإنّ a وp متشاركان؛ لذلك، يجب أن يكون b عنصر وحدة، وإذا كان $\langle a\rangle \neq \langle p\rangle$، فيجب أن يكون $\langle a\rangle = \langle 1\rangle = \langle D\rangle$؛ لأن $\langle p\rangle$ أعظمي، لكن a و1 عندها متشاركان؛ إذن، a عنصر وحدة؛ ولذلك، إذا كان $p = ab$، فإما a أو b عنصر وحدة؛ ولذلك،

p غير مختزل في D. في المقابل، افترض أنّ p غير مختزل في D، فإذا كان $\langle p\rangle \subseteq \langle a\rangle$، فيجب أن يكون عندنا $p = ab$، الآن، إذا كان a عنصر وحدة، فإنّ $\langle a\rangle = \langle 1\rangle = \mathrm{D}$، أمّا إذا لم يكن a عنصر وحدة، فيجب أن يكون b عنصر وحدة؛ لذلك، يوجد $u \in D$، بحيث $bu = 1$، وعندها $pu = abu = a$، وبهذا $\langle a\rangle \subseteq \langle p\rangle$ أي $\langle a\rangle = \langle p\rangle$؛ إذن، $\langle p\rangle \subseteq \langle a\rangle$ يؤدي إلى أنّ $\langle a\rangle = \mathrm{D}$ أو $\langle a\rangle = \langle p\rangle$ و $\langle p\rangle \neq \mathrm{D}$ وإلّا سيكون p عنصر وحدة؛ إذن، $\langle p\rangle$ مثالي أعظمي. ◆

13.45 تمهيدية (**تعميم للمبرهنة 27.27**) في PID، إذا كان p غير مختزل، ويقسم ab، فإمّا $p|a$ أو $p|b$.

البرهان لتكن D PID، وافترض أنه لغير المختزل، p في D عندنا $p|ab$.

إذن، $(ab) \in \langle p\rangle$؛ ولأن كل مثالي أعظمي في D هو مثالي أولي بحسب النتيجة 16.27، فإنّ $(ab) \in \langle p\rangle$ يؤدي إلى أنّه إما $a \in \langle p\rangle$ أو $b \in \langle p\rangle$، وهذا يعطينا إما $p|a$ أو $p|b$. ◆

14.45 نتيجة إذا كان p غير مختزل في PID، و p يقسم حاصل الضرب $a_1a_2 \ldots a_n$ حيث $a_i \in D$، فإنّ $p|a_i$ لـ i واحدة على الأقل.

البرهان برهان هذه النتيجة مباشرة من التمهيدية 13.45 إذا استخدمنا الاستقراء الرياضي. ◆

15.45 تعريف ليكن العنصر p ليس صفريًّا، وليس عنصر وحدة في الحلقة التامة D، فيكون p **أوّليًّا (prime)**، إذا كان لكل $a, b \in D$، $p|\ ab$ يؤدي إلى أن $p|a$ أو $p|b$. ■

وجَّهت التمهيدية 13.45 انتباهنا إلى خاصية تعريف الأوّليّ، وسنسألك في التمرينين 25 و 26 أن تبيِّن أنَّ الأولي في الحلقة التامة هو غير مختزل دائمًا، وأنَّ غير المختزل في UFD هو أوّلي أيضًا ؛ لذلك، المفهومان الأوّلي وغير المختزل متطابقان في UFD، وسيظهر مثال 16.45 حلقة تامة تحوى بعض غير المختزلات التي تكون غير أوّلية؛ لذلك، المفهومان لا يتطابقان في كل حلقة تامة.

16.45 مثال ليكن F حقلًا، ولتكن D الحلقة التامة الجزئية $F[x^3, xy, y^3]$ من $F[x, y]$، فإنّ x^3, xy و y^3 غير مختزلة في D، لكن

$$(x^3)\ (y^3) = (xy)\ (xy)\ (xy).$$

لأن xy يقسم x^3y^3 لكن لا يقسم x^3 أو y^3، فنرى أنَّ xy ليس أوّليًّا.

إجراءات مشابهة توضح أنَّ x^3 و y^3 غير أوّليين. ▲

خاصية تعريف الأوّلي هي بالضبط ما نحتاج إليه لبناء وحدانية التحليل، الشرط الثاني في تعريف UFD. نكمل الآن إثبات المبرهنة 17.45 بتوضيح وحدانية التحليل في PID.

17.45 مبرهنة (**تعميم للمبرهنة 20.23**) كل PID تكون UFD.

البرهان تُبيِّن المبرهنة 11.45 أنه إذا كان D PID، فإنّ كل $a \in D$ ليس 0 ولا عنصر وحدة له تحليل

$$a = p_1 p_2 \dots p_r$$

إلى غير مختزلات، بقي علينا أن نوضّح الوحدانية. ليكن:

$$a = q_1 q_2 \dots q_s$$

تحليل آخر إلى غير مختزلات، حيث ينتج عندنا أنّ $p_1|(q_1 q_2 \dots q_s)$، الذي يؤدي إلى أنّ $p_1|q_j$ لأحد الـ j كما في النتيجة 14.45، وبتغيير ترتيب q_j إذا كان ضروريًّا، فنستطيع أن نفترض أنّ $j = 1$؛ إذن، $p_1|\ q_1$، وبهذا، فإنَّ $q_1 = p_1 u_1$؛ ولأن p_1 غير مختزلة u_1 عنصر وحدة؛ إذن، p_1 و q_1 متشاركان، وهذا يُنتج :

$$p_1 p_2 \dots p_r = p_1 u_1 q_2 \dots q_s.$$

لذلك، وباستخدام قانون الحذف في D، نحصل على:

$$p_2 \dots p_r = u_1 q_2 \dots q_s.$$

بالاستمرار في هذا العمل، مبتدئين بـ p_2 وهكذا، نحصل أخيرًا على:

$$1 = u_1 u_2 \dots u_r q_{r+1} \dots q_s .$$

ولأنّ q_j غير مختزلة، فيجب أن يكون عندنا $r = s$. ◆

سيبيِّن لنا المثال 31.45 في نهاية هذا الفصل، أنَّ عكس المبرهنة 17.45 خطأ، أي إنّ ألـ UFD ليس بالضرورة PID.

تبدأ كثير من كتب الجبر بإثبات النتيجة الآتية للمبرهنة 17.45، وقد افترضنا أنك على علم بهذه النتيجة، واستخدمناها بحرية في عملنا الآخر.

18.45 نتيجة: (**المبرهنة الأساسية في الحساب**) الحلقة التامة $\mathbb{Z}$ هي UFD.

البرهان رأينا أنّ المثاليات في $\mathbb{Z}$ كلها على الصورة $n\mathbb{Z} = \langle n \rangle$ لـ $n \in \mathbb{Z}$؛ لذلك، $\mathbb{Z}$ هي PID والمبرهنة 17.45 تنطبق. ◆

من الجدير بالملاحظة في إثبات أنّ $\mathbb{Z}$ هي PID، فإننا نعود فعليًّا إلى النتيجة 7.6، فقد أثبتنا المبرهنة 6.6 باستخدام خوارزمية القسمة على $\mathbb{Z}$، تمامًا كما أثبتنا في المبرهنة 24.27، أنَّ $F[x]$ هي PID باستخدام خوارزمية القسمة على $F[x]$ وسنختبر في الفصل 46 هذين الأمرين المتوازيين بصورة أكثر قربًا.

إذا كانت D UFD، فإنّ $D[x]$ UFD

نبدأ بإثبات المبرهنة 29.45، ثاني أكبر نتيجة في هذا الفصل، حيث إنّ فكرة هذا المفهوم هي كالآتي:

لتكن D UFD، فيمكننا تكوين حقل خارج القسمة F لـ D، إنّ $F[x]$ UFD بحسب المبرهنة 20.23، وسنبيِّن أنه يمكننا استعادة تحليل $f(x) \in D[x]$ من تحليلها في $F[x]$ وسيكون من الضروري مقارنة غير المختزلات في $F[x]$ بتلك التي في $D[x]$. هذه المقارنة، التي نفضلها لأنها عملية أكثر من بعض المقارنات الحديثة الفعّالة، وهي تنسب لجاوس بصورة أساسية.

19.45 تعريف لتكن D UFD، ولتكن $a_1, a_2, \ldots, a_n$ عناصر غير صفرية في D، فالعنصر d في D هو **قاسم مشترك أكبر (greatest common divisor)** (باختصار ق م أ) لكل a_i ، إذا كان $d|a_i$ لـ $i = 1, \ldots, n$، وأيّ $d' \in D$ يقسم كل a_i يقسم d أيضًا. ■

سمينا d في التعريف ق م أ بدلاً من ألـ ق م أ؛ لأن ق م أ معرفة فقط نسبةً إلى عناصر الوحدة. افترض أنّ d و d' هما ق م أ لـ a_i ، حيث $i = 1, \ldots, n$، فإنّ $d'|d$ و $d|d'$ من التعريف؛ لذلك، $d = q' d'$ و $d' = qd$ لبعض $q, q' \in D$؛ إذن، $1d = q'qd$، ونرى بالحذف في D، أنَّ $q'q= 1$ ؛ لذلك، q و q' بالفعل عناصر وحدة. توضّح التقنية في المثال المقبل وجود ق م أ في UFD.

20.45 مثال لنحسب ق م أ لـ 420، 168− و 252 في ألـ $\mathbb{Z}$ UFD. بالتحليل نحصل على $420=2^2.3.5.7$، $-168=2^3.(-3).7$ و $252=2^2.3^2.7$. نختار أحد هذه الأرقام، وليكن 420، أكبر قوَّة لكل معامل غير مختزل (بالنسبة إلى المشاركة) الذي يقسم الأعداد كلها 420، 168−، و252 في حالتنا هذه، حيث نأخذ حاصل ضرب هذه القوى الأكبر لغير المختزلات بوصفه ق م أ، ولمثالنا هذا، هذه القوى للعوامل غير المختزلة لـ 420 هي 2^2، 3^1، 5^0 و 7^1 ، نأخذ ق م أ $d = 4.3.1.7 = 84$، ألـ ق م أ الآخر لهذه الأعداد في $\mathbb{Z}$ هو 84−؛ لأن 1،1− هي فقط عناصر الوحدة. ▲

يعتمد تنفيذ التقنية في المثال 20.45 على قدراتنا على تحليل أيّ عنصر في UFD إلى حاصل ضرب غير المختزلات، وقد يكون هذا عملًا مضنيًا حتى في $\mathbb{Z}$.

سيوضح الفصل 46 تقنية الخوارزمية الإقليدية، التي ستسمح لنا بإيجاد ألـ ق م أ من غير التحليل في ألـ UFD، التي تحوي $\mathbb{Z}$ و $F[x]$ للحقل F.

21.45 تعريف لتكن D UFD، تسمى كثيرة الحدود غير الصفرية

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

في $D[x]$ **بدائية (primitive)**، إذا كان ألـ 1 هو ق م أ لـ a_i لـ $i = 0, 1, \ldots, n$. ■

22.45 مثال في $\mathbb{Z}[x]$، $4x^2 + 3x + 2$ بدائية، بينما $4x^2 + 6x + 2$ ليست بدائية؛ لأن 2 وهو ليس عنصر وحدة، هو القاسم المشترك لـ 4، و6 و2. ▲

لاحظ أنّ كل كثيرة حدود غير ثابتة وغير مختزلة في $D[x]$ يجب أن تكون كثيرة حدود بدائية،

23.45 تمهيدية إذا كانت D UFD، فلكل غير ثابت $f(x) \in D[x]$ عندنا $f(x) = (c)\ g(x)$ ، حيث $c \in D$، $g(x) \in D[x]$ و $g(x)$ بدائي، والعنصر c وحيد ما عدا الضرب بعنصر وحدة في D وهو **محتوى (content)** لـ $f(x)$. أيضًا $g(x)$ وحيد ما عدا الضرب بعنصر وحدة في D.

