

التماثلات الذاتية ومبرهنة جالوا  
**Automorphisms and Galois Theory**

|          |  |
|----------|--|
| الفصل 48 | التماثلات الذاتية للحقول<br>Automorphisms of Fields                        |
| الفصل 49 | مبرهنة تمديد التماثل<br>The Isomorphism Extension Theorem                  |
| الفصل 50 | حقول الانشطار<br>Splitting Fields  |
| الفصل 51 | الامتدادات القابلة للفصل<br>Separable Extensions                           |
| الفصل 52 | الامتدادات غير القابلة للفصل كلياً<br>Totally Inseparable Extensions       |
| الفصل 53 | مبرهنة جالوا<br>Galois Theory  |
| الفصل 54 | توضيحات على مبرهنة جالوا<br>Illustrations of Galois Theory                 |
| الفصل 55 | الامتدادات الدورية<br>Cyclotomic Extensions                                |
| الفصل 56 | عدم قابلية المعادلة من الدرجة الخامسة للحل<br>Insolvability of the Quintic |

## الفصل 48

## التماثلات الذاتية للحقول Automorphisms of Fields

تماثلات الترافق في مبرهنة الحقول الجبرية

ليكن  $F$  حقلاً، وليكن  $\bar{F}$  إغلاقاً جبرياً لـ  $F$ ، أي امتداد جبري لـ  $F$  ومغلق جبرياً. فالحقل  $\bar{F}$  موجود، بحسب المبرهنة 17.31، واختيارنا له محدد، وليس حاسماً؛ وذلك - وكما سنرى في الفصل 49- لأن أي إغلاقين جبريين لـ  $F$  يكونان متماثلين باستخدام دالة تبقى  $F$  ثابتة، وسنفرض في عملنا من الآن فصاعداً أن الامتدادات الجبرية والعناصر الجبرية على الحقل  $F$  قيد الدراسة كلها محتواة في إغلاق جبري ثابت  $\bar{F}$  لـ  $F$ .

تذكر أننا نعمل على دراسة أصفار كثيرات الحدود، وباستخدام مصطلحات الفصل 31، دراسة أصفار كثيرات الحدود في  $F[x]$  تعادل دراسة بناء الامتدادات الجبرية لـ  $F$  والعناصر الجبرية على  $F$ ، وسنثبت أنه إذا كان  $E$  امتداداً جبرياً لـ  $F$  وكانت  $\alpha, \beta \in E$ ، فإن لـ  $\alpha$  و  $\beta$  الخصائص الجبرية نفسها، إذا فقط إذا كانت  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$  سنصوغ هذه الحقيقة باستخدام الدوال - كما كنا نعمل دائماً في مبرهنة الحقول - وسوف نحقق هذا من خلال إثبات أنه إذا كانت  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$ ، فإنه يوجد تماثل  $\psi_{\alpha, \beta}$  من  $F(\alpha)$  وغامر لـ  $F(\beta)$ ، ويربط كل عنصر من  $F$  بنفسه، ويربط  $\alpha$  بـ  $\beta$ . تعرض المبرهنة الآتية هذا التماثل  $\psi_{\alpha, \beta}$ ، حيث ستصبح هذه التماثلات أدواتنا الأساسية في دراسة الامتدادات الجبرية، وهي تخلف تشاكلات التعويض  $\psi_{\alpha}$  في المبرهنة 4.22، التي تجعل آخر مشاركتاتها تعريف هذه التماثلات قبل النص على هذه المبرهنة وإثباتها، لنقدم المزيد من المصطلحات.

## 48.1 تعريف

ليكن الحقل  $E$  امتداداً جبرياً لـ  $F$ ، حيث يقال عن العنصرين  $\alpha, \beta \in E$ : إنهما مترافقان على  $F$  (*Conjugate over F*) إذا كان  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$  بمعنى أن  $\alpha$  و  $\beta$  صفران لكثيرة الحدود نفسها غير المختزلة على  $F$ .

## 48.2 مثال

مفهوم العناصر المترافقة الذي عرّف توّاً يتوافق مع التعريف الكلاسيكي لفكرة الأعداد المركبة المترافقة، إذا فهمنا أن الأعداد المركبة المترافقة تعني عناصر مترافقة على  $\mathbb{R}$ ، فإذا كان  $a, b \in \mathbb{R}$ ،  $b \neq 0$ ، فإن المترافقين  $a + bi$  و  $a - bi$  صفران لـ  $x^2 - 2ax + a^2 + b^2$ ، التي تكون غير مختزلة في  $\mathbb{R}[x]$ .

## 48.3 مبرهنة

(تماثلات الترافق): ليكن  $F$  حقلاً، ولتكن  $\alpha$  و  $\beta$  جبرية على  $F$  و  $\text{deg}(\alpha, F) = n$ . تكون الدالة  $\psi_{\alpha, \beta}: F(\alpha) \rightarrow F(\beta)$  والمعرفة بـ:

$$\psi_{\alpha, \beta}(c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \dots + c_{n-1}\beta^{n-1}$$

حيث  $c_i \in F$  تماثل من  $F(\alpha)$  غامر لـ  $F(\beta)$ ، إذا فقط إذا كانت  $\alpha$  و  $\beta$  مترافقتين على  $F$ .

افتراض أن  $\psi_{\alpha, \beta}: F(\alpha) \rightarrow F(\beta)$  المعرفة في نص المبرهنة تماثل. ليكن

$$\text{irr}(\alpha, F) = a_0 + a_1x + \dots + a_nx^n = 0, \text{ إذن، } a_0 + a_1\alpha + \dots + a_n\alpha^n = 0, \text{ ما يعني أن}$$

$$\psi_{\alpha, \beta}(a_0 + a_1\alpha + \dots + a_n\alpha^n) = a_0 + a_1\beta + \dots + a_n\beta^n = 0.$$

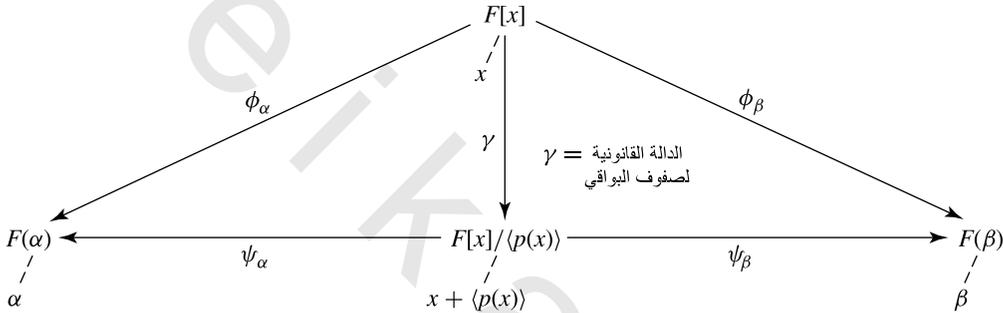
بحسب العبارة الأخيرة في نص المبرهنة 13.29، ينتج أن  $\text{irr}(\beta, F)$  تقسم  $\text{irr}(\alpha, F)$  وبأسلوب مشابه باستخدام التماثل  $\psi_{\beta, \alpha} = (\psi_{\alpha, \beta})^{-1}$  يتبين أن  $\text{irr}(\alpha, F)$  تقسم  $\text{irr}(\beta, F)$ ، وهذا يؤدي - ولأن كثيرتي الحدود أحاديّتان - إلى أن  $\text{irr}(\beta, F) = \text{irr}(\alpha, F)$ .

إذن،  $\alpha$  و  $\beta$  مترافقان على  $F$ .

البرهان

في المقابل، افترض أن  $\text{irr}(\alpha, F) = \text{irr}(\beta, F) = p(x)$ ، هذا يؤدي إلى أن تشاكلي التعويض  $\phi_\alpha: F[x] \rightarrow F(\alpha)$  و  $\phi_\beta: F[x] \rightarrow F(\beta)$  بحسب المبرهنة 17.26 وبالرجوع إلى  $F(\alpha)$  -  $\phi_\alpha: F[x] \rightarrow F(\alpha)$  يوجد تماثل طبيعي  $\psi_\alpha$  يربط  $F[x]/\langle p(x) \rangle$  بصورة غامرة بـ  $F(\alpha)$  وبالتماثل، يعطي  $\phi_\beta$  تماثلاً  $\psi_\beta$  يربط  $F[x]/\langle p(x) \rangle$  بصورة غامرة بـ  $F(\beta)$ . ليكن  $\psi_{\alpha, \beta} = \psi_\beta (\psi_\alpha)^{-1}$  يعطي الشكل 4.48 رسمًا توضيحيًا لهذه الدوال، حيث تشير الخطوط المقطعة إلى العناصر المتقابلة في هذه الدوال، ولأن تركيب تماثلين  $\psi_{\alpha, \beta}$  هو أيضًا تماثل، ويربط  $F(\alpha)$  بصورة غامرة بـ  $F(\beta)$ ، فإذا كانت  $(c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}) \in F(\alpha)$ ، فإن:

$$\begin{aligned} & \psi_{\alpha, \beta}(c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}) \\ &= (\psi_\beta \psi_\alpha^{-1})(c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}) \end{aligned}$$



الشكل 4.48

$$\begin{aligned} &= \psi_\beta ((c_0 + c_1x + \dots + c_{n-1}x^{n-1}) + \langle p(x) \rangle) \\ &= c_0 + c_1\beta + \dots + c_{n-1}\beta^{n-1}. \end{aligned}$$

إذن،  $\psi_{\alpha, \beta}$  هي الدالة المعرفة في نص المبرهنة.

النتيجة الآتية للمبرهنة 3.48 هي حجر الزاوية في برهاننا لمبرهنة امتداد التماثلات المهمة في الفصل 49 وفي معظم بقية عملنا.

### 5.48 نتيجة

لنكن  $\alpha$  جبرية على الحقل  $F$ . كل تماثل  $\psi$  يربط  $F(\alpha)$  بصورة غامرة بحقل جزئي من  $\bar{F}$  بحيث  $\psi(a) = a$  لكل  $a \in F$ ، فإنه يربط  $\alpha$  بمرافق له  $\beta$  على  $F$ ، وفي المقابل، لكل مرافق  $\beta$  لـ  $\alpha$  على  $F$ ، يوجد بالضبط تماثل واحد  $\psi_{\alpha, \beta}$  من  $F(\alpha)$  وبصورة غامرة إلى حقل جزئي من  $\bar{F}$  ويربط  $\alpha$  بـ  $\beta$  ويربط كل  $a \in F$  بنفسه.

ليكن  $\psi$  تماثلاً من  $F(\alpha)$  وبصورة غامرة إلى حقل جزئي من  $\bar{F}$ ، بحيث إن  $\psi(a) = a$  لكل  $a \in F$ . لتكن  $\text{irr}(\alpha, F) = a_0 + a_1x + \dots + a_nx^n$ ؛ إذن:

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = 0,$$

وهكذا ينتج

$$0 = \psi(a_0 + a_1\alpha + \dots + a_n\alpha^n) = a_0 + a_1\psi(\alpha) + \dots + a_n\psi(\alpha)^n,$$

و  $\beta = \psi(\alpha)$  مرافق لـ  $\alpha$ .

في المقابل، لكل مرافق  $\beta$  لـ  $\alpha$  على  $F$ ، يكون تماثل الترافق  $\psi_{\alpha, \beta}$  في المبرهنة 3.48 هو تماثل بالصفات المطلوبة؛ ولأن  $\psi_{\alpha, \beta}$  هو التماثل الوحيد الذي ينتج من حقيقة أن أي تماثل على  $F(\alpha)$  يتحدد تماماً من قيمه على عناصر  $F$  وقيمه على  $\alpha$ .

وبوصفها نتيجة ثانية للمبرهنة 3.48، فيمكننا إثبات نتيجة مشهورة. لتكن  $f(x) \in \mathbb{R}[x]$ ، فإذا كانت  $f(a + bi) = 0$ ، حيث  $(a + bi) \in \mathbb{C}$ ، و  $a, b \in \mathbb{R}$ ، فإن  $f(a - bi) = 0$  كذلك، وبصورة أكثر بساطة، الأصفار المركبة لكثيرات حدود ذات معاملات حقيقية تكون أزواجاً مترافقة. رأينا أن  $\mathbb{C} = \mathbb{R}(i)$ ، الآن:

$$\text{irr}(i, \mathbb{R}) = \text{irr}(-i, \mathbb{R}) = x^2 + 1$$

إذن،  $i$  و  $-i$  مترافقان على  $\mathbb{R}$  بحسب المبرهنة 3.48، دالة الترافق  $\psi_{i, -i}: \mathbb{C} \rightarrow \mathbb{C}$

حيث  $\psi_{i, -i}(a + bi) = a - bi$ ، وإذا كان  $a_i \in \mathbb{R}$

$$f(a + bi) = a_0 + a_1(a + bi) + \dots + a_n(a + bi)^n = 0$$

فإنه

$$\begin{aligned} 0 = \psi_{i, -i}(f(a + bi)) &= a_0 + a_1(a - bi) + \dots + a_n(a - bi)^n \\ &= f(a - bi), \end{aligned}$$

بمعنى أن  $f(a - bi) = 0$  كذلك.

افتراض  $\mathbb{Q}(\sqrt{2})$  على  $\mathbb{Q}$ . أصفار  $\text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$  هي  $\sqrt{2}$  و  $-\sqrt{2}$ ، ما يعني أن  $\sqrt{2}$  و  $-\sqrt{2}$  مترافقان على  $\mathbb{Q}$ . وبحسب المبرهنة 3.48 تكون الدالة  $\psi_{\sqrt{2}, -\sqrt{2}}: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$  المعرفة بـ

$$\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$$

تماثلاً من  $\mathbb{Q}(\sqrt{2})$  إلى نفسها.

**التماثلات الذاتية والحقول الثابتة**

كما تم توضيحه في النتيجة والمثال السابقين، يمكن أن يكون للحقل تماثل غير بدهي مع نفسه. هذه الدوال ستكون ذات أهمية قصوى في العمل المقبل.

البرهان

6.48 نتيجة

البرهان

7.48 مثال

8.48 تعريف

التماثل من الحقل إلى نفسه يسمى تماثلاً ذاتياً للحقول (*automorphism of fields*).

9.48 تعريف

إذا كانت  $\sigma$  تماثلاً من الحقل  $E$  إلى أي حقل، فيسمى العنصر  $a$  من  $E$  متروكاً ثابتاً (*left Fixed*) بـ  $\sigma$ . إذا كان  $\sigma(a) = a$ ، مجموعة التماثلات  $S$  على  $E$ ، التي تترك الحقل الجزئي  $F$  من  $E$  ثابتاً (*leaves a subfield  $F$  of  $E$  fixed*)، إذا كان كل  $a \in F$  متروكاً ثابتاً بكل  $\sigma \in S$ . إذا كانت  $\{\sigma\}$  تترك  $F$  ثابتاً، فإن  $\sigma$  تترك  $F$  ثابتاً (*leaves  $F$  fixed*).

10.48 مثال

ليكن  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  الدالة  $\sigma: E \rightarrow E$  المعرفة بـ

$$\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

حيث  $a, b, c, d \in \mathbb{Q}$  تكون تماثلاً ذاتياً على  $E$ : إنها تماثل الترافق  $\sqrt{3}, -\sqrt{3}$  من  $E$  إلى نفسها. إذا تصورنا  $E$  على الصورة  $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ ، فسوف نرى أن  $\sigma$  تترك  $\mathbb{Q}(\sqrt{2})$  ثابتاً. هدفنا دراسة بنية التمدد الجبري  $E$  للحقل  $F$  من خلال دراسة التماثلات الذاتية على  $E$ ، التي تترك كل عنصر في  $F$  ثابتاً، وسنثبت في الوقت الحاضر أن هذه التماثلات تشكل زمرة بطريقة طبيعية، ثم بعد ذلك سنطبق هذه النتائج الخاصة ببنية الزمرة للحصول على معلومات عن بنية امتداد الحقول؛ إذن، الكثير من عملنا السابق سيجمع الآن معاً، والمبرهنات الثلاث اللاحقة تبرهن بسهولة، ولكن الأفكار المحتواة فيها تمثل الأساس لكل شيء قادم؛ لذلك، فهذه المبرهنات ذات أهمية بالغة لنا، إنها في الحقيقة تعادل ملاحظات أكثر منها مبرهنات، والمهم هو الأفكار التي تحويها، فالخطوات الكبيرة في الرياضيات ليست دائماً مكوّنة من مبرهنات صعبة، بل من الممكن أن تتكوّن من ملاحظة كيف أن معلومات رياضية معروفة قد توصل إلى مواقف جديدة، سنحضر هنا مبرهنة الزمر لدراسة أصفار كثيرات الحدود، وحاول أن تتأكد من فهمك لهذه الأفكار، حيث إنها المفتاح لحل هدفنا النهائي في هذا الكتاب، وذلك بخلاف ما يبدو.

الهدف النهائي (سيتمّ النصّ عليه بدقة لاحقاً): إثبات أنه ليست الأصفار كلها لأي كثيرة حدود من الدرجة الخامسة  $f(x)$ ، يمكن التعبير عنها باستخدام الجذور بدءاً بعناصر من الحقل الذي يحوي معاملات  $f(x)$ .

## ■ نبذة تاريخية

كان ريتشارد ديدكند (*Richard Dedekind*) أول من طوّر فكرة التماثلات الذاتية للحقول - التي أطلق عليها "تباديل الحقول" - عام 1894م، وكان التطبيق المبكر لمبرهنة الزمر في مبرهنة المعادلات من خلال زمر التباديل لجذور كثيرات حدود خاصة، وقد عمم ديدكند هذه الفكرة إلى دوال على كامل الحقل، وأثبت كثيراً من مبرهنات هذا الفصل.

على الرغم من أن هنريك ويبر (*Heinrich Weber*) أكمل طريقة ديدكند إلى زمر التأثير في الحقول في كتابه في الجبر عام 1895م، إلا أن هذه الطريقة لم تتابع في كتب أخرى إلى عام 1920 - بعد أن أصبحت معالجة إيمي نوثير (*Emmy Noether*) المجردة للجبر مؤثرة في جامعة جوتنجن - حيث طوّر إميل آرتن (1898-1962) (*Emil Artin*) هذه العلاقة بين الزمر والحقول بكثير من التفصيل، وقد أكد آرتن أن الهدف مما أصبح يعرف الآن بمبرهنة جالوا ليس تحديد شروط الحل للمعادلات الجبرية، بل اكتشاف العلاقة بين امتدادات الحقول وزمرة التماثلات الذاتية، لقد فصل آرتن طريقته في محاضرة أعطيت عام 1926م؛ ونشرت مقارنته أول مرة عن طريق ب. ل. فان دير واردن (*B. L. Van der Waerden*) في كتابه الجبر الحديث (*Modern Algebra*) عام 1930م، ثم نشرها آرتن نفسه في ملخص محاضرات في العامين 1938م و 1942م. في الواقع، بقية هذا الكتاب مبنية على تطوير آرتن لمبرهنة جالوا.

إذا كانت  $\{\sigma_i \mid i \in I\}$  مجموعة من التماثلات الذاتية للحقل  $E$ ، فإنّ العناصر في  $E$  التي تعطي  $\{\sigma_i \mid i \in I\}$  أقل قدر من المعلومات هي  $a \in E$  المتروكة ثابتة من كل  $\sigma_i$  حيث  $i \in I$ ، وأول مبرهناتنا الثلاث تقريباً تحوي معظم ما يمكن قوله عن هذه العناصر الثابتة في  $E$ .

لتكن  $\{\sigma_i \mid i \in I\}$  مجموعة من التماثلات الذاتية على الحقل  $E$ ، فتكون المجموعة  $E_{\{\sigma_i\}}$  المؤلفة من العناصر جميعها  $a \in E$  المتروكة ثابتة بكل  $\sigma_i$ ،  $i \in I$ ، حقلاً جزئياً من  $E$ . إذا كانت  $\sigma_i(a) = a$  و  $\sigma_i(b) = b$  لكل  $i \in I$ ، فإنّ:

$$\sigma_i(a \pm b) = \sigma_i(a) \pm \sigma_i(b) = a \pm b$$

$$\sigma_i(ab) = \sigma_i(a)\sigma_i(b) = ab \quad \text{و}$$

لكل  $i \in I$ ، كذلك إذا كانت  $b \neq 0$ ، فإنّ:

$$\sigma_i(a/b) = \sigma_i(a) / \sigma_i(b) = a/b$$

لكل  $i \in I$ ، ولأنّ  $\sigma_i$  تماثل ذاتي، فنحصل على

$$\sigma_i(0) = 0 \quad \text{و} \quad \sigma_i(1) = 1$$

◆ لكل  $i \in I$ ؛ إذن،  $0, 1 \in E_{\{\sigma_i\}}$ ، ما يعني أنّ  $E_{\{\sigma_i\}}$  حقل جزئي من  $E$ .

يسمى الحقل  $E_{\{\sigma_i\}}$  في المبرهنة 11.48 الحقل الثابت لـ  $\{\sigma_i \mid i \in I\}$  (**fixed field**). سوف نشير في حالة التماثل الذاتي الوحيد  $\sigma$ ، إلى  $E_{\{\sigma\}}$  بحقل الثابت بـ  $\sigma$  (**fixed field of  $\sigma$** )

## 12.48 تعريف

ليكن التماثل الذاتي  $\psi_{\sqrt{2}, -\sqrt{2}}$  على  $\mathbb{Q}(\sqrt{2})$  المعطى في المثال 7.48، فإذا كانت  $a, b \in \mathbb{Q}$  فإنّ

## 13.48 مثال

فإنّ  $\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$  و  $a - b\sqrt{2} = a + b\sqrt{2}$ ، إذا وفقط إذا كانت  $b = 0$ ؛ إذن، الحقل الثابت بـ  $\psi_{\sqrt{2}, -\sqrt{2}}$  هو  $\mathbb{Q}$ .



لاحظ أن أي تماثل ذاتي للحقل  $E$  هو بصورة خاصة دالة أحادية وغامرة من  $E$  إلى  $E$ ، أي إنها تبادل على  $E$ . إذا كانت  $\sigma$  و  $\tau$  تماثلين ذاتيين على  $E$ ، فإن التبدلية  $\sigma \tau$  هي كذلك تماثل ذاتي على  $E$ ؛ لأن - وبوجه عام - تركيب تشاكليين يعطي تشاكلاً. هكذا تصنع مبرهنة الزمر المدخل للموضوع.

مجموعة التماثلات الذاتية كلها المعرفة على الحقل  $E$  تكون زمرة بالنسبة إلى عملية تركيب الدوال.

14.48 مبرهنة

ضرب التماثلات الذاتية على  $E$  معرّف بوصفه تركيب الدوال، وهكذا، فإنه تجميعي (إنه ضرب التباديل). التبدلية المحايدة  $i: E \rightarrow E$  المعرفة بالقاعدة  $i(\alpha) = \alpha$  لكل  $\alpha \in E$  تكون تماثلاً ذاتياً على  $E$ ، فإذا كانت  $\sigma$  تماثلاً ذاتياً، فإن التبدلية  $\sigma^{-1}$  هي كذلك تماثل ذاتي؛ إذن، تشكل مجموعة التماثلات الذاتية كلها المعرفة على  $E$  زمرة جزئية من  $S_E$ ، زمرة التباديل جميعها المعرفة على  $E$  المعطاة في المبرهنة 5.8.

البرهان

ليكن  $E$  حقلاً، وليكن  $F$  حقلاً جزئياً من  $E$ . تشكل المجموعة  $G(E/F)$  المكونة من التماثلات الذاتية جميعها على  $E$ ، التي تترك  $F$  ثابتة - زمرة جزئية من زمرة التماثلات الذاتية جميعها على  $E$ . إضافة إلى ذلك  $F \leq G(E/F)$ .

15.48 مبرهنة

إذا كانت  $\sigma, \tau \in G(E/F)$  و  $a \in F$ ، فإن

البرهان

$$(\sigma \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a$$

إذن،  $\sigma \tau \in G(E/F)$ ، بالطبع، فإن التماثل الذاتي المحايد  $i$  عنصر في  $G(E/F)$ . وكذلك، فإن كان  $\sigma(a) = a$  حيث  $a \in F$ ، فإن  $a = \sigma^{-1}(a)$ ؛ إذن،  $\sigma \in G(E/F)$  يؤدي إلى  $\sigma^{-1} \in G(E/F)$ .

إذن،  $G(E/F)$  زمرة جزئية من زمرة التماثلات الذاتية على  $E$ .

لأن كل عنصر في  $F$  يترك ثابتاً بكل عنصر في  $G(E/F)$ ، فينتج مباشرة أن الحقل  $E_{G(E/F)}$  المكوّن من عناصر  $E$  جميعها المتروكة ثابتة بـ  $G(E/F)$  تحوي  $F$ .

تسمى الزمرة  $G(E/F)$  في المبرهنة السابقة زمرة التماثلات الذاتية على  $E$  التي تترك  $F$  ثابتاً (group of automorphisms of  $E$  leaving  $F$  fixed)، أو باختصار زمرة  $E$  على  $F$  (group of  $E$  over  $F$ ).

16.48 تعريف

لا تفكر في  $E/F$  في الرمز  $G(E/F)$  بوصفه مؤشراً على فضاء خارج قسمة من نوع ما، بل بالأحرى إنه يعني أن  $E$  حقل امتداد للحقل  $F$ .

ستوضّح الأفكار المحتواة في المبرهنات الثلاث السابقة في المثال الآتي، ويجب أن تدرس هذا المثال بعناية.

■

## 17.48 مثال

افترض الحقل  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . أظهر المثال 9.31 أن  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ ، وإذا نظرنا إلى  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  على الصورة  $(\mathbb{Q}(\sqrt{3}))(\sqrt{2})$ ، فإن تماثل الترافق  $\psi_{\sqrt{2}, -\sqrt{2}}$  من المبرهنة 3.48 المعرف بـ

$$\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$$

حيث  $a, b \in \mathbb{Q}(\sqrt{3})$  يشكل تماثلاً ذاتياً على  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ، ويترك الحقل  $\mathbb{Q}(\sqrt{3})$  ثابتاً. وبالمثل، فإن التماثل الذاتي  $\psi_{\sqrt{3}, -\sqrt{3}}$  على  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  يترك الحقل  $\mathbb{Q}(\sqrt{2})$  ثابتاً، ولأن ضرب تماثلين ذاتيين يعطي تماثلاً ذاتياً، فيمكن اعتبار  $\psi_{\sqrt{2}, -\sqrt{2}}\psi_{\sqrt{3}, -\sqrt{3}}$  الذي يحرك كلاً من  $\sqrt{2}$  و  $\sqrt{3}$ ، أي لا يثبت أيّاً من العددين.

ليكن تماثل العنصر المحايد  $l$

$$\sigma_1 = \psi_{\sqrt{2}, -\sqrt{2}}$$

$$\sigma_2 = \psi_{\sqrt{3}, -\sqrt{3}}$$

$$\sigma_3 = \psi_{\sqrt{2}, -\sqrt{2}}\psi_{\sqrt{3}, -\sqrt{3}}$$

لزمرة التماثلات الذاتية كلها على  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  حقلاً ثابتاً، فبحسب المبرهنة 11.48، يجب أن يحوي هذا الحقل  $\mathbb{Q}$ : لأن كل تماثل ذاتي يجب أن يترك 1 ثابتاً، ويؤدي هذا إلى أن يكون الحقل الجزئي الأولي ثابتاً. أساس  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  على  $\mathbb{Q}$  هو  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$  لأن

$\sigma_1(\sqrt{2}) = -\sqrt{2}$ ،  $\sigma_1(\sqrt{6}) = -\sqrt{6}$ ،  $\sigma_2(\sqrt{3}) = -\sqrt{3}$ ،  $\sigma_2(\sqrt{6}) = -\sqrt{6}$ ، فإننا نرى أن  $\mathbb{Q}$  هو بالضبط الحقل الثابت لـ  $\{l, \sigma_1, \sigma_2, \sigma_3\}$ ، ومن السهل التحقق أن  $G = \{l, \sigma_1, \sigma_2, \sigma_3\}$  تشكل زمرة بالنسبة إلى ضرب التماثلات الذاتية (تركيب الدوال). جدول الزمرة  $G$  معطى في الجدول 18.48، على سبيل المثال:

$$\sigma_1\sigma_3 = \psi_{\sqrt{2}, -\sqrt{2}}\left(\psi_{\sqrt{2}, -\sqrt{2}}\psi_{\sqrt{3}, -\sqrt{3}}\right) = \psi_{\sqrt{3}, -\sqrt{3}} = \sigma_2$$

الزمرة  $G$  تماثل زمرة كلاين الرباعية (*Klein 4-group*)، ويمكننا إثبات أن  $G$  هي كامل الزمرة

$\mathbb{G}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ : لأن كل تماثل ذاتي  $\tau$  على  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  يقرب  $\sqrt{2}$  بـ  $\pm\sqrt{2}$  وبحسب النتيجة 5.48. وبالمثل يقرب  $\tau$   $\sqrt{3}$  بـ  $\pm\sqrt{3}$ ، ولأن  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$  أساس لـ  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  على  $\mathbb{Q}$ ، فإن أي تماثل ذاتي على  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  ويبقى  $\mathbb{Q}$  ثابتاً، يحدد بقيمه على  $\sqrt{2}$  و  $\sqrt{3}$ .

## الجدول 18.48

|            |            |            |            |            |
|------------|------------|------------|------------|------------|
|            | $l$        | $\sigma_1$ | $\sigma_2$ | $\sigma_3$ |
| $l$        | $l$        | $\sigma_1$ | $\sigma_2$ | $\sigma_3$ |
| $\sigma_1$ | $\sigma_1$ | $l$        | $\sigma_3$ | $\sigma_2$ |
| $\sigma_2$ | $\sigma_2$ | $\sigma_3$ | $l$        | $\sigma_1$ |
| $\sigma_3$ | $\sigma_3$ | $\sigma_2$ | $\sigma_1$ | $l$        |

الآن،  $i, \sigma_1, \sigma_2, \sigma_3$  تعطي التراكيب جميعها الممكنة لصور  $\sqrt{2}$  و  $\sqrt{3}$ ، وإذن، فهي التماثلات الذاتية كلها الممكنة على  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ .

لاحظ أنّ  $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$  من الرتبة 4، و  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}] = 4$  فهذه ليست مصادفة، بل هي حالة من الظاهرة العامة، كما سنرى لاحقاً.

### التماثل الذاتي لفروبينس

ليكن  $F$  حقلاً منتهياً، سنرى لاحقاً أنّ زمرة التماثلات الذاتية على  $F$  جميعها دورية. الآن، وبحسب التعريف، فإنّ للزمرة الدورية مولداً، ويمكن أن تكون لها مولدات عدة، بالنسبة إلى الزمرة الدورية المجردة، ولا توجد طريقة لجعل أحد المولدات أكثر أهمية من الأخرى. على أيّ حال، بالنسبة إلى الزمرة الدورية للتماثلات الذاتية جميعها لحقل منته، فيوجد مولد قانوني (طبيعي) هو التماثل الذاتي لفروبينس (بصورة كلاسيكية تعويض فروبينس). هذه الحقيقة ذات أهمية كبيرة في بعض العمل المتقدم في الجبر. تقدم المبرهنة الآتية التماثل الذاتي لفروبينس.

ليكن  $F$  حقلاً منتهياً ذا مميز  $p$ . تكون الدالة  $\sigma_p: F \rightarrow F$  المعرفة بـ  $\sigma_p(a) = a^p$  لكل  $a \in F$  تماثلاً ذاتياً - التماثل الذاتي لفروبينس - على  $F$ . وكذلك فإنّ  $F_{\{op\}} \simeq \mathbb{Z}_p$ .