البرهان لتكن $f(x) \in D[x]$ معطاة حيث $f(x)$ كثيرة حدود غير ثابتة معاملاتها $a_0, a_1, \ldots, a_n$، ولتكن c ق م أ لـ a_i لـ $i= 0, 1, \ldots, n$ ، فلكل i، يكون $a_i = cq_i$ ، حيث $q_i \in D$، وباستخدام قانون التوزيع، نحصل على $f(x) = (c)g(x)$ ، حيث لا يوجد غير مختزل في D يقسم المعاملات كلها $q_0, q_1, \ldots, q_n$ لـ $g(x)$؛ إذن، $g(x)$ بدائية.

بالنسبة إلى الوحدانية، إذا كان أيضًا $f(x) = (d)h(x)$، حيث $h(x) \in D[x]$ ،$d \in D$ ،$h(x)$، و $h(x)$ بدائية، فإن كل معامل غير مختزل لـ c يجب أن يقسم d وبالعكس، وبوضع $(c)g(x) =(d)h(x)$ وحذف المعاملات غير المختزلة لـ c في d، نصل إلى $(u)g(x) = (v)h(x)$، حيث $u \in D$ عنصر وحدة؛ لكن عندها يجب أن يكون v عنصر وحدة D، وإلا فسنكون قادرين على حذف معامل غير مختزل لـ v في u؛ إذن، v, u كلاهما عنصرا وحدة؛ لذلك، c وحيدة ما عدا الضرب بعنصر وحدة، ومن $f(x) = (c)g(x)$ ، نرى أنَّ كثيرة الحدود البدائية $g(x)$ وحيدة ما عدا الضرب بعنصر وحدة. ◆

24.45 مثال في $\mathbb{Z}[x]$،

$$4x^2 + 6x - 8 = (2)(2x^2 + 3x - 4)$$

حيث $2x^2 + 3x - 4$ بدائية. ▲

25.45 تمهيدية (تمهيدية جاوس): إذا كانت D UFD، فإنّ حاصل ضرب كثيرتي حدود بدائيتين في $D[x]$ تكون أيضًا بدائية.

البرهان لتكن

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

و

$$g(x) = b_0 + b_1x + \cdots + b_mx^m$$

بدائيتين في $D[x]$ ، ولتكن $h(x) = f(x)g(x)$، ليكن p غير مختزل في D، فإنّ p لا يقسم كل a_i، وp لا يقسم كل b_j؛ لأن $g(x)$ و $f(x)$ بدائيتان، ليكن a_r أول معامل لـ $f(x)$ غير قابل للقسمة على p؛ أي إنّ $p|a_i$ لـ $i < r$ ، لكنّ $p\nmid a_r$ (أي إنّ p لا يقسم a_r)، وبالمثل، ليكن $p|b_j$ لكل $j < s$ ، لكن $p\nmid b_s$ معامل x^{r+s} في $h(x)= f(x)g(x)$ هو:

$$c_{r+s} = (a_0b_{r+s} + \cdots + a_{r-1}b_{s+1}) + a_rb_s + (a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0).$$

الآن $p|a_i$ لـ $i < r$ يؤدي إلى:

$$p \mid (a_0b_{r+s} + \cdots + a_{r-1}b_{s+1})$$

وأيضًا $p|b_j$ لـ $j < s$ يؤدي إلى:

$$p \mid (a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0)$$

لكن p لا يقسم a_r أو b_s؛ لذلك، p لا يقسم $a_r\, b_s$، وعليه، p لا يقسم c_{r+s}، وهذا يوضح أنه إذا أعطينا غير مختزل $p\in D$، فيوجد معامل لـ $f(x)g(x)$ غير قابل للقسمة على p إذن، $f(x)g(x)$ بدائي. ◆

26.45 نتيجة إذا كانت D UFD، فإنّ حاصل ضرب عدد منتهٍ من كثيرات الحدود البدائية في $D[x]$، يكون أيضًا بدائيًا.

البرهان نحصل على النتيجة من التمهيدية 25.45 بالاستقراء الرياضي. ◆

الآن، لتكن D UFD، وليكن F حقل خوارج القسمة على D، فبحسب المبرهنة 20.23 يكون $F[x]$ UFD، وكما قلنا سابقًا، سنبين أنّ $D[x]$ هو UFD عن طريق نقل التحليل في $F[x]$ لـ $f(x) \in D[x]$ إلى تحليل في $D[x]$، التمهيدية المقبلة تربط غير المختزلات غير الثابتة في $D[x]$ بمثيلاتها في $F[x]$، وهذه آخر خطوة مهمّة.

27.45 تمهيدية لتكن D UFD ، وليكن F حقل خوارج القسمة على D، لتكن $f(x) \in D[x]$، حيث (درجة $f(x)$)> 0، فإذا كان $f(x)$ غير مختزل في $D[x]$، فإنّ $f(x)$ غير مختزل في $F[x]$ أيضًا، وكذلك، إذا كان $f(x)$ بدائيًّا في $D[x]$ وغير مختزل في $F[x]$ ، فإنّ $f(x)$ غير مختزل في $D[x]$.

البرهان افترض أنّ غير الثابتة $f(x) \in D[x]$ تتحلل إلى كثيرات حدود ذات درجات أقلّ في $F[x]$ أي إنّ

$$f(x) = r(x)s(x)$$

حيث $r(x), s(x) \in F[x]$؛ ولأنَّ F حقل خوارج القسمة على D، فإنّ كل معامل في $s(x)$ و $r(x)$ على صورة $a|b$ حيث $a, b \in D$، ويمكننا بإلغاء المقامات أن نحصل على:

$$(d)\ f(x) = r_1(x)s_1(x)$$

حيث $d \in D$ و $r_1(x), s_1(x) \in D[x]$، و رتب $s_1(x)$ و $r_1(x)$ هي رتب $s(x)$ و $r(x)$ نفسها على الترتيب، عن طريق التمهيدية 23.45، $f(x) = (c)g(x)$, $r_1(x) = (c_1)r_2(x)$،
و $s_1(x) = (c_2)s_2(x)$ لكثيرات الحدود البدائية $s_2(x)$ و $g(x), r_2(x)$ و $c, c_1, c_2 \in D$.

وهكذا، فإنّ

$$(dc)g(x) = (c_1c_2)r_2(x)s_2(x).$$

وبحسب التمهيدية 25.45، تكون $r_2(x)s_2(x)$ بدائية، باستخدام جزء الوحدانية للتمهيدية 23.45، $c_1c_2 = dcu$ ، حيث u عنصر وحدة في D؛ إذن:

$$(dc)g(x) = (dcu)r_2(x)s_2(x),$$

وهكذا

$$f(x) = (c)g(x) = (cu)r_2(x)s_2(x).$$

أوضحنا أنه إذا كانت $f(x)$ تتحلل بصورة غير تافهة في $F[x]$، فإنّ $f(x)$ تتحلل بصورة غير تافهة إلى كثيرات حدود من الرتب نفسها في $D[x]$؛ لذلك، إذا كانت $f(x) \in D[x]$ غير مختزلة في $D[x]$، فيجب أن تكون غير مختزلة في $F[x]$.

غير الثابتة $f(x) \in D[x]$ البدائية في $D[x]$ وغير مختزلة في $F[x]$ هي أيضًا غير مختزلة في $D[x]$؛ لأن $D[x] \subseteq F[x]$. ◆

توضح **التمهيدية** 27.45 أنه إذا كانت D UFD، فإنّ غير المختزلات في $D[x]$ هي نفسها غير المختزلات في D، وكثيرات الحدود البدائية غير الثابتة وغير المختزلة في $F[x]$، حيث F حقل خوارج القسمة لـ D.

التمهيدية السابقة مهمة في ذاتها، ويظهر هذا في النتيجة القادمة، وهي حالة خاصة من مبرهنتنا 11.23. (نعترف بأنه ليس من اللائق أن نطلق على حالة خاصة لنتيجة تمهيدية مبرهنة، حيث يعتمد الرقم الذي يشير إلى النتيجة بطريقة أو بأخرى على المحتوى حيثما ظهر).

28.45 نتيجة إذا كانت D UFD و F حقل خوارج القسمة على D، فإنّ غير الثابتة $f(x) \in D[x]$ تتحلل الى حاصل ضرب كثيرتي حدود ذات درجة أقل r و s في $F[x]$ إذا وفقط إذا كان لها التحليل إلى كثيرات حدود من الدرجة نفسها r و s في $D[x]$.

البرهان لقد أُثبت في برهان التمهيدية 27.45 أنه إذا كانت $f(x)$ تتحلل إلى حاصل ضرب كثيرتي حدود ذات درجة أقل في $F[x]$، فإنّ لها تحليلا إلى كثيرتي حدود من الدرجة نفسها في $D[x]$ (انظر الآتي لآخر جملة من الفقرة الأولى للبرهان)، ويتحقق العكس؛ لأن $D[x] \subseteq F[x]$. ◆

صرنا الآن جاهزين لإثبات مبرهنتنا الرئيسة:

29.45 مبرهنة إذا كانت D UFD، فإنّ $D[x]$ UFD.

البرهان لتكن $f(x) \in D[x]$، حيث $f(x)$ ليست 0 ولا عنصر وحدة، فإذا كانت $f(x)$ من الدرجة 0، فنكون قد انتهينا؛ لأن D UFD. افترض أنّ درجة $(f(x)) > 0$ وليكن

$$f(x) = g_1(x)g_2(x) \cdots g_r(x)$$

تحليل لـِ $f(x)$ في $D[x]$ له أكبر عدد r من العوامل ذات الدرجات الموجبة. (يوجد مثل هذا العدد الأكبر من العوامل؛ لأن r لا يستطيع أن يزيد على درجة $f(x)$. الآن حلل $g_i(x)$ كلها إلى الصيغة $g_i(x)= c_ih_i(x)$ ، حيث c_i محتوى $h_i(x)$ و $g_i(x)$. و $h_i(x)$ كثيرة حدود بدائية، $h_i(x)$ كلها غير مختزلة؛ لأنه إن أمكن تحليلها، فإنّ أيًّا من عواملها يمكن أن يقع في D؛ لذلك، سيكون لها كلها درجات موجبة، ما يؤدي إلى تحليل مماثل لـ $g_i(x)$، وهكذا لتحليل $f(x)$ لأكثر من r من العوامل ذات الدرجات الموجبة، مناقضًا لاختيارنا لـ r؛ لذلك، نحصل الآن على:

$$f(x) = c_1h_1(x)c_2h_2(x) \cdots c_r h_r(x)$$

حيث $h_i(x)$ غير مختزلة في $D[x]$، وإذا حللنا c_i الآن إلى غير مختزلات في D، نحصل على تحليل لـ $f(x)$ إلى حاصل ضرب غير المختزلات في $D[x]$.

تحليل $f(x) \in D[x]$، إذا كانت درجة $f(x)$ تساوي 0، فيكون وحيدًا؛ لأن D UFD، انظر التعليق بعد التمهيدية 27.45، وإذا كانت درجة $f(x)$ أكبر من 0، فيمكننا تصوّر أيّ تحليل لـ $f(x)$ إلى حاصل ضرب غير مختزلات في $D[x]$ كتحليل في $F[x]$ إلى عناصر وحدة (أي العوامل في D) وكثيرات حدود غير مختزلات في $F[x]$ بحسب التمهيدية 27.45، وبحسب المبرهنة 20.23، كثيرات الحدود هذه وحيدة ما عدا الضرب بعوامل ثابتة من F، لكن بوصفها غير مختزلة في $D[x]$، كل كثيرة حدود ذات درجة > 0 تظهر في تحليل $f(x)$ في $D[x]$ هي بدائية، وبحسب جزء الوحدانية للتمهيدية 23.45، فهذا يوضح أنّ كثيرات الحدود هذه وحيدة في $D[x]$ ما عدا الضرب بعناصر وحدة، أي إنها متشاركة، التي هي مرة أخرى وحيدة ما عدا الضرب بعنصر وحدة بحسب التمهيدية 23.45؛ لذلك، كل غير المختزلات في $D[x]$ الظاهرة في التحليل وحيدة ما عدا الترتيب والمشاركة. ◆

30.45 نتيجة إذا كان F حقلًا و $x_1, \dots, x_n$ غير معينات، فإنّ $F[x_1, \dots, x_n]$ UFD.

البرهان بحسب المبرهنة 20.23، $F[x_1]$ UFD، وبحسب المبرهنة 29.45، كذلك $(F[x_1])[x_2] = F[x_1, x_2]$، وبالاستمرار بهذا الإجراء، نرى (بالاستقراء الرياضي) أنَّ $F[x_1, \dots, x_n]$ UFD. ♦

رأينا أنَّ أيّ PID يكون UFD، وقد جعلت النتيجة 30.45 الأمر سهلاً أن نقدم مثالاً يوضح أنّه ليس كل UFD يكون PID.

31.45 مثال ليكن F حقلًا، ولتكن x , y غير معينات، فإنّ $F[x,y]$ UFD بحسب النتيجة 30.45. افترض المجموعة N من كثيرات الحدود في x, y في $F[x,y]$ ذات الحدّ الثابت 0، فإنّ N مثالية، لكن ليست مثالية رئيسة؛ إذن، $F[x,y]$ ليست PID. ▲

مثال آخر على UFD وليس PID هو $\mathbb{Z}[x]$، كما سيظهر في تمرين 12، فصل 46.

تمارين 45

حسابات

في التمارين من 1 إلى 8، بيِّن فيما إذا كان العنصر غير مختزل في الحلقة التامة المبينة

1. 5 في $\mathbb{Z}$

2. -17 في $\mathbb{Z}$

3. 14 في $\mathbb{Z}$

4. $2x - 3$ في $\mathbb{Z}[x]$

5. $2x - 10$ في $\mathbb{Z}[x]$

6. $2x - 3$ في $\mathbb{Q}[x]$

7. $2x - 10$ في $\mathbb{Q}[x]$

8. $2x - 10$ في $\mathbb{Z}_{11}[x]$

9. أعطِ أربع مشاركات مختلفة لـ $2x - 7$ بوصفها عنصرًا في $\mathbb{Z}[x]$؛ في $\mathbb{Q}[x]$؛ $\mathbb{Z}_{11}[x]$، إذا كان ذلك ممكنًا.

10. حلّل كثيرة الحدود $4x^2 - 4x + 8$ إلى حاصل ضرب غير مختزلات، بوصفها عنصرًا في الحلقة التامة $\mathbb{Z}[x]$؛ في الحلقة التامة $\mathbb{Q}[x]$؛ في الحلقة التامة $\mathbb{Z}_{11}[x]$.

في التمارين من 11 إلى 13 أوجد ق م أ للعناصر المعطاة في $\mathbb{Z}$

11. 234 ،3250 ،1690

12. 784 ،-1960 ،448

13. 2178 ،396 ،792 ،594.

في التمارين من 14 إلى 17، عبّر عن كثيرة الحدود المعطاة بوصفها حاصل ضرب محتواها في كثيرة حدود بدائية في ألـ UFD المبينة.

14. $18x^2 - 12x + 48$ في $\mathbb{Z}[x]$

15. $18x^2 - 12x + 48$ في $\mathbb{Q}[x]$

16. $2x^2 - 3x + 6$ في $\mathbb{Z}[x]$

17. $2x^2 - 3x + 6$ في $\mathbb{Z}_7[x]$

مفاهيم

في التمارين من 18 إلى 20، صحّح تعريف الحد المكتوب بخط مائل دون الرجوع إلى الكتاب –إذا كانت هناك حاجة للتصحيح– بحيث يكون بصيغة قابلة للنشر.

18. العنصران a و b في الحلقة التامة D متشاركان في D، إذا وفقط إذا كان الكسر $a|b$ في D عنصر وحدة.

19. العنصر في الحلقة التامة D غير مختزل في D، إذا وفقط إذا كان لا يمكن تحليله إلى حاصل ضرب عنصرين من D.

20. العنصر في الحلقة التامة D أولي في D، إذا وفقط إذا كان لا يمكن تحليله إلى حاصل ضرب عنصرين أصغر في D.

21. ضع إشارة صح أو إشارة خطأ:

________ أ. كلّ حقل UFD.

________ ب. كلّ حقل PID.

________ جـ. كلّ PID يكون UFD.

________ د. كلّ UFD يكون PID.

________ هـ. $\mathbb{Z}[x]$ UFD.

ـــــــــ و. أيّ غير مختزلين في UFD متشاركان.
ـــــــــ ز. إذا كان D PID ، فإنّ $D[x]$ PID.
ـــــــــ ح. إذا كان D UFD ، فإنّ $D[x]$ UFD.
ـــــــــ ط. في أيّ UFD، إذا كان $p|a$ لأيّ غير مختزل p، فإنّ p نفسه يظهر في كل تحليل لـ a.
ـــــــــ ي. UFD لا يحوي قواسم لـ 0.

22. ليكن D UFD صف غير المختزلات في $D[x]$ بدلالة غير المختزلات في D وغير المختزلات في $F[x]$، حيث F هو حقل خوارج القسمة على D.

23. نصّت التمهيدية 26.45 على أنّه إذا كان D UFD و F حقل خوارج القسمة، فإنّ غير المختزلة وغير الثابتة $f(x)$ في $D[x]$ أيضًا غير مختزلة في $F[x]$. بيّن بمثال أنه إذا كانت $g(x) \in D[x]$ غير مختزلة في $F[x]$، فإنها ليست بالضرورة غير مختزلة في $D[x]$.

مفاهيم

24. ركّز عملنا كله في هذا الفصل على الحلقات التامة، بأخذ التعريف نفسه في هذا الفصل، لكن على الحلقة الإبدالية التي لها عنصر محايد، افترض التحليل إلى غير مختزلات في $\mathbb{Z} \times \mathbb{Z}$. ماذا يمكن أن يحدث؟ افترض بصورة خاصة $(1، 0)$.

براهين

25. أثبت أنه إذا كان p أوليًا في حلقة تامة D، فإنّ p غير مختزل.

26. أثبت أنه إذا كان p غير مختزل في UFD، فإنّ p أولي.

27. بالنسبة إلى حلقة إبدالية R فيها عنصر محايد. بيّن أنّ العلاقة $a \backsim b$ إذا كانت a تشارك b (أي إنه، إذا كان $a = bu$ حيث u عنصر وحدة في R) هي علاقة تكافؤ على R.

28. لتكن D حلقة تامة. وقد بيّن تمرين 37، فصل 18 أنَّ $\langle U,. \rangle$ زمرة ، حيث U هي مجموعة عناصر الوحدة في D، بيِّن أنّ المجموعة $D^* - U$ لغير عناصر الوحدة عدا 0 مغلقة تحت عملية الضرب. هل هذه المجموعة زمرة تحت عملية الضرب على D؟

29. لتكن D UFD. بيِّن أنّ القاسم غير الثابت لكثيرة حدود بدائية في $D[x]$ هي أيضًا كثيرة حدود بدائية.

30. بيِّن أنّ كل مثالية فعلية في PID، محتواة في مثالية أعظمية. [مساعدة: استخدم التمهيدية 10.45].

31. حلِّل $x^3 - y^3$ إلى غير مختزلات في $\mathbb{Q}[x,y]$ ، وأثبت أنَّ هذه العوامل كلها غير مختزلة.

هناك مفاهيم أخرى عدة معتبرة عادة ومشابهة في تشخيص شرط السلسلة المتصاعدة على المثاليات في الحلقة. التمارين الثلاثة الآتية تهتم ببعض هذه المفاهيم.

32. لتكن R أيّ حلقة، **شرط السلسلة التصاعدية** (ACC) لمثاليات متحقق في R ، إذا كانت كل متتالية متزايدة فعليًا $N_1 \subset N_2 \subset N_3 \subset \cdots$ من المثاليات في R ذات طول منته. **الشرط الأعظمي** (MC) لمثاليات متحقق في R ، إذا كانت كل مجموعة غير خالية S من المثاليات في R ، تحوي مثالية ليست محتواة بصورة فعلية في أيّ مثالية أخرى من المجموعة S. **شرط الأساس المنتهي** (FBC) لمثاليات متحقق في R ، إذا كان لكل مثالية N في R، توجد مجموعة منتهية $B_N = \{b_1, \cdots, b_n\} \subseteq N$، بحيث N تقاطع المثاليات كلها في R التي تحوي B_N. المجموعة B_N **مجموعة منتهية مولدة لـ N**.

بيِّن أنّ الشروط ACC، MC، FBC متكافئة لكل حلقة R.

33. لتكن R أي حلقة، **شرط السلسلة التنازلية** (DCC) لمثاليات متحقق في R ، إذا كانت كل متتالية متناقصة فعليًا $N_1 \supset N_2 \supset N_3 \supset \cdots$ لمثاليات في R ذات طول منته، و**الشرط الأصغري** (mC) لمثاليات متحقق في R ، إذا أعطينا أيّ مجموعة S من المثاليات في R، يوجد مثالية في S لا تحوي بصورة فعلية أيّ مثالية أُخرى من المجموعة S.

بيِّن أنّ الشرطين DCC و mC متكافئان لكل حلقة.

34. أعطِ مثالًا لحلقة، بحيث ACC متحقق لكنّ DCC غير متحقق. (انظر التمرينين 32 و 33).

الفصل 46 حلقات تامة إقليدية Euclidean Domains

أشرنا مرات عدّة إلى أهمية خوارزميات القسمة، وأول اتصالنا بها كان بخوارزمية القسمة على $\mathbb{Z}$ في الفصل 6، إذ استخدمت تلك الخوارزمية مباشرة في إثبات المبرهنة المهمّة، التي تنصّ على أنَّ الزمرة الجزئية من زمرة دورية تكون دورية، أي إنَّ لها مولِّدًا واحدًا، وبالطبع، هذا يتّضح للوهلة الأولى؛ لأن $\mathbb{Z}$ PID خوارزمية القسمة على $F[x]$ التي ظهرت في المبرهنة 1.23، واستخدمت بطريقة مشابهة بالكامل في إثبات أنَّ $F[x]$ PID، أمّا الآن، فالتقنية الحديثة في الرياضيات تعتمد على أخذ أوضاع متشابهة تمامًا، ومحاولة جمعها في برهان واحد عن طريق تجريد أفكار مهمّة مشتركة بينها، والتعريف المقبل هو توضيح لهذه التقنية، كما هو هذا الكتاب كله، لنرى ماذا يمكننا أن نطوِّر عندما نبدأ بإيجاد خوارزمية قسمة عامة لائقة في حلقة تامة.