19.48 مبرهنة

لتكن  $a, b \in F$ . خذ  $n = 1$  في التمهيدية 9.33، فسنرى أنّ  $(a + b)^p = a^p + b^p$  إذن:

$$\sigma_p(a + b) = (a + b)^p = a^p + b^p = \sigma_p(a) + \sigma_p(b)$$

البرهان

وبالطبع:

$$\sigma_p(ab) = (ab)^p = a^p b^p = \sigma_p(a)\sigma_p(b),$$

إذن،  $\sigma_p$  على الأقل تشاكل، فإذا كان  $\sigma_p(a) = 0$ ، فإنّ  $a^p = 0$ ، وهكذا  $a = 0$ ؛ إذن، نواة  $\sigma_p$  هي  $\{0\}$ ، ما يعني أنّ  $\sigma_p$  دالة أحادية. أخيراً؛ لأنّ  $F$  منتهية، فإنّ  $\sigma_p$  وباستخدام العد غامرة، وهكذا فإنّ  $\sigma_p$  تماثل ذاتي على  $F$ .

يجب أن يكون الحقل الأولي  $\mathbb{Z}_p$  (تبعاً للتماثل) محتوياً في  $F$ ؛ لأنّ  $F$  ذو مميز  $p$ . وإذا كانت  $c \in \mathbb{Z}_p$ ، فإنّ  $\sigma_p(c) = c^p = c$  بحسب مبرهنة فيرما (انظر النتيجة 2.20)؛ إذن، كثيرة الحدود  $x^p - x$  لها  $p$  من الأصفار في  $F$ ، عناصر  $\mathbb{Z}_p$  تحديداً، وبحسب النتيجة 5.23، فإنّ أيّ كثيرة حدود من الدرجة  $n$  على حقل لها على الأكثر  $n$  من الأصفار في الحقل. لأنّ العناصر الثابتة بـ  $\sigma_p$  هي تحديداً أصفار  $x^p - x$  في  $F$ ، نرى أنّ

$$\mathbb{Z}_p = F_{\{op\}}$$

يخطئ الطالب الساذج أحياناً عندما يقول:  $(a+b)^n = a^n + b^n$  نرى هنا أنّ أسس الطالب الساذج،  $(a+b)^p = a^p + b^p$  مع الأس  $p$ ، متحققة في حقل  $F$  ذي مميز  $p$ .

## ■ تمارين 48

## حسابات

في التمارين من 1 إلى 8، أوجد المرافقات جميعها في  $\mathbb{C}$  للأعداد المعطاة على الحقول:

1.  $\sqrt{2}$  على  $\mathbb{Q}$
2.  $\sqrt{2}$  على  $\mathbb{R}$
3.  $3 + \sqrt{2}$  على  $\mathbb{Q}$
4.  $\sqrt{2} - \sqrt{3}$  على  $\mathbb{Q}$
5.  $\sqrt{2} + i$  على  $\mathbb{Q}$
6.  $\sqrt{2} + i$  على  $\mathbb{R}$
7.  $\sqrt{1 + \sqrt{2}}$  على  $\mathbb{Q}$
8.  $\sqrt{1 + \sqrt{2}}$  على  $\mathbb{Q}(\sqrt{2})$

في التمارين من 9 إلى 14، سنفترض الحقل  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ ، من الممكن إثبات أن  $[E : \mathbb{Q}] = 8$  باستخدام المصطلحات في المبرهنة 3.48، ينتج لدينا تماثلات الترافق الآتية (التي هي هنا تماثلات ذاتية على  $E$ ):

$$\begin{aligned}\psi_{\sqrt{2}, -\sqrt{2}} &: (\mathbb{Q}(\sqrt{3}, \sqrt{5}))(\sqrt{2}) \rightarrow (\mathbb{Q}(\sqrt{3}, \sqrt{5}))(-\sqrt{2}), \\ \psi_{\sqrt{3}, -\sqrt{3}} &: (\mathbb{Q}(\sqrt{2}, \sqrt{5}))(\sqrt{3}) \rightarrow (\mathbb{Q}(\sqrt{2}, \sqrt{5}))(-\sqrt{3}), \\ \psi_{\sqrt{5}, -\sqrt{5}} &: (\mathbb{Q}(\sqrt{2}, \sqrt{3}))(\sqrt{5}) \rightarrow (\mathbb{Q}(\sqrt{2}, \sqrt{3}))(-\sqrt{5}).\end{aligned}$$

باستخدام ترميز مختصر، لتكن  $\tau_5 = \psi_{\sqrt{5}, -\sqrt{5}}$  و  $\tau_2 = \psi_{\sqrt{2}, -\sqrt{2}}$ ،  $\tau_3 = \psi_{\sqrt{3}, -\sqrt{3}}$  احسب العنصر المشار إليه في  $E$ .

9.  $\tau_2(\sqrt{3})$
10.  $\tau_2(\sqrt{2} + \sqrt{5})$
11.  $(\tau_3 \tau_2)(\sqrt{2} + 3\sqrt{5})$
12.  $(\tau_5 \tau_3)\left(\frac{\sqrt{2} - 3\sqrt{5}}{2\sqrt{3} - \sqrt{2}}\right)$
13.  $(\tau_5^2 \tau_3 \tau_2)(\sqrt{2} + \sqrt{45})$
14.  $\tau_3[\tau_5(\sqrt{2} - \sqrt{3} + (\tau_2 \tau_5)(\sqrt{30}))]$
15. بالرجوع إلى المثال 17.48، أوجد الحقول الثابتة في  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ .

$$\text{أ. } E_{\{\sigma_1, \sigma_3\}} \quad \text{ب. } E_{\{\sigma_3\}} \quad \text{ج. } E_{\{\sigma_2, \sigma_3\}}$$

في التمارين من 16 إلى 21، ارجع إلى تعليمات التمارين من 9 إلى 14 وأوجد الحقل الثابت لكل تماثل ذاتي أو مجموعة تماثلات ذاتية على  $E$ .

16.  $\tau_3$
17.  $\tau_3^2$
18.  $\{\tau_2, \tau_3\}$
19.  $\tau_5 \tau_2$
20.  $\tau_5 \tau_3 \tau_2$
21.  $\{\tau_2, \tau_3, \tau_5\}$

22. ارجع إلى تعليمات التمارين من 9 إلى 14 في هذا التمرين.  
 أ. أثبت أن التماثلات الذاتية جميعها  $\tau_2, \tau_3$ ، و  $\tau_3$  من الرتبة 2 في  $G(E/\mathbb{Q})$ . (تذكر ماذا تعني رتبة العنصر في الزمرة).  
 ب. أوجد الزمرة الجزئية  $H$  من  $G(E/\mathbb{Q})$  المولدة من العناصر  $\tau_2, \tau_3$ ، و  $\tau_3$ ، وأوجد جدول هذه الزمرة. [مساعدة: يوجد ثمانية عناصر].  
 ج. تمامًا كما فعل في المثال 17.48، ناقش كيف أن  $H$  في الفرع (ب) هي كل الزمرة  $G(E/\mathbb{Q})$ .

### مفاهيم

- في التمرينين 23 و24، صحّح تعريف الحدّ المكتوب بخط مائل دون الرجوع إلى الكتاب -إذا كانت هناك حاجة للتصحيح- بحيث يكون بصيغة قابلة للنشر.  
 23. يكون العنصران  $\alpha$  و  $\beta$ ، في الامتداد الجبري  $E$  على الحقل  $F$  مترافقين على  $F$ ، إذا وفقط إذا كانا صفرين لكثيرة الحدود نفسها  $f(x)$  في  $F[x]$ .  
 24. يكون العنصران  $\alpha$  و  $\beta$ ، في الامتداد الجبري  $E$  على الحقل  $F$  مترافقين على  $F$ ، إذا وفقط إذا كان لتساكلي التعويض  $\phi_\alpha: F[x] \rightarrow E$  و  $\phi_\beta: F[x] \rightarrow E$  النواة نفسها.  
 25. الحقلان  $(\sqrt{2})$  و  $(3+\sqrt{2})$  متساويان بالطبع. لتكن  $\alpha = 3 + \sqrt{2}$ .  
 أ. أوجد مرافق  $\alpha \neq \beta$  على  $\mathbb{Q}$ .  
 ب. بالرجوع إلى الفرع (أ)، قارن بين تماثل الترافق الذاتي  $\sigma_{\sqrt{2}, -\sqrt{2}}$  على  $(\sqrt{2})$  و تماثل الترافق الذاتي  $\psi_{\alpha, \beta}$ .  
 26. أوجد قيمة تماثل فروبينس الذاتي  $\sigma_2$  على كل عنصر في الحقل المنتهي من أربعة عناصر المعطى في المثال 19.29. أوجد الحقل الثابت لـ  $\sigma_2$ .  
 27. أوجد قيمة تماثل فروبينس الذاتي  $\sigma_3$  على كل عنصر في الحقل المنتهي من تسعة عناصر المعطى في التمرين 18 في الفصل 29. أوجد الحقل الثابت لـ  $\sigma_3$ .  
 28. ليكن  $F$  حقلًا ذا مميز  $p \neq 0$ . أعط مثالًا يبين أن الدالة  $\sigma_p: F \rightarrow F$  المعرفة بـ  $\sigma_p(a) = a^p$ ، حيث  $a \in F$  ليست بالضرورة تماثلًا ذاتيًا إذا كان  $\bar{F}$  غير منتهٍ. ما الخطأ الذي يمكن أن يحدث؟  
 29. ضع إشارة صح أو إشارة خطأ:

- أ. لكل  $\alpha, \beta \in E$ ، يوجد دائمًا تماثل ذاتي على  $E$  يربط  $\alpha$  بـ  $\beta$ .  
 ب. لكل  $\alpha, \beta$  جبريان على الحقل  $F$ ، يوجد دائمًا تماثل من  $F(\alpha)$  غامر لـ  $F(\beta)$ .  
 ج. لكل  $\alpha, \beta$  جبريان ومترافقان على الحقل  $F$ ، يوجد دائمًا تماثل من  $F(\alpha)$  غامر لـ  $F(\beta)$ .  
 د. كل تماثل ذاتي لأي حقل  $E$ ، يترك كل عنصر في الحقل الجزئي الأولي لـ  $E$  ثابتًا.  
 هـ. كل تماثل ذاتي لأي حقل  $E$ ، يترك عددًا لا نهائيًا من عناصر  $E$  ثابتة.  
 و. كل تماثل ذاتي لأي حقل  $E$ ، يترك على الأقل عنصرين ثابتين في  $E$ .  
 ز. كل تماثل ذاتي لأي حقل  $E$  ذا مميز 0، يترك عددًا لا نهائيًا من عناصر  $E$  ثابتة.  
 ح. التماثلات الذاتية كلها لحقل  $E$  تشكل زمرة بالنسبة إلى عملية تركيب الدوال.  
 ط. مجموعة عناصر حقل  $E$  التي تركت ثابتة بتماثل ذاتي واحد على  $E$  تشكل حقلًا جزئيًا من  $E$ .  
 ي. للحقول  $G(K/E) \leq G(K/F)$ ،  $F \leq E \leq K$ .

براهين مختصرة

30. أعط برهاناً مختصراً من جملة واحدة لجزء «إذا كان» في المبرهنة 3.48.

31. أعط برهاناً مختصراً من جملة واحدة لجزء «و فقط إذا كان» في المبرهنة 3.48.

براهين

32. لتكن  $\alpha$  جبرية من الدرجة  $n$  على  $F$ . أثبت - باستخدام النتيجة 5.48 - أنه يوجد على الأكثر  $n$  من التماثلات المختلفة من  $F(\alpha)$  إلى حقل جزئي من  $\overline{F}$  تاركة  $F$  ثابتة.33. ليكن  $F(\alpha_1, \dots, \alpha_n)$  امتداداً للحقل  $F$ . أثبت أن أي تماثل ذاتي  $\sigma$  على  $F(\alpha_1, \dots, \alpha_n)$  ويترك  $F$  ثابتة، يتحدد تماماً بأحد  $n$  قيمة لـ  $\sigma(\alpha_i)$ .34. ليكن  $E$  امتداداً جبرياً للحقل  $F$ ، ولتكن  $\sigma$  تماثلاً ذاتياً على  $E$  ويترك  $F$  ثابتة. لتكن  $\alpha \in E$ . أثبت أن  $\sigma$  تنتج تبديل على أصفار  $(\alpha, F)$  الموجودة في  $E$ .35. ليكن  $E$  امتداداً جبرياً للحقل  $F$ . لتكن  $S = \{\sigma_i \mid i \in I\}$  مجموعة من التماثلات الذاتية على  $E$ ، بحيث إن كل  $\sigma_i$  تترك عناصر  $F$  كلها ثابتة. أثبت أنه إذا كانت  $S$  تولد زمرة جزئية  $H$  من  $G(E/F)$ ، فإن  $E_S = E_H$ .

36. رأينا في النتيجة 17.23 أن كثيرة الحدود الدورية:

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

غير مختزلة على  $\mathbb{Q}$  لكل عدد أولي  $p$ . ليكن  $\zeta$  صفراً لـ  $\Phi_p(x)$ ، وافترض الحقل  $\mathbb{Q}(\zeta)$ .أ. أثبت أن  $\zeta^{-1}, \zeta^2, \dots, \zeta^{p-1}$  أصفار مختلفة لـ  $\Phi_p(x)$ ، واستنتج أنها أصفار  $\Phi_p(x)$  جميعها.ب. استنتج من النتيجة 5.48 ومن الفرع (أ) في هذا التمرين أن  $G(\mathbb{Q}(\zeta)/\mathbb{Q})$  تبديلية من الرتبة  $p-1$ .ج. أثبت أن  $\mathbb{Q}$  هو الحقل الثابت لـ  $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ . [مساعدة: أثبت أن  $\{\zeta, \zeta^2, \dots, \zeta^{p-1}\}$  أساس لـ  $\mathbb{Q}(\zeta)$  على  $\mathbb{Q}$ ، ثم عين أياً من التراكيب الخطية لـ  $\zeta, \zeta^2, \dots, \zeta^{p-1}$  تبقى ثابتة مع عناصر  $G(\mathbb{Q}(\zeta)/\mathbb{Q})$  كلها.37. تصف المبرهنة 3.48 تماثلات الترافق في حال كانت  $\alpha$  و  $\beta$  عناصر جبرية مترافقة على  $F$ . هل يوجد تماثلمشابه بين  $F(\alpha)$  و  $F(\beta)$  عندما يكون كل من  $\alpha$  و  $\beta$  متساميين على  $F$ ؟38. ليكن  $F$  حقلاً، وليكن  $x$  أي غير معين على  $F$ . أوجد التماثلات الذاتية على  $F(x)$  كلها التي تترك  $F$  ثابتة من خلال وصف قيمها على  $x$ .

39. أثبت سلسلة المبرهنات الآتية:

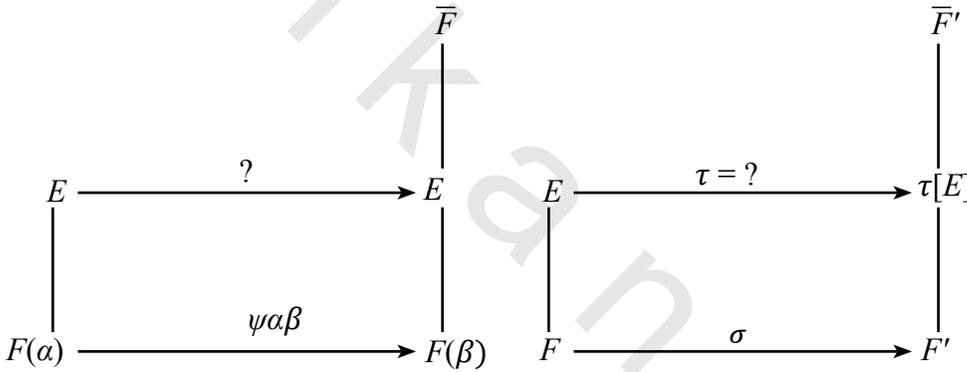
أ. يحمل التماثل الذاتي على  $E$  مربعات عناصر في  $E$  إلى عناصر هي مربعات لعناصر في  $E$ .ب. يحمل التماثل الذاتي على  $\mathbb{R}$  الأعداد الموجبة إلى أعداد موجبة.ج. إذا كانت  $\sigma$  تماثلاً ذاتياً على  $\mathbb{R}$  و  $a < b$ ، حيث  $a, b \in \mathbb{R}$ ، فإن  $\sigma(a) < \sigma(b)$ .د. التماثل الذاتي الوحيد على  $\mathbb{R}$  هو التماثل الذاتي المحايد.

The Isomorphism Extension Theorem مبرهنة تمديد التماثل

مبرهنة التمديد

لنكمل دراسة التماثلات الذاتية للحقل. في هذا الفصل الذي يليه، سنكون مهتمين بإثبات وجود تماثلات ذاتية على حقل  $E$  وعددها.

افترض أن  $E$  امتداد جبري لـ  $F$ ، ونريد أن نجد بعض التماثلات على  $E$ . نعرف من المبرهنة 3.48 أنه إذا كانت  $\alpha, \beta \in E$  مترافقتين على  $F$ ، فإنه يوجد تماثل  $\psi_{\alpha, \beta}$  من  $F(\alpha)$  غامر لـ  $F(\beta)$ . بالطبع  $\alpha, \beta \in E$  يؤدي إلى أن كلا  $F(\alpha) \leq E$  و  $F(\beta) \leq E$ . من الطبيعي أن نتساءل ما إذا كان مجال تعريف  $\psi_{\alpha, \beta}$  يمكن تكبيره من  $F(\alpha)$  إلى حقل أكبر، وربما كل  $E$ ، وما إذا أدى هذا إلى تماثل ذاتي على  $E$ . رسم بياني لهذه الدوال في هذه الحالة معروض في الشكل 1.49. عوضاً عن الحديث عن «تكبير مجال تعريف  $\psi_{\alpha, \beta}$ »



الشكل 1.49

الشكل 2.49

من المؤلف الحديث عن «تمديد الدالة  $\psi_{\alpha, \beta}$  إلى الدالة  $\tau$ »، التي هي دالة معرفة على  $E$  كلها. تذكر أننا دائماً نفترض أن الامتدادات الجبرية قيد الدراسة جميعها محتواة في إغلاق جبري محدد  $\bar{F}$  لـ  $F$ . تثبت مبرهنة تمديد التماثل أن الدالة  $\psi_{\alpha, \beta}$  يمكن تمديدها دائماً إلى تماثل من  $E$  إلى حقل جزئي من  $\bar{F}$ . والسؤال: ما إذا كان هذا التمديد يعطي تماثلاً ذاتياً على  $E$ ، بمعنى تربط  $E$  بنفسها؟ هو سؤال سندرسه في الفصل 50.

تضمن مبرهنة التمديد هذه وباستخدام تماثل الترافق  $\psi_{\alpha, \beta}$  وجود كثير من دوال التماثل، على الأقل لكثير من الحقول، إذ إن مبرهنات التمديد مهمة جداً في الرياضيات، وخاصة في الجبر والطبولوجيا.

لنأخذ نظرة أكثر شمولاً لهذه الحالة. افترض أن  $E$  امتداد جبري للحقل  $F$ ، وأن لدينا تماثل  $\sigma$  من  $F$  غامراً للحقل  $F'$ ، وليكن  $\bar{F}$  الإغلاق الجبري لـ  $F$ . نرغب في تمديد  $\sigma$  إلى تماثل  $\tau$  من  $E$  إلى حقل جزئي من  $\bar{F}$ ، حيث يعرض هذا الوضع ببساطة في الشكل 2.49، سنختار  $\alpha \in E$  ولكن ليست في  $F$ ، ونحاول تمديد  $\sigma$  إلى  $F(\alpha)$ . إذا كان:

$$p(x) = \text{irr}(\alpha, F) = a_0 + a_1x + \dots + a_nx^n,$$

ليكن  $\beta$  صفرًا في  $\bar{F}$  لـ

$$q(x) = \sigma(a_0) + \sigma(a_1)x + \dots + \sigma(a_n)x^n.$$

هنا  $q(x) \in F[x]$ ، نعلم أن  $q(x)$  غير مختزلة في  $F[x]$ ؛ لأن  $\sigma$  تماثل، فيبدو منطقيًا أنه يمكن ربط  $F(\alpha)$  بتماثل غامر مع  $F(\beta)$  بدالة تمديد  $\sigma$  وتربط  $\alpha$  بـ  $\beta$ ، هذه ليست تمامًا المبرهنة 3.48، ولكنها قريبة منها، وقد غُيّرت أسماء بعض العناصر باستخدام  $\sigma$ ، فإذا كانت  $F(\alpha) = E$  فقد انتهينا، أما إذا كانت  $F(\alpha) \neq E$ ، فعلينا أن نجد عنصرًا آخر في  $E$  وليس في  $F(\alpha)$ ، ونكمل العملية، إنه موقف شبيه جدًا ببناء الإغلاق الجبري  $\overline{F} \downarrow F$ ، ومرة أخرى المشكلة بوجه عام، عندما لا يكون  $E$  امتدادًا منتهيًا، فالعملية يمكن أن تكرر (من المحتمل الكثير) عددًا لا نهائيًا من المرات، وسنحتاج إلى بدهية زورن لمعالجتها، ولهذا السبب، سنؤجل إثبات المبرهنة 3.49 إلى نهاية هذا الفصل.

(مبرهنة تمديد التماثل): ليكن  $E$  امتدادًا جبريًا للحقل  $F$ ، ولتكن  $\sigma$  تماثلًا من  $F$  وبصورة غامرة إلى الحقل  $F'$ . ليكن  $\overline{F}'$  الإغلاق الجبري لـ  $F'$ .

3.49 مبرهنة

يمكن تمديد  $\sigma$  إلى تماثل  $\tau$  من  $E$  إلى حقل جزئي من  $\overline{F}'$ ، بحيث  $\tau(a) = \sigma(a)$  لكل  $a \in F$ .

وبوصفها نتيجة إثبات، سوف نجد تمديدًا لأحد تماثلات الترافق  $\psi_{\alpha,\beta}$  كما ذكر في بداية هذا الفصل.

إذا كان  $\overline{F} \geq E$  امتدادًا جبريًا لـ  $F$  و  $\alpha, \beta \in E$  مترافقة على  $F$ ، فيمكن تمديد تماثل الترافق  $\psi_{\alpha,\beta}: F(\alpha) \rightarrow F(\beta)$  - المعطى في المبرهنة 3.48 - إلى تماثل من  $E$  إلى حقل جزئي من  $\overline{F}$ .

4.49 نتيجة

ينتج إثبات هذه النتيجة مباشرة من المبرهنة 3.49، إذا استبدلنا في نص المبرهنة  $F(\alpha)$  بـ  $F$ ، و  $F(\beta)$  بـ  $\overline{F}$  و  $\overline{F}'$  بـ  $\overline{F}$ .

البرهان

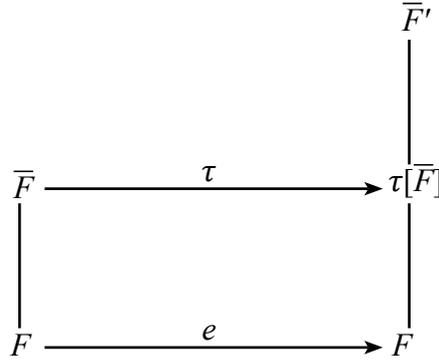
بوصفها نتيجة أخرى، يمكننا إثبات - كما وعدنا سابقًا - أن الإغلاق الجبري لـ  $F$  وحيد، تبعًا لتماثل يترك  $F$  ثابتة.

ليكن  $\overline{F}$  و  $\overline{F}'$  إغلاقين جبريين لـ  $F$ . إن  $\overline{F}$  يماثل  $\overline{F}'$  بتأثير تماثل يترك كل عنصر في  $F$  ثابتًا.

5.49 نتيجة

بحسب المبرهنة 3.49 فإن التماثل المحايد من  $F$  إلى  $F$  يمكن تمديده إلى تماثل  $\tau$  يربط  $\overline{F}$  بحقل جزئي من  $\overline{F}'$  ويترك  $F$  ثابتًا. (انظر الشكل 6.49) نحتاج فقط إلى إثبات أن  $\tau$  غامر لـ  $\overline{F}'$ ، ولكن بحسب المبرهنة 3.49، فإن الدالة يمكن تمديدها إلى تماثل من  $\overline{F}'$  إلى حقل جزئي من  $\overline{F}$ ، ولأن  $\tau^{-1}$  بالتأكيد غامرة لـ  $\overline{F}$ ، فيجب أن تكون  $\tau[\overline{F}] = \overline{F}'$ .

البرهان



الشكل 6.49

دليل امتداد الحقل

بعد مناقشتنا لسؤال الوجود، ننتقل الآن للسؤال عن العدد. لامتداد منته  $E$  للحقل  $F$ ، نود أن نحصي عدد التماثلات من  $E$  إلى حقل جزئي من  $\bar{F}$  التي تترك  $F$  ثابتة، سنثبت وجود عدد منته من التماثلات، ولأن أن كل تماثل ذاتي في  $G(E/F)$  هو أحد هذه التماثلات، فإن إحصاء هذه التماثلات سيتضمن التماثلات الذاتية، وقد أثبت المثال 17.48 أن  $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$

يحتوي أربعة عناصر و  $4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ ، فعلى الرغم من أن هذه المعادلة ليست دائماً صحيحة، إلا أنها صحيحة في حالة مهمة جداً، وتأخذ المبرهنة الآتية أول خطوة كبيرة في برهان ذلك، وسنذكر نص المبرهنة بصورة أكثر عمومية ما سنحتاج إليه، ولكنها لن تجعل البرهان أكثر صعوبة.

7.49 مبرهنة

ليكن  $E$  امتداداً منتهياً للحقل  $F$ ، ولتكن  $\sigma$  تماثلاً من  $F$  إلى حقل جزئي من  $F'$ ، وليكن  $\bar{F}'$  الإغلاق الجبري لـ  $F'$ . إن عدد التمديدات لـ  $\sigma$  إلى تماثل  $\tau$  من  $E$  إلى حقل جزئي من  $\bar{F}'$  منته ومستقل عن  $F'$ ،  $\bar{F}'$  و  $\sigma$ . بمعنى أن عدد التمديدات يحدد تماماً من الحقلين  $E$  و  $F'$ ؛ فهو جوهري لهما.

البرهان

ربما يساعدنا الرسم في الشكل 8.49 على تتبع الإنشاء الذي سنصنعه، إذ إن هذا الرسم يصنع كما يأتي: افترض تماثلين

$$\sigma_2 : F \xrightarrow{\text{غامر}} F'_2, \quad \sigma_1 : F \xrightarrow{\text{غامر}} F'_1,$$

حيث  $\bar{F}'_2$  و  $\bar{F}'_1$  إغلاقان جبريان لـ  $F'_2$  و  $F'_1$  على الترتيب. الآن  $\sigma_2 \sigma_1^{-1}$  تماثل من  $F'_1$  غامر لـ  $F'_2$ ؛ إذن، وبحسب المبرهنة 3.49 والنتيجة 5.49 يوجد تماثل

$$\lambda : \bar{F}'_1 \xrightarrow{\text{غامر}} \bar{F}'_2$$

يمدد التماثل  $\sigma_2 \sigma_1^{-1} : F_1' \xrightarrow{\text{غامر}} F_2'$ ، وبالرجوع إلى الشكل 8.49 ومطابقة كل من  $\tau_1 : E \rightarrow \overline{F}_1'$

التي تمدد  $\sigma_1$  نحصل على تماثل  $\tau_2 : E \rightarrow \overline{F}_2'$

بالبدء بـ  $E$  والذهاب أولاً إلى اليسار، ثم إلى أعلى، ثم إلى اليمين. وبالكتابة جبرياً

$$\tau_2(\alpha) = (\lambda \tau_1)(\alpha)$$

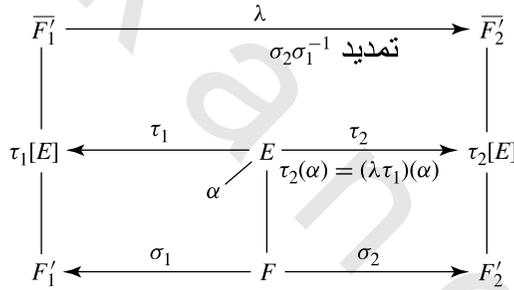
حيث  $\alpha \in E$ ، واضح أنّ  $\tau_2$  تمدد  $\sigma_2$ ، كان بإمكاننا البدء بـ  $\tau_2$  واستعادة  $\tau_1$  بتعريف

$$\tau_1(\alpha) = (\lambda^{-1} \tau_2)(\alpha),$$

أي بالمتابعة من الجهة الأخرى للرسم، يمكن إثبات أنّ المطابقة بين  $\tau_1 : E \rightarrow \overline{F}_1'$

و  $\tau_2 : E \rightarrow \overline{F}_2'$  أحادية، ومن وجهة هذا التقابل الأحادي الغامر، فإنّ عدد  $\tau$  الممددة لـ  $\sigma$  مستقل عن  $F'$ ،  $\overline{F}'$  و  $\sigma$ .

يُستنتج أنّ عدد الدوال الممددة لـ  $\sigma$  منته من حقيقة أنّ  $E$  امتداد منته لـ  $F$ ،  $E = F(\alpha_1, \dots, \alpha_n)$ ، حيث  $\alpha_1, \dots, \alpha_n \in E$  وبحسب المبرهنة 11.31.



الشكل 8.49

يوجد عدد منته من الاحتمالات المرشحة بوصفها صوراً لـ  $\tau(\alpha_i)$  في  $F'$ ؛ لذلك، إذا كان

$$\text{irr}(\alpha_i, F) = a_{i_0} + a_{i_1}x + \dots + a_{i_{m_i}}x^{m_i}$$

حيث  $a_{ik} \in F$ ، فإنّ  $\tau(\alpha_i)$  يجب أن يكون أحد الأصفار لـ  $\overline{F}'$

$$. [\sigma(a_{i_0}) + \sigma(a_{i_1})x + \dots + \sigma(a_{i_{m_i}})x^{m_i}] \in F'[x]$$

◆

ليكن  $E$  امتداداً منتهياً للحقل  $F$ ، فيسمى عدد التماثلات من  $E$  إلى حقل جزئي من  $\overline{F}$  التي تترك  $F$

ثابتة، دليل  $\{E : F\}$  على  $F$ .  $F$  (index  $\{E : F\}$  of  $E$  over  $F$ )

9.49 تعريف

إذا كان  $F \leq E \leq K$ ، حيث الحقل  $K$  امتداد منته للحقل  $F$ ، فإنّ  $\{K : F\} = \{K : E\} \{E : F\}$ .

10.49 نتيجة

ينتج من المبرهنة 7.49 أنّ كلاً من ألد  $\{E : F\}$  تماثل  $\tau_i$  من  $E$  إلى حقل جزئي من  $\overline{F}$  وتترك  $F$

البرهان:

◆

ثابتة، لها  $\{K : F\}$  من التمديدات إلى تماثلات من  $K$  إلى حقل جزئي من  $\overline{F}$ .

في الحقيقة، كانت النتيجة السابقة هي الشيء الرئيس الذي نسعى إليه، لاحظ أنها تُعد شيئاً، فلا تقلل من قدر أي نتيجة مثلها، حتى لو كان اسمها "نتيجة".