1.46 تعريف **المعيار الإقليدي (Euclidean norm)** على حلقة تامة D هو دالة v تربط العناصر غير الصفرية من D بأعداد غير سالبة، بحيث يتحقق الشرطان الآتيان:

1. لكل $a, b \in D$ حيث $b \neq 0$، يوجد q وr في D حيث $a = bq + r$، وإمّا $r = 0$ أو $v(r) < v(b)$.
2. لكل $a, b, \in D$ حيث a, b لا يساويان 0، $v(a) \leq v(ab)$.

تسمّى الحلقة التامة D **حلقة تامة إقليدية (Euclidean domain)** إذا وجد معيار إقليدي على D. ■

أهمية الشرط الأول واضحة من خلال مناقشتنا، وأهمية الشرط الثاني تكمن في أنه يمكننا من تشخيص عناصر الوحدة في الحلقة التامة الإقليدية D.

2.46 مثال الحلقة $\mathbb{Z}$ حلقة تامة إقليدية؛ لأن الدالة v المعرفة بـ $v(n) = |n|$ لـ $n \neq 0$ في $\mathbb{Z}$ هي معيار إقليدي على $\mathbb{Z}$ فالشرط الأول متحقّق عن طريق خورازمية القسمة على $\mathbb{Z}$ الشرط الثاني يأتي من $|ab| = |a|\ |b|$ و $|a| \geq 1$ لـ $a \neq 0$ في $\mathbb{Z}$. ▲

3.46 مثال إذا كان F حقلًا، فإنّ $F[x]$ حلقة تامة إقليدية؛ لأن الدالة v المعرفة بـ $v(f(x)) =$ (درجة $f(x)$) لـ $f(x) \in F[x]$ و $f(x) \neq 0$ هي معيار إقليدي، فالشرط الأول متحقق بحسب المبرهنة 1.23، والشرط الثاني متحقق؛ لأن درجة حاصل ضرب كثيرتي حدود هي مجموع درجتيهما. ▲

بالطبع، سنقدم بعض الأمثلة على حلقات تامة إقليدية غير تلك المشهورة التي عززت التعريف. سنفعل ذلك في الفصل 47، وباستعراض الملحوظات الافتتاحية، نعجِّل بالمبرهنة الآتية:

4.46 مبرهنة تكون كل حلقة تامة إقليدية PID.

البرهان لتكن D حلقة تامة إقليدية مع المعيار الإقليدي v، ولتكن N مثالية في D، فإذا كانت $N = \{0\}$، فإنّ $N= \langle 0 \rangle$ و N رئيسة. افترض أنَّ $N \neq \{0\}$؛ إذن، يوجد $b \neq 0$ في N، دعنا نختار b ، بحيث $v(b)$ هي الأصغر بين كل $v(n)$ ، حيث $n \in N$، وندَّعي أنَّ $N = \langle b \rangle$. لتكن $a \in N$، فباستخدام الشرط الأول للحلقة التامة الإقليدية، يوجد q و r في D بحيث:

$$a = bq + r$$

حيث إما $r = 0$ أو $v(r) < v(b)$. الآن، $r = a - bq$ و $a,b \in N$؛ لذلك، $r \in N$ ؛ لأن N مثالية. ولكن $v(r) < v(b)$ وهذا مستحيل من خلال اختيارنا لـ b؛ لذلك، $r = 0$، وبذلك $a = bq$، ولأنَّ a كان عنصرًا عشوائيًّا في N، فنحصل على $N = \langle b \rangle$. ◆

5.46 نتيجة الحلقة التامة الإقليدية هي UFD.

البرهان بحسب المبرهنة 4.46 الحلقة التامة الإقليدية PID، وبحسب المبرهنة 17.45 ألـ PID هي UFD. ◆

أخيرًا، يجب علينا أن نذكر أنَّه بينما كل حلقة تامة إقليدية هي PID بحسب المبرهنة 4.46، فليس كل PID حلقة تامة إقليدية. ليس من السهل إيجاد أمثلة على PID وليست إقليدية.

الحساب في حلقات تامة إقليدية

سنكتشف الآن بعض خصائص الحلقات التامة الإقليدية التي لها علاقة بتركيبتها الضربية، حيث نشدد على أنَّ البناء الحسابي للحلقة التامة الإقليدية غير متأثر بأيّ حال من الأحوال بالمعيار الإقليدي v على الحلقة التامة، والمعيار الإقليدي فقط أداة مفيدة ربمًا في إلقاء بعض الضوء على ذلك التركيب الحسابي للحلقة التامة، والبنية الحسابية للحلقة التامة D مُحدَّدة بالكامل بالمجموعة D والعمليتين الثنائيتين $+$، $.$ على D. لتكن D حلقة تامة إقليدية مع المعيار الإقليدي v. نستطيع أن نستخدم الشرط الثاني للمعيار الإقليدي في تمييز عناصر الوحدة في D.

6.46 مبرهنة للحلقة التامة الإقليدية مع المعيار الإقليدي v، $v(1)$ الأصغر بين كل $v(a)$ لغير الصفري $a \in D$، و $u \in D$ عنصر وحدة، إذا وفقط كان $v(u) = v(1)$.

البرهان يخبرنا الشرط الثاني لـ v من الوهلة الأولى بأنَّه لـ $a \neq 0$.

$$v(1) \leq v(1a) = v(a).$$

من ناحية أخرى، إذا كان u عنصر وحدة في D، فإنَّ

$$v(u) \leq v(uu^{-1}) = v(1).$$

إذًا

$$v(u) = v(1)$$

لعنصر وحدة u في D.

في المقابل، افترض أنَّ غير الصفري $u \in D$ ، حيث $v(u) = v(1)$، فيوجد باستخدام خوارزمية القسمة q و r في D ، حيث

$$1= uq + r.$$

حيث إما $r = 0$ أو $v(r) < v(u)$، ولكن لأن $v(u) = v(1)$ هي الأقل بين كل $v(d)$ لغير الصفري $d \in D$، $v(r) < v(u)$ مستحيل؛ إذن، $r = 0$ و $1 = uq$؛ لذلك، يكون u عنصر وحدة. ◆

مثال 7.46 بالنسبة إلى $\mathbb{Z}$، حيث $v(n) = |n|$، أصغر قيمة لـ $v(n)$ لغير صفري $n \in \mathbb{Z}$ هو 1، ولكن 1 و -1 هي فقط العناصر في $\mathbb{Z}$ ، حيث $v(n) = 1$، وبالطبع 1 و -1 هي بالضبط عناصر الوحدة في $\mathbb{Z}$. ▲

مثال 8.46 بالنسبة إلى $F[x]$، حيث $v(f(x)) =$ (درجة $(f(x)$) لـ $f(x) \neq 0$، أقل قيمة لـ $v(f(x))$ لكل غير صفري $f(x) \in F[x]$ هو 0، وكثيرات الحدود غير الصفرية من الدرجة 0 هي بالضبط العناصر غير الصفرية لـ F، وهذه هي فقط عناصر الوحدة في $F[x]$. ▲

نشدد على أنَّ كل شيء أثبتناه هنا متحقق في كل حلقة تامة إقليدية، بوجه خاص في $\mathbb{Z}$ و $F[x]$، وكما أشرنا في المثال 20.45، نستطيع أن نبيِّن أنَّ أيّ a و b في UFD لها ق م أ، ونحسبه فعلًا عن طريق تحليل a و b إلى غير مختزلات؛ لكن من الممكن أن يكون إيجاد هذه التحليلات صعبًا، أمّا إذا كانت ألـ UFD هي في الواقع إقليدية، ولدينا معيار إقليدي سهل الحساب، فتوجد طريقة فعّالة وسهلة لإيجاد ق م أ، كما توضح المبرهنة الآتية.

▪ **نبذة تاريخية**

ظهرت الخوارزمية الإقليدية في كتاب العناصر لإقليدس كالقضيتين 1 و 2 في الكتاب السابع، حيث استخدمت كما استخدمت هنا في إيجاد القاسم المشترك الأكبر بين عددين صحيحين.

واستخدمها إقليدس أيضًا في الكتاب الخامس (القضيتان 2 و 3) في إيجاد القياس المشترك الأعظم لمقدارين (إذا وجد)، ولتحديد فيما إذا كان المقداران غير قابلين للقياس.

تظهر الخوارزمية مرة أخرى في (*Brahme sphutasiddhanta*) (تصحيح نظام براهما الفلكي) (628) للرياضي والفلكي الهندي في القرن السابع برهما جوبتا، فلحلّ المعادلة غير المحددة $rx + c = sy$ في الأعداد الصحيحة، يستخدم براهما جوبتا إجراء إقليدس "ليقسم بصورة تتابعية" r على s ؛ حتى يصل إلى آخر باقٍ غير صفري، بعدها وباستخدام التعويض معتمدًا على خوارج القسمة السابقة والبواقي، ينتج خوارزمية مباشرة لإيجاد أصغر حل موجب لمعادلته.

عالم الجبر الصيني كِن جيوشاو استخدم أيضًا خوارزمية إقليدس في القرن الثالث عشر، في حله لما يُسمَّى معضلة الباقي الصينية التي نشرت في (*Shushu jiuzhang*) (رسالة رياضية في تسعة فصول) (1247)، فقد كان هدف كِن صياغة طريقة لحل نظام تطابقات $N \equiv r_i$ (مقياس m_i) وبوصفه جزءًا من هذه الطريقة، احتاج إلى حل تطابقات على صورة $Nx \equiv 1$ (مقياس m)، حيث N و m أوّليان نسبيًّا، حيث إنّ حلّ التطابق من هذا النوع يمكن إيجاده أيضًا عن طريق إجراء التعويض، بطريقة مختلفة عن الطريقة الهندية، التي تستخدم خوارج القسمة والبواقي من تطبيق خوارزمية إقليدس على N و m، وليس من المعلوم فيما إذا كان العنصر المشترك في الخوارزميات الهندية والصينية، وخوارزمية إقليدس نفسها، قد اكتشفت بصورة منفصلة في هذه الحضارات، أم أنها اقتبست من المصادر اليونانية.

9.46 مبرهنة (الخوارزمية الإقليدية): لتكن D حلقة تامة إقليدية مع المعيار الإقليدي v، ولتكن a و b عناصر غير صفرية في D. ليكن r_1 كما في الشرط الأول من المعيار الإقليدي، أي إنَّ

$$a = bq_1 + r_1,$$

حيث إما $r_1 = 0$ أو $v(r_1) < v(b)$. إذا كان $r_1 \neq 0$، ليكن r_2 ، حيث

$$b = r_1 q_2 + r_2,$$

وحيث إما $r_2 = 0$ أو $v(r_2) < v(r_1)$. بوجه عام، ليكن r_{i+1} ، حيث:

$$r_{i-1} = r_i q_{i+1} + r_{i+1},$$

وحيث إما $r_{i+1} = 0$ أو $v(r_{i+1}) < v(r_i)$، فإنَّ المتتالية $r_1, r_2, \ldots$ يجب أن تتوقف عند بعض $r_s = 0$. إذا كان $r_1 = 0$ ، فإنّ b ق م أ لـ a و b، وإذا كان $r_1 \neq 0$ و r_s هو أوّل $r_i = 0$، فإنّ ألـ ق م أ لـ a و b هو r_{s-1}.

إضافة إلى ذلك، إذا كان d ق م أ لـ a و b، فإنه يوجد λ و μ في D ، بحيث $d = \lambda a + \mu b$.

البرهان لأن $v(r_i) < v(r_{i-1})$ و $v(r_i)$ عدد غير سالب، يؤدي إلى أنَّه بعد عدد منتهٍ من الخطوات يجب أن نصل إلى $r_s = 0$.

إذا كان $r_1 = 0$، فإنّ $a = bq_1$ و b هو ق م أ لـ a و b. افترض أنَّ $r_1 \neq 0$، فإنَّه إذا كان $d|a$ و $d|b$، فإننا نحصل على:

$$d|\,(a - bq_1).$$

لذلك، $d|r_1$، ومع ذلك، إذا كان $d_1|r_1$ و $d_1|b$، فإنّ

$$d_1|\,(bq_1 + r_1).$$

لذلك، $d_1|a$؛ إذن، مجموعة القواسم المشتركة لـ a و b هي نفسها مجموعة القواسم المشتركة لـ b و r_1. وبإجراء مشابه، إذا كان $r_2 \neq 0$ ، فإنّ مجموعة القواسم المشتركة لـ b و r_1 هي نفسها مجموعة القواسم المشتركة لـ r_1 و r_2، ومستمرون على هذا العمل، فنرى أخيرًا أنّ مجموعة القواسم المشتركة لـ a و b هي مجموعة القواسم المشتركة نفسها r_{s-2} و r_{s-1}، حيث r_s هو أوّل r_i يساوي 0.

لذلك، ق م أ لـ r_{s-2} و r_{s-1} هو أيضًا ق م أ لـ a و b. لكن المعادلة

$$r_{s-2} = q_s r_{s-1} + r_s = q_s r_{s-1}$$

توضّح أنّ ق م أ لـ r_{s-2} و r_{s-1} هو r_{s-1}.

يبقى علينا أن نبيِّن أنه يمكننا أن نعبِّر عن ألـ ق م أ d لـ a و b بـ $d = \lambda a + \mu b$. بدلالة البناء الذي أعطي توًّا، فإذا كان $d = b$، فإنّ $d = 0a + 1b$ ، وبذلك نكون انتهينا. إذا كان $d = r_{s-1}$ ، فإنه وبالرجوع العكسي خلال معادلاتنا، يمكننا أن نعبِّر عن r_i كلها بالصيغة $\lambda_i r_{i-1} + \mu_i r_{i-2}$، حيث $\lambda_i, \mu_i \in D$. للتوضيح مستخدمين الخطوة الأولى، فنحصل من المعادلة:

$$r_{s-3} = q_{s-1} r_{s-2} + r_{s-1}$$

على

$$d = r_{s-1} = r_{s-3} - q_{s-1} r_{s-2} \qquad (1)$$

بعدها نعبّر عن r_{s-2} بدلالة r_{s-3} و r_{s-4}، ونعوض في المعادلة (1) للتعبير عن d بدلالة r_{s-3} و r_{s-4}، حيث سيكون لدينا في آخر الأمر:

$$d = \lambda_3 r_2 + \mu_3 r_1 = \lambda_3(b - r_1 q_2) + \mu_3 r_1 = \lambda_3 b + (\mu_3 - \lambda_3 q_2) r_1$$
$$= \lambda_3 b + (\mu_3 - \lambda_3 q_2)(a - b q_1)$$

الذي يمكن التعبير عنه على الصورة $d = \lambda a + \mu b$. إذا كان d' أي ق م آخر لـ a و b ، فإنّ $d' = ud$ حيث u عنصر وحدة؛ إذن، $d' = (\lambda u)a + (\mu u)b$. ◆

الشيء الجميل في المبرهنة 9.46 أنّه يمكن تنفيذها باستخدام الحاسوب، وبالطبع، نتوقع ذلك من أيّ شيء مسمّى بـ " خوارزمية".

مثال 10.46 لنوضح خوارزمية القسمة على المعيار الإقليدي | | على $\mathbb{Z}$ عن طريق حساب ق م أ لـ 22,471 و3,266. نطبّق فقط خوارزمية القسمة مرات عدّة وآخر باقٍ غير صفري هو ق م أ، حيث نرمز إلى الأرقام التي حصلنا عليها كما في المبرهنة 9.46 ؛ لنوضح نصّ المبرهنة وإثباتها بصورة أكثر، إذ يمكن التحقق من الحسابات بسهولة.

	$a = 22{,}471$
	$b = 3{,}266$
$22{,}471 = (3{,}266)6 + 2{,}875$	$r_1 = 2{,}875$
$3{,}266 = (2{,}875)1 + 391$	$r_2 = 391$
$2{,}875 = (391)7 + 138$	$r_3 = 138$
$391 = (138)2 + 115$	$r_4 = 115$
$138 = (115)1 + 23$	$r_5 = 23$
$115 = (23)5 + 0$	$r_6 = 0$

إذن، $r_5 = 23$ هو ق م أ لـ 22, 471 و 3, 266. أوجدنا ق م أ من غير تحليل وهذا مهم، إذ من الصعوبة بمكان تحليل عدد صحيح إلى أعداد أولية في بعض الأحيان. ▲

مثال 11.46 لاحظ أنه في خوارزمية القسمة وفي الشرط الأول في تعريف المعيار الإقليدي، لم نقل أيّ شيء عن أنّ r "موجب"، وقد كان اهتمامنا بالتأكيد في حساب ق م أ في $\mathbb{Z}$ عن طريق خوارزمية إقليدس لـ | |، كما في المثال 10.46، أن نجعل $|r_i|$ أصغر ما يمكن في كل حاصل قسمة؛ لذلك، بإعادة المثال 10.46 سيكون أكثر فاعلية أن نكتب:

	$a = 22{,}471$
	$b = 3{,}266$
$22{,}471 = (3{,}266)7 - 391$	$r_1 = -391$
$3{,}266 = (391)8 + 138$	$r_2 = 138$
$391 = (138)3 - 23$	$r_3 = -23$
$138 = (23)6 + 0$	$r_4 = 0$

يمكننا أن نبدل إشارة r_i من سالب إلى موجب عندما نريد؛ لأن قواسم r_i و $-r_i$ هي نفسها. ▲

تمارين 46

حسابات

في التمارين من 1 إلى 5، اذكر فيما إذا كانت الدالة المعطاة v معيارًا إقليديًّا للحلقة التامة المعطاة.

1. الدالة v لـ $\mathbb{Z}$ المعطاة بـ $v(n) = n^2$ لغير الصفرى $n \in \mathbb{Z}$.

2. الدالة v لـ $\mathbb{Z}[x]$ المعطاة بـ $v(f(x))=$ (درجة $f(x)$) لـ $f(x)) \in\mathbb{Z}[x]$، $f(x) \neq 0$.

3. الدالة v لـ $\mathbb{Z}[x]$ المعطاة بـ $v(f(x)) =$ (القيمة المطلقة لمعامل أعلى درجة غير صفرية لحد في $f(x)$) لغير الصفري $f(x) \in \mathbb{Z}[x]$.

4. الدالة v لـ $\mathbb{Q}$ المعطاة بـ $v(a) = a^2$ لغير الصفري $a \in \mathbb{Q}$.

5. الدالة v لـ $\mathbb{Q}$ المعطاة بـ $v(a) = 50$ لغير الصفري $a \in \mathbb{Q}$.

6. بالعودة إلى المثال 11.46، عَبِّرْ عن ق م أ 23 بالصيغة: $\lambda(22,471) + \mu(3,266)$ حيث $\lambda, \mu \in \mathbb{Z}$. [مساعدة: في السطر قبل الأخير في حسابات المثال 11.46، $391 - 3(138) = 23$. ومن السطر الذي قبله، $3,266 - 8(391) = 138$، إذن، تحصل بالتعويض على $391 - 3[3,266 - 8(391)] = 23$، وهكذا. أي ، سر في طريقك من الأسفل إلى الأعلى حتى تجد فعليًّا قيم λ و μ].

7. أوجد ق م أ لـ 49,349 و 15,555 في $\mathbb{Z}$.

8. باتباع الفكرة في تمرين 6 وبالعودة إلى تمرين 7، عبِّرْ عن ق م أ الموجب لـ 49,349 و 15,555 في $\mathbb{Z}$ بالصيغة $\lambda(49,349) + \mu(15,555)$، حيث $\lambda,\mu \in \mathbb{Z}$.

9. أوجد ق م أ لـ

$$x^{10} - 3x^9 + 3x^8 - 11x^7 + 11x^6 - 11x^5 + 19x^4 - 13x^3 + 8x^2 - 9x + 3$$

و

$$x^6 - 3x^5 + 3x^4 - 9x^3 + 5x^2 - 5x + 2$$

في $\mathbb{Q}[x]$.

10. صف كيف يمكن استخدام خوارزمية إقليدس في إيجاد ق م أ لـ n من الأعداد $a_1, a_2, \cdots, a_n$ في حلقة تامة إقليدية.

11. باستخدام الطريقة المستنبطة من تمرين 10، أوجد ق م أ لـ 2178، 396، 792، 726.

مفاهيم

12. لنفترض $\mathbb{Z}[x]$.

أ. هل $\mathbb{Z}[x]$ UFD؟ لماذا؟

ب. بيِّن أنَّ $\{a + xf(x) \mid a \in 2\mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$ مثالية في $\mathbb{Z}[x]$.

جـ. هل $\mathbb{Z}[x]$ PID؟ (استخدم الجزء (ب)).

د. هل $\mathbb{Z}[x]$ حلقة تامة إقليدية؟ لماذا؟

13. ضع إشارة صح أو إشارة خطأ:

________ أ. كل حلقة تامة إقليدية PID.

________ **ب**. كل PID حلقة تامة إقليدية.

________ **جـ**. كل حلقة تامة إقليدية UFD.

________ د. كل UFD حلقة تامة إقليدية.

________ هـ. ق م أ لـ 2 و 3 في $\mathbb{Q}$ هو $\frac{1}{2}$.

________ و. خوارزمية إقليدس تقدِّم طريقة لإيجاد ق م أ لعددين صحيحين.

________ ز. إذا كان v معيارًا إقليديًّا على حلقة تامة إقليدية D، فإنّ $v(1) \leq v(a)$ لكل غير صفري $a \in D$.

________ ح. إذا كان v معيارًا إقليديًّا على حلقة تامة إقليدية D، فإنّ $v(1) < v(a)$ لكل غير صفري $a \in D$، $a \neq 1$.

________ ط. إذا كان v معيارًا إقليديًّا على حلقة تامة إقليدية D، فإنّ $v(1) < v(a)$ لكل غير صفري، وليس عنصر وحدة $a \in D$.

________ ي. لأي حقل F، $F[x]$ حلقة تامة إقليدية.

14. هل اختيار معيار إقليدي محدّد v على حلقة تامة إقليدية D، هو تدخل غير مشروع في البناء الحسابي لـ D بأيّ صورة في الصور؟ وضِّح.

براهين

15. لتكن D حلقة تامة إقليدية، وليكن v معيارًا إقليديًّا على D. بيِّن أنَّه إذا كان a و b متشاركين في D، فإنّ $v(a) = v(b)$.