سنثبت في الفصل 51 أنه ما لم يكن  $F$  حقلاً غير منته ذا مميز  $p \neq 0$ ، فإنه دائماً يكون  $[E : F] = \{E : F\}$  لكل امتداد منته  $E \mid F$ . وفي حالة  $E = F(\alpha)$  فإن  $\{E : F\} = \{F(\alpha) : F\}$  تمديد للدالة المحايدة  $i: F \rightarrow F$ ، التي تربط  $F(\alpha)$  بحقل جزئي من  $\bar{F}$ ، معطاة بتماثلات الترافق  $\psi_{\alpha, \beta}$  لكل مرافق  $\beta$  في  $\bar{F}$  لـ  $\alpha$  على  $F$ ، فإذا كان لـ  $irr(\alpha, F)$  عدد  $n$  من الأصفار المختلفة في  $\bar{F}$ ، فإن  $\{E : F\} = n$ ، سنثبت لاحقاً أنه ما لم يكن  $F$  حقلاً غير منته ذا مميز  $p \neq 0$ ، فإن عدد الأصفار المختلفة لـ  $irr(\alpha, F)$  يساوي  $\deg(\alpha, F) = [F(\alpha) : F]$ .

### 11.49 مثال

افتراض  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  على  $\mathbb{Q}$ ، كما في المثال 17.48، فقد أثبت عملنا في ذلك المثال أن  $[E : \mathbb{Q}] = [E : \mathbb{Q}] = 4$ ، وكذلك  $\{E : \mathbb{Q}(\sqrt{2})\} = 2$  و  $\{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = 2$ ، إذن:

$$4 = \{E : \mathbb{Q}\} = \{E : \mathbb{Q}(\sqrt{2})\} \{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = (2)(2)$$

▲

هذا يوضح النتيجة 10.49.

إثبات مبرهنة التمديد

سنعيد صياغة مبرهنة التمديد التماثل 3.49.

مبرهنة تمديد التماثل: ليكن  $E$  امتداداً جبرياً للحقل  $F$ ، ولتكن  $\sigma$  تماثلاً من  $F$  غامراً للحقل  $F'$ ، ليكن  $\bar{F}'$  الإغلاق الجبري لـ  $F'$ ، فيمكن تمديد  $\sigma$  إلى تماثل  $\tau$  من  $E$  إلى حقل جزئي من  $\bar{F}'$  بحيث  $\tau(a) = \sigma(a)$  لكل  $a \in F$ .

البرهان

افتراض الأزواج كلها  $(L, \lambda)$ ، حيث  $L$  حقل يحقق  $F \leq L \leq E$  و  $\lambda$  تماثل من  $L$  إلى حقل جزئي من  $\bar{F}'$ ، بحيث إن  $\lambda(a) = \sigma(a)$  لكل  $a \in F$ . المجموعة  $S$  المكونة من الأزواج  $(L, \lambda)$  غير خالية؛ لأن  $(F, \sigma)$  هو أحد هذه الأزواج. عرّف ترتيباً جزئياً على  $S$ ، بحيث  $(L_1, \lambda_1) \leq (L_2, \lambda_2)$  إذا كان  $L_1 \leq L_2$  و  $\lambda_1(a) = \lambda_2(a)$  لكل  $a \in L_1$ . من السهل التحقق أن هذه العلاقة  $\leq$  تعطي ترتيباً جزئياً على  $S$ .

لتكن  $T = \{(H_i, \lambda_i) \mid i \in I\}$  أي سلسلة في  $S$ . نزعم أن  $H = \bigcup_{i \in I} H_i$  حقل جزئي من  $E$ . لتكن  $a, b \in H$ ، حيث  $a \in H_1$  و  $b \in H_2$ ؛ إذن، إما  $H_1 \leq H_2$  أو  $H_2 \leq H_1$ ؛ لأن  $T$  سلسلة. إذا كان - فرضاً -  $H_1 \leq H_2$ ، فإن  $a, b \in H_2$ ، وهذا يؤدي إلى أن  $a \pm b$  و  $ab$  و  $a/b$  إذا كانت  $b \neq 0$  كلها في  $H_2$  ومن ثم في  $H$ ، ولأنه لكل  $i \in I$ ،  $F \subseteq H_i \subseteq E$ ، فإن  $F \subseteq H \subseteq E$ . إذن،  $H$  حقل جزئي من  $E$ .

عرّف كالاتي: ليكن  $c \in H$ ، إذن،  $c \in H_i$  حيث  $i \in I$ ، ولتكن:

$$\lambda(c) = \lambda_i(c)$$

الدالة  $\lambda$  حسنة التعريف؛ لأنه إذا كانت  $c \in H_1$  و  $c \in H_2$ ، فإنما  $(H_1, \lambda_1) \leq (H_2, \lambda_2)$  أو  $(H_2, \lambda_2) \leq (H_1, \lambda_1)$ ؛ لأن  $T$  سلسلة، وفي كلتا الحالتين  $\lambda_1(c) = \lambda_2(c)$ . نزع  $\lambda$  تماثل من  $H$  إلى حقل جزئي من  $\overline{F'}$ ، فإذا كان  $a, b \in H$ ، فيوجد  $H_i$  بحيث إن  $a, b \in H_i$

$$\lambda(a + b) = \lambda_i(a + b) = \lambda_i(a) + \lambda_i(b) = \lambda(a) + \lambda(b)$$

وبالمثل

$$\lambda(ab) = \lambda_i(ab) = \lambda_i(a)\lambda_i(b) = \lambda(a)\lambda(b).$$

إذا كان  $\lambda(a) = 0$ ، فيوجد  $i$  حيث  $a \in H_i$  و  $\lambda_i(a) = 0$  وهذا يؤدي إلى أن  $a = 0$ .

إذن،  $\lambda$  تماثل. وهكذا، فإن  $(H, \lambda) \in S$ ، وواضح من تعريف  $H$  و  $\lambda$  أن  $(H, \lambda)$  حد أعلى لـ  $T$ . أثبتنا أن كل سلسلة في  $S$  لها حد أعلى في  $S$ ، وهكذا، فإن شروط بديهية زورن متحققة؛ إذن، يوجد عنصر أعظمي  $(K, \tau)$  في  $S$ . ليكن  $\tau(K) = K'$  حيث  $K' \leq \overline{F'}$ . الآن، إذا كانت  $K \neq E$ ، فلتكن  $\alpha \in E$  ولكن  $\alpha \notin K$ . الآن  $\alpha$  جبرية على  $F$ ، وهذا يؤدي إلى أن  $\alpha$  جبرية على  $K$ ، وكذلك فلتكن  $p(x) = \text{irr}(\alpha, K)$  ليكن  $\psi_\alpha$  التماثل القانوني

$$\psi_\alpha : K[x] / \langle p(x) \rangle \rightarrow K(\alpha)$$

المرتبط بتساكُل التعويض  $\phi_\alpha : K[x] \rightarrow K(\alpha)$ . إذا كانت

$$p(x) = a_0 + a_1x + \dots + a_nx^n$$

افترض

$$q(x) = \tau(a_0) + \tau(a_1)x + \dots + \tau(a_n)x^n$$

في  $K'[x]$ . لأن  $\tau$  تماثل، فإن  $q(x)$  غير مختزلة في  $K'[x]$ ، ولأن  $K' \leq \overline{F'}$ ، يوجد صفر  $\alpha'$  لـ  $q(x)$  في  $\overline{F'}$ . لتكن

$$\psi_{\alpha'} : K'[x] / \langle q(x) \rangle \rightarrow K'(\alpha')$$

$$\begin{array}{ccccc} K[x] & \xrightarrow{\tau_x} & K'[x] & & \\ \downarrow \text{القانوني } \gamma & & \downarrow \text{القانوني } \gamma' & & \\ K & \xrightarrow{\tau} & K' & & \\ \downarrow \psi_\alpha & & \downarrow \psi_{\alpha'} & & \\ K[x]/\langle p(x) \rangle & \xrightarrow{\bar{\tau}} & K'[x]/\langle q(x) \rangle & \xrightarrow{\psi_{\alpha'}} & K'(\alpha') \\ \psi_\alpha \swarrow & \bar{\tau} = \gamma' \tau_x \gamma^{-1} & & & \end{array}$$

الشكل 12.49

التماثل المشابه لـ  $\psi_\alpha$ . أخيرًا، ليكن

$$\bar{\tau} : K[x] / \langle p(x) \rangle \rightarrow K'[x] / \langle q(x) \rangle$$

التماثل الممدد لـ  $\tau$  على  $K$ ، ويربط  $\langle p(x) \rangle$  بـ  $\langle q(x) \rangle$ . (انظر الشكل 12.49). إذن، تركيب الدوال

$$\psi_{\alpha'} \bar{\tau} \psi_\alpha^{-1} : K(\alpha) \rightarrow K'(\alpha')$$

تماثل من  $K(\alpha)$  إلى حقل جزئي من  $\bar{F}$ ، وواضح أن  $(K(\alpha), \psi_{\alpha} \bar{\tau} \psi_{\alpha}^{-1}) < (K, \tau)$ ، ما يناقض أن  $(K, \tau)$  عنصر أعظمي؛ إذن، يجب أن تكون  $K = E$ .

### ■ تمارين 49

#### حسابات

لتكن  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ ، بالإمكان إثبات أن  $[E : \mathbb{Q}] = 8$ . في التمارين من 1 إلى 3، لكل تماثل معطى على حقل جزئي من  $E$ ، أوجد التمديدات كلها للدالة إلى تماثل من  $E$  إلى حقل جزئي من  $\mathbb{Q}$ ، وصف التمديدات بإعطاء قيمها على

مجموعة المولدات  $\{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$  لـ  $E$  على  $\mathbb{Q}$ .

1.  $\tau : \mathbb{Q}(\sqrt{2}, \sqrt{15}) \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{15})$  حيث  $\tau$  الدالة المحايدة.

2.  $\sigma : \mathbb{Q}(\sqrt{2}, \sqrt{15}) \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{15})$  بحيث  $\sigma(\sqrt{2}) = \sqrt{2}$  و  $\sigma(\sqrt{15}) = -\sqrt{15}$ .

3.  $\psi_{\sqrt{30}, -\sqrt{30}} : \mathbb{Q}(\sqrt{30}) \rightarrow \mathbb{Q}(\sqrt{30})$ .

إنها حقيقة يمكن إثباتها بالتكعيب أن أصفار  $x^3 - 2$  في  $\mathbb{Q}$  هي:

$$\alpha_1 = \sqrt[3]{2}, \alpha_2 = \sqrt[3]{2} \frac{-1+i\sqrt{3}}{2} \text{ و } \alpha_3 = \sqrt[3]{2} \frac{-1-i\sqrt{3}}{2}$$

حيث  $\sqrt[3]{2}$  - كالعادة - الجذر التكعيبي الحقيقي لـ 2. استخدم هذه المعلومات في التمارين 4 إلى 6.

4. صف التمديدات للدالة المحايدة على  $\mathbb{Q}$  إلى تماثل يربط  $(\sqrt[3]{2})$  بحقل جزئي من  $\bar{\mathbb{Q}}$ .

5. صف التمديدات جميعها للدالة المحايدة على  $\mathbb{Q}$  إلى تماثل يربط  $(\sqrt[3]{2}, \sqrt{3})$  بحقل جزئي من  $\bar{\mathbb{Q}}$ .

6. صف التمديدات جميعها للتماثل الذاتي  $\psi_{\sqrt{3}, -\sqrt{3}}$  على  $\mathbb{Q}(\sqrt{3})$  إلى تماثل يربط بحقل جزئي من  $\bar{\mathbb{Q}}$ .

7. ليكن  $\sigma$  تماثلاً ذاتياً على  $\mathbb{Q}(\pi)$  التي تربط  $\pi$  بـ  $-\pi$ .

أ. صف الحقل الثابت لـ  $\sigma$ .

ب. صف تمديدات  $\sigma$  جميعها إلى تماثل يربط الحقل  $(\sqrt{\pi})$  بحقل جزئي من  $\bar{\mathbb{Q}(\pi)}$ .

#### مفاهيم

8. ضع إشارة صح أو إشارة خطأ:

أ. \_\_\_\_\_ ليكن  $F(\alpha)$  أي امتداد بسيط للحقل  $F$ ، فكل تماثل من  $F$  إلى حقل جزئي من  $\bar{F}$  له تمديد إلى تماثل من  $F(\alpha)$  إلى حقل جزئي من  $\bar{F}$ .

ب. \_\_\_\_\_ ليكن  $F(\alpha)$  أي امتداد جبري بسيط للحقل  $F$ ، فكل تماثل من  $F$  إلى حقل جزئي من  $\bar{F}$  له تمديد إلى تماثل من  $F(\alpha)$  إلى حقل جزئي من  $\bar{F}$ .

ج. \_\_\_\_\_ كل تماثل من  $F$  إلى حقل جزئي من  $\bar{F}$  له العدد نفسه من التمديدات لكل امتداد جبري بسيط لـ  $F$ .

د. \_\_\_\_\_ الإغلاقات الجبرية للحقول المتماثلة دائماً متماثلة.

هـ. \_\_\_\_\_ الإغلاقات الجبرية للحقول غير المتماثلة لا يمكن أبداً أن تكون متماثلة.

و. \_\_\_\_\_ الإغلاق الجبري لـ  $\mathbb{Q}(\sqrt{2})$  متماثل مع الإغلاق الجبري لـ  $\mathbb{Q}(\sqrt{17})$ .

- ز. دليل الامتداد المنتهي  $E$  على الحقل  $F$  منته. \_\_\_\_\_  
 ح. يتصرف الدليل ضربياً بالنسبة إلى الأبراج المنتهية للامتدادات المنتهية للحقول. \_\_\_\_\_  
 ط. ملاحظتنا السابقة للنص الأول للمبرهنة 3.49 تشكل أساساً لإثبات هذه المبرهنة للامتدادات المنتهية  $E \supset F$ . \_\_\_\_\_

ي. تثبت النتيجة 5.49 أن  $\mathbb{C}$  يماثل  $\overline{\mathbb{Q}}$ . \_\_\_\_\_

براهين

9. ليكن  $K$  حقلاً مغلقاً جبرياً. أثبت أن أي تماثل  $\sigma$  من  $K$  إلى حقل جزئي منه، بحيث تكون  $K$  جبرية على  $\sigma[K]$  يكون تماثلاً ذاتياً على  $-K$  بمعنى أنه دالة غامرة. [مساعدة: استخدم المبرهنة 3.49 على  $\sigma^{-1}$ ].
10. ليكن  $E$  امتداداً جبرياً على الحقل  $F$ . أثبت أن كل تماثل من  $E$  إلى حقل جزئي من  $\overline{F}$  ويترك  $F$  ثابتة، يمكن تمديده إلى تماثل ذاتي على  $\overline{F}$ .
11. أثبت أنه إذا كان  $E$  امتداداً جبرياً للحقل  $F$ ، فإن أي إغلاقين جبريين  $\overline{F}$  و  $\overline{E}$  لـ  $F$  و  $E$ ، على الترتيب، متماثلان.
12. أثبت أن الإغلاق الجبري لـ  $(\sqrt{\pi})$  في  $\mathbb{Q}$  يماثل أي إغلاق جبري لـ  $(x)$  في  $\overline{\mathbb{Q}}$ ، حيث  $\overline{\mathbb{Q}}$  هو حقل الأعداد الجبرية و  $x$  غير معين.
13. أثبت أنه إذا كان  $E$  امتداداً منتهياً للحقل  $F$ ، فإن  $[E : F] \leq \{E : F\}$ .
- [مساعدة: تثبت الملاحظات السابقة للمثال 11.49 بصورة أساسية هذا بالنسبة إلى امتداد جبري بسيط  $F(\alpha)$  لـ  $F$ . استخدم حقيقة أن الامتداد المنتهي هو برج من الامتدادات البسيطة، بالترافق مع الخصائص الضربية للدليل والدرجة].

حقول الانشطار Splitting Fields

سنكون مهتمين بصورة رئيسة بالتماثلات الذاتية للحقل  $E$ ، وليس مجرد التماثلات التي تربط  $E$  بحقل جزئي من  $\bar{E}$ . إنها التماثلات الذاتية للحقل التي تشكل زمرة، ونتساءل ما إذا كان للتمدد  $E$  للحقل  $F$ ، كل تماثل يربط  $E$  بحقل جزئي من  $\bar{F}$  ويترك  $F$  ثابتة هو في الحقيقة تماثل ذاتي لـ  $E$ .

افتراض أن  $E$  تمدد جبري للحقل  $F$ ، فإذا كانت  $\alpha \in E$  و  $\beta \in \bar{F}$  مرافقة لـ  $\alpha$  على  $F$ ، فإنه يوجد تماثل ترافق

$$\psi_{\alpha,\beta} : F(\alpha) \rightarrow F(\beta).$$

بحسب النتيجة 4.49، يمكن تمديد  $\psi_{\alpha,\beta}$  إلى تماثل يربط  $E$  بحقل جزئي من  $\bar{F}$ . الآن، إذا كانت  $\beta \notin E$ ، فإن مثل هذا التماثل على  $E$  لا يمكن أن يكون تماثلاً ذاتياً على  $E$ ؛ إذن، إذا كان امتداد جبري  $E$  للحقل  $F$  يحقق خاصية أن تماثلاته كلها التي تربطه بحقل جزئي من  $\bar{F}$  وتترك  $F$  ثابتة هي في الحقيقة تماثلات ذاتية على  $E$ ، فإن لكل  $\alpha \in E$ ، يجب أن يحوي  $E$  مرافقات  $\alpha$  على  $F$  جميعها كذلك، يمكن ملاحظة هذا بسهولة. نشير هنا إلى أننا استخدمنا الكثير من القوة، تحديداً وجود تماثلات الترافق ومبرهنة تمديد التماثل 3.49.

تقترح هذه الأفكار صياغة للتعريف الآتي:

1.50 تعريف

ليكن  $F$  حقلاً له إغلاق جبري  $\bar{F}$ ، ولتكن  $\{f_i(x) \mid i \in I\}$  مجموعة من كثيرات الحدود في  $F[x]$ ، فيسمى الحقل  $E \leq \bar{F}$  حقل انشطار لـ  $\{f_i(x) \mid i \in I\}$  على  $F$  (splitting field) إذا كان  $E$  أصغر حقل جزئي من  $\bar{F}$  يحوي  $F$  والأصفار جميعها في  $\bar{F}$  لكل  $f_i(x)$  حيث  $i \in I$ ، ويسمى  $K \leq \bar{F}$  حقل انشطار على  $F$  إذا كان حقل انشطار لبعض كثيرات الحدود في  $F[x]$ .

2.50 مثال

رأينا أن  $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$  حقل انشطار لـ  $\{x^2-2, x^2-3\}$  وكذلك  $\{x^4-5x^2+6\}$ .  
 ▲ لكثيرة حدود واحدة  $f(x) \in F[x]$ ، سوف نشير عادة إلى حقل انشطار لـ  $\{f(x)\}$  على  $F$ ، بحقل انشطار  $f(x)$  على  $F$ ، لاحظ أن حقل الانشطار لـ  $\{f_i(x) \mid i \in I\}$  على  $F$  في  $\bar{F}$  هو تقاطع الحقول الجزئية جميعها من  $\bar{F}$  التي تحوي  $F$ ، والأصفار جميعها في  $\bar{F}$  لكل  $f_i(x)$  حيث  $i \in I$ ؛ إذن، مثل حقل الانشطار هذا موجود بالتأكيد.

سنثبت الآن أن حقول الانشطار على  $F$  هي تحديداً تلك الحقول  $E \leq \bar{F}$ ، مع خاصية أن التماثلات جميعها التي تربط  $E$  بحقل جزئي من  $\bar{F}$  وتترك  $F$  ثابتة، هي تماثلات ذاتية على  $E$ ، وستكون هذه نتيجة للمبرهنة المقبلة. مرة أخرى، نشخص مفهوماً باستخدام الدوال، وتذكر أننا دائماً نفترض أن الامتدادات الجبرية للحقل  $F$  قيد الدراسة جميعها محتواة في إغلاق جبري محدد  $\bar{F}$  لـ  $F$ .

3.50 مبرهنة

يكون الحقل  $E$ ، حيث  $F \leq E \leq \bar{F}$  حقل انشطار على  $F$ ، إذا وفقط إذا كان كل تماثل ذاتي لـ  $\bar{F}$  ويترك  $F$  ثابتة، يربط  $E$  بنفسها، وهكذا فهو يصنع تماثلاً ذاتياً لـ  $E$  ويبقي  $F$  ثابتة.

## البرهان

ليكن  $E$  حقل انشطار على  $F$  في  $\bar{F}$  لـ  $\{f_i(x) \mid i \in I\}$ ، ولتكن  $\sigma$  تماثلاً ذاتياً على  $\bar{F}$  وتترك  $F$  ثابتة، ولتكن  $\{\alpha_j \mid j \in J\}$  مجموعة الأصفار جميعها في  $\bar{F}$  لكل  $f_i(x)$  حيث  $i \in I$ . يثبت عملنا السابق أن لـ  $\alpha_j$  محددة، وتكون عناصر  $F(\alpha_j)$  هي التراكيب جميعها على الصورة:

$$g(\alpha_j) = a_0 + a_1\alpha_j + \dots + a_{n_j-1}\alpha_j^{n_j-1},$$

حيث  $n_j$  هي درجة  $\text{irr}(\alpha_j, F)$  و  $a_k \in F$ . افترض المجموعة  $S$  المكوّنة من المجاميع المنتهية كلها لحاصل الضرب المنتهي لعناصر من الشكل  $g(\alpha_j)$  لكل  $j \in J$ . المجموعة  $S$  محتواة في  $E$  ومغلقة بالنسبة إلى الجمع والضرب، وتحتوي 0 و 1 ومعكوساً جمعياً لكل عنصر، ولأن كل عنصر في  $S$  محتوي في  $S \subseteq F(\alpha_{j_1}, \dots, \alpha_{j_r})$  فنرى أن  $S$  تحوي كذلك المعكوس الضربي لكل عنصر لا يساوي الصفر؛ إذن،  $S$  حقل جزئي من  $E$ ، وتحتوي  $\alpha_j$  لكل  $j \in J$ ، وبحسب تعريف حقل الانشطار لـ  $E$  نرى أنه يجب أن تكون  $S=E$ ، هذا العمل كان فقط لإثبات أن  $\{\alpha_j \mid j \in J\}$  تولد  $E$  على  $F$ ، بطريقة أخذ المجاميع المنتهية وحاصل الضرب المنتهي. وبمعرفة هذا، نرى مباشرة أن قيمة  $\sigma$  لأي عنصر في  $E$  تتحدد تماماً بقيم  $\sigma(\alpha_j)$ ، ولكن بحسب النتيجة 5.48، يجب أن تكون  $\sigma(\alpha_j)$  كذلك صفراً لـ  $\text{irr}(\alpha_j, F)$ .

بحسب المبرهنة 13.29، فإن  $\text{irr}(\alpha_j, F)$  تقسم  $f_i(x)$  التي تحقق  $f_i(\alpha_j) = 0$ ، إذن  $\sigma(\alpha_j) \in E$  كذلك، وهكذا فإن  $\sigma$  تربط  $E$  بحقل جزئي من  $E$  تماثلياً. على أي حال، فإن المثل صحيح بالنسبة إلى التماثل الذاتي  $\sigma^{-1}$  على  $\bar{F}$ . ولأن لكل  $\beta \in E$

$$\beta = \sigma(\sigma^{-1}(\beta)),$$

نرى أن  $\sigma$  تربط  $E$  بصورة غامرة بـ  $E$ ، وهكذا، فهي تعطي تماثلاً ذاتياً على  $E$ .

افترض العكس، أي إن كل تماثل ذاتي على  $\bar{F}$  ويترك  $F$  ثابتة، يعطي تماثلاً ذاتياً على  $E$ . لتكن  $g(x)$  كثيرة حدود غير مختزلة في  $F[x]$  ولها صفر  $\alpha$  في  $E$ ، فإذا كان  $\beta$  أي صفر لـ  $g(x)$  في  $\bar{F}$ ، فإنه وبحسب المبرهنة 3.48، يوجد تماثل ترافق  $\psi_{\alpha, \beta}$  من  $F(\alpha)$  غامر لـ  $F(\beta)$ ، ويترك  $F$  ثابتة بحسب المبرهنة 3.49، يمكن تمديد  $\psi_{\alpha, \beta}$  إلى تماثل  $\tau$  من  $\bar{F}$  إلى حقل جزئي من  $\bar{F}$ . ولكن

$$\tau^{-1}: \tau[\bar{F}] \rightarrow \bar{F}$$

يمكن تمديدتها إلى تماثل يربط  $\bar{F}$  بحقل جزئي من  $\bar{F}$ ، ولأن صورة  $\tau^{-1}$  هي كل  $\bar{F}$ ، فإننا نرى أن  $\tau$  يجب أن تكون غامرة لـ  $\bar{F}$ ، بمعنى أن  $\tau$  تماثل ذاتي على  $\bar{F}$ ، ويترك  $F$  ثابتة؛ إذن، وبحسب الفرض، تولد  $\tau$  تماثلاً ذاتياً على  $E$ ، ما يؤدي إلى أن  $\beta = \tau(\alpha)$  موجودة في  $E$ . لقد أثبتنا أنه إذا كانت  $g(x)$  كثيرة حدود غير مختزلة في  $F[x]$  ولها صفر في  $E$ ، فإن أصفار  $g(x)$  الموجودة في  $\bar{F}$  جميعها تنتمي لـ  $E$ ؛ إذن، إذا كانت  $\{g_k(x)\}$  مجموعة كثيرات الحدود جميعها غير المختزلة في  $F[x]$  ولها صفر في  $E$ ، فإن  $E$  هي حقل الانشطار لـ  $\{g_k(x)\}$ . ♦

ليكن  $E$  امتداداً للحقل  $F$ ، فنقول: إن كثيرة الحدود  $f(x)$  تنشطر في  $E$  (splits) إذا أمكن تحليلها إلى حاصل ضرب عوامل خطية في  $E[x]$ . ■

## 4.50 تعريف

كثيرة الحدود  $x^4+5x^2+6$  في  $\mathbb{Q}[x]$  تنشطر في الحقل  $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$  إلى

## 5.50 مثال

$$(x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$$



### 6.50 نتيجة

إذا كان  $E \leq \bar{F}$  حقل انشطار على  $F$ ، فإن كل كثيرة حدود غير مختزلة في  $F[x]$  ولها صفر في  $E$  تنشط في  $E$ .

البرهان

إذا كان  $E$  حقل انشطار على  $F$  في  $\bar{F}$ ، فإن كل تماثل ذاتي على  $\bar{F}$  يولد تماثلاً ذاتياً على  $E$ ، الجزء الثاني من إثبات المبرهنة 3.50، يبرهن بالضبط أن  $E$  كذلك حقل الانشطار على  $F$  للمجموعة  $\{g_i(x)\}$  المكوّنة من كثيرات الحدود غير المختزلة في  $F[x]$  ولها صفر في  $E$ ؛ إذن، أي كثيرة حدود غير مختزلة  $f(x)$  في  $F[x]$  ولها صفر في  $E$  تكون أصفارها في  $\bar{F}$  جميعها تنتمي لـ  $E$ ، وهكذا، فإن تحليلها إلى عوامل خطية في  $F[x]$  المعطى في المبرهنة 5.31- في الحقيقة يحدث في  $E[x]$ ، وهكذا، فإن  $f(x)$  تنشط في  $E$ . ♦

### 7.50 نتيجة

إذا كان  $E \leq \bar{F}$  حقل انشطار على  $F$ ، فإن كل تماثل يربط  $E$  بحقل جزئي من  $\bar{F}$  ويترك  $F$  ثابتة، هو في الحقيقة تماثل ذاتي على  $E$ ، وبوجه خاص، إذا كان  $E$  حقل انشطار من درجة منتهية على  $F$ ، فإن

$$\{E : F\} = |G(E/F)|$$

البرهان

كل تماثل  $\sigma$  يربط  $E$  بحقل جزئي من  $\bar{F}$  ويترك  $F$  ثابتة، يمكن تمديده إلى تماثل ذاتي  $\tau$  على  $\bar{F}$ ، بحسب المبرهنة 3.49 ومناقشة الغمر في الجزء الثاني من إثبات المبرهنة 3.50. إذا كان  $E$  حقل انشطار على  $F$ ، فإنه وبحسب المبرهنة 3.50، قصر  $\tau$  على  $E - \sigma$  يعطي تماثلاً ذاتياً على  $E$ ، وهكذا لحقل انشطار  $E$  على  $F$ ، كل تماثل يربط  $E$  بحقل جزئي من  $\bar{F}$  ويترك  $F$  ثابتة، هو تماثل ذاتي على  $E$ . ♦

تنتج المعادلة  $\{E : F\} = |G(E/F)|$  مباشرة لحقل انشطار  $E$  ذي درجة منتهية على  $F$ ؛ لأن  $\{E:F\}$  تم تعريفها بوصفها عدد التماثلات المختلفة التي تربط  $E$  بحقل جزئي من  $\bar{F}$  وتترك  $F$  ثابتة. ♦

### 8.50 مثال

لاحظ أن  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  حقل انشطار لـ

$$\{x^2-2, x^2-3\}$$

على  $\mathbb{Q}$  يثبت المثال 17.48 أن الدوال  $\sigma_1, \sigma_2, \sigma_3, i$  هي التماثلات الذاتية كلها لـ  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  التي تترك  $\mathbb{Q}$  ثابتة. (في الحقيقة؛ لأن كل تماثل ذاتي للحقل الجزئي يجب أن يترك الحقل الجزئي الأولي ثابتاً، فإننا نرى أنها التماثلات الذاتية الوحيدة على  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ؛ إذن:

$$\{\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\} = |G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = 4$$

موضحاً النتيجة 7.50.

نود أن نحدد شروطاً تؤدي إلى أن

$$|G(E/F)| = \{E : F\} = [E : F]$$

▲

لامتداد منته  $E$  على  $F$ ، هذا هو موضوعنا الآتي، وسنثبت في الفصل المقبل أن هذه المعادلة تتحقق دائماً عندما يكون  $E$  حقل انشطار على الحقل  $F$  ذي المميز  $0$ ، أو عندما يكون  $F$  حقلاً منتهياً. هذه المعادلة ليست بالضرورة صحيحة، عندما يكون  $F$  حقلاً غير منته ذا مميز  $p \neq 0$ .

## 9.50 مثال

ليكن  $\sqrt[3]{2}$  الجذر التكعيبي الحقيقي لـ  $2$ ، كالعادة، الآن  $x^3-2$  لا تنشطر في  $\mathbb{Q}(\sqrt[3]{2})$ : لأن  $\mathbb{Q}(\sqrt[3]{2}) < \mathbb{R}$  وهناك صفر حقيقي واحد فقط لـ  $x^3-2$ : إذن،  $x^3-2$  تتحلل في  $(\mathbb{Q}(\sqrt[3]{2}))[x]$  إلى عامل خطي  $x - \sqrt[3]{2}$  وعامل تربيعي غير مختزل.

حقل الانشطار  $E$  لـ  $x^3-2$  على  $\mathbb{Q}$  هو لذلك من الدرجة  $2$  على  $\mathbb{Q}(\sqrt[3]{2})$ : إذن،

$$[E:\mathbb{Q}] = [E:\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = (2)(3) = 6$$

أثبتنا أن حقل الانشطار على  $\mathbb{Q}$  لـ  $x^3-2$  من الدرجة  $6$  على  $\mathbb{Q}$ ، ويمكننا التحقق باستخدام التكعيب أن:

$$\sqrt[3]{2} \frac{-1+i\sqrt{3}}{2} \quad \text{و} \quad \sqrt[3]{2} \frac{-1-i\sqrt{3}}{2}$$

هي الأصفار الأخرى لـ  $x^3-2$  في  $\mathbb{C}$ : إذن، حقل الانشطار  $E$  لـ  $x^3-2$  على  $\mathbb{Q}$  هو  $(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}))$ . (هذا ليس الحقل  $(\mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3}))$ ، الذي له درجة  $12$  على  $\mathbb{Q}$ ). ستترك دراسة أخرى لهذا المثال المشوق إلى التمارين (انظر التمارين  $7, 8, 9, 16, 21, 23$ ). ▲

■ تمارين 50

حسابات

في التمارين من 1 إلى 6، أوجد درجة حقل الانشطار على  $\mathbb{Q}$  لكثيرات الحدود المعطاة في  $\mathbb{Q}[x]$ .