16. لتكن D حلقة تامة إقليدية، وليكن v معيارًا إقليديًّا على D. أثبت أنَّه لغير الصفرين $a,b \in D$، نحصل على $v(a) < v(ab)$، إذا وفقط إذا كان b ليس عنصر وحدة في D. [**مساعدة**: يظهر من التمرين 15، أنَّ $v(a) < v(ab)$ يؤدي إلى أنّ b ليس عنصر وحدة في D. باستخدام الخوارزمية الإقليدية، بيِّن أنّ $v(a) = v(ab)$ يؤدي إلى أنّ $\langle a \rangle = \langle ab \rangle$. استنتج أنَّه إذا كان b ليس عنصر وحدة، فإنّ $v(a) < v(ab)$].

17. أثبت أو انفِ الجملة الآتية: إذا كان v معيارًا إقليديًّا على حلقة تامة إقليدية D، فإنّ $\{a \in D \mid v(a) > v(1)\} \cup \{0\}$ مثالية في D.

18. بيِّن أنَّ كل حقل يكون حلقة تامة إقليدية.

19. ليكن v معيارًا إقليديًّا على الحلقة التامة الإقليدية D.

أ. بيِّن أنه إذا كان $s \in \mathbb{Z}$ حيث $s + v(1) > 0$، فإنّ $n : D^* \to \mathbb{Z}$ المعرفة بـ $n(a) = v(a) + s$ لغير الصفري $a \in D$ معيار إقليدي على D. كالعادة D^* هي مجموعة العناصر غير الصفرية في D.

ب. أثبت أنَّه لـ $t \in \mathbb{Z}^+$، $\lambda : D^* \to \mathbb{Z}$ المعطاة بـ $\lambda(a) = t.\ v(a)$ لغير الصفري $a \in D$، معيار إقليدي على D.

جـ. بيِّن أنه يوجد معيار إقليدي μ على D ، حيث $\mu(1) = 1$ و $\mu(a) > 100$ لكل غير صفري، وليس عنصر وحدة $a \in D$.

20. لتكن D UFD. العنصر c في D **مضاعف مشترك أصغر (least common multiple)** (باختصار م م أ) لعنصرين a و b في D ، إذا كان $a|c$، $b|c$ ، وإذا كان c يقسم كل عنصر في D قابل للقسمة على كلٍّ من a و b. بيِّن أنَّ كل عنصرين غير صفريين a و b في حلقة إقليدية D لهما م م أ في D. [مساعدة: بيِّن أنَّ المضاعفات المشتركة كلها – بالمعنى الواضح – لكلٍّ من a و b تشكل مثالية في D].

21. استخدم العبارة الأخيرة في المبرهنة 9.46 لتبيِّن أنَّ كل عنصرين غير صفريين $r, s \in \mathbb{Z}$ يولدان الزمرة $\langle \mathbb{Z}, + \rangle$، إذا وفقط إذا كان r ،s، بوصفهما عنصرين في الحلقة التامة $\mathbb{Z}$، **أوليّين نسبيًا (reatively prime)**، أي إنَّ ق م أ لهما هو 1.

22. باستخدام الجملة الأخيرة في المبرهنة 9.46 بيِّن أنه للقيم غير الصفرية $a, b, n \in \mathbb{Z}$ التطابق $ax \equiv b$ (مقياس n) له حل في $\mathbb{Z}$ إذا كان a و n أوليين نسبيًّا.

23. عمِّم التمرين 22 موضحًا أنه للقيم غير الصفرية $a, b, n \in \mathbb{Z}$، التطابق $ax \equiv b$ (مقياس n) له حل في $\mathbb{Z}$ ، إذا وفقط إذا كان ق م أ الموجب لـ a و n في $\mathbb{Z}$ يقسم b.

ترجم هذه النتيجة في الحلقة $\mathbb{Z}_n$.

24. متّبعًا الفكرة في التمرينين 6 و 23، أوجز طريقة بنّاءة لإيجاد الحل في $\mathbb{Z}$ للتطابق $ax \equiv b$ (مقياس n) للقيم غير الصفرية $a,b,n \in \mathbb{Z}$ وإذا كان للتطابق حل، استخدم هذه الطريقة في إيجاد الحلّ للتطابق $22x \equiv 18$ (مقياس 42).

الفصل 47 أعداد جاوس والمعايير الضربية Gaussian Integers and Multiplicative Norms

أعداد جاوس الصحيحة

سنقدِّم مثالًا على حلقة تامة إقليدية تختلف عن $\mathbb{Z}$ و $F[x]$.

1.47 تعريف عدد جاوس الصحيح **(Gaussian Integer)** هو العدد المركَّب $a + bi$، حيث $a, b \in \mathbb{Z}$.
ولعدد جاوس الصحيح $\alpha = a + bi$، **المعيار (norm)** $N(\alpha)$ لـ α هو $a^2 + b^2$. ■

سنجعل $\mathbb{Z}[i]$ تعني مجموعة أعداد جاوس الصحيحة. ستقدِّم التمهيدية الآتية بعض الخصائص الأساسية لدالة المعيار N على $\mathbb{Z}[i]$ ، وستقود إلى توضيح أنَّ الدالة v المعرفة بـ $v(\alpha) = N(\alpha)$ لغير صفري $\alpha \in \mathbb{Z}[i]$، هي معيار إقليدي على $\mathbb{Z}[i]$. لاحظ أنَّ أعداد جاوس الصحيحة تشمل الأعداد النسبية الصحيحة كلها ، أي عناصر $\mathbb{Z}$ كلها.

نبذة تاريخية

درس جاوس بالتفصيل في كتابه (*Disquisitiones Arithmeticae*) مبرهنة البواقي التربيعية، التي هي مبرهنة الحلول للمتطابقة $x^2 \equiv p$ (مقياس q) ، وأثبت مبرهنة المقلوبية التربيعية المشهورة، موضِّحًا العلاقة بين حلول المتطابقتين $x^2 \equiv p$ (مقياس q) $x^2 \equiv q$ (مقياس p) ، حيث p و q أعداد أولية، وفي محاولته لتعميم نتائجه إلى مبرهنات البواقي التربيعية، أدرك أنَّه من الطبيعي أكثر الأخذ في الحسبان أعداد جاوس الصحيحة بدلاً من الأعداد الصحيحة العادية.

اكتشافات جاوس على أعداد جاوس الصحيحة محتواة في بحث طويل منشور عام 1832م، وقد أثبت فيه وجود كثير من أوجه الشبه بينها وبين الأعداد الصحيحة العادية، على سبيل المثال: بعد أن لاحظ وجود أربعة عناصر وحدة (عناصر لها معكوس ضربي) من أعداد جاوس الصحيحة، هي 1، -1، i و $-i$ وبتعريف المعيار كما في التعريف 1.47، عمَّم مفهوم العدد الأولي بتعريفه عدد جاوس الأولي؛ ليكون العدد الذي لا يمكن التعبير عنه بوصفه حاصل ضرب عددين صحيحين ليس أيًّا منهما عنصر وحدة، وأصبح قادرًا – بعدها –على تحديد أيّ من أعداد جاوس أولي:

عدد جاوس غير الحقيقي يكون أوليًا، إذا وفقط إذا كان معياره عددًا حقيقيًّا أوليًّا، الذي يمكن أن يكون 2 أو على الصيغة $4n+1$. العدد الأوليّ الحقيقي $2= (1+i)(1-i)$ والأعداد الحقيقية الأولية المطابقة لـ 1 مقياس 4 مثل $13= (2+3i)(2-3i)$ ، تتحلل إلى حاصل ضرب عددي جاوس أوَّليين، والأعداد الأولية الحقيقية على صيغة $4n+3$ مثل 7 و 11، لا تزال أولية في الحلقة التامة لأعداد جاوس الصحيحة. انظر التمرين 10.

2.47 تمهيدية في $\mathbb{Z}[i]$، الخصائص الآتية لدالة المعيار N متحققة لكل $\alpha, \beta \in \mathbb{Z}[i]$:

.1 $N(\alpha) \geq 0$.

.2 $N(\alpha) = 0$ إذا وفقط إذا كان $\alpha = 0$.

.3 $N(\alpha\beta) = N(\alpha)N(\beta)$.

البرهان إذا جعلنا $\alpha= a_1 + a_2 i$ و $\beta = b_1+ b_2 i$، هذه النتائج هي حسابات مباشِرة، ونترك إثبات هذه الخصائص بوصفها تمرينًا (انظر التمرين 11). ♦

3.47 تمهيدية $\mathbb{Z}[i]$ حلقة تامة.

البرهان من الواضح أنّ $\mathbb{Z}[i]$ حلقة إبدالية فيها عنصر محايد، سنبيِّن أنه لا توجد قواسم لـ 0. لتكن $\alpha, \beta \in \mathbb{Z}[i]$. باستخدام التمهيدية 2.47، إذا كان $\alpha\beta = 0$ ، فإنَّ

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(0) = 0$$

إذن، $\alpha\beta = 0$ يؤدي إلى أنَّ $N(\alpha) = 0$ أو $N(\beta) = 0$، مرّة أخرى وباستخدام التمهيدية 2.47، يؤدي هذا إلى أنه إما $\alpha = 0$ أو $\beta = 0$؛ إذن، $\mathbb{Z}[i]$ لا تحوي قواسم لـ 0؛ لذلك، $\mathbb{Z}[i]$ حلقة تامة. ♦

بالطبع، لأن $\mathbb{Z}[i]$ حلقة جزئية من $\mathbb{C}$، حيث $\mathbb{C}$ حقل الأعداد المركبة، فإنَّه من الواضح حقيقةً أنَّ $\mathbb{Z}[i]$ لا تحوي قواسم لـ 0. قدَّمنا برهان التمهيدية 3.47 لتوضيح استخدام الخاصية الضربية 3 للمعيار الدالي N ، ولتجنُّب الذهاب خارج $\mathbb{Z}[i]$.

4.47 مبرهنة الدالة ν المعطاة بـ $\nu(\alpha) = N(\alpha)$ لغير الصفري $\alpha \in \mathbb{Z}[i]$ هي معيار إقليدي على $\mathbb{Z}[i]$، إذن، $\mathbb{Z}[i]$ حلقة تامة إقليدية.

البرهان لاحظ أنَّه لـ $\beta = b_1 + b_2 i \neq 0$، $N(b_1 + b_2 i) = b_1^2 + b_2^2$؛ إذن، $N(\beta) \geq 1$.

إذن، لكل $\alpha, \beta \neq 0$ في $\mathbb{Z}[i]$، $N(\alpha) \leq N(\alpha)N(\beta) = N(\alpha\beta)$، وهذا يثبت الشرط الثاني للمعيار الإقليدي في التعريف 1.46.