1.  $x^2+3$       2.  $x^4-1$       3.  $(x^2-2)(x^2-3)$

4.  $x^3-3$       5.  $x^3-1$       6.  $(x^2-2)(x^3-2)$

ارجع إلى المثال 9.50 في التمارين من 7 إلى 9.

7. ما رتبة  $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$  ؟

8. ما رتبة  $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q})$  ؟

9. ما رتبة  $G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}(\sqrt[3]{2}))$  ؟

10. ليكن  $\alpha$  صفراً لـ  $x^3+x^2+1$  على  $\mathbb{Z}_2$ . أثبت أن  $x^3+x^2+1$  تنشطر في  $\mathbb{Z}_2(\alpha)$  [مساعدة: يوجد ثمانية عناصر في  $\mathbb{Z}_2(\alpha)$ . أوجد صفرين لـ  $x^3+x^2+1$  - إضافة إلى  $\alpha$  - من هذه العناصر الثمانية. أو عوضاً عن ذلك استخدم نتائج الفصل 33].

مفاهيم

في التمرينين 11 و 12، صحّح تعريف الحد المكتوب بخط مائل دون الرجوع إلى الكتاب - إذا كانت هناك حاجة للتصحيح - بحيث يكون بصيغة قابلة للنشر.

11. ليكن  $F \leq E \leq \bar{F}$  حيث  $\bar{F}$  الإغلاق الجبري للحقل  $F$ . يكون الحقل  $E$  حقل انشطار على  $F$  إذا وفقط إذا كانت  $E$  تحوي الأصفار جميعها في  $\bar{F}$  لكل كثيرة حدود في  $F[x]$ ، التي لها صفر في  $E$ .

12. كثيرة الحدود  $f(x)$  في  $F[x]$  تنشطر في الامتداد الحقلي  $E \supset F$ ، إذا وفقط إذا كانت تحلل إلى عوامل في  $E[x]$ ، هي حاصل ضرب كثيرات حدود من درجة أقل.

13. لتكن  $f(x)$  كثيرة حدود في  $F[x]$  من الدرجة  $n$ ، وليكن  $E \leq \bar{F}$  حقل الانشطار لـ  $f(x)$  على  $F$  في  $\bar{F}$ . ما الحدود التي يمكن وضعها لـ  $[E:F]$  ؟

14. ضع إشارة صح أو إشارة خطأ:

\_\_\_\_\_ أ. لتكن  $\alpha, \beta \in E$  حيث  $E \leq \bar{F}$  حقل انشطار على  $F$ ؛ إذن، يوجد تماثل ذاتي على  $E$  ويترك  $F$

ثابتاً، ويربط  $\alpha$  بـ  $\beta$ ، إذا وفقط إذا كانت  $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$

\_\_\_\_\_ ب.  $\mathbb{R}$  حقل انشطار على  $\mathbb{Q}$ .

\_\_\_\_\_ ج.  $\mathbb{R}$  حقل انشطار على  $\mathbb{R}$ .

د. حقل انشطار على  $\mathbb{R}$ .

هـ. حقل انشطار على  $\mathbb{Q}(i)$ .

و. حقل انشطار على  $\mathbb{Q}(\pi^2)$ .

ز. لكل حقل انشطار  $E$  على  $F$ ، حيث  $E \leq \bar{F}$ ، كل تماثل على  $E$  هو تماثل ذاتي على  $E$ .

ح. لكل حقل انشطار  $E$  على  $F$ ، حيث  $E \leq \bar{F}$ ، كل تماثل من  $E$  إلى حقل جزئي من  $\bar{F}$  هو تماثل ذاتي على  $E$ .

ط. لكل حقل انشطار  $E$  على  $F$ ، حيث  $E \leq \bar{F}$ ، كل تماثل على  $E$  إلى حقل جزئي من  $\bar{F}$  ويترك  $F$  ثابتة، هو تماثل ذاتي على  $E$ .

ي. يكون كل إغلاق جبري  $\bar{F}$  للحقل  $F$  حقل انشطار على  $F$ .

15. أثبت مستخدماً مثلاً أن النتيجة 6.50 لن تبقى صحيحة إذا أزيلت الكلمة «غير مختزل».

16. أ. هل  $|G(E/F)|$  ضربية على الأبراج المنتهية للامتدادات المنتهية، أي هل صحيح أن:

$$|G(K/F)| = |G(K/E)| |G(E/F)|$$

حيث  $F \leq E \leq K \leq \bar{F}$  ؟

لماذا نعم أو لماذا لا؟ [مساعدة: استخدم التمارين من 7 إلى 9].

ب. هل  $|G(E/F)|$  ضربية على الأبراج المنتهية للامتدادات المنتهية التي كل منها حقل انشطار على الحقل الذي أسفل منه؟ لماذا نعم أو لماذا لا؟

براهين

17. أثبت أنه إذا كان الامتداد المنتهي  $E$  للحقل  $F$  حقل انشطار على  $F$ ، فإن  $E$  حقل انشطار لكثيرة حدود واحدة في  $F[x]$ .

18. أثبت أنه إذا كان  $[E:F]=2$ ، فإن  $E$  حقل انشطار على  $F$ .

19. أثبت أنه إذا كان  $F \leq E \leq \bar{F}$ ، فإن  $E$  حقل انشطار على  $F$ ، إذا وفقط إذا كان  $E$  يحوي المترافقات كلها على  $F$  في  $\bar{F}$  لكل عنصر من عناصره.

20. أثبت أن  $\mathbb{Q}(\sqrt[3]{2})$  التماثل الذاتي المحايد فقط.

21. بالرجوع إلى المثال 9.50، أثبت أن:

$$G(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) / \mathbb{Q}(i\sqrt{3})) \cong \langle \mathbb{Z}_3, + \rangle$$

22. أ. أثبت أن التماثل الذاتي لحقل الانشطار  $E$  على  $F$  لكثيرة الحدود  $f(x) \in F[x]$  يكون تباديل على أصفار  $f(x)$  في  $E$ .

ب. أثبت أن التماثل الذاتي لحقل الانشطار  $E$  على  $F$  لكثيرة الحدود  $f(x) \in F[x]$  يتعين تماماً بالتباديل على أصفار  $f(x)$  في  $E$  المعطاة في الفرع (أ).

ج. أثبت أنه إذا كان  $E$  حقل انشطار على  $F$  لكثيرة الحدود  $f(x) \in F[x]$ ، فإنه يمكن النظر لـ  $G(E/F)$  بطريقة طبيعية بوصفها زمرة تباديل.

23. ليكن  $E$  حقل الانشطار لـ  $x^3 - 2$  على  $\mathbb{Q}$ ، كما في المثال 9.50.

أ. ما رتبة  $G(E/\mathbb{Q})$ ؟ [مساعدة: استخدم النتيجة 7.50 والنتيجة 4.49 المطبقة على البرج  $\mathbb{Q} \leq \mathbb{Q}(i\sqrt{3}) \leq E$ ].

ب. أثبت أن  $G(E/\mathbb{Q}) = S_3$ ، زمرة التناظر على ثلاثة أحرف. [مساعدة: استخدم التمرين 22 مع الفرع (أ)].

24. أثبت أنه لأي عدد أولي  $p$ ، تكون درجة حقل الانشطار على  $\mathbb{Q}$  لـ  $x^p - 1$  هي  $p - 1$ . [مساعدة: ارجع إلى النتيجة 17.23].

25. ليكن  $\bar{F}$  و  $\bar{F}'$  إغلاقين جبريين للحقل  $F$ ، ولتكن  $f(x) \in F[x]$ ، أثبت أن حقل الانشطار  $E$  على  $F$  لـ  $f(x)$  في  $\bar{F}$ ، يماثل حقل الانشطار  $E'$  على  $F$  لـ  $f(x)$  في  $\bar{F}'$ . [مساعدة: استخدم النتيجة 5.49].

obeyikamal.com

## الامتدادات القابلة للفصل Separable Extensions

## الفصل 51

تكرارات أصفار كثيرة الحدود

تذكر أننا الآن نفترض دائماً أن الامتدادات الجبرية للحقل  $F$  قيد الدراسة جميعها محتواة في إغلاق جبري محدد  $\bar{F} \perp F$ .

هدفنا الآتي هو تحديد الشروط الواجب توافرها - لامتداد  $E$  منته  $F \perp E$  - لكي يكون  $\{E:F\} = [E:F]$ . مفتاح الإجابة عن هذا السؤال هو افتراض تكرار أصفار كثيرات الحدود.

ليكن  $f(x) \in F[x]$ . يكون العنصر  $\alpha$  من  $\bar{F}$  حيث  $f(\alpha) = 0$  صفراً ذا تكرار  $v$  لـ  $f(x)$

## 1.51 تعريف

(zero of  $f(x)$  of multiplicity  $v$ )، إذا كان  $v$  أكبر عدد صحيح، بحيث يكون  $(x - \alpha)^v$  عاملاً من عوامل  $f(x)$  في  $\bar{F}[x]$ .

تثبت المبرهنة الآتية أن تكرارات أصفار كثيرة حدود غير مختزلة ومعطاة على حقل، كلها متساوية. السهولة التي يمكننا بها إثبات هذه المبرهنة، هي دليل آخر على قوة تماثلات الترافق، وطريقتنا كلها في دراسة أصفار كثيرات الحدود هي عن طريق الدوال. لتكن  $f(x)$  غير مختزلة في  $F[x]$ . كل أصفار  $f(x)$  في  $\bar{F}$  لها التكرار نفسه.

## 2.51 مبرهنة

لتكن  $\alpha$  و  $\beta$  أصفاراً لـ  $f(x)$  في  $\bar{F}$  بحسب المبرهنة 3.48، يوجد تماثل ترافق  $\psi_{\alpha,\beta} : F(\alpha) \xrightarrow{\text{غامر}} F(\beta)$  بحسب النتيجة 4.49، يمكن تمديد  $\psi_{\alpha,\beta}$  إلى تماثل  $\tau : \bar{F} \rightarrow \bar{F}$ . يُنتج  $\tau$  تماثلاً طبيعياً  $\tau_x : \bar{F}[x] \rightarrow \bar{F}[x]$ ، حيث  $\tau_x(x) = x$ ، الآن،  $\tau_x$  تترك  $\tau_x f(x)$  ثابتة؛ لأن  $f(x) \in F[x]$  و  $\psi_{\alpha,\beta}$  تترك  $F$  ثابتة. ولكن

البرهان

$$\tau_x((x - \alpha)^v) = (x - \beta)^v,$$

ما يثبت أن تكرار  $\beta$  في  $f(x)$  أكبر أو يساوي تكرار  $\alpha$ . بالطريقة نفسها يمكن الحصول على المتباينة العكسية؛ إذن، تكرار  $\alpha$  يساوي تكرار  $\beta$ .  
إذا كانت  $f(x)$  غير مختزلة في  $F[x]$ ، فيمكن تحليل  $f(x)$  في  $F[x]$  على الصورة:

## 3.51 نتيجة

$$a \prod_i (x - \alpha_i)^v,$$

حيث  $\alpha_i$  الأصفار المختلفة لـ  $f(x)$  في  $\bar{F}$  و  $a \in F$ .

النتيجة مباشرة من المبرهنة 2.51.

البرهان

عند هذه النقطة، يحتمل أنه يتعين علينا الإثبات بمثال، أن ظاهرة الأصفار ذات التكرار أكبر من 1 لكثيرة حدود غير مختزلة، هي ظاهرة ممكنة الحدوث، وسوف نعرض لاحقاً في هذا الفصل، أنها يمكن أن تحدث فقط لكثيرة حدود في حقل غير منته ذي مميز  $p \neq 0$ .

مثال 4.51

لتكن  $E = \mathbb{Z}_p(y)$ ، حيث  $y$  غير معين. لتكن  $t = y^p$ ، وليكن  $F$  الحقل الجزئي  $\mathbb{Z}_p(t)$  من  $E$ . (انظر الشكل 5.51). الآن،  $E = F(y)$  جبري على  $F$ ؛ لأن  $y$  صفر لـ  $F[x]$   $(x^p - t) \in F[x]$ . بحسب المبرهنة 13.29،  $\text{irr}(y, F)$  يجب أن تقسم  $x^p - t$  في  $F[x]$ . [في الحقيقة،  $\text{irr}(y, F) = x^p - t$ ، وسنترك برهان هذا إلى التمارين انظر التمرين 10].

$$\begin{array}{l} E = \mathbb{Z}_p(y) = F(y) \\ \Big| \\ F = \mathbb{Z}_p(t) = \mathbb{Z}_p(y^p) \\ \Big| \\ \mathbb{Z}_p \end{array}$$

لأن  $F(y)$  لا يساوي  $F$ ، فيجب أن تكون درجة  $\text{irr}(y, F) \geq 2$ ، ولكن لاحظ أن

$$x^p - t = x^p - y^p = (x - y)^p,$$

لأن  $E$  ذو مميز  $p$  (انظر المبرهنة 19.48 والملاحظة التي بعدها).

إذن،  $y$  صفر لـ  $\text{irr}(y, F)$  وذو تكرار  $< 1$ . في الحقيقة  $\text{irr}(y, F) = x^p - t$ ، ما يعني أن تكرار  $y$  يساوي  $p$ . ▲

الشكل 5.51

من الآن فصاعداً، سنعتمد بصورة مكثفة على المبرهنة 7.49 ونتيجتها. تثبت المبرهنة 3.48 ونتيجتها أنه لا امتداد جبري بسيط  $F \triangleleft F(\alpha)$ ، يوجد تمديد واحد لتمائل العنصر المحايد  $i$ ، الذي يربط  $F \rightarrow F$  للأصفار المختلفة جميعها لـ  $\text{irr}(\alpha, F)$ ، وهذه هي التمديدات الوحيدة لـ  $i$ ؛ إذن،  $\{F(\alpha) : F\}$  يساوي عدد الأصفار المختلفة لـ  $\text{irr}(\alpha, F)$ . بالنظر لعملنا في مبرهنة لاجرانج والمبرهنة 4.31، فيجب أن ندرك قوة مبرهنة مثل هذه المقبلة.

مبرهنة 6.51

إذا كان  $E$  امتداداً لـ  $F$ ، فإن  $\{E:F\}$  يقسم  $[E:F]$ .

البرهان

بحسب المبرهنة 11.31، إذا كان  $E$  منتهياً على  $F$ ، فإن  $E = F(\alpha_1, \dots, \alpha_n)$ ، حيث  $\alpha_i \in \bar{F}$ . لتكن  $(\text{irr}(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1})))$  لها  $\alpha_i$  بوصفه أحد أصفارها ألد  $n_i$  التي لها جميعها التكرار  $v_i$  بحسب المبرهنة 2.51؛ إذن:

$$[F(\alpha_1, \dots, \alpha_n) : F(\alpha_1, \dots, \alpha_{i-1})] = n_i v_i = \{F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})\} v_i.$$

بحسب المبرهنة 4.31 والنتيجة 10.49.

$$[E : F] = \prod_i n_i v_i$$

$$\{E : F\} = \prod_i n_i \quad \text{و}$$

إذن،  $\{E:F\}$  تقسم  $[E:F]$ .



## الامتدادات القابلة للفصل

## 7.51 تعريف

يسمى الامتداد المنتهي  $E \perp F$  امتداداً قابلاً للفصل على  $F$  (separable extension)، إذا كان  $\{E:F\} = [E:F]$ . العنصر  $\alpha$  في  $\overline{F}$  قابل للفصل على  $F$ ، إذا كان  $F(\alpha)$  امتداداً قابلاً للفصل على  $F$ . كثيرة الحدود غير المختزلة  $f(x) \in F[x]$  قابلة للفصل على  $F$ ، إذا كانت أصفار  $f(x)$  في  $\overline{F}$  جميعها قابلة للفصل على  $F$ .

الحقل  $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$  قابل للفصل على  $\mathbb{Q}$ ؛ لأننا رأينا في المثال 8.50 أن  $[E:\mathbb{Q}] = 4 = [E:\mathbb{Q}]$ .

## 8.51 مثال

ولجعل الأمور أكثر بساطة، سنحدد تعريفنا للامتدادات القابلة للفصل للحقل  $F$  على الامتدادات المنتهية  $E \perp F$ . للتعريف المقابل للامتدادات غير المنتهية، انظر التمرين 12.

نعلم أن  $\{F(\alpha): F\}$  يساوي عدد الأصفار المختلفة لـ  $\text{irr}(\alpha, F)$ ، وكذلك تكرار  $\alpha$  في  $\text{irr}(\alpha, F)$  مساوٍ لتكرار كل مرافق لـ  $\alpha$  على  $F$ ، بحسب المبرهنة 2.51.

إن  $\alpha$  قابلة للفصل على  $F$ ، إذا وفقط إذا كانت  $\text{irr}(\alpha, F)$  لها أصفار ذات تكرار 1، وهذا يخبرنا بأن كثيرة الحدود غير المختزلة  $f(x) \in F[x]$  قابلة للفصل على  $F$ ، إذا وفقط إذا كانت أصفارها جميعها ذات تكرار 1.

إذا كان  $K$  امتداداً منتهياً لـ  $E$ ، وكانت  $E$  امتداداً منتهياً لـ  $F$ ، أي إن  $F \leq E \leq K$ ، فإن  $K$  قابلة للفصل على  $F$ ، إذا وفقط إذا كانت  $K$  قابلة للفصل على  $E$  و  $E$  قابلة للفصل على  $F$ .

## 9.51 مبرهنة

البرهان:

$$[K:F] = [K:E][E:F],$$

و

$$\{K:F\} = \{K:E\}\{E:F\}.$$

إذا كانت  $K$  قابلة للفصل على  $F$ ، فإن  $[K:F] = \{K:F\}$ ، وهذا يجب أن يؤدي إلى أن  $[E:F] = \{E:F\}$  و  $[K:E] = \{K:E\}$ ؛ لأنه في كل حالة يقسم الدليل الدرجة بحسب المبرهنة 6.51. إذن، إذا كانت  $K$  قابلة للفصل على  $F$ ، فإن  $K$  قابلة للفصل على  $E$  و  $E$  قابلة للفصل على  $F$ .

في المقابل، لاحظ أن  $[K:E] = \{K:E\}$  و  $[E:F] = \{E:F\}$  يؤدي إلى:

$$\{K:F\} = [K:F] = [K:E][E:F] = \{K:E\}\{E:F\} = \{K:F\}.$$

يمكن تعميم المبرهنة 9.51 بصورة واضحة - باستخدام الاستقراء الرياضي - إلى أي برج منته من الامتدادات المنتهية. الحقل الأعلى امتداد قابل للفصل على الحقل في الأسفل، إذا وفقط إذا كان كل حقل امتداداً قابلاً للفصل على الحقل أسفله مباشرة.

إذا كان  $E$  امتداداً منتهياً على  $F$ ، فإن  $E$  قابل للفصل على  $F$ ، إذا وفقط إذا كان كل  $\alpha$  في  $E$  قابلاً للفصل على  $F$ .

## 10.51 نتيجة

البرهان

افترض أن  $E$  قابل للفصل على  $F$ ، ولتكن  $\alpha \in E$ . فإن

$$F \leq F(\alpha) \leq E,$$

وتثبت المبرهنة 9.51 أن  $F(\alpha)$  قابل للفصل على  $F$ .

افترض - في الحالة المقابلة- أن كل  $\alpha \in E$  قابلة للفصل على  $F$ ، ولأن  $E$  امتداد منته على  $F$ ، فيوجد  $\alpha_1, \dots, \alpha_n$ ، حيث:

$$F < F(\alpha_1) < F(\alpha_1, \alpha_2) < \dots < E = F(\alpha_1, \dots, \alpha_n).$$

لأن  $\alpha_i$  قابلة للفصل على  $F$ ،  $\alpha_i$  قابلة للفصل على  $F(\alpha_1, \dots, \alpha_{i-1})$ : لأن

$$q(x) = \text{irr}(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1}))$$

تقسم  $\text{irr}(\alpha_i, F)$ ، وهذا يؤدي إلى أن  $\alpha_i$  صفر لـ  $q(x)$  ذو تكرار 1؛ إذن،  $F(\alpha_1, \dots, \alpha_i)$  قابل للفصل على  $F(\alpha_1, \dots, \alpha_{i-1})$ ؛ إذن،  $E$  قابل للفصل على  $F$  بحسب المبرهنة 9.51، معممًا بالاستقراء

الرياضي.  
الحقول الكاملة

نتحول الآن إلى إثبات أن  $\alpha$  يمكن أن تفشل في أن تكون قابلة للفصل على  $F$  فقط، إذا كان  $F$  حقلاً غير منته ذا مميز  $p \neq 0$ ، إحد الطرق هي تقديم المشتقات الشكلية لكثيرات الحدود، وعلى الرغم من أنها تقنية رائعة ومفيدة كذلك، فإننا - ورغبة في الاختصار- سنستخدم بدلاً منها التمهيدية الآتية، ستقدم المشتقات الشكلية في التمارين من 15 إلى 22.

ليكن  $\bar{F}$  إغلاقاً جبرياً لـ  $F$ ، ولتكن:

11.51 تمهيدية

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

أي كثيرة حدود أحادية في  $\bar{F}[x]$ ، فإذا كانت  $(f(x))^m \in F[x]$  و  $m \cdot 1 \neq 0$  في  $F$ ، فإن  $f(x) \in F[x]$ ؛ أي إن كل  $a_i \in F$ .

يجب أن نثبت أن  $a_i \in F$ ، سنعمل - باستخدام الاستقراء الرياضي على  $-r$  لإثبات أن  $a_{n-r} \in F$  إذا كان  $r=1$

البرهان

$$(f(x))^m = x^{mn} + (m \cdot 1)a_{n-1}x^{mn-1} + \dots + a_0^m$$

ولأن  $(f(x))^m \in F[x]$ ، فإننا نحصل وبوجه خاص على:

$$(m \cdot 1)a_{n-1} \in F$$

إذن،  $a_{n-1} \in F$ ؛ لأن  $m \cdot 1 \neq 0$  في  $F$ .

بوصفها فرضية للاستقراء، افترض أن  $a_{n-r} \in F$  و  $r = 1, 2, \dots, k$ ؛ إذن، معامل  $x^{mn-(k+1)}$  في  $(f(x))^m$  يكون على الصورة:

$$(m \cdot 1)a_{n-(k+1)} + g_{k+1}(a_{n-1}, a_{n-2}, \dots, a_{n-k}),$$

حيث  $g_{k+1}(a_{n-1}, a_{n-2}, \dots, a_{n-k})$  هي تعبير بكثيرة حدود شكلية في  $a_{n-1}, a_{n-2}, \dots, a_{n-k}$ . بحسب فرضية الاستقراء التي ذكرناها آنفاً،  $g_{k+1}(a_{n-1}, a_{n-2}, \dots, a_{n-k}) \in F$ ، وهكذا، فإن  $a_{n-(k+1)} \in F$ ؛ لأن

$m \cdot 1 \neq 0$  في  $F$ .

نحن الآن في موضع معالجة الحقول  $F$  ذات المميز صفر، وإثبات أنه لا امتداد منته  $E \perp F$ ، فإن  $\{E:F\} = [E:F]$ . وبحسب التعريف، هذا يعادل إثبات أن كل امتداد منتهٍ لحقل ذي مميز صفر، يكون امتدادًا قابلاً للفصل، نعطي في البداية تعريفًا.

**12.51 تعريف**

يكون الحقل كاملاً (Perfect) إذا كان كل امتداد منتهٍ قابلاً للفصل.

**13.51 مبرهنة**

كل حقل مميزه صفر كامل.

## البرهان

ليكن  $E$  امتداداً منتهياً للحقل  $F$  ذي المميز صفر، ولتكن  $\alpha \in E$ ؛ إذن، تتحلل

$f(x) = \text{irr}(\alpha, F)$  في  $\bar{F}[x]$  إلى  $\prod_i (x - \alpha_i)^v$ ، حيث  $\alpha_i$  الأصفار المختلفة لـ  $\text{irr}(\alpha, F)$  وافترض  $\alpha = \alpha_1$ ؛ إذن:

$$f(x) = \left( \prod_i (x - \alpha_i) \right)^v$$

ولأن  $v \neq 0$  في حقل  $F$  مميزه صفر، فيجب أن يكون:

$$\left( \prod_i (x - \alpha_i) \right) \in F[x]$$

بحسب التمهيدية 11.51؛ ولأن  $f(x)$  غير مختزلة وذات درجة صغرى في  $F[x]$  و  $\alpha$  صفر لها، نرى أن  $v = 1$ ؛ إذن،  $\alpha$  قابلة للفصل على  $F$  لكل  $\alpha \in E$ . وهذا يعني، وبحسب النتيجة 10.51 أن  $E$  امتداد قابل للفصل على  $F$ .

ستدخلنا التمهيدية 11.51 لحالة الحقول المنتهية على الرغم من أن برهانها أصعب قليلاً. كل حقل منتهٍ كامل.

**14.51 مبرهنة**

## البرهان

ليكن  $F$  حقلاً منتهياً مميزه  $p$ ، وليكن  $E$  امتداداً منتهياً لـ  $F$ ، ولتكن  $\alpha \in E$ . نريد إثبات أن  $\alpha$  قابلة للفصل على  $F$ . الآن،  $f(x) = \text{irr}(\alpha, F)$  تتحلل في  $\bar{F}$  إلى  $\prod_i (x - \alpha_i)^v$ ، حيث  $\alpha_i$  الأصفار المختلفة لـ  $f(x)$ ؛ وافترض أن  $\alpha = \alpha_1$ . لتكن  $v = p^e e$ ، حيث  $p$  لا تقسم  $e$ ؛ إذن:

$$f(x) = \prod_i (x - \alpha_i)^v = \left( \prod_i (x - \alpha_i)^{p^e} \right)^e$$

تنتمي إلى  $F[x]$ ، وبحسب التمهيدية 11.51، فإن  $\prod_i (x - \alpha_i)^{p^e}$  تنتمي إلى  $F[x]$ ؛ لأن  $e \neq 0$  في  $F$ ، ولأن  $f(x) = \text{irr}(\alpha, F)$  ذات درجة صغرى على  $F$  و  $\alpha$  صفر لها، فيجب أن يكون  $e = 1$ .

تثبت المبرهنة 19.48 والملاحظة اللاحقة لها أن:

$$f(x) = \prod_i (x - \alpha_i)^{p^e} = \left( \prod_i x^{p^e} - \alpha_i^{p^e} \right)$$

إذن، إذا افترضنا  $f(x)$  مثل  $g(x^{p^t})$ ، فيجب أن تكون  $g(x) \in F[x]$ . الآن،  $g(x)$  قابلة للفصل على  $F$  وأصفارها المختلفة  $\alpha_i^{p^t}$ . افترض  $F(\alpha_1^{p^t}) = F(\alpha^{p^t})$ ؛ إذن،  $F(\alpha^{p^t})$  قابل للفصل على  $F$ ، ولأن  $x^{p^t} - \alpha^{p^t} = (x - \alpha)^{p^t}$ ، فنرى أن  $\alpha$  هو الصفر الوحيد لـ  $x^{p^t} - \alpha^{p^t}$  في  $\bar{F}$ . يجب أن يكون كذلك حقلاً منتهياً - لأنه فضاء متجهات منتهي البعد على حقل منته  $F$  - إذن، الدالة

$$\sigma_p : F(\alpha^{p^t}) \rightarrow F(\alpha^{p^t})$$

المعطاة بـ  $\sigma_p(a) = a^p$ ، حيث  $a \in F(\alpha^{p^t})$ ، تماثل ذاتي على حسب المبرهنة 19.48. وعليه،  $(\sigma_p)^t$  تماثل ذاتي كذلك على  $F(\alpha^{p^t})$ ، و  $(\sigma_p)^t(a) = a^{p^t}$ .

لأن التماثل الذاتي على  $F(\alpha^{p^t})$  هو دالة غامرة، فيوجد  $\beta \in F(\alpha^{p^t})$  بحيث  $(\sigma_p)^t(\beta) = \alpha^{p^t}$ . وهكذا،  $\beta^{p^t} = \alpha^{p^t}$  وقد رأينا أن  $\alpha$  هو الصفر الوحيد لـ  $x^{p^t} - \alpha^{p^t}$ ؛ ولذلك، فيجب أن يكون  $\beta = \alpha$ . لأن  $\beta \in F(\alpha^{p^t})$ ، فإننا نحصل على  $F(\alpha) = F(\alpha^{p^t})$ ، ولأن  $F(\alpha^{p^t})$  كانت قابلة للفصل على  $F$ ، فإننا نرى الآن أن  $F(\alpha)$  قابلة للفصل على  $F$ ؛ لذلك،  $\alpha$  قابلة للفصل على  $F$  و  $t = 0$ . أثبتنا أنه لـ  $\alpha \in E$ ،  $\alpha$  قابلة للفصل على  $F$ ؛ إذن وبحسب النتيجة 10.51،  $E$  امتداد قابل للفصل على  $F$ . ♦

لقد أكملنا هدفنا، الذي كان إثبات أن كل حقل مميزه 0 وكل حقل منته له فقط امتدادات منتهية قابلة للفصل، أي إن هذه الحقول كاملة، وللامتدادات المنتهية  $E$  لمثل هذه الحقول الكاملة  $F$  يكون  $[E:F] = \{E:F\}$ .

#### مبرهنة العناصر البدائية

المبرهنة الآتية كلاسيكية في مبرهنة الحقول.

### 15.51 مبرهنة

(مبرهنة العناصر البدائية): ليكن  $E$  امتداداً منتهياً قابلاً للفصل على الحقل  $F$ ؛ إذن، يوجد  $\alpha \in E$  بحيث  $F = F(\alpha)$  (مثل هذا العنصر  $\alpha$  يسمى عنصراً بدائياً ((Primitive element)). بمعنى أن الامتداد المنتهي القابل للفصل لحقل يكون امتداداً بسيطاً. إذا كان  $F$  حقلاً منتهياً، فإن  $E$  حقل منته كذلك، لتكن  $\alpha$  مولدة للزمرة الدورية  $E^*$  من العناصر غير الصفريية في  $E$  بالنسبة إلى الضرب. (انظر المبرهنة 5.33). من الواضح أن  $E = F(\alpha)$ ، وهكذا فإن  $\alpha$  عنصر بدائي في هذه الحالة.

البرهان :

نفترض الآن أن  $F$  غير منته، ونثبت مبرهنتنا في حالة  $E = F(\beta, \gamma)$ ، فالمناقشة بالاستدلال الرياضي من هنا إلى الحالة العامة واضحة. لتكن  $\text{irr}(\beta, F)$  لها أصفار مختلفة  $\beta_1, \dots, \beta_n$ ، ولتكن  $\text{irr}(\gamma, F)$  لها أصفار مختلفة  $\gamma_1, \dots, \gamma_m$  في  $\bar{F}$ ، حيث الأصفار جميعها ذات تكرار 1؛ لأن  $E$  امتداد قابل للفصل على  $F$ ، ولأن  $F$  غير منته، فنستطيع أن نجد  $a \in F$ ، بحيث:

$$a \neq (\beta_i - \beta)(\gamma - \gamma_j)$$

لكل  $i$  و  $j \neq 1$  حيث  $j \neq 1$ ، بمعنى أن  $\beta_i - \beta_j \neq a(\gamma - \gamma_j)$ ، وبجعل  $a = \beta + a\gamma$ ، فإننا نحصل على

$$\alpha - a\gamma_j \neq \beta_i$$

لكل  $i$  ولكل  $j \neq 1$ . لتكن  $f(x) = \text{irr}(\beta, F)$ ، وافترض

$$h(x) = f(\alpha - ax) \in (F(\alpha))[x].$$

الآن،  $h(\gamma) = f(\beta) = 0$ ، على أي حال،  $h(\gamma_j) \neq 0$  لكل  $j \neq 1$  بالتعريف؛ لأن  $\beta_i$  هي الأصفار الوحيدة لـ  $f(x)$ ؛ إذن،  $h(x)$  و  $g(x) = \text{irr}(\gamma, F)$  لهما عامل مشترك في  $(F(\alpha))[x]$ ، وهو  $\text{irr}(\gamma, F(\alpha))$  الذي يجب أن يكون خطياً؛ لأن  $\gamma$  هو الصفر الوحيد المشترك لـ  $g(x)$  و  $h(x)$ ؛ إذن،  $\gamma \in F(\alpha)$ ، ولذلك،

$$\beta = \alpha - a\gamma \in F(\alpha), \text{ إذن، } F(\beta, \gamma) = F(\alpha).$$

يكون الامتداد المنتهي لحقل مميزه صفر امتداداً بسيطاً.

تثبت النتيجة مباشرة من المبرهنتين 13.51 و 15.51.

نرى أن الاحتمال الوحيد "للحالة السيئة" حيث يمكن أن يكون الامتداد المنتهي غير بسيط هو الامتداد المنتهي لحقل غير منتهٍ مميزه  $p \neq 0$ .

### 16.51 نتيجة

البرهان

■ تمارين 51

حسابات

في التمارين من 1 إلى 4، أوجد  $\alpha$  بحيث يكون الحقل المعطى  $\mathbb{Q}(\alpha)$ ، وأثبت أن  $\alpha$  هي بالتأكيد في الحقل المعطى، تحقق مستخدمًا الحسابات المباشرة أن المولدات المعطاة للامتداد على  $\mathbb{Q}$ ، يمكن بالتأكيد التعبير عنها بوصفها كثيرة حدود شكلية باستخدام  $\alpha$  ومعاملات من  $\mathbb{Q}$ .

1.  $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$       2.  $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$

3.  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$       4.  $\mathbb{Q}(i, \sqrt[3]{2})$

مفاهيم

في التمرينين 5 و 6، صحّح تعريف الحد المكتوب بخط مائل دون الرجوع إلى الكتاب، - إذا كانت هناك حاجة للتصحيح- بحيث يكون بصيغة قابلة للنشر.

5. ليكن  $\bar{F}$  الإغلاق الجبري للحقل  $F$ ، تكرر الصفر  $\alpha \in F$  لكثيرة الحدود  $f(x) \in F[x]$  هو  $v \in \mathbb{Z}^+$ ، إذا وفقط إذا كان  $(x - \alpha)^v$  هو أعلى قوة لـ  $x - \alpha$ ، وتكون عاملاً لـ  $f(x)$  في  $F[x]$ .

6. ليكن  $\bar{F}$  إغلاقاً جبرياً لـ  $F$ . العنصر  $\alpha$  في  $\bar{F}$  قابل للفصل على  $F$ ، إذا وفقط إذا كانت  $\alpha$  صفراً ذا تكرار 1 لـ  $\text{irr}(\alpha, F)$ .

7. أعط مثلاً على  $f(x) \in \mathbb{Q}[x]$  لا أصفار لها في  $\mathbb{Q}$ ، ولكن أصفارها في  $\mathbb{C}$  لها تكرار 2. فسّر كيف يتوافق هذا مع المبرهنة 13.51، التي تثبت أن  $\mathbb{Q}$  حقل كامل.

8. ضع إشارة صح أو إشارة خطأ:

أ. كل امتداد منتهٍ لأيّ حقل  $F$  قابل للفصل على  $F$ .

ب. كل امتداد منتهٍ لأيّ حقل منتهٍ  $F$  قابل للفصل على  $F$ .

ج. كل حقل ذي مميز 0 كامل.

د. كل كثيرة حدود من الدرجة  $n$  على أيّ حقل  $F$ ، لها دائماً  $n$  من الأصفار المختلفة في  $\bar{F}$ .

هـ. كل كثيرة حدود من الدرجة  $n$  على أيّ حقل كامل  $F$ ، لها دائماً  $n$  من الأصفار المختلفة في  $\bar{F}$ .

و. كل كثيرة حدود غير مختزلة من الدرجة  $n$  على أيّ حقل كامل  $F$ ، لها دائماً  $n$  من الأصفار المختلفة في  $\bar{F}$ .

ز. كل حقل مغلق جبرياً كامل.

ح. كل حقل  $F$  له امتداد جبري  $E$  بحيث يكون كاملاً.

ط. إذا كان الحقل  $E$  امتداد انشطار منتهياً قابلاً للفصل على  $F$ ، فإن  $[E : F] = |G(E/F)|$ .

ي. إذا كان الحقل  $E$  امتداد انشطار منتهياً لـ  $F$ ، فإن  $|G(E/F)|$  يقسم  $[E:F]$ .

براهين

9. أثبت أنه إذا كان كلا  $\alpha, \beta \in \bar{F}$  قابليين للفصل على  $F$ ، فإن  $\alpha \pm \beta$  و  $\alpha/\beta$  و  $a\beta$ ، إذا كانت  $\beta \neq 0$  كلها قابلة للفصل على  $F$ .

[مساعدة: استخدم المبرهنة 9.51 ونتيجتها].

10. أثبت أن  $\{1, y, \dots, y^{p-1}\}$  أساس لـ  $\mathbb{Z}_p(y)$  على  $\mathbb{Z}_p(y^p)$ ، حيث  $y$  غير معينة. بالرجوع إلى المثال 4.51، استنتج

بمناقشة الدرجة أن  $x^p - t$  غير مختزلة على  $\mathbb{Z}_p(t)$ ، حيث  $t = y^p$ .

11. أثبت أنه إذا كان  $E$  امتدادًا جبريًا لحقل كامل  $F$ ، فإن  $E$  كامل.

12. الامتداد الجبري - الذي يمكن أن يكون غير منته -  $E$  على الحقل  $F$  امتداد قابل للفصل على  $F$  (Separable extension).

(tension). إذا كان لكل  $\alpha \in E$  امتداد قابل للفصل على  $F$ ، بالمعنى المعرف في الكتاب. أثبت أن  $E$  امتداد يمكن أن يكون غير منته - قابل للفصل على  $F$  و  $K$  امتداد - يمكن أن يكون غير منته - قابل للفصل على  $E$ ، فإن  $K$  امتداد قابل للفصل على  $F$ .

13. ليكن  $E$  امتدادًا جبريًا للحقل  $F$ . أثبت أن مجموعة عناصر  $E$  جميعها القابلة للفصل على  $F$  تشكل حقلًا جزئيًا من  $E$ ، الإغلاق القابل للفصل لـ  $F$  في  $E$  (Separable Closure). [مساعدة: استخدم التمرين 9].

14. ليكن  $E$  حقلًا منتهيًا من الرتبة  $p^n$ .

أ. أثبت أن التماثل الذاتي لفروبينس  $\sigma_p$  له رتبة  $n$ .

ب. استنتج من الفرع (أ) أن  $G(E/\mathbb{Z}_p)$  دورية من الرتبة  $n$  ومولدة بـ  $\sigma_p$ .

[مساعدة: تذكر أن  $[E:F] = \{E:F\} = |G(E/\mathbb{Z}_p)|$  لا امتداد الانشطار المنتهي القابل للفصل  $E$  على  $F$ ].

تقدم التمارين من 15 إلى 22 المشتقات الشكلية في  $F[x]$ .

15. ليكن  $F$  أي حقل، ولتكن  $f(x) = a_0 + a_1x + \dots + a_nx^n$ ، ولتكن  $f(x) = a_0 + a_1x + \dots + a_nx^n$  المشتقة

$f'(x)$  لـ  $f(x)$  (derivative) هي كثيرة الحدود

$$f'(x) = a_1 + \dots + (i-1)a_ix^{i-1} + \dots + (n-1)a_nx^{n-1}$$

حيث  $i \geq 1$  لها معناها الطبيعي لـ  $i \in \mathbb{Z}^+$  و  $i \in F$ . هذه مشتقات شكلية؛ لا «نهايات» مطلوبة هنا.

أ. أثبت أن الدالة  $D: F[x] \rightarrow F[x]$  المعطاة بـ  $D(f(x)) = f'(x)$ ، تشاكل على  $\langle F[x], + \rangle$ .

ب. أوجد نواة  $D$  في حالة مميز  $F$  يساوي 0.

ج. أوجد نواة  $D$  في حالة مميز  $F$  يساوي  $p \neq 0$ .

16. استكمالاً لأفكار التمرين 15، أثبت أن:

أ.  $D(\alpha f(x)) = \alpha D(f(x))$  لكل  $f(x) \in F[x]$  و  $\alpha \in F$ .

ب.  $D(f(x)g(x)) = f(x)g'(x) + f'(x)g(x)$  لكل  $f(x), g(x) \in F[x]$ . [مساعدة: استخدم الفرع (أ) من هذا التمرين والتمرين السابق، ثم أكمل مستخدمًا الاستقراء الرياضي على درجة  $f(x)g(x)$ ].

ج.  $D((f(x))^m) = (m-1)f(x)^{m-1}f'(x)$  لكل  $f(x) \in F[x]$ . [مساعدة: استخدم الفرع (ب)].

17. لتكن  $f(x) \in F[x]$  وليكن  $a \in \bar{F}$  صفرًا لـ  $f(x)$  تكرر  $v$ ، فأثبت أن  $v > 1$  إذا وفقط إذا كانت  $\alpha$  صفرًا كذلك لـ  $f'(x)$ .

[مساعدة: طبق الفرع (ب) و(ج) في التمرين 16 على التحليل  $f(x) = (x-\alpha)^v g(x)$  لـ  $f(x)$  في الحلقة].

18. أثبت مستخدمًا التمرين 17، أن كل كثيرة حدود غير مختزلة على حقل  $F$  مميزه 0 قابلة للفصل.

[مساعدة: استخدم حقيقة أن  $\text{IIT}(\alpha, F)$  كثيرة حدود ذات درجة صغرى لـ  $\alpha$  على  $F$ ].

19. أثبت مستخدمًا التمرين 17، أن كثيرة الحدود غير المختزلة  $q(x)$  على حقل  $F$  مميزه  $p \neq 0$  غير قابلة للفصل، إذا وفقط إذا كان كل أس لكل حد في  $q(x)$  يقسم بـ  $p$ .

20. عمّم التمرين 17، بإثبات أن  $f(x) \in F[x]$  لا أصفار لها بتكرار  $< 1$ ، إذا وفقط إذا كانت  $f(x)$  و  $f'(x)$  بلا قواسم مشتركة في  $\bar{F}[x]$  من درجة  $< 0$ .

21. يجعل العمل أكثر صعوبة من العمل في التمرين 20، أثبت أن  $f(x) \in F[x]$  لا أصفار لها بتكرار  $< 1$ ، إذا وفقط إذا كانت  $f(x)$  و  $f'(x)$  بلا قواسم مشتركة غير ثابتة في  $F[x]$ . [مساعدة: استخدم المبرهنة 9.46 في إثبات أنه إذا كان 1 هو القاسم المشترك الأكبر لـ  $f(x)$  و  $f'(x)$  في  $F[x]$ ، فإنه القاسم المشترك الأكبر لهما في  $\bar{F}[x]$  كذلك].

22. صف إجراءً حسابيًا عملياً لتحديد ما إذا كانت  $f(x) \in F[x]$  لها أصفار تكررهما  $< 1$ ، من غير إيجاد أصفار  $f(x)$  فعلياً. [مساعدة: استخدم التمرين 21].

## الفصل 52

الامتدادات غير القابلة للفصل كلياً<sup>1</sup> Totally Inseparable Extensions

يثبت هذا الفصل أن الامتداد المنتهي  $E$  للحقل  $F$  يمكن أن يقسم إلى مرحلتين، هما: امتداد قابل للفصل  $K$  على  $F$ ، متبوعاً بامتداد آخر  $L$  إلى  $K$ ، الذي يكون أبعد عن أنه قابل للفصل بوصفه أبعد ما يمكن أن يتخيله المرء.

سنطور نظريتنا عن الامتدادات غير القابلة للفصل كلياً بطريقة موزاية لطريقة تطوير الامتدادات القابلة للفصل.

## 1.52 تعريف

يكون الامتداد المنتهي  $E$  للحقل  $F$  غير قابل للفصل كلياً على  $F$  (**totally inseparable extension**)، إذا كان  $[E:F] = 1$ ، ويكون العنصر  $a$  في  $\bar{F}$  غير قابل للفصل كلياً على  $F$ ، إذا كان  $F(a)$  غير قابل للفصل كلياً على  $F$ .

نعلم أن  $\{F(a):F\}$  يساوي عدد الأصفار المختلفة لـ  $\text{irr}(\alpha, F)$ ؛ إذن،  $\alpha$  غير قابلة للفصل كلياً على  $F$ ، إذا وفقط إذا كانت  $\text{irr}(\alpha, F)$  لها صفر واحد تكراره  $1 < 1$ .

## 2.52 مثال

بالعودة إلى المثال 5.51، نرى أن  $\mathbb{Z}_p(y)$  غير قابل للفصل كلياً على  $\mathbb{Z}_p(y^p)$ ، حيث  $y$  غير معينة.

## 3.52 مبرهنة

(نظيرة المبرهنة 9.51): إذا كان  $K$  امتداداً منتهياً لـ  $E$ ، وكان  $E$  امتداداً منتهياً لـ  $F$ ، و  $F \leq E \leq K$ ، فإن  $K$  غير قابل للفصل كلياً على  $F$ ، إذا وفقط إذا كان  $K$  غير قابل للفصل كلياً على  $E$ ، و  $E$  غير قابل للفصل كلياً على  $F$ .

## البرهان

لأن  $E < K$ ، فإننا نحصل على  $[K:E] > 1$  و  $[E:F] > 1$ . افترض أن  $K$  غير قابل للفصل كلياً على  $F$ ،

كلياً على  $F$ ؛ إذن،  $\{K:F\} = 1$ ، و  $\{K:E\}\{E:F\}$ ، و  $\{K:F\} = 1$ ، يجب أن نحصل على:

$$\{K:E\} = 1 < [E:F] \text{ و } \{E:F\} = 1 < [K:E]$$

وبذلك،  $K$  غير قابل للفصل كلياً على  $E$ ، و  $E$  غير قابل للفصل كلياً على  $F$ .

في المقابل، إذا كان  $K$  غير قابل للفصل كلياً على  $E$ ، و  $E$  غير قابل للفصل كلياً على  $F$ ، فإن:

$$\{K:F\} = \{K:E\}\{E:F\} = (1)(1) = 1,$$



و  $[K:F] > 1$ ؛ إذن  $K$  غير قابل للفصل كلياً على  $F$ .

## 4.52 نتيجة

(نظيرة النتيجة 10.51): إذا كان  $E$  امتداداً منتهياً لـ  $F$ ، فإن  $E$  غير قابل للفصل كلياً على  $F$ ، إذا وفقط إذا كانت كل  $\alpha$  في  $E$  و  $\alpha \notin F$  غير قابلة للفصل كلياً على  $F$ .

## البرهان

افترض أن  $E$  غير قابل للفصل كلياً على  $F$ ، ولتكن  $\alpha \in E$  و  $\alpha \notin F$ ، فإن

$$F < F(\alpha) \leq E$$

إذا كان  $F(\alpha) = E$ ، نكون قد انتهينا، بحسب تعريف  $\alpha$  غير قابلة للفصل كلياً على  $F$ .

إذا كان  $F < F(\alpha) < E$ ، فإن المبرهنة 3.52 تثبت ذلك؛ ولأن  $E$  غير قابل للفصل كلياً على  $F$ ، فإن  $F(\alpha)$  غير قابل للفصل كلياً على  $F$ .

<sup>1</sup> لن يستخدم هذا الفصل فيما تبقى من الكتاب

في المقابل، افترض أنه لكل  $\alpha \in E$ ،  $\alpha \notin F$  و  $\alpha$  غير قابلة للفصل كلياً على  $F$ . لأن  $E$  منتهية على  $F$ ، فيوجد  $\alpha_1, \dots, \alpha_n$ ، بحيث:

$$F < F(\alpha_1) < F(\alpha_1, \alpha_2) < \dots < E = F(\alpha_1, \dots, \alpha_n).$$

ولأن كل  $\alpha_i$  غير قابلة للفصل كلياً على  $F$ ،  $\alpha_i$  غير قابلة للفصل كلياً على  $F(\alpha_1, \dots, \alpha_{i-1})$ : لأن  $q(x) = \text{irr}(\alpha_i, F(\alpha_1, \dots, \alpha_{i-1}))$  تقسم  $\text{irr}(\alpha_i, F)$  بحيث  $\alpha_i$  هو الصفر الوحيد لـ  $q(x)$  وله تكرار  $< 1$ ؛ إذن،  $F(\alpha_1, \dots, \alpha_i)$  غير قابل للفصل كلياً على  $F(\alpha_1, \dots, \alpha_{i-1})$ ، و  $E$  غير قابل للفصل كلياً على  $F$ ، بحسب المبرهنة 3.52 معممة باستخدام الاستقراء الرياضي. ♦

لقد قمنا بعمل موازٍ لعملنا في الفصل 51، بحيث نستطيع التعامل مع هذه الأفكار معاً.

### الإغلاقات القابلة للفصل

نأتي الآن للسبب الرئيس لإدراج هذه المادة.

ليكن  $F$  ذا مميز  $p \neq 0$ ، وليكن  $E$  امتداداً منتهياً لـ  $F$ ؛ إذن،  $\alpha \in E$  و  $\alpha \notin F$  غير قابلة للفصل كلياً على  $F$ ، إذا وفقط إذا وجد عدد صحيح  $t \geq 1$ ، بحيث  $\alpha^{p^t} \in F$ .

وكذلك يوجد امتداد وحيد لـ  $F$ ، بحيث  $F \leq K \leq E$  و  $K$  قابل للفصل على  $F$ ، وإما  $E = K$  أو  $E$  غير قابل للفصل كلياً على  $K$ .

لتكن  $\alpha \in E$ ،  $\alpha \notin F$ ، غير قابلة للفصل كلياً على  $F$ ؛ إذن، يوجد صفر وحيد  $\alpha$  لـ  $\text{irr}(\alpha, F)$  (تكراره  $< 1$ ، وكما جاء في إثبات المبرهنة 14.51، يجب أن تكون  $\text{irr}(\alpha, F)$  على الصورة:

$$x^{p^t} - \alpha^{p^t}.$$

إذن،  $\alpha^{p^t} \in F$ ، حيث  $t \geq 1$ .

في المقابل، إذا كانت  $\alpha^{p^t} \in F$  حيث  $t \geq 1$  و  $\alpha \notin F$ ، فإن:

$$x^{p^t} - \alpha^{p^t} = (x - \alpha)^{p^t}$$

و  $(x^{p^t} - \alpha^{p^t}) \in F[x]$ ، مثبتاً أن  $\text{irr}(\alpha, F)$  تقسم  $(x - \alpha)^{p^t}$ ؛ إذن،  $\alpha$  هو الصفر الوحيد لـ  $\text{irr}(\alpha, F)$ ، وهذا الصفر تكراره  $< 1$ ، ما يعني أن  $\alpha$  غير قابلة للفصل كلياً على  $F$ .

للجزء الثاني من المبرهنة، لتكن  $E = F(\alpha_1, \dots, \alpha_n)$ ؛ إذا كان

$$\text{irr}(\alpha_i, F) = \prod_j (x^{p^{t_j}} - \alpha_{ij} p^{t_j})$$

حيث  $\alpha_{i1} = \alpha_i$ ، لتكن  $\beta_{ij} = \alpha_{ij} p^{t_j}$ ، نحصل على  $F(\beta_{11}, \beta_{21}, \dots, \beta_{n1}) \leq E$ ، و  $\beta_{i1}$  صفر لـ

$$f_i(x) = \prod_j (x - \beta_{ij})$$

مبرهنة 5.52

البرهان

حيث  $f_i(x) \in F[x]$ ، لأنَّ الرفع للقوة  $p$  يعطي التماثل  $\sigma_p$  من  $E$  إلى حقل جزئي من  $E$ ، الرفع إلى القوة  $p^t$  هو دالة التماثل  $(\sigma_p)^t$  من  $E$  إلى حقل جزئي من  $E$ ، ولأنَّ  $\alpha_{ij}$  كلها مختلفة لـ  $i$  محددة، فكذا  $\beta_{ij}$  لـ  $i$  محددة؛ لذلك،  $\beta_{ij}$  قابلة للفصل على  $F$ .

لأنَّه صفر لكثيرة الحدود  $f_i(x)$  في  $F[x]$ ، التي أصفارها ذات تكرار 1؛ إذن:

$$K = F(\beta_{11}, \beta_{21}, \dots, \beta_{n1})$$

قابل للفصل على  $F$ ، بحسب برهان النتيجة 10.51.

إذا كانت كل  $\alpha_i^{p^t} \neq 1$ ، فإن  $K = E$ ، أما إذا كان بعض  $\alpha_i^{p^t} = 1$ ، فإن  $K \neq E$ ، و  $\alpha_i^{p^t} = \beta_{i1}$ ، عنصر في  $K$ ، ما يثبت أنَّ كل  $\alpha_i \notin K$  غير قابل للفصل كلياً على  $K$  - بحسب الجزء الأول من هذه المبرهنة -.

إذن،  $E = K(\alpha_1, \dots, \alpha_n)$  غير قابلة للفصل كلياً على  $K$  - بحسب برهان النتيجة 4.52.

ينتج من النتيجتين 10.51 و 4.52 أنَّ الحقل  $K$  يتكوّن من العناصر  $\alpha$  جميعها في  $E$  القابلة للفصل على  $F$ ؛ إذن  $K$  وحيد.

يسمى الحقل الوحيد  $K$  في المبرهنة 5.52 الإغلاق القابل للفصل لـ  $F$  في  $E$

## 6.52 تعريف

(separable closure).

تعرض المبرهنة السابقة التركيب الدقيق للامتدادات غير القابلة للفصل كلياً لحقل مميزه  $0 \neq p$ . يمكن الحصول على هذا الامتداد بتكرار إضافة الأصفار التي ترتيبها  $p$  لعناصر ليست قوى لـ  $p$ . نشير إلى أنَّ المبرهنة 5.52 صحيحة للامتدادات الجبرية غير المنتهية  $E$  لـ  $F$ . إثبات الجزء الأول من المبرهنة صحيح كذلك في حالة الامتدادات غير المنتهية، أما الجزء الثاني، فلأنَّ  $\alpha \pm \beta, \alpha\beta$ ، و  $\alpha/\beta$ ، عندما  $\beta \neq 0$  كلها محتواة في الحقل  $F(\alpha, \beta)$ ، فإنَّ عناصر  $E$  جميعها القابلة للفصل على  $F$  تشكل حقلاً جزئياً  $K$  من  $E$  - الإغلاق القابل للفصل لـ  $F$  في  $E$ ، ما يؤدي إلى أنَّ  $\alpha \in E$  و  $\alpha \notin K$  غير قابلة للفصل كلياً على  $K$ ؛ لأنَّ  $\alpha$  ومعاملات  $\text{irr}(\alpha, K)$  جميعها محتواة في امتداد منتهٍ لـ  $F$ ، وعليه، يمكن تطبيق المبرهنة 5.52.

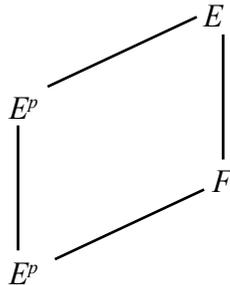
■ تمارين 52

مفاهيم

1. لتكن  $y$  و  $z$  غير معينة، ولتكن  $u = y^{12}$  و  $v = z^{18}$ . صف الإغلاق القابل للفصل لـ  $\mathbb{Z}_3(u, v)$  في  $\mathbb{Z}_3(y, z)$ .
2. لتكن  $y$  و  $z$  غير معينة، ولتكن  $u = y^{12}$  و  $v = y^2 z^{18}$ . صف الإغلاق القابل للفصل لـ  $\mathbb{Z}_3(u, v)$  في  $\mathbb{Z}_3(y, z)$ .
3. بالرجوع إلى التمرين 1، صف الإغلاق غير القابل للفصل كلياً (انظر التمرين 6) لـ  $\mathbb{Z}_3(u, v)$  في  $\mathbb{Z}_3(y, z)$ .
4. بالرجوع إلى التمرين 2، صف الإغلاق غير القابل للفصل كلياً لـ  $\mathbb{Z}_3(u, v)$  في  $\mathbb{Z}_3(y, z)$ . (انظر التمرين 6).
5. ضع إشارة صح أو إشارة خطأ:
  - أ. لا يوجد امتداد جبري فعلي لحقل غير منتهٍ مميزه  $p \neq 0$ ، يمكن أن يكون امتداداً قابلاً للفصل.
  - ب. إذا كان  $F(\alpha)$  غير قابل للفصل كلياً على  $F$  ذي المميز  $p \neq 0$ ، فإن  $\alpha^t \in F$  حيث  $t > 0$ .
  - ج. لغير المعين  $y$ ، قابل للفصل على  $\mathbb{Z}_5(y)$  قابل للفصل على  $\mathbb{Z}_5(y^5)$ .
  - د. لغير المعين  $y$ ، قابل للفصل على  $\mathbb{Z}_5(y)$  قابل للفصل على  $\mathbb{Z}_5(y^{10})$ .
  - هـ. لغير المعين  $y$ ،  $\mathbb{Z}_5(y)$  غير قابل للفصل كلياً على  $\mathbb{Z}_5(y^{10})$ .
  - و. إذا كان  $F$  حقلاً و  $a$  جبرية على  $F$ ، فإن  $a$  إما قابلة للفصل أو غير قابلة للفصل كلياً على  $F$ .
  - ز. إذا كان  $E$  امتداداً جبرياً للحقل  $F$ ، فإن  $F$  إغلاقاً قابلاً للفصل في  $E$ .
  - ح. إذا كان  $E$  امتداداً جبرياً للحقل  $F$ ، فإن  $E$  غير قابل للفصل كلياً على الإغلاق القابل للفصل لـ  $F$  في  $E$ .
  - ط. إذا كان  $E$  امتداداً جبرياً للحقل  $F$ ، و  $E$  ليس امتداداً قابلاً للفصل على  $F$ ، فإن  $E$  غير قابل للفصل كلياً على الإغلاق القابل للفصل لـ  $F$  في  $E$ .
  - ي. إذا كانت  $\alpha$  غير قابلة للفصل كلياً على  $F$ ، فإن  $\alpha$  هو الصفر الوحيد لـ  $\text{irr}(\alpha, F)$ .

براهين

6. أثبت أنه إذا كان  $E$  امتداداً جبرياً للحقل  $F$ ، فإن اتحاد  $F$  ومجموعة عناصر  $E$  غير القابلة للفصل كلياً على  $F$ ، تشكل حقلاً جزئياً من  $E$ ، الإغلاق غير القابل للفصل كلياً لـ  $F$  في  $E$  (totally inseparable closure).
7. أثبت أن الحقل  $F$  ذا المميز  $p \neq 0$  كامل إذا وفقط إذا كان  $F^p = F$ ، بمعنى أن كل عنصر في  $F$  هو القوة  $p$  لعنصر في  $F$ .
8. ليكن  $E$  امتداداً منتهياً للحقل  $F$  ذي المميز  $p$ . باستخدام مصطلحات التمرين 7، أثبت أن  $E^p = E$  إذا وفقط إذا كان  $E^p = E$ . [مساعدة: الدالة  $\sigma_p: E \rightarrow E$  المعرفة بـ  $\sigma_p(\alpha) = \alpha^p$ ، حيث  $\alpha \in E$  تماثل إلى حقل جزئي من  $E$ . افترض المخطط في الشكل 7.52 ثم ناقش الدرجة].



الشكل 7.52

## الفصل 53

## ملخص

## مبرهنة جالوا Galois Theory

هذا الفصل ربما يكون ذروة مادة البحث في كل الكتاب، حيث تعطي مبرهنة جالوا التفاعل الجميل بين نظريتي الزمر والحقول، وقد كان عملنا يقصد هذا الهدف بدءاً من الفصل 48، وسنبداً باستذكار النتائج الرئيسية التي طورناها، حيث يتعين أن تكون في الذاكرة تماماً:

1. ليكن  $F \leq E \leq \bar{F}$ ،  $\alpha \in E$ ، ولتكن  $\beta$  مرافقة لـ  $\alpha$  على  $F$  بمعنى أن  $\beta$  صفر كذلك لـ  $\text{irr}(\alpha, F)$ ؛ إذن، يوجد تماثل  $\psi_{\alpha, \beta}$  يربط  $F(\alpha)$  بصورة غامرة مع  $F(\beta)$ ، ويترك  $F$  ثابتة، ويربط  $\alpha$  بـ  $\beta$ .
2. إذا كان  $F \leq E \leq \bar{F}$  و  $\alpha \in E$ ، فإن التماثل الذاتي  $\sigma$  على  $\bar{F}$  ويترك  $F$  ثابتة، يجب أن يربط  $\alpha$  بأحد مرافقات  $\alpha$  على  $F$ .
3. إذا كانت  $F \leq E$ ، تشكل مجموعة التماثلات الذاتية على  $E$  التي تترك  $F$  ثابتة الزمرة  $G(E/F)$ ، فلأي مجموعة جزئية  $S$  من  $G(E/F)$ ، تشكل مجموعة عناصر  $E$  جميعها التي تترك ثابتة بعناصر  $S$  كلها، حقلاً  $E_S$ ، وكذلك فإن  $F \leq E_{G(E/F)}$ .
4. يكون الحقل  $E$ ،  $F \leq E \leq \bar{F}$ ، حقل انشطار على  $F$ ، إذا وفقط إذا كان كل تماثل من  $E$  إلى حقل جزئي من  $\bar{F}$  ويترك  $F$  ثابتة، تماثل ذاتي على  $E$ ، وإذا كان  $E$  امتداداً منتهياً وحقل انشطار على  $F$ ، فإن  $|G(F/E)| = \{F : E\}$ .
5. إذا كان  $E$  امتداداً منتهياً لـ  $F$ ، فإن  $\{E : F\}$  يقسم  $[E : F]$ ، وإذا كان  $E$  قابلاً للفصل على  $F$  كذلك، فإن  $[E : F] = \{E : F\}$ ، وكذلك فإن  $E$  قابل للفصل على  $F$ ، إذا وفقط إذا كانت أصفار  $\text{irr}(\alpha, F)$  جميعها تكرر لها 1، لكل  $\alpha \in E$ .
6. إذا كان  $E$  امتداداً منتهياً على  $F$  وقابلاً للفصل وحقل انشطار على  $F$ ، فإن:  $|G(E/F)| = \{E : F\} = [E : F]$ .

## الامتدادات الناظمية

سنكون مهتمين بالامتدادات المنتهية  $K$  لـ  $F$ ، بحيث إن كل تماثل من  $K$  إلى حقل جزئي من  $\bar{F}$  ويترك  $F$  ثابتة، يكون تماثلاً ذاتياً على  $K$ ، ويحقق:

$$[K : F] = \{K : F\}.$$

بالنظر إلى النتيجتين 4 و 5، هذه هي الامتدادات المنتهية لـ  $F$  التي تكون قابلة للفصل وحقول انشطار على  $F$ .

يكون الامتداد المنتهي  $K$  لـ  $F$  امتداداً ناظمياً منتهياً لـ  $F$  (finite normal extension)، إذا كان  $K$  قابلاً للفصل وحقل انشطار على  $F$ .