بقي أن نثبت خوارزمية القسمة، الشرط الأول، لـ N. لتكن $\alpha = a_1 + a_2 i$ و $\beta = b_1 + b_2 i$، حيث $\beta \neq 0$. يجب علينا أن نجد σ و ρ في $\mathbb{Z}[i]$ ، بحيث $\alpha = \beta\sigma + \rho$ وإمّا $\rho = 0$ أو $N(\rho) < N(\beta) = b_1^2 + b_2^2$. لتكن $\alpha/\beta = r + si$ حيث $r, s \in \mathbb{Q}$، لتكن q_1 و q_2 أعدادًا صحيحة في $\mathbb{Z}$ ، أقرب ما تكون إلى الأعداد النسبية r و s على الترتيب. لتكن $\sigma = q_1 + q_2 i$ و $\rho = \alpha - \beta\sigma$، فإذا كان $\rho = 0$، فقد انتهينا. وإلّا، وبحسب بناء σ، نرى أنَّ $|r - q_1| \leq \frac{1}{2}$ و $|s - q_2| \leq \frac{1}{2}$؛ إذن:

$$\begin{aligned} N\left(\frac{\alpha}{\beta} - \sigma\right) &= N((r + si) - (q_1 + q_2 i)) \\ &= N((r - q_1) + (s - q_2)i) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}. \end{aligned}$$

لذلك نحصل على

$$N(\rho) = N(\alpha - \beta\sigma) = N\left(\beta\left(\frac{\alpha}{\beta} - \sigma\right)\right) = N(\beta)N\left(\frac{\alpha}{\beta} - \sigma\right) \leq N(\beta)\frac{1}{2},$$

إذن، حصلنا فعلًا على $N(\rho) < N(\beta)$ كما هو مطلوب. ♦

5.47 مثال يمكننا تطبيق نتائجنا جميعها في الفصل 46 على $\mathbb{Z}[i]$، بالتحديد؛ لأنَّ $N(1) = 1$، عناصر الوحدة في $\mathbb{Z}[i]$ هي بالضبط $\alpha = a_1 + a_2 i$، حيث $N(\alpha) = a_1^2 + a_2^2 = 1$، ومن حقيقة أنَّ a_1 و a_2 أعداد صحيحة، فإنّ الاحتمالات هي فقط $a_1 = \pm 1$ مع $a_2 = 0$ أو $a_1 = 0$ مع $a_2 = \pm 1$؛ إذن، عناصر الوحدة في $\mathbb{Z}[i]$ هي ± 1 و $\pm i$. يمكن استخدام خوارزمية القسمة لحساب ق م أ لعنصرين غير صفريين. سنترك مثل هذه الحسابات للتمارين.

أخيرًا، لاحظ إنَّه، بينما 5 غير مختزل في $\mathbb{Z}$ أصبح 5 مختزلًا في $\mathbb{Z}[i]$ لأنَّ $5 = (1 + 2i)(1 - 2i)$، وليس $1 + 2i$ أو $1 - 2i$ عنصر وحدة. ▲

المعايير الضربيّة

لنُشر مرّة أخرى إلى أنه للحلقة التامة D، المفاهيم الحسابية لغير المختزلات وعناصر الوحدة، لا تتأثر بأيّ حال بالمعيار الذي ربما يُعرَّف على الحلقة التامة، مع ذلك كما في الفصل السابق ، وعملنا إلى الآن في هذا الفصل يوضحان أنَّ معيارًا مناسبًا معرَّفًا ربما يساعد على تحديد البنية الحسابية لـ D. هذا موضَّح بصورة لافتة للنظر في مبرهنة الأعداد الجبرية، فبالنسبة إلى الحلقة التامة للأعداد الجبرية، نفترض معايير كثيرة مختلفة على الحلقة التامة، كل منها له دوره في المساعدة على تحديد البنية الحسابية للحلقة التامة، وعندنا في الحلقة التامة للأعداد الجبرية معيار واحد جوهري لكل غير مختزل (تبعًا للمشاركة)، وكل معيارٍ منها يقدّم معلومات عن سلوك غير المختزلات في الحلقة التامة التي ترتبط بها.

هذا مثال على أهمية دراسة خصائص العناصر في بنية جبرية من خلال دوال مرتبطة بها.

لندرس حلقة تامة لها معيار ضربي محقق للخصائص 2 و 3 لـ N على $\mathbb{Z}[i]$ المعطاة في التمهيدية 2.47.

6.47 تعريف لتكن D حلقة تامة. **المعيار الضربي N على D** (***multiplicative norm***) هو دالة تربط D بالأعداد الصحيحة $\mathbb{Z}$ ، حيث تتحقق الشروط الآتية:

1. $N(\alpha) = 0$ ، إذا وفقط إذا كان $\alpha = 0$.

2. $N(\alpha\beta) = N(\alpha)\, N(\beta)$ لكل $\alpha, \beta \in D$. ■

7.47 مبرهنة إذا كانت D حلقة تامة مع المعيار الضريبي N، فإنّ $N(1) = 1$ و $|N(u)| = 1$ لكل عنصر وحدة u في D، وإذا كان– إضافة إلى ذلك – كل α بحيث $|N(\alpha)| = 1$ عنصر وحدة في D، فإنّ العنصر π في D ، بحيث $|N(\pi)| = p$ و $p \in \mathbb{Z}$ عدد أوّليّ غير مختزل في D.

البرهان لتكن D حلقة تامة مع المعيار الضربي N؛ إذن:

$$N(1) = N((1)(1)) = N(1)\, N(1)$$

تبيّن أنّ $N(1) = 1$. كذلك، إذا كان u عنصر وحدة في D، فإنَّ

$$1 = N(1) = N(uu^{-1}) = N(u)\, N(u^{-1})$$

ولأن $N(u)$ عدد صحيح، فهذا يؤدي إلى أنّ $|N(u)| = 1$.

افترض الآن أنَّ عناصر الوحدة في D هي بالضبط العناصر ذات المعيار ± 1. لتكن $\pi \in D$ بحيث $p = |N(\pi)|$، حيث p عدد أوّلي في $\mathbb{Z}$، فإذا كان $\pi = \alpha\beta$، فنحصل على:

$$p = |N(\pi)| = |N(\alpha)N(\beta)|$$

لذلك، إما $|N(\alpha)| = 1$ أو $|N(\beta)| = 1$. وبالإفتراض، هذا يعني أنه إما α أو β عنصر وحدة في D؛ إذن، π غير مختزل في D. ♦

مثال 8.47 في $\mathbb{Z}[i]$، الدالة N المعرفة بـ $N(a + bi) = a^2 + b^2$ تقدِّم معيارًا ضربيًّا يتناسب مع تعريفنا. رأينا أنَّ الدالة v المعطاة بـ $v(\alpha) = N(\alpha)$ لغير الصفري $\alpha \in \mathbb{Z}[i]$ هي معيار إقليدي على $\mathbb{Z}[i]$؛ لذلك، عناصر الوحدة هي بالضبط العناصر α في $\mathbb{Z}[i]$ ، حيث $N(\alpha) = N(1) = 1$؛ إذن، الجزء الثاني من المبرهنة 7.47 متحقق في $\mathbb{Z}[i]$.

رأينا في المثال 5.47 أنّ 5 مختزلة في $\mathbb{Z}[i]$؛ لأنَّ $(1-2i)(1+2i)=5$. ولأنَّ $N(1+2i) = N(1-2i) = 1^2 + 2^2 = 5$ و 5 عدد أولي في $\mathbb{Z}$، فنرى من المبرهنة 7.47 أنَّ $1+2i$ و $1-2i$ كليهما غير مختزل في $\mathbb{Z}[i]$.

بوصفه تطبيقًا على المعايير الضربية، سنقدم الآن مثالًا على حلقة تامة ليست UFD، فقد رأينا مثالاً واحدًا في المثال 16.45، والآتي هو توضيح أساسي.

مثال 9.47 لتكن $\mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$، وبوصفها مجموعة جزئية من الأعداد المركبة، فهي مغلقة تحت الجمع، والطرح، والضرب وتحوي 0 و 1؛ إذن، $\mathbb{Z}[\sqrt{-5}]$ حلقة تامة.
عرِّف N على $\mathbb{Z}[\sqrt{-5}]$ بـ

$$N(a + b\sqrt{-5}) = a^2 + 5b^2$$

من الواضح أنّ $N(\alpha) = 0$، إذا وفقط إذا كان $\alpha = a + b\sqrt{-5} = 0$؛ ولأنّ $N(\alpha\beta) = N(\alpha)N(\beta)$ هو حساب مباشر، فسنتركه للتمارين (انظر التمرين 12). لنجد عناصر الوحدة كلها المرشحة في $\mathbb{Z}[\sqrt{-5}]$، عن طريق إيجاد العناصر α في $\mathbb{Z}[\sqrt{-5}]$، حيث $N(\alpha) = 1$، فإذا كان $\alpha = a + b\sqrt{-5}$ و $N(\alpha) = 1$، فيجب أن يكون عندنا $a^2 + 5b^2 = 1$ وللأعداد الصحيحة a و b، هذا ممكن فقط إذا $b = 0$ و $a = \pm 1$؛ إذن، ± 1 هي فقط المرشحة بوصفها عناصر وحدة، ولأنَّ ± 1 عناصر وحدة، فإنها بالضبط عناصر الوحدة في $\mathbb{Z}[\sqrt{-5}]$
الآن في $\mathbb{Z}[\sqrt{-5}]$، عندنا $21 = (3)(7)$ ، وكذلك:

$$21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) .$$

إذا استطعنا أن نبيِّن أنَّ $1+2\sqrt{-5}$، 7، 3 و $1-2\sqrt{-5}$ كلها غير مختزلة في $\mathbb{Z}[\sqrt{-5}]$ ، فسنعلم عندها أنّ $\mathbb{Z}[\sqrt{-5}]$ لا يمكن أن يكون UFD؛ لأنَّه لا 3 ولا 7 يساوي $\pm(1 + 2\sqrt{-5})$.

افترض أنَّ $3 = \alpha\beta$، فإنَّ.

$$9 = N(3) = N(\alpha)N(\beta)$$

توضح أنه يجب أن يكون عندنا $N(\alpha)$ تساوي 1، 3 أو 9، فإذا كان $N(\alpha)=1$، فإنّ α عنصر وحدة، وإذا كان $\alpha=a+b\sqrt{-5}$، فإنّ $N(\alpha)=a^2+5b^2$، وليس هناك أيّ خيار لأعداد صحيحة a و b، حيث $N(\alpha)=3$. فإذا كان $N(\alpha)=9$، فإنّ $N(\beta)=1$؛ إذن، β عنصر وحدة؛ ولذلك، 3 غير مختزل في $\mathbb{Z}[\sqrt{-5}]$ وبمناقشة مشابهة يتبيّن أنّ 7 غير مختزل في $\mathbb{Z}[\sqrt{-5}]$.

إذا كان $1+2\sqrt{-5}=\gamma\,\delta$ ، فنحصل على:

$$21 = N(1+2\sqrt{-5}) = N(\gamma)N(\delta)$$

إذن، $N(\gamma)$ تساوي 1، أو 3، أو 7 أو 21. رأينا أنّه لا يوجد عنصر في $\mathbb{Z}[\sqrt{-5}]$ معياره 3 أو 7؛ لذلك، إمّا $N(\gamma)=1$، وγ عنصر وحدة، أو $N(\gamma)=21$ ؛ وبذلك، فإنّ $N(\delta)=1$، و δ عنصر وحدة؛ إذن، $1+2\sqrt{-5}$ غير مختزل في $\mathbb{Z}[\sqrt{-5}]$. وبمناقشة موازية يتّضح أنّ $1-2\sqrt{-5}$ أيضًا غير مختزلة في $\mathbb{Z}[\sqrt{-5}]$.