افترض أن  $K$  امتداد منته ناظمي على  $F$ ، حيث  $F \leq K$  - كالعادة - إذن وبحسب النتيجة 4، كل تماثل على  $\bar{F}$  ويترك  $F$  ثابتة، ينتج تماثلاً ذاتياً على  $K$ ، وكما في السابق نترك  $G(K/F)$  لتكون زمرة التماثلات الذاتية جميعها المعرفة على  $K$  وتترك  $F$  ثابتة، إذ سنكون جاهزين بعد خطوة واحدة أخرى لتوضيح المبرهنة الأساسية.

ليكن  $K$  امتداداً منتهياً ناظمياً على  $F$ ، وليكن  $E$  امتداداً لـ  $F$ ، بحيث  $F \leq E \leq \bar{F}$ ؛ إذن،  $K$  امتداد منته ناظمي على  $E$ ، و  $G(K/E)$  هو بالتحديد الزمرة الجزئية.

## 1.53 تعريف

## 2.53 مبرهنة

من  $G(K/F)$  المكوّنة من التماثلات الذاتية التي تترك  $E$  ثابتة. إضافة إلى ذلك، يولد التماثلان الذاتيَّان  $\sigma$  و  $\tau$  من  $G(K/F)$  التماثل نفسه من  $E$  إلى حقل جزئي من  $\bar{F}$ ، إذا وفقط إذا كانا في المجموعة المشاركة اليسرى نفسها لـ  $G(K/E)$  في  $G(K/F)$ .

البرهان

إذا كان  $K$  حقل انشطار للمجموعة  $\{f_i(x) \mid i \in I\}$  من كثيرات الحدود في  $F[x]$ ، فإن  $K$  حقل انشطار على  $E$  لهذه المجموعة نفسها من كثيرات الحدود معتبرة بوصفها عناصر في  $E[x]$ . حيث تثبت المبرهنة 9.51 أن  $K$  قابل للفصل على  $E$ ؛ لأنه قابل للفصل على  $F$ ؛ إذن،  $K$  امتداد ناظمي على  $E$ ، وهذا يبرهن الزعم الأول.

الآن كل عنصر في  $G(K/E)$  هو تماثل ذاتي على  $K$  ويترك  $F$  ثابتة؛ لأنها تترك الحقل الأكبر  $E$  ثابتاً؛ إذن، يمكن النظر إلى  $G(K/E)$  بوصفها مجموعة جزئية من  $G(K/F)$ ، ولأن  $G(K/E) \leq G(K/F)$  زمرة مع عملية تركيب الدوال كذلك، فإننا نرى أن  $G(K/E) \leq G(K/F)$ .

أخيراً، لـ  $\sigma$  و  $\tau$  في  $G(K/E)$ ، تقع  $\sigma$  و  $\tau$  في المجموعة المشاركة اليسرى نفسها لـ  $G(K/E)$ ، إذا وفقط إذا كان  $\tau^{-1}\sigma \in G(K/E)$ ، أو إذا وفقط إذا كان  $\sigma = \tau\mu$ ، حيث  $\mu \in G(K/E)$ ؛ ولكن، إذا كان  $\sigma = \tau\mu$ ، فإنه لكل  $\alpha \in E$

$$\sigma(\alpha) = (\tau\mu)(\alpha) = \tau(\mu(\alpha)) = \tau(\alpha),$$

لأن  $\mu(\alpha) = \alpha$  لكل  $\alpha \in E$ . في المقابل، إذا كان  $\sigma(\alpha) = \tau(\alpha)$  لكل  $\alpha \in E$ ، فإن

$$(\tau^{-1}\sigma)(\alpha) = \alpha$$

لـ  $\alpha \in E$ ، وهذا يعني أن  $\tau^{-1}\sigma$  تترك  $E$  ثابتة، و  $\mu = \tau^{-1}\sigma$  لذلك تنتمي إلى  $G(K/E)$ . ♦

تثبت المبرهنة السابقة أن هناك تقابلاً بين المجموعات المشاركة اليسرى لـ  $G(K/E)$  في  $G(K/F)$ ، والتماثلات من  $E$  إلى حقل جزئي من  $K$  وتترك  $F$  ثابتة. لاحظ أننا لا نستطيع القول: إن هذه المجموعات المشاركة اليسرى تقابل تماثلات ذاتية من  $E$  على  $F$ ؛ لأن  $E$  قد لا يكون حقل انشطار على  $F$ . بالطبع، لو كان  $E$  امتداداً ناظماً على  $F$ ، فإن هذه التماثلات ستصبح تماثلات ذاتية من  $E$  على  $F$ ، حيث يمكننا أن نزن أن هذا سيحدث، إذا وفقط إذا كان  $G(K/E)$  زمرة جزئية ناظمية من  $G(K/F)$ ، وهذه هي الحالة حقاً.

بمعنى أن الاستخدامين المختلفين لكلمة ناظمي وثيق الصلة بصورة حقيقية؛ إذن، إذا كان  $E$  امتداداً ناظماً لـ  $F$ ، فإن المجموعات المشاركة اليسرى لـ  $G(K/E)$  في  $G(K/F)$  يمكن النظر إليها بوصفها عناصر في زمرة العامل  $G(K/F)/G(K/E)$ ، وهي زمرة التماثلات الذاتية المؤثرة في  $E$  وتترك  $F$  ثابتة، سوف تثبت أن زمرة العامل هذه تماثل  $G(E/F)$ .

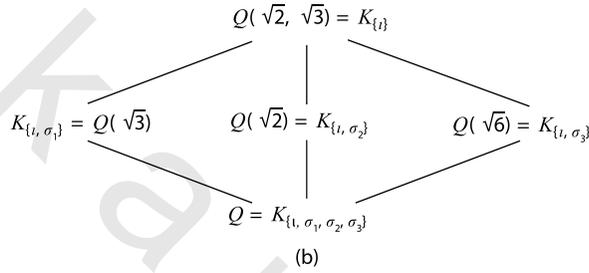
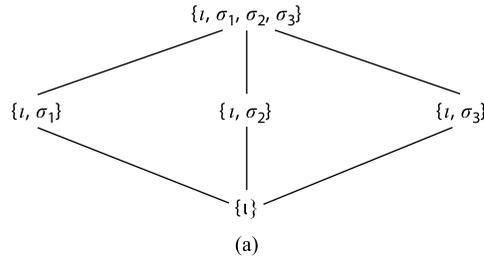
#### المبرهنة الأساسية

تنص المبرهنة الأساسية في مبرهنة جالوا على أنه لامتداد ناظمي منته  $K$  للحقل  $F$ ، يوجد تقابل بين الزمر الجزئية لـ  $G(K/F)$  والحقول المتوسطة  $E$ ، حيث  $F \leq E \leq K$ .

هذا التقابل يربط بكل حقل متوسط  $E$  الزمرة الجزئية  $G(K/E)$ . ويمكننا كذلك الانتقال للجهة الأخرى، والبدء بالزمرة الجزئية  $H$  من  $G(K/F)$ ، ونقابل  $H$  بالحقل الثابت  $K_H$ . سنوضح هذا بمثال، ثم نقدّم نصّ المبرهنة، ونناقش إثباتها.

## 3.53 مثال

ليكن  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  الآن  $K$  امتداد ناظمي لـ  $\mathbb{Q}$ . ويثبت المثال 17.48 أنه يوجد أربعة تماثلات ذاتية على  $K$  وتترك  $\mathbb{Q}$  ثابتة، نُذكرُ بها بإعطاء قيمها على الأساس  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$  لـ  $K$  على  $\mathbb{Q}$ .



الشكل 4.53 (أ) مخطط الزمر (ب) مخطط الحقول

$\tau$ : الدالة المحايدة.

$\sigma_1$ : تربط  $\sqrt{2}$  بـ  $-\sqrt{2}$ ،  $\sqrt{3}$  بـ  $\sqrt{3}$ ، و  $\sqrt{6}$  بـ  $-\sqrt{6}$  وتترك الباقي ثابتًا.

$\sigma_2$ : تربط  $\sqrt{3}$  بـ  $-\sqrt{3}$ ،  $\sqrt{2}$  بـ  $\sqrt{2}$ ، و  $\sqrt{6}$  بـ  $-\sqrt{6}$  وتترك الباقي ثابتًا.

$\sigma_3$ : تربط  $\sqrt{2}$  بـ  $-\sqrt{2}$ ،  $\sqrt{3}$  بـ  $\sqrt{3}$ ، و  $\sqrt{6}$  بـ  $\sqrt{6}$  وتترك الباقي ثابتًا.

رأينا أن  $\{1, \sigma_1, \sigma_2, \sigma_3\}$  تماثل زمرة كلاين الرباعية، والقائمة الكاملة للزمر الجزئية، ومقرونة بكل زمرة جزئية الحقل المتوسط الذي تتركه ثابتًا، هي كما يأتي:

$$\{i, \sigma_1, \sigma_2, \sigma_3\} \leftrightarrow \mathbb{Q},$$

$$\{i, \sigma_1\} \leftrightarrow \mathbb{Q}(\sqrt{3}),$$

$$\{i, \sigma_2\} \leftrightarrow \mathbb{Q}(\sqrt{2}),$$

$$\{i, \sigma_3\} \leftrightarrow \mathbb{Q}(\sqrt{6}),$$

$$\{i\} \leftrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

الزمر الجزئية كلها من الزمرة الإبدالية  $\{1, \sigma_1, \sigma_2, \sigma_3\}$  زمر جزئية ناظمية، والحقول المتوسطة كلها امتدادات ناظمية لـ  $\mathbb{Q}$ ، أليس هذا رائعًا؟!

لاحظ أنه إذا كانت إحدى الزمر الجزئية محتواة في أخرى، فإن الأكبر من هاتين الزمرتين الجزئيتين تقابل الأصغر من الحقلين الثابتين المقابلين، فكلما كبرت الزمرة الجزئية، أي كلما زاد عدد التماثلات الذاتية صغر الحقل الثابت، أي قل عدد العناصر المتروكة ثابتة، لقد أعطينا في الشكل 4.53 الرسوم المتقابلة للزمر الجزئية والحقول المتوسطة، ولاحظ مرة ثانية أن الزمر قرب القمة تقابل الحقول قرب القاع، بمعنى أن أحد الرسمين يشبه الآخر مقلوباً رأساً على عقب، ولأن الرسم هنا في الحقيقة يشبه نفسه مقلوباً رأساً على عقب، فإنه ليس مثلاً جيداً لنا.

لتوضيح المبدأ المقابل، تقدّم إلى الأمام للشكل 6.54 لترى الرسم الذي لا يشبه معكوسه. ▲

### 5.53 تعريف

إذا كان  $K$  امتداداً ناظماً منتهياً للحقل  $F$ ، فإن  $G(K/F)$  زمرة جالوا لـ  $K$  على  $F$  (Galois group).

سنذكر الآن نصّ المبرهنة الرئيسية، ثم نعطي مثلاً آخر، وأخيراً نكمل إثبات المبرهنة الأساسية.

### 6.53 مبرهنة

(المبرهنة الرئيسية في مبرهنة جالوا): ليكن  $K$  امتداداً منتهياً ناظماً على الحقل  $F$ ، مع زمرة جالوا  $G(K/F)$ . لأي حقل  $E$ ، حيث  $F \leq E \leq K$ ، لتكن  $\lambda(E)$  الزمرة الجزئية من  $G(K/E)$  التي تترك  $E$  ثابتة؛ إذن،  $\lambda$  دالة تقابل من مجموعة هذه الحقول المتوسطة  $E$  إلى مجموعة الزمر الجزئية من  $G(K/F)$ ، حيث تتحقق الخصائص الآتية لـ  $\lambda$ :

$$1. \lambda(E) = G(K/E).$$

$$2. E = K_{G(K/E)} = K_{\lambda(E)}.$$

$$3. \lambda(E_H) = H, \text{ إذا كانت } H \leq G(K/F).$$

$$4. [K : E] = |\lambda(E)| \text{ و } [E : F] = (G(K/F) : \lambda(E)), \text{ عدد المجموعات المشاركة اليسرى لـ } G(K/F) \text{ في } \lambda(E).$$

5.  $E$  امتداد ناظمي على  $F$ ، إذا وفقط إذا كانت  $\lambda(E)$  زمرة جزئية ناظمية من  $G(K/F)$ ، وعندما تكون  $\lambda(E)$  زمرة جزئية ناظمية في  $G(K/F)$ ، فإن:

$$G(E/F) \cong G(K/F) / G(K/E).$$

6. الرسم البياني للزمر الجزئية من  $G(K/F)$ ، هو معكوس الرسم البياني للحقول المتوسطة من  $K$  على  $F$ .

ملاحظات على البرهان: في الحقيقة أثبتنا تَوْاً جزءاً كبيراً من هذه المبرهنة، لنرَكم تبقى علينا لنثبته.

الخاصية 1 هي مجرد تعريف  $\lambda$  المذكور في نصّ المبرهنة، وتثبت المبرهنة 15.48 للخاصية 2 أن:

$$E \leq K_{G(K/E)}.$$

لتكن  $\alpha \in K$ ، حيث  $\alpha \notin E$ ، ولأن  $K$  امتداد ناظمي على  $E$ ، وباستخدام تماثل الترافق ومبرهنة تمدد التماثلات، فيمكننا أن نجد تماثلاً ذاتياً على  $K$ ، ويترك  $E$  ثابتة، ويربط  $\alpha$  بالأصفار المختلفة لـ  $\text{irr}(\alpha, F)$ ، وهذا يؤدي إلى أن:

$$K_{G(K/E)} \leq E,$$

إذن،  $E = K_{G(K/E)}$ ، وهذا يثبت الخاصية 2، ويخبرنا كذلك بأن  $\lambda$  أحادية؛ لأنه إذا كان  $\lambda(E_1) = \lambda(E_2)$ ، فإننا وبحسب الخاصية 2 نحصل على:

$$E_1 = K_{\lambda(E_1)} = K_{\lambda(E_2)} = E_2$$

الآن، ستكون الخاصية 3 عملنا الأساسي، وهذا يعادل تماماً إثبات أن  $\lambda$  دالة غامرة. بالطبع، إذا كانت  $H \leq G(K/F)$ ، فإن  $H \leq \lambda(K_H)$ ؛ لأن  $H$  متضمنة بالتأكيد في مجموعة التماثلات الذاتية كلها التي تترك  $K_H$  ثابتة، حيث سنستخدم هنا بقوة خاصيتنا  $\{K : E\} = [K : E]$ .

نستنتج الخاصية 4 من،  $[E : F] = \{E : F\}$ ،  $[K : E] = \{K : E\}$ ، والعبارة الأخيرة في المبرهنة 2.53.

سيبقى علينا إثبات أن المعنيين لكلمة ناظمي تتقابل في الخاصية 5.

وقد أثبتنا توأماً الخاصية 6 في المثال 3.53؛ إذن، يبقى علينا إثبات الخاصيتين 3 و 5.

المبرهنة الرئيسة لمبرهنة جالوا أداة قوية لدراسة أصفار كثيرات الحدود. فإذا كانت  $f(x) \in F[x]$ ، بحيث إن كل عامل غير مختزل لـ  $f(x)$  قابل للفصل على  $F$ ، فإن حقل الانشطار  $K$  لـ  $f(x)$  على  $F$  امتداد ناظمي لـ  $F$ . زمرة جالوا  $G(K/F)$  هي زمرة كثيرة الحدود  $f(x)$  على  $F$ ، ويمكن أن تعطى بنية هذه الزمرة معلومات ذات فائدة بخصوص أصفار  $f(x)$ ، سيوضح هذا بصورة مدهشة في الفصل 56 عندما نحقق هدفنا النهائي.

### زمر جالوا على الحقول المنتهية

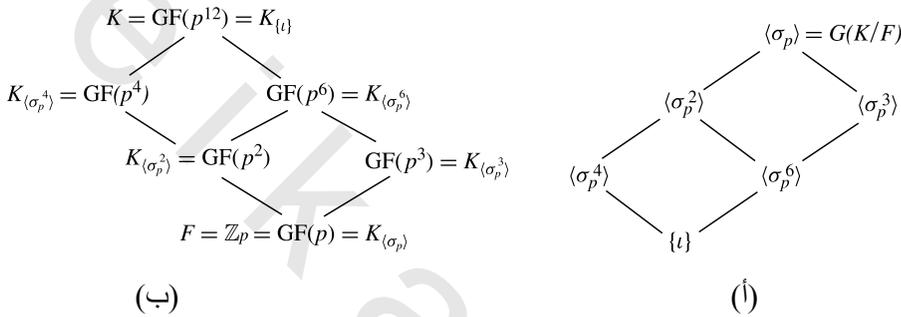
ليكن  $K$  امتداداً منتهياً للحقل المنتهي  $F$ ، لقد رأينا أن  $K$  امتداد قابل للفصل على  $F$  (الحقل المنتهي كامل). افترض أن رتبة  $F$  هي  $p^r$  و  $[K : F] = n$ ، إذن، رتبة  $K$  تساوي  $p^{rn}$ ، وقد رأينا أن  $K$  هو حقل الانشطار لـ  $x^{p^n} - x$  على  $F$ ؛ إذن،  $K$  امتداد ناظمي على  $F$ . الآن أحد التماثلات الذاتية التي تترك  $F$  ثابتة  $\sigma_{p^r}$ ، حيث لكل  $\alpha \in K$ ،  $\sigma_{p^r}(\alpha) = \alpha^{p^r}$ . لاحظ أن  $(\sigma_{p^r})^i(\alpha) = \alpha^{p^{ri}}$ ، ولأن كثيرة الحدود من الدرجة  $p^{ri}$  يمكن أن يكون لها على الأكثر  $p^{ri}$  من الأصفار في الحقل، فإننا نرى أن أصغراً لـ  $\sigma_{p^r}$  التي يمكن أن تترك كل  $\alpha \in K$  عنصرًا في  $K$  ثابتة، هي القوة  $n$ . بمعنى أن رتبة العنصر  $\sigma_{p^r}$  في  $G(K/F)$  هي على الأقل  $n$ ؛ ولذلك، لأن  $[K : F] = n$ ، فيجب أن تكون  $G(K/F)$  دورية ومولدة بـ  $\sigma_{p^r}$ . نلخص هذه الخطوات في مبرهنة.

ليكن  $K$  امتداداً منتهياً من الدرجة  $n$  للحقل المنتهي  $F$ ، الذي يحوي  $p^r$  من العناصر؛ إذن،  $G(K/F)$  دورية من الرتبة  $n$ ، ومولدة بـ  $\sigma_{p^r}$ ، حيث  $\sigma_{p^r}(\alpha) = \alpha^{p^r}$  لكل  $\alpha \in K$ .

7.53 مبرهنة

مثال 8.53

نستخدم هذه المبرهنة في إعطاء توضيح آخر للمبرهنة الرئيسية في مبرهنة جالوا. ليكن  $F = \mathbb{Z}_p$  ، ولتكن  $K = \text{GF}(p^{12})$ ؛ إذن،  $[K : F] = 12$ ، هذا يؤدي إلى أن  $G(K/F)$  تماثل الزمرة الدورية  $(\mathbb{Z}_{12}, +)$ ، إذ إنَّ الرسم البياني للزمر الجزئية والحقول المتوسطة معطى في الشكل 9.53. ومرة أخرى، كل رسم ليس معكوس الآخر فقط، بل للأسف، يشبه معكوس نفسه، ستُعطى أمثلة في الفصل 54، حيث الرسوم البيانية لا تشبه معكوسها، إضافة إلى أن نصف الزمر الجزئية الدورية



(ب) مخطط الحقول

الشكل 9.53 (أ) مخطط الزمر

من  $G(K/F) = \langle \sigma_p \rangle$  بإعطاء مولداتها، على سبيل المثال:

$$\langle \sigma_p^4 \rangle = \{1, \sigma_p^4, \sigma_p^8\}$$

إتمام إثبات المبرهنة الرئيسية

رأينا أن الخاصيتين 3 و 5، هما كل ما تبقى لإثباته في المبرهنة الرئيسية في مبرهنة جالوا.

بالعودة إلى الخاصية 3، يجب أن تثبت أنه  $\lambda(K_H) = H$ ،  $H \leq G(K/F)$

البرهان

نعلم أن  $H \leq \lambda(K_H) \leq G(K/F)$ ؛ إذن، ما يجب علينا في الحقيقة إثباته، أنه من المستحيل أن تكون  $H$  زمرة جزئية فعلية من  $\lambda(K_H)$ . سنفرض أن:

$$H < \lambda(K_H)$$

ثم نجد تناقضًا، وبوصفه امتدادًا منتهيًا قابلاً للفصل،  $K = K_H(\alpha)$  حيث  $\alpha \in K$ . بحسب المبرهنة 15.51، ولتكن:

$$n = [K : K_H] = \{K : K_H\} = |G(K/K_H)|.$$

إذن،  $H < G(K/K_H)$  يؤدي إلى أن  $|H| < |G(K/K_H)| = n$ ، ما يعني أن  $|H| < [K : K_H] = n$  لتكن

عناصر  $H$   $\sigma_1, \dots, \sigma_{|H|}$ ، وافترض كثيرة الحدود

$$f(x) = \prod_{i=1}^{|H|} (x - \sigma_i(\alpha)).$$

إذن، درجة  $f(x)$  تساوي  $|H|$  تساوي  $n > |H|$ ، وتكون معاملات كل قوة لـ  $x$  في  $f(x)$  تعابير متماثلة في  $\sigma_i(\alpha)$ ، على سبيل المثال: معامل  $x^{|H|-1}$  يساوي  $\sigma_1(\alpha) - \sigma_2(\alpha) - \dots - \sigma_{|H|}(\alpha)$ ، إذن، لا تتغير هذه المعاملات تحت أي تماثل  $\sigma_i \in H$ ؛ لأنه إذا كانت  $\sigma \in H$ ، فإن:

$$\sigma\sigma_1, \dots, \sigma\sigma_{|H|}$$

هي مرة أخرى المتتالية  $\sigma_1, \sigma_2, \dots, \sigma_{|H|}$ ، ما عدا طبقاً للترتيب؛ لأن  $H$  زمرة؛ إذن، تنتمي معاملات  $f(x)$  إلى  $K_H$ ، ولأن إحدى  $\sigma_i$  هي  $i$ ، نرى أن  $\sigma_i(\alpha)$  هي  $\alpha$ ، وهكذا  $f(\alpha) = 0$ ؛ إذن، نحصل على:  $\deg(\alpha, K_H) \leq |H| < n = [K : K_H] = [K_H(\alpha) : K_H]$ .

وهذا مستحيل، وهكذا نكون قد أثبتنا الخاصية 3.

نتوجه الآن للخاصية 5. كل امتداد  $E \mid F \leq E \leq K$ ، يكون قابلاً للفصل بحسب المبرهنة 9.51؛ إذن،  $E$  ناظمي على  $F$ ، إذا وفقط إذا كان  $E$  حقل انشطار على  $F$ ، وبحسب مبرهنة تمديد التماثل، كل تماثل من  $E$  إلى حقل جزئي من  $\bar{F}$  ويترك  $F$  ثابتة، يمكن تمديده إلى تماثل ذاتي على  $K$ ؛ لأن  $K$  ناظمي على  $F$ ؛ إذن، التماثلات الذاتية في كلها تنتج التماثلات الممكنة من  $E$  إلى حقل جزئي من  $\bar{F}$  وتترك  $F$  ثابتة، وبحسب المبرهنة 3.50، فإن هذا يثبت أن  $E$  حقل انشطار على  $F$ ؛ ولذا، فهو ناظمي على  $F$ ، إذا وفقط إذا كان لكل  $\sigma \in G(K/F)$  و  $\alpha \in E$ ،  $\sigma(\alpha) \in E$

بحسب الخاصية 2،  $E$  هو الحقل الثابت لـ  $G(K/E)$ ؛ وإذن،  $\sigma(\alpha) \in E$ ، إذا وفقط إذا كان لكل  $\tau \in G(K/E)$

$$\tau(\sigma(\alpha)) = \sigma(\alpha).$$

وهذا بدوره يتحقق إذا وفقط إذا كان:

$$(\sigma^{-1}\tau\sigma)(\alpha) = \alpha$$

لكل  $\alpha \in E$ ،  $\sigma \in G(K/F)$  و  $\tau \in G(K/E)$ ، ولكن هذا يعني أنه لكل  $\sigma \in G(K/F)$  و  $\tau \in G(K/E)$ ،  $\sigma^{-1}\tau\sigma$  تترك كل عنصر في  $E$  ثابتاً، أي:  $(\sigma^{-1}\tau\sigma) \in G(K/E)$ .

هذا بالتحديد شرط أن  $G(K/F)$  زمرة جزئية ناظمية في  $G(K/F)$ .

بقي علينا إثبات أنه عندما يكون  $E$  امتداداً ناظمياً لـ  $F$ ، فإن:

$G(E/F) \simeq G(K/F)/G(K/E)$ . إذا كانت  $\sigma \in G(K/F)$ ، دع  $\sigma_E$  تكون التماثل الذاتي على  $E$  المتولد من  $\sigma$  (نفترض أن  $E$  امتداد ناظمي لـ  $F$ )؛ إذن،  $\sigma_E \in G(E/F)$ . الدالة  $\phi : G(K/F) \rightarrow G(K/F)$  المعطاة بـ

$$\phi(\sigma) = \sigma_E$$

حيث  $\sigma \in G(K/F)$ ، تمثل تشاكلاً بحسب مبرهنة تمديد التماثل، كل تماثل ذاتي على  $E$  ويترك  $F$  ثابتة، يمكن تمديده إلى تماثل ذاتي على  $K$ ، أي إنه  $\tau_E$  حيث  $\tau \in G(K/F)$ ؛ إذن،  $\phi$  غامر لـ  $G(K/F)$ ، ونواة  $\phi$  هي  $G(K/E)$ ، وهكذا وبحسب المبرهنة الأساسية للتماثل،

◆  $G(E/F) \simeq G(K/F)/G(K/E)$  إضافة إلى ذلك، هذا التماثل طبيعي.

■ تمارين 53

حسابات

الحقل  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  امتداد ناظمي منته على  $\mathbb{Q}$ . يمكن إثبات أن  $[K : \mathbb{Q}] = 8$  في التمارين 1 إلى 8، احسب الكمية العددية المطلوبة. استخدمت الرموز في المبرهنة 6.53.

1.  $\{K : \mathbb{Q}\}$
2.  $|G(K/\mathbb{Q})|$
3.  $|\lambda(\mathbb{Q})|$
4.  $|\lambda(\mathbb{Q}(\sqrt{2}, \sqrt{3}))|$
5.  $|\lambda(\mathbb{Q}(\sqrt{6}))|$
6.  $|\lambda(\mathbb{Q}(\sqrt{30}))|$
7.  $|\lambda(\mathbb{Q}(\sqrt{2} + \sqrt{6}))|$
8.  $|\lambda(K)|$
9. صف زمرة كثيرة الحدود  $\mathbb{Q}[x] \in (x^4 - 1)$  على  $\mathbb{Q}$ .
10. أوجد الرتبة، وصف المولد للزمرة  $G(GF(729)/GF(9))$ .
11. ليكن  $K$  حقل انشطار  $x^3 - 2$  على  $\mathbb{Q}$ . (ارجع للمثال 9.50).
  - أ. صف العناصر الستة لـ  $G(K/\mathbb{Q})$  بإيجاد قيمها على  $\sqrt[3]{2}$  و  $i\sqrt{3}$ . (بحسب المثال 9.50  $K = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ ).
  - ب. أيّ الزمر التي رأيناها سابقاً تماثل  $G(K/\mathbb{Q})$ ؟
  - ج. باستخدام الرموز المعطاة لإجابة الفرع (أ) في نهاية الكتاب، أوجد الرسم البياني للحقول الجزئية من  $K$  والزمرة الجزئية من  $G(K/\mathbb{Q})$ ، مظهرًا الحقول المتوسطة والزمرة الجزئية المتقابلة، كما فعلنا في الشكل 4.53.
12. صف زمرة كثيرة الحدود  $\mathbb{Q}[x] \in (x^4 - 5x^2 + 6)$  على  $\mathbb{Q}$ .
13. صف زمرة كثيرة الحدود  $\mathbb{Q}[x] \in (x^3 - 1)$  على  $\mathbb{Q}$ .

مفاهيم

14. أعط مثلاً على امتدادين ناظميين منتهيين  $K_1$  و  $K_2$  للحقل  $F$  نفسه، بحيث  $K_1$  لا يماثل  $K_2$ ، ولكن:  $G(K_1/F) \simeq G(K_2/F)$ .
15. ضع إشارة صح أو إشارة خطأ:
  - أ. يمكن أن يكون لزمرتين جزئيتين مختلفتين من زمرة جالوا الحقل الثابت نفسه.
  - ب. برموز المبرهنة 6.53، إذا كان  $F \leq E < L \leq K$ ، فإن  $\lambda(E) < \lambda(L)$ .
  - ج. إذا كان  $K$  امتداداً ناظماً منتهياً لـ  $F$ ، فإن  $K$  امتداد ناظمي لـ  $E$  حيث  $F \leq E \leq K$ .
  - د. إذا كان للامتدادين الناظميين المنتهيين  $E$  و  $L$  للحقل  $F$  زمرتي جالوا متماثلتين، فإن:  $[E : F] = [L : F]$ .
  - هـ. إذا كان  $E$  امتداداً ناظماً منتهياً لـ  $F$  و  $H$  زمرة جزئية ناظمية لـ  $G(E/F)$ ، فإن  $E_H$  امتداد ناظمي لـ  $F$ .
  - و. إذا كان  $E$  امتداداً بسيطاً ناظماً منتهياً للحقل  $F$ ، فإن زمرة جالوا  $G(E/F)$  زمرة بسيطة.
  - ز. زمرة جالوا لا تكون بسيطة.
  - ح. زمرة جالوا لا امتداد منتهٍ لحقل منتهٍ إبدالية.

- \_\_\_\_\_ ط. الامتداد  $E$  ذو الدرجة 2 على الحقل  $F$ ، يكون دائماً امتداداً ناظماً لـ  $F$ .  
 \_\_\_\_\_ ي. الامتداد  $E$  ذو الدرجة 2 على الحقل  $F$ ، يكون دائماً امتداداً ناظماً لـ  $F$ ، إذا كان مميز  $F$  ليس 2.

براهين

16. يسمى الامتداد المنتهي الناظمي  $K$  للحقل  $F$  إبدالياً على  $F$ ، إذا كانت  $G(E/F)$  زمرة إبدالية. أثبت أنه إذا كان  $K$  إبدالياً على  $F$ ، وكان  $E$  امتداداً ناظماً لـ  $F$ ، بحيث  $F \leq E \leq K$ ، فإن  $K$  إبدالياً على  $E$  و  $E$  إبدالية على  $F$ .  
 17. ليكن  $K$  امتداداً ناظماً منتهياً للحقل  $F$ . أثبت أنه لكل  $\alpha \in K$ ، فإن معيار  $\alpha$  على  $F$  (norm of  $\alpha$  over  $F$ ) المعطى بـ:

$$N_{K/F}(\alpha) = \prod_{\sigma \in G(K/F)} \sigma(\alpha)$$

وأثر  $\alpha$  في  $F$  (trace of  $\alpha$ ) المعطى بـ:

$$Tr_{K/F}(\alpha) = \sum_{\sigma \in G(K/F)} \sigma(\alpha),$$

تكون عناصر في  $F$ .

18. افترض  $K = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$ . بالرجوع إلى التمرين 17، احسب كلاً مما يأتي (انظر المثال 3.53):

|     |                               |    |  |
|-----|-------------------------------|----|--|
| أ.  | $N_{K/\mathbb{Q}}(\sqrt{2})$  | ب. | $N_{K/\mathbb{Q}}(\sqrt{2} + \sqrt{3})$  |
| ج.  | $N_{K/\mathbb{Q}}(\sqrt{6})$  | د. | $N_{K/\mathbb{Q}}(2)$                    |
| هـ. | $Tr_{K/\mathbb{Q}}(\sqrt{2})$ | و. | $Tr_{K/\mathbb{Q}}(\sqrt{2} + \sqrt{3})$ |
| ز.  | $Tr_{K/\mathbb{Q}}(\sqrt{6})$ | ح. | $Tr_{K/\mathbb{Q}}(2)$                   |

19. ليكن  $K$  امتداداً ناظماً لـ  $F$ ، ولتكن  $K = F(\alpha)$ ، ولتكن:

$$\text{irr}(\alpha, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

بالرجوع إلى التمرين 17، أثبت أن:

$$\text{أ. } N_{K/F}(\alpha) = (-1)^n a_0 \quad \text{ب. } Tr_{K/F}(\alpha) = -a_{n-1}$$

20. لتكن  $f(x) \in F[x]$  كثيرة حدود من الدرجة  $n$ ، بحيث إن كل عامل غير مختزل لها قابل للفصل على  $F$ . أثبت أن رتبة زمرة  $f(x)$  على  $F$  تقسم  $n!$ .

21. لتكن  $f(x) \in F[x]$  كثيرة حدود، بحيث إن كل عامل غير مختزل لـ  $f(x)$  كثيرة حدود قابلة للفصل على  $F$ . أثبت أن زمرة  $f(x)$  على  $F$  يمكن أن تُعد بصورة طبيعية زمرة تباديل أصفار  $f(x)$  في  $\bar{F}$ .

22. ليكن  $F$  حقلاً، ولتكن  $\zeta$  جذراً بدائياً من الرتبة  $n$  للواحد في  $\bar{F}$ ، حيث مميز  $F$  يساوي 0 أو لا يقسم  $n$ .

أ. أثبت أن  $F(\zeta)$  امتداد ناظمي على  $F$ .ب. أثبت أن  $G(F(\zeta)/F)$  إبدالية. [مساعدة: كل  $\sigma \in G(F(\zeta)/F)$  تربط  $\zeta$  بأحد  $\zeta^r$  وتتحدد تماماً بهذه القيمة  $r$ ].

23. يسمى الامتداد الناظمي المنتهي  $K$  للحقل  $F$  دورياً على  $F$  (cyclic)، إذا كانت  $G(K/F)$  زمرة دورية.

- أ. أثبت أنه إذا كان  $K$  دورياً على  $F$ ، وكان  $E$  امتداداً ناظماً على  $F$ ، بحيث  $F \leq E \leq K$ ، فإن  $E$  دوري على  $F$  و  $K$  دوري على  $E$ .

ب. أثبت أنه إذا كان  $K$  دورياً على  $F$ ، فإنه يوجد بالضبط حقل واحد  $E$ ،  $F \leq E \leq K$ ، من الدرجة  $d$  على  $F$  لكل قاسم  $d \mid [K : F]$ .

24. ليكن  $K$  امتداداً ناظماً منتهياً لـ  $F$ .

أ. ليكن  $\alpha \in K$ ، أثبت أن:

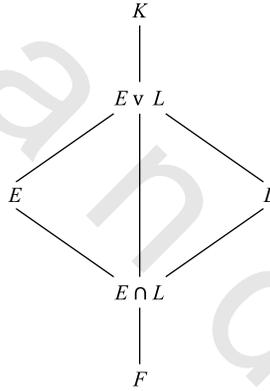
$$f(x) = \prod_{\sigma \in G(K/F)} (x - \sigma(\alpha))$$

عنصر في  $F[x]$

ب. بالإشارة إلى الفرع (أ)، أثبت أن  $f(x)$  قوة لـ  $\text{irr}(\alpha, F)$ ، و  $f(x) = \text{irr}(\alpha, F)$ ، إذا وفقط إذا كان  $K = F(\alpha)$ .

25. الموصل  $E \vee L$  (join) للامتدادين  $E$  و  $L$  للحقل  $F$  في  $\bar{F}$ ، هو أصغر حقل جزئي من  $\bar{F}$  ويحوي كلا من  $E$  و  $L$ ، بمعنى أن  $E \vee L$  هو تقاطع الحقول الجزئية كلها من  $\bar{F}$  التي تحوي كلا من  $E$  و  $L$ . ليكن  $K$  امتداداً ناظماً منتهياً للحقل  $F$ ، وليكن  $E$  و  $L$  امتدادين لـ  $F$  محتويين في  $K$ ، كما هو موضح في الشكل 10.53، صف  $G(K/(E \vee L))$  بدلالة  $G(K/E)$  و  $G(K/L)$ .

26. بالإشارة إلى الوضع في التمرين 25، صف  $G(K/(E \cap L))$  بدلالة  $G(K/E)$  و  $G(K/L)$ .



الشكل 9.53

## توضيحات على مبرهنة جالوا Illustrations of Galois Theory

## الفصل 54

## الدوال المتناظرة

ليكن  $F$  حقلاً، ولتكن  $y_1, \dots, y_n$  غير معينات، هناك تماثلات ذاتية طبيعية على  $F(y_1, \dots, y_n)$  تترك  $F$  ثابتة - يعني - تلك المعرفة بوصفها تباديل على  $\{y_1, \dots, y_n\}$ . لكن أكثر وضوحاً، لتكن  $\sigma$  تبديلة على  $\{1, \dots, n\}$  أي  $\sigma \in S_n$ ، إذن، تعمم  $\sigma$  إلى دالة طبيعية  $\sigma : F(y_1, \dots, y_n) \rightarrow F(y_{\sigma(1)}, \dots, y_{\sigma(n)})$  المعطاة بـ:

$$\overline{\sigma} \left( \frac{f(y_1, \dots, y_n)}{g(y_1, \dots, y_n)} \right) = \frac{f(y_{\sigma(1)}, \dots, y_{\sigma(n)})}{g(y_{\sigma(1)}, \dots, y_{\sigma(n)})}$$

حيث  $f(y_1, \dots, y_n), g(y_1, \dots, y_n) \in F[y_1, \dots, y_n]$  و  $g(y_1, \dots, y_n) \neq 0$  نستنتج على الفور أن  $\overline{\sigma}$  تماثل ذاتي على  $F(y_1, \dots, y_n)$  يترك  $F$  ثابتة، وعناصر  $F(y_1, \dots, y_n)$  التي تترك ثابتة بكل  $\overline{\sigma}$ ، لكل  $\sigma_n \in S$ ، هي الدوال النسبية المتناظرة في غير المعينات  $y_1, \dots, y_n$ .

## 1.54 تعريف

يسمى العنصر في الحقل  $F(y_1, \dots, y_n)$  دالة متناظرة في  $y_1, \dots, y_n$  على  $F$  (Symmetric function)، إذا تركت ثابتة بتباديل  $y_1, \dots, y_n$  كلها، بالمعنى الذي شرحناه تَوَّأً.

لتكن  $\overline{S}_n$  زمرة التماثلات الذاتية  $\overline{\sigma}$  كلها، حيث  $\sigma_n \in S$ ، لاحظ أن  $\overline{S}_n$  تماثل  $S_n$  بصورة طبيعية. ليكن  $K$  الحقل الجزئي من  $F(y_1, \dots, y_n)$  الذي يترك ثابتاً بـ  $\overline{S}_n$ . افترض كثيرة الحدود.

$$f(x) = \prod_{i=1}^n (x - y_i)$$

تسمى كثيرة الحدود  $[x] \in (F(y_1, \dots, y_n))$  كثيرة الحدود العامة من الدرجة  $n$

(general polynomial of degree n): لتكن  $\overline{\sigma}_x$  تمديداً لـ  $\overline{\sigma}$  بصورة طبيعية - إلى  $[x] \in (F(y_1, \dots, y_n))$ ، حيث

$$\overline{\sigma}_x(x) = x. \text{ الآن، تترك } f(x) \text{ ثابتة بكل دالة } \overline{\sigma}_x, \text{ حيث } \overline{\sigma}_x \in S_n. \text{ بمعنى أن:}$$

$$\prod_{i=1}^n (x - y_i) = \prod_{i=1}^n (x - y_{\sigma(i)}).$$

إذن، معاملات  $f(x)$  في  $K$ : إنها الدوال المتناظرة الابتدائية في  $y_1, \dots, y_n$ ، وبوصفه توضيحاً، لاحظ أن الحد الثابت في  $f(x)$  هو:

$$(-1)^n y_1 y_2 \cdots y_n$$

معامل  $x^{n-1}$  هو  $(y_1 + y_2 + \dots + y_n)$ ، وهكذا. هذه دوال متناظرة في  $y_1, \dots, y_n$ ، وأول دالة متناظرة ابتدائية في  $y_1, \dots, y_n$  هي:

$$s_1 = y_1 + y_2 + \cdots + y_n$$

والثانية هي:  $s_2 = y_1 y_2 + y_1 y_3 + \cdots + y_{n-1} y_n$ ، وهكذا، والدالة التي ترتيبها  $m$ ، هي  $s_m = y_1 y_2 \cdots y_m$

افتراض الحقل  $E = F(s_1, \dots, s_n)$ ، بالطبع  $E \leq K$ ، حيث  $K$  حقل الدوال المتناظرة جميعها في  $y_1, \dots, y_n$

على  $F$ . ولكن  $F$  امتداد ناظمي منته لـ  $E$  - تحديداً - حقل الانشطار لـ

$$f(x) = \prod_{i=1}^n (x - y_i)$$

على  $E$ . لأن درجة  $f(x)$  هي  $n$ ، فإننا نحصل مباشرة على:

$$[F(y_1, \dots, y_n) : E] \leq n!$$

(انظر التمرين 13، في الفصل 50). وعلى أي حال، لأن  $K$  هو الحقل الثابت بـ  $\bar{S}_n$

و

$$|\bar{S}_n| = |S_n| = n!,$$

نحصل كذلك على:

$$n! \leq \{F(y_1, \dots, y_n) : K\} \leq [F(y_1, \dots, y_n) : K].$$

ولذلك:

$$n! \leq [F(y_1, \dots, y_n) : K] \leq [F(y_1, \dots, y_n) : E] \leq n!,$$

إذن:

$$K = E.$$

لذلك، فإن زمرة جالوا الكاملة لـ  $F(y_1, \dots, y_n)$  على  $E$  هي  $\bar{S}_n$ ، وحقيقة أن  $K = E$  تثبت أنه يمكن التعبير عن الدوال المتناظرة جميعها بدوال نسبية من الدوال المتناظرة الابتدائية  $s_1, \dots, s_n$ . نلخص هذه النتائج في مبرهنة.

## 2.54 مبرهنة

لتكن  $s_1, \dots, s_n$  الدوال المتناظرة الابتدائية في غير المعينات  $y_1, \dots, y_n$ . كل دالة متناظرة في  $y_1, \dots, y_n$  على  $F$ ، هي دالة نسبية في الدوال المتناظرة الابتدائية، كذلك  $F(y_1, \dots, y_n)$  امتداد ناظمي منته من الدرجة  $n!$  على  $F(s_1, \dots, s_n)$ ، وزمرة جالوا لهذا الامتداد تماثل  $S_n$  بصورة طبيعية.

بالنظر في مبرهنة كيلى 16.8، يمكن الاستنتاج من المبرهنة 2.54 أن أي زمرة منتهية يمكن أن تظهر بوصفها زمرة جالوا (تبعاً للتماثل). (انظر التمرين 11).

أمثلة

لنعطي المثال الذي وعدنا به عن امتداد ناظمي منته له زمرة جالوا، بحيث يكون الرسم البياني لزمرة الجزئية لا يظهر بوصفه معكوساً لنفسه.

## 3.54 مثال

افترض حقل الانشطار في  $\mathbb{C}$  لـ  $x^4 - 2$  على  $\mathbb{Q}$ ،  $x^4 - 2$  غير مختزلة على  $\mathbb{Q}$  - حسب معيار إيزنستين، حيث  $p = 2$  - لتكن  $\alpha = \sqrt[4]{2}$  الصفر الحقيقي الموجب لـ  $x^4 - 2$ ، والأصفار الأربعة لـ  $x^4 - 2$  في  $\mathbb{C}$  هي  $\alpha, -\alpha, i\alpha, -i\alpha$ ، حيث  $i$  هو الصفر المعروف لـ  $x^2 + 1$  في  $\mathbb{C}$ ، وحقل الانشطار  $K$  لـ  $x^4 - 2$  على  $\mathbb{Q}$  يحتوي على

$(i\alpha)/\alpha = i$ . لأن  $\alpha$  عدد حقيقي،  $\mathbb{Q}(\alpha) < \mathbb{R}$ ؛ إذن،  $\mathbb{Q}(\alpha) \neq K$  على أي حال، لأن  $\mathbb{Q}(\alpha, i)$  تحوي أصفار  $x^4 - 2$  جميعها، فنرى أن  $K = \mathbb{Q}(\alpha, i)$ . لتكن  $E = \mathbb{Q}(\alpha)$ ، نحصل على الرسم البياني في الشكل 4.54.

الآن،  $\{1, \alpha, \alpha^2, \alpha^3\}$  أساس لـ  $E$  على  $\mathbb{Q}$ ، و  $\{1, i\}$  أساس لـ  $K$  على  $E$ : إذن:

$$\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$$

أساس لـ  $K$  على  $\mathbb{Q}$ ، ولأن  $[K : \mathbb{Q}] = 8$ ، فيجب أن نحصل على  $|G(K/\mathbb{Q})| = 8$ : لذا، نحتاج إلى أن نجد ثمانية تماثلات ذاتية على  $K$  تترك  $\mathbb{Q}$  ثابتة. نعرف أن أي تماثل ذاتي  $\sigma$  يتحدد تمامًا بقيمه على عناصر الأساس  $\{1, \alpha, \alpha^2, \alpha^3, i, i\alpha, i\alpha^2, i\alpha^3\}$ ، وهذه القيم بدورها تتحدد بـ  $\sigma(\alpha)$  و  $\sigma(i)$ : ولكن  $\sigma(\alpha)$  يجب أن تكون دائمًا مرافقًا لـ  $\alpha$  على  $\mathbb{Q}$ ، أي أحد الأصفار الأربعة لـ  $x^4 - 2 = \text{irr}(\alpha, \mathbb{Q})$ . وكذلك  $\sigma(i)$  يجب أن تكون صفرًا لـ  $x^2 + 1 = \text{irr}(i, \mathbb{Q})$ : إذن، الاحتمالات الأربعة لـ  $\sigma(\alpha)$ ، منضمة لاحتمالي  $\sigma(i)$ ، يجب أن تعطي التماثلات الذاتية الثمانية. نصفها في الجدول 5.54، على سبيل المثال:  $\rho_3(\alpha) = i\alpha$  و  $\rho_3(i) = i$ ، بينما  $\rho_0$  هو التماثل الذاتي المحايد. الآن،

$$(\mu_1 \rho_1)(\alpha) = \mu_1(\rho_1(\alpha)) = \mu_1(i\alpha) = \mu_1(i)\mu_1(\alpha) = -i\alpha$$

وبالمثل كذلك

$$(\mu_1 \rho_1)(i) = -i,$$

إذن،  $\mu_1 \rho_1 = \delta_2$ ، وتثبت حسابات مشابهة أن

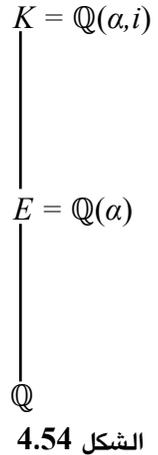
$$(\rho_1 \mu_1)(\alpha) = i\alpha \quad \text{و} \quad (\rho_1 \mu_1)(i) = -i.$$

إذن،  $\rho_1 \mu_1 = \delta_1$ ، ما يعني أن  $\rho_1 \mu_1 \neq \mu_1 \rho_1$  و  $G(K/\mathbb{Q})$  ليست إبدالية؛ لذلك، يجب أن تكون  $G(K/\mathbb{Q})$  تماثل أحد الزمرتين غير الإبداليتين من الرتبة 8 الموصوفة في المثال 6.40.

بالحساب من الجدول 5.54، نرى أن رتبة  $\rho_1$  تساوي 4، و  $\mu_1$  من الرتبة 2،  $\{\rho_1, \mu_1\}$  تولد  $G(K/\mathbb{Q})$ ، و  $\rho_1 \mu_1 = \mu_1 \rho_1^3 = \delta_1$ : إذن،  $G(K/\mathbb{Q})$  تماثل الزمرة  $G_1$  في المثال 6.40، الزمرة الثمانية.

لقد اخترنا ترميز العناصر في  $G(K/\mathbb{Q})$  ليكون جدول الزمرة منطبقًا مع جدول الزمرة الثمانية في الجدول 12.8. حيث إن الرسم البياني للزمر الجزئية  $H_i$  من  $G(K/\mathbb{Q})$  معطى في الشكل 13.8، ونعيد كتابته هنا في الشكل 6.54، ونعطي كذلك الرسم البياني للحقول المتوسطة بين  $\mathbb{Q}$  و  $K$ ، هذا في النهاية يوضح بصورة لطيفة أن أحد الرسمين هو معكوس الآخر.

تحديد الحقول الثابتة  $K_{H_i}$  يحتاج أحيانًا إلى بعض الإبداع، لنوضح ذلك، لإيجاد  $K_{H_2}$ ، لا يجب علينا غير إيجاد امتداد لـ  $\mathbb{Q}$  من الدرجة 2 يترك ثابتًا بـ  $\{\rho_0, \rho_1, \rho_2, \rho_3\}$ ، ولأن كل  $\rho_j$  تترك  $i$  ثابتة، فإن  $\mathbb{Q}(i)$  هو الحقل الذي نبحث عنه، وإيجاد  $K_{H_4}$ ، يجب علينا إيجاد امتداد لـ  $\mathbb{Q}$  من الدرجة 4 يترك ثابتًا بـ  $\rho_0$  و  $\mu_1$ ، ولأن  $\mu_1$  تترك  $\alpha$  ثابتة و  $\alpha$  صفر لـ  $x^4 - 2 = \text{irr}(\alpha, \mathbb{Q})$ ، نرى أن  $\mathbb{Q}(\alpha)$  و يترك ثابتًا بـ  $\{\rho_0, \mu_1\}$ . بحسب مبرهنة جالوا، إنه الحقل الوحيد. نستخدم هنا بقوة التقابل المعطى بمبرهنة جالوا، فإذا وجدنا حقلًا يلائم القائمة، فإنه الحقل الذي نبحث عنه، أضف إلى ذلك، إيجاد  $K_{H_7}$  يحتاج إلى مزيد من الإبداع، فلأن  $H_7 = \{\rho_0, \delta_1\}$  زمرة، فلكل  $\beta \in K$  نرى أن  $\rho_0(\beta) + \delta_1(\beta)$  تترك ثابتة بـ  $\rho_0$  و  $\delta_1$ ، وبأخذ  $\beta = \alpha$ ، نرى أن  $\rho_0(\alpha) + \delta_1(\alpha) = \alpha + i\alpha$ ، حيث يمكننا التحقق ورؤية أن  $\rho_0$  و  $\delta_1$  هي

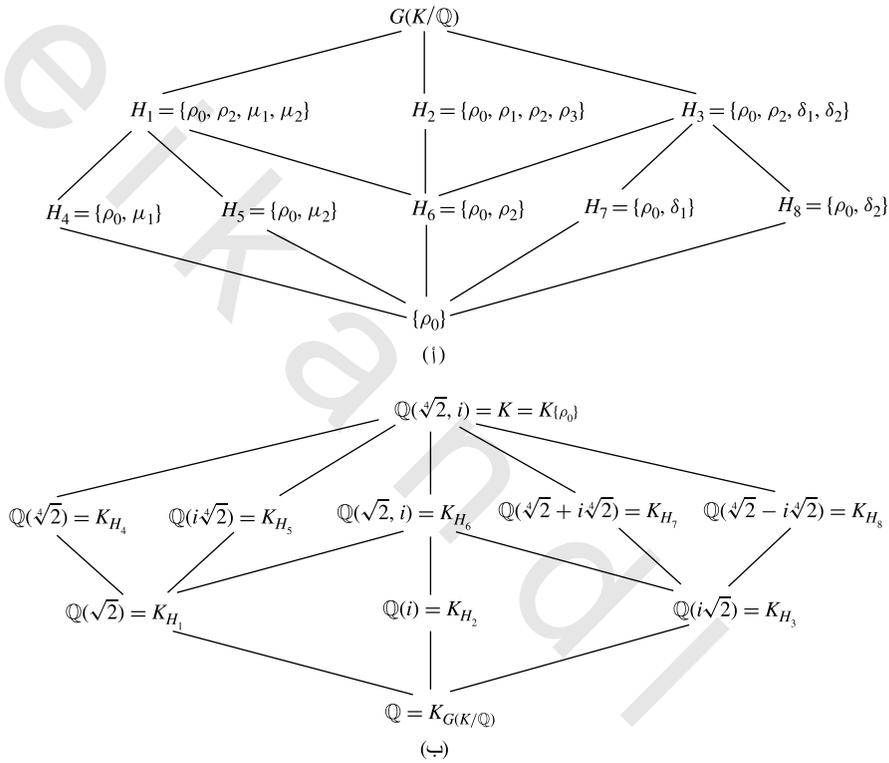


الشكل 4.54

التماثلات الذاتية الوحيدة التي تترك  $\alpha + i\alpha$  ثابتة؛ إذن:

جدول 5.54

|                      |          |           |           |            |          |            |           |            |
|----------------------|----------|-----------|-----------|------------|----------|------------|-----------|------------|
|                      | $\rho_0$ | $\rho_1$  | $\rho_2$  | $\rho_3$   | $\mu_1$  | $\delta_1$ | $\mu_2$   | $\delta_2$ |
| $\alpha \rightarrow$ | $\alpha$ | $i\alpha$ | $-\alpha$ | $-i\alpha$ | $\alpha$ | $i\alpha$  | $-\alpha$ | $-i\alpha$ |
| $i \rightarrow$      | $i$      | $i$       | $i$       | $i$        | $-i$     | $-i$       | $-i$      | $-i$       |



الشكل 6.54 (أ) الرسم البياني للزمر (ب) الرسم البياني للحقول

بحسب التقابل، يجب أن نحصل على:

$$\mathbb{Q}(\alpha + i\alpha) = \mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) = K_{H_7}$$

افتراض أننا نود إيجاد  $\text{irr}(\alpha + i\alpha, \mathbb{Q})$ ، فإذا كانت  $\gamma = \alpha + i\alpha$ ، فإن لكل مرافق  $\gamma$  على  $\mathbb{Q}$ ، يوجد تماثل ذاتي على  $K$  يربط  $\gamma$  بمرافق لها؛ إذن، نحتاج فقط إلى حساب القيم المختلفة لـ  $\sigma(\gamma)$ ، حيث  $\sigma \in G(K/\mathbb{Q})$  لإيجاد بقية أصفار  $\text{irr}(\gamma, \mathbb{Q})$ ، وبحسب المبرهنة 2.53، عناصر  $\sigma$  في  $G(K/\mathbb{Q})$  التي تعطي هذه القيم المختلفة، يمكن إيجادها بأخذ مجموعة الممثلات للمجموعة المشاركة اليسرى  $G(K/\mathbb{Q}(\gamma)) = \{\rho_0, \delta_1\}$  في  $G(K/\mathbb{Q})$ . مجموعة الممثلات لهذه المجموعات المشاركة اليسرى هي:

$$\{\rho_0, \rho_1, \rho_2, \rho_3\}.$$

إذن، مرافقات  $\gamma = \alpha + i\alpha$  هي  $\alpha + i\alpha$ ،  $\alpha - i\alpha$ ،  $-i\alpha + \alpha$  و  $-i\alpha - \alpha$ .

إذن:

$$\begin{aligned} \text{irr}(\gamma, \mathbb{Q}) &= [(x - (\alpha + i\alpha))(x - (i\alpha - \alpha))] \\ &\cdot [(x - (-\alpha - i\alpha))(x - (-i\alpha + \alpha))] \\ &= (x^2 - 2i\alpha x - 2\alpha^2)(x^2 + 2i\alpha x - 2\alpha^2) \\ &= x^4 + 4\alpha^4 = x^4 + 8. \end{aligned}$$

▲

رأينا أمثلة فيها حقل الانشطار لكثيرة حدود من الدرجة الرابعة على حقل  $F$ ، يكون امتدادًا على  $F$  من الدرجة 8 (المثال 3.54) ومن الدرجة 24 (المبرهنة 2.54، حيث  $n=4$ ). درجة امتداد للحقل  $F$  الذي يكون حقل انشطار لرباعي الدرجة على  $F$ ، يجب أن تقسم دائمًا  $24=4!$ ، وحقل الانشطار لـ  $(x-2)^4$  على  $\mathbb{Q}$  هو  $\mathbb{Q}$ ، امتداد من الدرجة 1، وحقل الانشطار لـ  $(x^2-2)^2$  على  $\mathbb{Q}$  هو  $\mathbb{Q}(\sqrt{2})$ ، امتداد من الدرجة 2. مثالنا الأخير سيعطي امتدادًا من الدرجة 4 لحقل امتداد لرباعي الدرجة.

افتراض حقل الانشطار لـ  $x^4 + 1$  على  $\mathbb{Q}$ ، فيمكننا بحسب المبرهنة 11.23 إثبات أن  $x^4 + 1$  غير مختزلة على  $\mathbb{Q}$ ، بمناقشة عدم إمكانية تحليلها في  $\mathbb{Z}[x]$ . (انظر التمرين 1). العمل في الأعداد المركبة في الفصل 1 يثبت أن أصفار  $x^4 + 1$  هي:  $(1 \pm i) / \sqrt{2}$  و  $(-1 \pm i) / \sqrt{2}$ . تثبت الحسابات أنه إذا كانت:

مثال 7.54

$$\alpha = \frac{1+i}{\sqrt{2}}$$

فإن

$$\alpha^7 = \frac{1-i}{\sqrt{2}} \text{ و } \alpha^5 = \frac{-1-i}{\sqrt{2}}, \quad \alpha^3 = \frac{-1+i}{\sqrt{2}}.$$

إذن، حقل الانشطار  $K$  لـ  $x^4 + 1$  على  $\mathbb{Q}$ ، هو  $\mathbb{Q}(\alpha)$ ، و  $[K: \mathbb{Q}] = 4$ . لنحسب  $G(K/\mathbb{Q})$ ، ونعطي الرسم البياني للزمر والحقول، فلأنه توجد تماثلات ذاتية على  $K$  تربط  $\alpha$  بكل مرافق لها؛ ولأن أي تماثل  $\sigma$  على  $\mathbb{Q}(\alpha)$  يتحدد تمامًا بـ  $\sigma(\alpha)$ ، فنرى أن العناصر الأربعة لـ  $G(K/\mathbb{Q})$  معرفة بالجدول 54.8، ولأن  $\alpha^k = (\alpha')^k = \alpha^{ik}$ ، ولأن  $\sigma_j(\sigma_k)(\alpha) = \sigma_j(\alpha^k) = (\alpha')^k = \alpha^{ik}$ ، ولأن  $\alpha^8 = 1$ ، فنرى أن  $G(K/\mathbb{Q})$  يماثل الزمرة  $\{1, 3, 5, 7\}$  مع الضرب مقياس 8. هذه هي الزمرة  $G_8$  في المبرهنة 6.20، ولأن  $\sigma_j^2 = \sigma_1$  - الدالة المحايدة - لكل  $j$ ، فيجب أن تكون  $G(K/\mathbb{Q})$  مماثلة لزمرة كلاين الرباعية. الرسوم البيانية معطاة في الشكل 9.54.

لإيجاد  $K_{\{\sigma_1, \sigma_3\}}$ ، فإنه من الضروري فقط إيجاد عنصر في  $K$  وليس في  $\mathbb{Q}$  يترك ثابتاً بـ  $\{\sigma_1, \sigma_3\}$ ، لأن  $[K_{\{\sigma_1, \sigma_3\}} : \mathbb{Q}] = 2$ . من الواضح أن  $\sigma_1(\alpha) + \sigma_3(\alpha)$  تترك ثابتة بكلا  $\sigma_1$  و  $\sigma_3$ : ولأن  $\{\sigma_1, \sigma_3\}$  زمرة نحصل على:

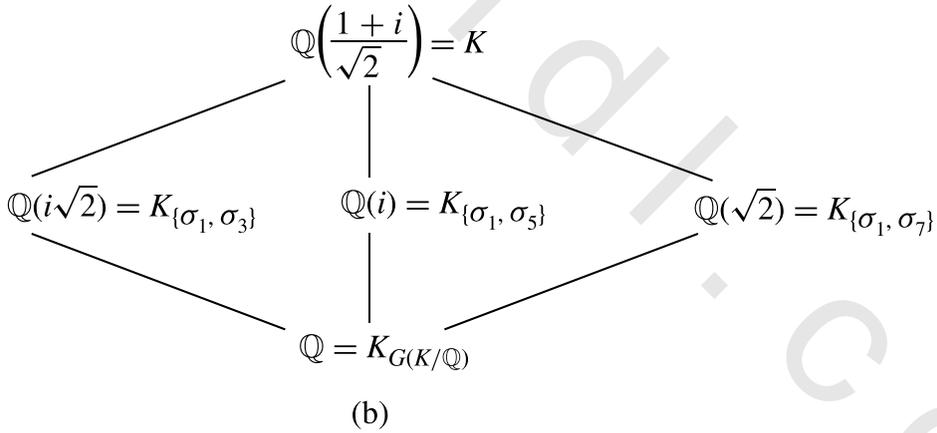
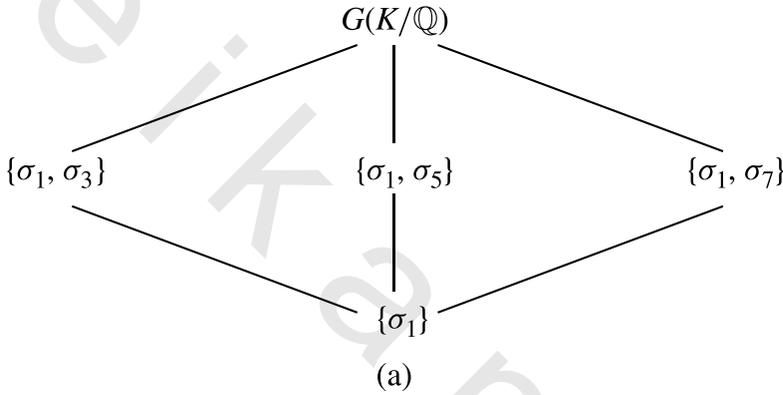
$$\sigma_1(\alpha) + \sigma_3(\alpha) = \alpha + \alpha^3 = i\sqrt{2}.$$

بالمثل:

$$\sigma_1(\alpha) + \sigma_7(\alpha) = \alpha + \alpha^7 = \sqrt{2}$$

الجدول 8.54

|                      |            |            |            |            |
|----------------------|------------|------------|------------|------------|
|                      | $\sigma_1$ | $\sigma_3$ | $\sigma_5$ | $\sigma_7$ |
| $\alpha \rightarrow$ | $\alpha$   | $\alpha^3$ | $\alpha^5$ | $\alpha^7$ |



الشكل 9.54 (أ) الرسم البياني للزمرة. (ب) الرسم البياني للحقول.

يترك ثابتاً بـ  $\{\sigma_1, \sigma_7\}$ . لن نجد هذه التقنيات لإيجاد  $E_{\{\sigma_1, \sigma_5\}}$ : لأن

$$\sigma_1(\alpha) + \sigma_5(\alpha) = \alpha + \alpha^5 = 0$$

و  $0 \in \mathbb{Q}$ ، ولكن بمناقشة مشابهة،  $\sigma_1(\alpha) \sigma_5(\alpha)$  تترك ثابتة بكلا  $\sigma_1$  و  $\sigma_5$ ،

$$\sigma_1(\alpha)\sigma_5(\alpha) = \alpha\alpha^5 = -i \text{ و}$$

إن،  $\mathbb{Q}(-i) = \mathbb{Q}(i)$  هو الحقل الذي نسعى وراءه.