باختصار، بيَّنا أنَّ

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

هي حلقة تامة، لكنها ليست UFD، وبالتحديد هناك تحليلان مختلفان

$$21 = 3\cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$$

لـ 21 إلى غير مختزلات. غير المختزلات هذه لا يمكن أن تكون أولية؛ لأنها لو كانت أولية لأمكننا إثبات وحدانية التحليل (انظر إثبات المبرهنة 17.45). ▲

نختم بالسؤال التقليدي، حدِّد أيّ الأعداد الأوّلية p في $\mathbb{Z}$ تساوي حاصل جمع مربعي عددين في $\mathbb{Z}$. على سبيل المثال $2=1^2+1^2$ ، $5=1^2+2^2$، و $13=2^2+3^2$ هي مجموع مربعات؛ ولأننا أجبنا الآن عن هذا السؤال للعدد الزوجي الأولي الوحيد 2، فنستطيع أن نقيِّد أنفسنا بالأعداد الأولية الفردية.

10.47 مبرهنة (مبرهنة فيرما $\boldsymbol{p=a^2+b^2}$) ليكن p عددًا أوليًّا فرديًّا في $\mathbb{Z}$، فإنّ $p=a^2+b^2$ للعددين الصحيحين a و b في $\mathbb{Z}$ ، إذا وفقط إذا كان $p\equiv 1$ (مقياس 4).

البرهان أولًا، افترض أنّ $p=a^2+b^2$. الآن، لا يمكن أن يكون a و b كلاهما زوجي أو كلاهما فردي؛ لأن p عدد فردي، فإذا كان $a=2r$ و $b=2s+1$، فإنّ $a^2+b^2=4r^2+4(s^2+s)+1$؛ إذن، $p\equiv 1$ (مقياس 4). هذا يهتم باتجاه واحد لهذه المبرهنة: إذا وفقط إذا كان.

بالنسبة إلى الاتجاه الآخر، نفترض أنّ $p\equiv 1$ (مقياس 4). الآن، الزمرة الضربية للعناصر غير الصفرية للحقل المنتهي $\mathbb{Z}_p$ دورية ورتبتها 1؛ ولأنّ 4 قاسم لـ $p-1$، نرى أنَّ $\mathbb{Z}_p$ يحوى عنصر n رتبته الضربية 4. وعليه، n^2 رتبتها الضربية 2؛ إذن، $n^2=-1$ في $\mathbb{Z}_p$؛ لذلك، نحصل في $\mathbb{Z}$ على: $n^2\equiv -1$ (مقياس p)؛ إذن، p يقسم n^2+1 في $\mathbb{Z}$.

باستعراض p و n^2+1 في $\mathbb{Z}[i]$؛ نرى أنّ p تقسم $(n-i)(n+i) = n^2+1$. افترض أنَّ p غير مختزلة في $\mathbb{Z}[i]$ فيجب على p أن تقسم $n+i$ أو $n-i$، فإذا كانت p تقسم $n+i$ ، فإنّ $n+i = p(a+bi)$، حيث $a, b \in \mathbb{Z}$، وبمساواة معاملات i، نحصل على $1 = pb$ ، وذلك غير ممكن، وبالمثل، إذا كانت p تقسم $n-i$ ، فإنّ ذلك يقود إلى معادلة غير ممكنة، وهي: $-1 = pb$. إذن، افتراضنا أنَّ p غير مختزلة في $\mathbb{Z}[i]$ يجب أن يكون خاطئًا.

لأنّ p مختزلة في $\mathbb{Z}[i]$، فإننا نحصل على $p = (a+bi)(c+di)$ ، حيث $a+bi$ و $c+di$ ليسا عناصر وحدة، وبأخذ المعايير، يكون عندنا $p^2 = (a^2+b^2)(c^2+d^2)$، حيث لا $a^2+b^2 = 1$ ولا $c^2+d^2 = 1$ بناءً على ذلك، يكون عندنا $p = a^2+b^2$، الذي يكمل إثباتنا.

[لأن $a^2+b^2 = (a+bi)(a-bi)$ نرى أنَّ هذا هو التحليل لـ $\boldsymbol{p}$ ، أي إنَّ $c+di = a-bi$.] ♦

يسألك التمرين 10 لتحدد أيّ الأعداد الأوّلية p من $\mathbb{Z}$ تبقى أوّلية في $\mathbb{Z}[i]$.

تمارين 47

حسابات

في التمارين من 1 إلى 4، حلل عدد جاوس الصحيح إلى حاصل ضرب غير مختزلات في $\mathbb{Z}[i]$. [مساعدة: لأنّ كل معامل غير مختزل لـ $\alpha \in \mathbb{Z}[i]$ يجب أن يكون معياره > 1 ويقسم $N(\alpha)$، فيوجد فقط عدد منته من أعداد جاوس الصحيحة $a + \mathrm{bi}$ لأن تُعدّ عوامل غير مختزلة ممكنة لأيّ α معطاة. قسم α على كل منها في $\mathbb{C}$، وانظر أيًّا من نواتج القسمة مرة أخرى في $\mathbb{Z}[i]$].

1. 5 **2.** 7 **3.** $4 + 3i$ **4.** $6 - 7i$

5. بيِّن أنَّ 6 لا يتحلل بصورة وحيدة (تبعًا للمشاركات) إلى غير مختزلات في $\mathbb{Z}[\sqrt{-5}]$. أعطِ تحليلين مختلفين.

6. افترض $\alpha = 7 + 2i$ و $\beta = 3 - 4i$ في $\mathbb{Z}[i]$. أوجد σ و ρ في $\mathbb{Z}[i]$ بحيث:

$$\alpha = \beta\sigma + \rho \text{ حيث } N(\rho) < N(\beta)$$

[مساعدة: استخدم البناء في إثبات المبرهنة 4.47].

7. استخدم الخوارزمية الإقليدية في $\mathbb{Z}[i]$ في إيجاد ق م أ لـ $8 + 6i$ و $5 - 15i$ في $\mathbb{Z}[i]$. [مساعدة: استخدم البناء في إثبات المبرهنة 4.47].

مفاهيم

8. ضع إشارة صح أو إشارة خطأ:

_______ أ. $\mathbb{Z}[i]$ هي PID.

_______ ب. $\mathbb{Z}[i]$ حلقة إقليدية.

_______ ج. كل عدد صحيح في $\mathbb{Z}$ هو عدد جاوس صحيح.

_______ د. الخوارزمية الإقليدية متحققة في $\mathbb{Z}[i]$.

_______ هـ. كل عدد مركب هو عدد جاوس صحيح.

_______ و. المعيار الضربي على حلقة تامة يساعد في بعض الأحيان على إيجاد غير مختزلات في الحلقة التامة.

_______ ز. إذا كان N معيارًا ضربيًّا على حلقة تامة D، فإنّ $|N(u)| = 1$ لكل عنصر وحدة u في D.

_______ ح. إذا كان F حقلًا، فإنّ الدالة N المعرفة بـ $N(f(x)) = (\text{درجة } f(x))$ هي معيار ضربي على $F[x]$.

_______ ط. إذا كان F حقلًا، فإنَّ الدالة المعرفة بـ $N(f(x)) = 2^{(\text{درجة } f(x))}$ لـ $f(x) \neq 0$ و $N(0) = 0$ هي معيار ضربي على $F[x]$ تبعًا لتعريفنا.

_______ ي. $\mathbb{Z}[\sqrt{-5}]$ حلقة تامة ليست UFD.

9. لتكن D حلقة تامة مع المعيار الضربي N ، بحيث $|N(\alpha)| = 1$ لـ $\alpha \in D$، إذا وفقط إذا كان α عنصر وحدة في D. لتكن π بحيث $|N(\pi)|$ الأصغر بين كل $|N(\beta)| > 1$، حيث $\beta \in D$. بيِّن أنّ π غير مختزل في D.

10. أ. أثبت أنّ 2 يساوي حاصل ضرب عنصر وحدة ومربع غير مختزل في $\mathbb{Z}[i]$.

ب. أثبت أنّ العدد الأوّلي p في $\mathbb{Z}$ غير مختزل في $\mathbb{Z}[i]$ ، إذا وفقط إذا كان $p \equiv 3$ (مقياس 4). (استخدم المبرهنة 10.47).

11. أثبت التمهيدية 2.47.

12. أثبت أنّ N في المثال 9.47 ضربية، أي إنّ $N(\alpha\beta) = N(\alpha)\, N(\beta)$ لكل $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.

13. لتكن D حلقة تامة مع المعيار الضربي N، بحيث $|N(\alpha)| = 1$ لـ $\alpha \in D$ إذا وفقط إذا كان α عنصر وحدة في D. بيّن أنّ أيّ عنصر ليس صفرًا، وليس عنصر وحدة في D له تحليل إلى غير مختزلات في D.

14. استخدم الخوارزمية الإقليدية في $\mathbb{Z}[i]$ في إيجاد ق م أ لـ $16 + 7i$ و $10 - 5i$ في $\mathbb{Z}[i]$. [مساعدة: استخدم البناء في إثبات المبرهنة 4.47].

15. لتكن $\langle\alpha\rangle$ مثالية رئيسة غير صفرية في $\mathbb{Z}[i]$.

أ. أثبت أنَّ $\mathbb{Z}[i]/\langle\alpha\rangle$ حلقة منتهية. [مساعدة: استخدم خوارزمية القسمة].

ب. أثبت أنه إذا كان π غير مختزل في $\mathbb{Z}[i]$، فإنّ $\mathbb{Z}[i]/\langle\pi\rangle$ حقل.

جـ. بالرجوع إلى الجزء (ب)، أوجد رتبة وميِّز كل من الحقول الآتية:

i. $\mathbb{Z}[i]/\langle 3\rangle$ **ii.** $\mathbb{Z}[i]/\langle 1+i\rangle$ **iii.** $\mathbb{Z}[i]/\langle 1+2i\rangle$

16. لتكن $n \in \mathbb{Z}^+$ حرّة من المربعات، أي أنها لا تقبل القسمة على مربع أيّ عدد أوّلي صحيح.

لتكن $\mathbb{Z}[\sqrt{-n}] = \{a + ib\sqrt{n} \mid a, b \in \mathbb{Z}\}$.

أ. أثبت أنّ المعيار N ، المعرّف بـ $N(\alpha) = a^2 + nb^2$، لـ $\alpha = a + ib\sqrt{n}$ هو معيار ضربي على $\mathbb{Z}[\sqrt{-n}]$.

ب. أثبت أنّ $N(\alpha) = 1$ لـ $\alpha \in \mathbb{Z}[\sqrt{-n}]$ إذا وفقط إذا كان α عنصر وحدة في $\mathbb{Z}[\sqrt{-n}]$.

جـ. أثبت أنّ كل عنصر غير صفري $\alpha \in \mathbb{Z}[\sqrt{-n}]$ وبحيث إنَّه ليس عنصر وحدة له تحليل إلى غير مختزلات في $\mathbb{Z}[\sqrt{-n}]$. [مساعدة: استخدم الفرع (ب)].

17. أعد التمرين 16 لـ $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$، حيث N معرّفة بـ $N(\alpha) = a^2 - nb^2$ لـ $\alpha = a + b\sqrt{n}$ في $\mathbb{Z}[\sqrt{n}]$.

18. يُبيِّن ببناء مشابه لذلك الذي أُعطي في إثبات المبرهنة 4.47 ، أنَّ خوارزمية القسمة متحققة على الحلقة التامة $\mathbb{Z}[\sqrt{-2}]$ لـ $\nu(\alpha) = N(\alpha)$ لغير صفري α في هذه الحلقة التامة. (انظر التمرين 16). (إذن، هذه الحلقة التامة إقليدية. انظر (Hardy and Wright [29] في مناقشتهما أيّ الحلقات التامة $\mathbb{Z}[\sqrt{n}]$ و $\mathbb{Z}[\sqrt{-n}]$ إقليدية).