## ■ تمارين 54

حسابات (تتطلب استخدام مبرهنات أكثر من المعتاد)

1. أثبت أن  $x^4 + 1$  غير مختزل على  $\mathbb{Q}[x]$  - كما ذكرنا في المثال 7.54.
2. تحقق من أن الحقول المتوسطة المعطاة في الرسم البياني للحقول في الشكل 6.54 صحيحة. (تم التحقق من بعضها في الكتاب. تحقق من الباقي).
3. لكل حقل من الحقول في الرسم البياني في الشكل 6.54، أوجد العنصر البدائي المولد للحقل على  $\mathbb{Q}$  (انظر المبرهنة 5.51)، وأعطِ كثيرة الحدود غير المختزلة لها على  $\mathbb{Q}$ .
4. ليكن  $\zeta$  جذراً بدائياً من الرتبة 5 للواحد في  $\mathbb{Q}$ .  
أ. أثبت أن  $\mathbb{Q}(\zeta)$  حقل انشطار لـ  $x^5 - 1$  على  $\mathbb{Q}$ .  
ب. أثبت أن أي تماثل ذاتي على  $K = \mathbb{Q}(\zeta)$  يربط  $\zeta$  بأحد القوى  $\zeta^j$  لـ  $j$ .  
ج. مستخدماً الفرع (ب)، صف عناصر  $G(K/\mathbb{Q})$ .
- د. أعطِ الرسم البياني للزمر والحقول لـ  $\mathbb{Q}(\zeta)$  على  $\mathbb{Q}$ ، واحسب الحقول المتوسطة، كما فعلنا في المثالين 3.54 و 7.54.
5. صف زمرة كثيرة الحدود  $(\mathbb{Q}(\zeta)[x] / (x^5 - 2))$  على  $\mathbb{Q}(\zeta)$ ، حيث  $\zeta$  الجذر البدائي من الرتبة 5 للواحد.
6. أعد التمرين 4 لـ  $\zeta$  الجذر البدائي من الرتبة 7 للواحد في  $\mathbb{C}$ .
7. صف زمرة كثيرة الحدود بأسهل طريقة ممكنة على  $\mathbb{Q}$ .  
 $(x^8 - 1) \in \mathbb{Q}[x]$

8. أوجد حقل الانشطار  $K$  في  $\mathbb{C}$  لكثيرة الحدود  $(x^4 - 4x^2 - 1) \in \mathbb{Q}[x]$ ، احسب زمرة كثيرة الحدود على  $\mathbb{Q}$ ، وأظهر التقابل بين الزمر الجزئية لـ  $G(K/\mathbb{Q})$  والحقول المتوسطة. بعبارة أخرى، قم بالعمل كله.

9. عبّر عن الدوال المتناظرة الآتية كلها في  $y_1, y_2, y_3$  على  $\mathbb{Q}$  بوصفها دالة نسبية في الدوال المتناظرة البدائية

$$s_1, s_2, s_3$$

$$أ. \quad y_1^2 + y_2^2 + y_3^2$$

$$ب. \quad \frac{y_1}{y_2} + \frac{y_2}{y_1} + \frac{y_1}{y_3} + \frac{y_3}{y_1} + \frac{y_2}{y_3} + \frac{y_3}{y_2}$$

10. لتكن  $\alpha_1, \alpha_2, \alpha_3$  أصفاراً في  $\mathbb{C}$  لكثيرة الحدود

$$(x^3 - 4x^2 + 6x - 2) \in \mathbb{Q}[x].$$

أوجد كثيرة الحدود ذات الأصفار المحددة الآتية:

$$أ. \quad \alpha_1 + \alpha_2 + \alpha_3$$

$$ب. \quad \alpha_1^2, \alpha_2^2, \alpha_3^2$$

براهين

11. أثبت أن أي زمرة منتهية تماثل زمرة جالوا  $G(K/F)$  لامتداد منته ناظمي  $K$  لأحد الحقول  $F$ .

12. لتكن  $f(x) \in F[x]$  كثيرة حدود أحادية من الدرجة  $n$ ، بحيث إن عواملها غير المختزلة كلها قابلة للفصل على  $F$ . ليكن

$\bar{K} \leq K$  حقل انشطار  $f(x)$  على  $F$ ، وافترض أن  $f(x)$  تتحلل في  $K[x]$  إلى:

$$\prod_{i=1}^n (x - \alpha_i).$$

لتكن:

$$\Delta(f) = \prod_{i < j} (\alpha_i - \alpha_j);$$

يسمى حاصل الضرب  $\Delta(f)^2$  بالمايز لـ  $f(x)$  (discriminant)

أ. أثبت أن  $\Delta(f) = 0$ ، إذا وفقط إذا كان أحد عوامل  $f(x)$  مربعاً لكثيرة حدود غير مختزلة في  $F[x]$ .

ب. أثبت أن  $(\Delta(f))^2 \in F$ .

ج. يمكن النظر لـ  $G(K/F)$  بوصفها زمرة جزئية من  $\bar{S}_n$ ، حيث  $\bar{S}_n$  زمرة جميع التبادل  $\{\alpha_i \mid i=1, \dots, n\}$ . أثبت أن

$G(K/F) -$  عندما ينظر لها بهذه الطريقة - زمرة جزئية من  $\bar{A}_n$  - الزمرة المكوّنة من التباديل الزوجية جميعها في

$\{\alpha_i \mid i=1, \dots, n\}$ ، إذا وفقط إذا كان  $\Delta(f) \in F$ .

13. يسمى العنصر في  $\mathbb{C}$  عدداً صحيحاً جبرياً، (algebraic integer) إذا كان صفراً لكثيرة حدود أحادية في  $\mathbb{Z}[x]$ .

أثبت أن مجموعة العناصر الصحيحة الجبرية، تشكل حلقة جزئية من  $\mathbb{C}$ .

## الامتدادات الدورية Cyclotomic Extensions

## الفصل 55

## زمرة جالوا لامتداد دوري

سيعالج هذا الفصل حقول الامتداد لحقل  $F$ ، التي يحصل عليها بإضافة بعض جذور الواحد ل  $F$ ، غُطيت حالة الحقل المنتهي في الفصل 33؛ لذا، سنكون مهتمين بصورة أساسية بحالة  $F$  غير المنتهي.

1.55 تعريف يسمى حقل انشطار  $x^n - 1$  على  $F$  الامتداد الدوري من الرتبة  $n$  ل  $F$  (nth cyclotomic extension).

افترض أن  $F$  أي حقل، وافترض  $(x^n - 1) \in F[x]$ ، فباستخدام القسمة الطويلة - كما في برهان التمهيدية 8.33 نرى أنه إذا كانت  $\alpha$  صفراً ل  $x^n - 1$  و  $g(x) = (x^n - 1)/(x - \alpha)$ ، فإن  $g(\alpha) = (n \cdot 1) (1/\alpha) \neq 0$ ، بشرط أن مميز  $F$  لا يقسم  $n$ ؛ لذلك - وتحت هذا الشرط - يكون حقل انشطار  $x^n - 1$  قابلاً للفصل، وهكذا، فهو امتداد ناظمي ل  $F$ .

## نبذة تاريخية

عالم كارل جاوس كثيرات الحدود الدورية في الفصل الأخير من كتابه (*Disquisitiones Arithmeticae*) عام 1801 م. في ذلك الفصل، أعطى إجراءات بنائية لتحديد أصفار  $\Phi_p(x)$ ، حيث  $p$  عدد أولي.

أصبحت طريقة جاوس مثلاً مهماً لجالوا في تطوير المبرهنة العامة، التي كانت حلّ سلسلة من المعادلات المساعدة، كل من درجة أولية تقسم  $p - 1$ ، ومعاملات كل منها، وعليه، تحدد من جذور المعادلة السابقة، فقد علم جاوس - بلا ريب - أن جذور  $\Phi_p(x)$  هي قوى إحداها، وليكن  $\zeta$ ، وقد حدّد المعادلات المساعدة بأخذ مجموعات محددة من مجاميع الجذور  $\zeta^k$ ، التي كانت الجذور المطلوبة لهذه المعادلات، على سبيل المثال: في حالة  $p = 19$  و  $(p - 1 = 18 = 3 \times 3 \times 2)$ ، احتاج جاوس إلى إيجاد معادلتين من الدرجة 3 ومعادلة من الدرجة 2 بوصفها مساعدات، وقد تبين أن الأولى لها الجذور الثلاثة:

$$\alpha_1 = \zeta^{12} + \zeta^{11} + \zeta^{18} + \zeta^7 + \zeta^8 + \zeta$$

$$\alpha_2 = \zeta^5 + \zeta^3 + \zeta^{17} + \zeta^{14} + \zeta^{16} + \zeta^2, \quad \alpha_3 = \zeta^{10} + \zeta^6 + \zeta^{15} + \zeta^9 + \zeta^{13} + \zeta^4$$

في الحقيقة، هذه القيم الثلاث هي جذور المعادلة التكعيبية  $x^3 + x^2 - 6x - 7$ ، ثم وجد جاوس معادلة تكعيبية ثانية، تتألف معاملاتها من  $\alpha$ ، وكانت جذورها مجاميع قوتين ل  $\zeta$ ، وأخيراً معادلة تربيعية، تتألف معاملاتها من جذور المعادلة السابقة، التي كانت  $\zeta$  أحد جذورها.

صرّح جاوس بعدها (من غير برهان كامل): أن كل معادلة مساعدة يمكن أن تختزل إلى معادلة على الصورة  $x^m - A$ ، التي يمكن حلها باستخلاص الجذور، أي إنه أثبت أن قابلية الحل لزمرة جالوا في هذه الحالة - الزمرة الدورية من الرتبة  $p - 1$  - تؤدي إلى قابلية حلّ المعادلة الدورية باستخلاص الجذور. (انظر الفصل 56).

افترض من الآن فصاعداً أن هذه هي الحالة، وأن  $K$  حقل الانشطار ل  $x^n - 1$  على  $F$ ؛ إذن،  $x^n - 1$  لها  $n$  من الأصفار في  $K$ ، وبحسب النتيجة 6.23، تشكل هذه الأصفار زمرة دورية من الرتبة  $n$  مع عملية الضرب في الحقل، لقد رأينا في النتيجة 16.6، أن الزمرة الدورية من الرتبة  $n$  لها  $\varphi(n)$  من المولدات - حيث  $\varphi$  هي دالة - فاي لأويلر التي عرفت قبل المبرهنة 8.20. في حالتنا هذه، المولدات هي بالضبط الجذور البدائية من الرتبة  $n$  للواحد.

كثيرة الحدود

2.55 تعريف

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \alpha_i)$$

حيث  $\alpha_i$  الجذور البدائية من الرتبة  $n$  للواحد في  $\bar{F}$ ، هي كثيرة الحدود الدورية من الرتبة  $n$  على  $F$  (nth cyclotomic polynomial).

لأن التماثل من زمرة جالوا  $G(K/F)$ ، يجب أن يبادل بين الجذور البدائية من الرتبة  $n$  للواحد، فنرى أن  $\Phi_n(x)$  تترك ثابتة مع أي عنصر في  $G(K/F)$ ، معدوداً بوصفه تمديداً طبيعياً إلى  $K[x]$ ؛ إذن،  $\Phi_n(x) \in F[x]$ . بوجه خاص،  $F = \mathbb{Q}$ ،  $\Phi_n(x) \in \mathbb{Q}[x]$ ، و  $\Phi_n(x)$  تقسم  $x^{n-1} - 1$ ؛ إذن، على  $\mathbb{Q}$ ، يجب في الحقيقة أن نعد  $\Phi_n(x) \in \mathbb{Z}[x]$  بحسب المبرهنة 11.23. لقد رأينا أن  $\Phi_p(x)$  غير مختزلة على  $\mathbb{Q}$ ، في النتيجة 17.23، بينما  $\Phi_n(x)$  ليست بالضرورة غير مختزلة في حالة الحقول  $\mathbb{Z}_p$ ، حيث يمكن إثبات أن  $\Phi_n(x)$  غير مختزلة على  $\mathbb{Q}$ .

دعونا الآن نحدد نقاشنا بالميز  $0$ ، بوجه خاص الحقول الجزئية من الأعداد المركبة. ليكن  $i$  الصفر المركب العادي لـ  $x^2 + 1$ . عملنا بهذا العدد المركب في الفصل 1 يثبت أن:

$$\left( \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \right)^n = \cos 2\pi + i \sin 2\pi = 1,$$

إذن  $\cos(2\pi/n) + i \sin(2\pi/n)$  جذر من الرتبة  $n$  للواحد، وأقل عدد صحيح  $m$ ، بحيث  $(\cos(2\pi/n) + i \sin(2\pi/n))^m = 1$  هو  $n$ ؛ إذن  $\cos(2\pi/n) + i \sin(2\pi/n)$  جذر بدائي من الرتبة  $n$  للواحد، وصفر لـ

$$\phi_n(x) \in \mathbb{Q}[x].$$

الجذر البدائي من الرتبة 8 للواحد في  $\mathbb{C}$ ، هو:

3.55 مثال

$$\begin{aligned} \xi &= \cos \frac{2\pi}{8} + i \sin \frac{2\pi}{8} \\ &= \cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \\ &= \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}} = \frac{1+i}{\sqrt{2}}. \end{aligned}$$

بحسب مبرهنة الزمر الدورية، وبوجه خاص بحسب النتيجة 16.6، الجذور البدائية من الرتبة 8 للواحد في  $\mathbb{Q}$ ، هي:  $\zeta^3, \zeta^5, \zeta^7$ ؛ إذن:

$$\Phi_8(x) = (x - \zeta)(x - \zeta^3)(x - \zeta^5)(x - \zeta^7).$$

يمكننا الحساب مباشرة من هذا التعبير،  $\Phi_8(x) = x^4 + 1$  (انظر التمرين 1). قارن هذا بالمثال

7.54

لنظل محددين عملنا على  $F = \mathbb{Q}$ ، ولنفترض - من غير برهان - أن  $\Phi_n(x)$  غير مختزلة على  $\mathbb{Q}$ . لتكن :

$$\xi = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n},$$

إذن،  $\xi$  جذر بدائي من الرتبة  $n$  للواحد. لاحظ أن  $\xi$  مولد لزمرة الضرب الدورية من الرتبة  $n$ ، المكوّنة من الجذور من الرتبة  $n$  للواحد. الجذور البدائية كلها من الرتبة  $n$  - أي مولدات هذه الزمرة - تكون على الصورة  $\xi^m$ ، حيث  $1 \leq m < n$  و  $m$  أولية بالنسبة إلى  $n$ . الحقل  $\mathbb{Q}(\xi)$  هو كامل حقل الانشطار لـ  $x^n - 1$  على  $\mathbb{Q}$ . ليكن  $K = \mathbb{Q}(\xi^m)$ . إذا كان  $\xi^m$  جذراً بدائياً آخر من الرتبة  $n$  للواحد؛ إذن - ولأن  $\xi$  و  $\xi^m$  مترافقان على  $\mathbb{Q}$  - يوجد تماثل ذاتي  $\tau_m$  في  $G(K/\mathbb{Q})$  يربط  $\xi$  بـ  $\xi^m$ . ليكن  $\tau_r$  تماثلاً ذاتياً مشابهاً في  $G(K/\mathbb{Q})$  بالنسبة إلى الجذر البدائي من الرتبة  $n$  للواحد؛ إذن:

$$(\tau_m \tau_r)(\xi) = \tau_m(\xi^r) = (\tau_m(\xi))^r = (\xi^m)^r = \xi^{mr}.$$

هذا يثبت أن زمرة جالوا  $G(K/\mathbb{Q})$  تماثل الزمرة  $G_n$  في المبرهنة 6.20، المكوّنة من عناصر  $\mathbb{Z}_n$  الأولية بالنسبة إلى  $n$  مع عملية الضرب مقياس  $n$ ، وتحوي هذه الزمرة  $\varphi(n)$  من العناصر، وهي إبدالية.

ظهرت بعض الحالات الخاصة من هذه المادة مرات عدة في الكتاب والتمارين، على سبيل المثال:  $\alpha$  في المثال 7.54 جذر بدائي من الرتبة 8 للواحد، وقد ناقشنا في ذلك المثال مطابقة لتلك المعطاة هنا. نلخص هذه النتائج في مبرهنة.

زمرة جالوا للامتداد الدوري من الرتبة  $n$ ،  $\varphi(n)$  من العناصر، وتماثل الزمرة المولّفة من الأعداد الصحيحة الموجبة الأقل من  $n$  والأولية بالنسبة إلى  $n$  مع عملية الضرب مقياس  $n$ .

4.55 مبرهنة

يوضح المثال 7.54 هذه المبرهنة؛ لأنه من السهل رؤية أن حقل الانشطار لـ  $x^4 + 1$ ، هو نفسه حقل الانشطار لـ  $x^8 - 1$  على  $\mathbb{Q}$ ، حيث يستنتج هذا من حقيقة أن  $\Phi_8(x) = x^4 + 1$  (انظر المثال 3.55 والتمرين 1).

5.55 مثال

زمرة جالوا للامتداد الدوري من الرتبة  $p$  على  $\mathbb{Q}$ ، حيث  $p$  أولي، هي الزمرة الدورية من الرتبة  $p - 1$ .

6.55 نتيجة

بحسب المبرهنة 4.55، لزمرة جالوا للامتداد الدوري من الرتبة  $p$  على  $\mathbb{Q}$ ،  $\varphi(p) = p - 1$  من العناصر، وهي تماثل زمرة الأعداد الصحيحة الموجبة الأقل من  $p$  والأولية بالنسبة إلى  $p$  مع عملية الضرب مقياس  $p$ . هذه بالضبط زمرة الضرب  $(\mathbb{Z}_p^*, \cdot)$  المولّفة من العناصر غير الصفريّة في الحقل  $\mathbb{Z}_p$  مع عملية الضرب في الحقل، وبحسب النتيجة 6.23، هذه الزمرة دورية. ◆

البرهان

### المضلعات القابلة للإنشاء

نختم بتطبيق يحدد أيًا من المضلعات المنتظمة التي لها  $n$  من الأضلاع قابلة للإنشاء بالمسطرة والفرجار، لقد رأينا في الفصل 32، أن المضلع المنتظم الذي له  $n$  ضلعًا يكون قابلاً للإنشاء، إذا وفقط إذا كان  $\cos(2\pi/n)$  عددًا حقيقيًا قابلاً للإنشاء. الآن، لتكن:

$$\zeta = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

إذن

$$\frac{1}{\zeta} = \cos \frac{2\pi}{n} - i \sin \frac{2\pi}{n}$$

لأن:

$$\left( \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \right) \left( \cos \frac{2\pi}{n} - i \sin \frac{2\pi}{n} \right) = \cos^2 \frac{2\pi}{n} + \sin^2 \frac{2\pi}{n} = 1$$

ولكن

$$\zeta + \frac{1}{\zeta} = 2 \cos \frac{2\pi}{n}.$$

إذن، تثبت النتيجة 8.32 أن المضلع المنتظم الذي له  $n$  ضلعًا، يكون قابلاً للإنشاء، فقط إذا كان  $\zeta + 1/\zeta$  يولد امتدادًا على  $\mathbb{Q}$  درجته من قوى ألد 2.

إذا كان  $K$  حقل الانشطار لـ  $x^n - 1$  على  $\mathbb{Q}$ ، فإن  $[K : \mathbb{Q}] = \varphi(n)$ ، بحسب المبرهنة 4.55، وإذا كانت  $\sigma \in G(K/\mathbb{Q})$  و  $\sigma(\zeta) = \zeta^r$ ، فإن:

$$\begin{aligned} \sigma \left( \zeta + \frac{1}{\zeta} \right) &= \zeta^r + \frac{1}{\zeta^r} \\ &= \left( \cos \frac{2\pi r}{n} + i \sin \frac{2\pi r}{n} \right) + \left( \cos \frac{2\pi r}{n} - i \sin \frac{2\pi r}{n} \right) \\ &= 2 \cos \frac{2\pi r}{n}. \end{aligned}$$

ولكن إذا كان  $1 < r < n$ ، فنحصل على  $\cos(2\pi r/n) = 2 \cos(2\pi/n)$  فقط في حالة  $r = n - 1$ ؛ إذن، العناصر الوحيدة في  $G(K/G)$  التي تحمل  $\zeta \mapsto \zeta^{n-1} = 1/\zeta$  هي التماثل الذاتي المحايد والتماثل الذاتي  $\tau$ ، حيث  $\zeta \mapsto 1/\zeta$ ، يثبت هذا أن الزمرة الجزئية من  $G(K/\mathbb{Q})$  التي تترك  $\mathbb{Q}(\zeta + 1/\zeta)$  ثابتًا، هي من الرتبة 2؛ إذن وبحسب مبرهنة جالوا:

$$\left[ \mathbb{Q} \left( \zeta + \frac{1}{\zeta} \right) : \mathbb{Q} \right] = \frac{\varphi(n)}{2}.$$

إذن، يكون المضلع المنتظم الذي له  $n$  ضلعًا قابلاً للإنشاء، فقط إذا كان  $\varphi(n)/2 - \varphi(n)$  وهكذا  $\varphi(n)$  كذلك - من قوى ألد 2. يمكن الإثبات بمناقشة أولية في مبرهنة الأعداد، أنه إذا كانت:

$$n = 2^v p_1^{s_1} \cdots p_t^{s_t},$$

حيث أن  $p_i$  أعداد أولية مختلفة تقسم  $n$ : إذن:

$$(1) \quad \varphi(n) = 2^{v-1} p_1^{s_1-1} \cdots p_t^{s_t-1} (p_1 - 1) \cdots (p_t - 1).$$

إذا كانت  $\varphi(n)$  قوة لـ 2، فإن كل عدد أولي فردي يقسم  $n$ ، يجب أن يظهر فقط للقوة الأولى، ويجب أن يكون أكثر بواحد من إحدى قوى 2: إذن، يجب أن يكون كل

$$p_i = 2^m + 1$$

لأي  $m$ . ولأن  $-1$  صفر لـ  $x^q + 1$ ، حيث  $q$  عدد أولي فردي،  $x + 1$  تقسم  $x^q + 1$ ، حيث  $q$  عدد أولي فردي؛ إذن، إذا كانت  $m = q^u$ ، حيث  $q$  عدد أولي فردي، فإن  $2^m + 1 = (2^u)^q + 1$  تقسم  $2^m + 1$ ؛ وعليه، ليكون  $p_i = 2^m + 1$  عددًا أوليًا، يجب أن تكون  $m$  تقسم بـ 2 فقط، وبهذا يجب أن تكون  $p_i$  على الصورة:

$$p_i = 2^{(2^k)} + 1,$$

عدد فيرما الأولي (Fermat prime): خمن فيرما أن هذه الأعداد  $2^{(2^k)} + 1$  أعداد أولية لكل عدد صحيح غير سالب  $k$ ، ولكن أثبت أويلر أنه بينما تعطي  $k = 0, 1, 2, 3$  و  $k = 4$  الأعداد الأولية 3، 5، و 17، و 257 و 65537، فإن  $k = 5$ ، العدد الصحيح  $2^{(2^5)} + 1$  يقبل القسمة على 641، وقد أثبت أن  $5 \leq k \leq 19$ ، تكون الأعداد  $2^{(2^k)} + 1$  كلها غير أولية. حالة  $k = 20$  ما زالت غير محلولة على حد علمنا، وكذلك لـ 60 قيمة على الأقل لـ  $k$  أكبر من 20، بما فيها  $k = 9448$ ، وقد أثبت أن  $2^{(2^k)} + 1$  غير أولي، ومن غير المعروف ما إذا كان عدد أعداد فيرما الأولية منتهياً أم غير منته.

لقد أثبتنا أن المضلعات المنتظمة التي لها  $n$  ضلعاً والوحيدة التي يمكن أن تكون قابلة للإنشاء، هي تلك التي تكون الأعداد الأولية الفردية القاسمة لـ  $n$  أعداد فيرما الأولية، التي لا تقسم مربعاتها  $n$ ، بوجه خاص، المضلعات المنتظمة التي لها  $p$  ضلعاً الوحيدة التي يمكن أن تكون قابلة للإنشاء، حيث  $p$  أكبر من 2، هي تلك التي تكون حيث  $p$  عدد فيرما أولي.

المضلع المنتظم الذي له 7 أضلاع غير قابل للإنشاء؛ لأن 7 ليس عدد فيرما أولياً. بالمثل المضلع المنتظم الذي له 18 ضلعاً ليس قابلاً للإنشاء؛ لأنه على الرغم من أن 3 عدد فيرما أولي، فإن مربعها يقسم 18. ▲

### 7.55 مثال

سنبين الآن أن هذه المضلعات المنتظمة التي لها  $n$  ضلعاً المرشحة لتكون قابلة للإنشاء، هي في الحقيقة قابلة للإنشاء. لتكن مرة أخرى الجذر البدائي من الرتبة  $n$  للواحد  $\cos(2\pi/n) + i \sin(2\pi/n)$ . لقد رأينا قبل قليل أن:

$$2 \cos \frac{2\pi}{n} = \zeta + \frac{1}{\zeta},$$

وأن

$$\left[ \mathbb{Q} \left( \zeta + \frac{1}{\zeta} \right) : \mathbb{Q} \right] = \frac{\varphi(n)}{2}.$$

افترض الآن أن  $\varphi(n)$  القوة  $2^s$  لـ 2. ليكن  $E = \mathbb{Q}(\zeta + 1/\zeta)$ . لقد رأينا سابقاً أن  $\mathbb{Q}(\zeta + 1/\zeta)$  حقل جزئي من  $K = \mathbb{Q}(\zeta)$  يترك ثابتاً  $\tau$  حيث  $H_1 = \{1, \tau\}$ ، حيث  $i$  العنصر المحايد في  $G(K/\mathbb{Q})$  و  $\tau(\zeta) = 1/\zeta$ ، وبحسب مبرهنة سيلو، توجد زمرة جزئية إضافية  $H_j$  من الرتبة  $2^j$  من  $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ ، حيث  $j = 0, 2, 3, \dots, s$ ، بحيث إن:

$$\{H_j\} = H_0 < H_1 < \dots < H_s = G(\mathbb{Q}(\zeta)/\mathbb{Q}).$$

بحسب مبرهنة جالوا

$$\mathbb{Q} = K_{H_s} < K_{H_{s-1}} < \dots < K_{H_1} = \mathbb{Q}\left(\zeta + \frac{1}{\zeta}\right),$$

و  $[K_{H_{j-1}} : K_{H_j}] = 2$ . لاحظ أن  $(\zeta + 1/\zeta) \in \mathbb{R}$ ، وهكذا  $\mathbb{Q}(\zeta + 1/\zeta) < \mathbb{R}$  إذا كان  $K_{H_{j-1}} = K_{H_j}(\alpha_j)$ ، فإن  $\alpha_j$  صفر لـ  $K_{H_j}[x]$   $(a_j x^2 + b_j x + c_j) \in K_{H_j}$ . وبحسب "القانون العام" لحل المعادلة التربيعية المشهور، نحصل على:

$$K_{H_{j-1}} = K_{H_j}(\sqrt{b_j^2 - 4 a_j c_j})$$

لأننا رأينا في الفصل 33 أن إنشاء الجذور التربيعية لعدد موجب قابل للإنشاء يمكن تحقيقه بالمسطرة والفرجار، نرى أن كل عنصر في  $\mathbb{Q}(\zeta + 1/\zeta)$ ، وبوجه خاص،  $\cos(2\pi/n)$  قابل للإنشاء؛ إذن، المضلع المنتظم الذي له  $n$  ضلعاً، حيث  $\varphi(n)$  إحدى قوى 2 قابل للإنشاء.

نلخص عملنا تحت هذا العنوان بمبرهنة.

المضلع المنتظم الذي له  $n$  ضلعاً قابل للإنشاء بالمسطرة والفرجار، إذا وفقط إذا كانت الأعداد الأولية الفردية كلها التي تقسم  $n$ ، أعداد فيرما الأولية، وبحيث لا تقسم مربعاتها  $n$ .

8.55 مبرهنة

المضلع المنتظم الذي له 60 ضلعاً قابلاً للإنشاء؛ لأن  $(5) (3) (2^2) = 60$  وكلا 3 و 5 أعداد فيرما الأولية.

9.55 مثال

▲

## ■ تمارين 55

## حسابات

1. بالرجوع إلى المثال 3.55، أكمل الحسابات المشار إليها، مثبتاً أن  $\Phi_8(x) = x^4 + 1$ .  
[ اقتراح: احسب حاصل الضرب بدلالة  $\zeta$ ، ثم استخدم حقيقة أن  $\zeta^8 = 1$  و  $\zeta^4 = -1$  لتبسيط المعاملات.]
2. صنف زمرة كثيرة الحدود  $(x^2 - 1) \in \mathbb{Q}[x]$  على  $\mathbb{Q}$  بحسب المبرهنة الأساسية للزمر الإبدالية المنتهية التولد. [مساعدة: استخدم المبرهنة 4.55.]
3. مستخدماً صيغة  $\varphi(n)$  بدلالة تحليل  $n$ ، كما هو معطى في المعادلة (1)، احسب القيم المشار إليها:  
أ.  $\varphi(60)$       ب.  $\varphi(1000)$       ج.  $\varphi(8100)$
4. أعط القيم أول 30 الأولى لـ  $n \geq 3$ ، بحيث يكون المضلع المنتظم الذي له  $n$  ضلعاً قابلاً للإنشاء بالمسطرة والفرجار.
5. أوجد أصغر زاوية ذات درجة صحيحة، أي  $1^\circ$ ،  $2^\circ$ ،  $3^\circ$ ، إلى آخره، قابلة للإنشاء بالمسطرة والفرجار. [مساعدة: إنشاء الزاوية  $1^\circ$  يعادل إنشاء المضلع المنتظم الذي له 360 ضلعاً، وهكذا.]
6. ليكن  $K$  حقل انشطار  $x^{12} - 1$  على  $\mathbb{Q}$ .  
أ. أوجد  $[K : \mathbb{Q}]$ .  
ب. أثبت أنه لكل  $\sigma \in G(K/\mathbb{Q})$ ،  $\sigma^2$  هو التماثل الذاتي المحايد. صنف  $G(K/\mathbb{Q})$  بحسب المبرهنة الأساسية 12.11 للزمر الإبدالية منتهية التولد.
7. أوجد  $\Phi_3(x)$  على  $\mathbb{Z}_2$ ، وأوجد  $\Phi_8(x)$  على  $\mathbb{Z}_3$ .
8. كم عنصراً يوجد في حقل انشطار  $x^6 - 1$  على  $\mathbb{Z}_3$ ؟

## مفاهيم

9. ضع إشارة صح أو إشارة خطأ:  
أ.  $\Phi_n(x)$  غير مختزلة على أي حقل مميزه 0.  
ب. كل صفر في  $\mathbb{C}$  لـ  $\Phi_n(x)$ ، هو جذر بدائي من الرتبة  $n$  للواحد.  
ج. زمرة  $\Phi_n(x) \in \mathbb{Q}[x]$  على  $\mathbb{Q}$  تحوي  $n$  من العناصر.  
د. زمرة  $\Phi_n(x) \in \mathbb{Q}[x]$  على  $\mathbb{Q}$  إبدالية.  
هـ. زمرة جالوا لحقل انشطار  $\Phi_n(x)$  على  $\mathbb{Q}$  من الرتبة  $\varphi(n)$ .  
و. المضلع المنتظم الذي له 25 ضلعاً، قابل للإنشاء بالمسطرة والفرجار.  
ز. المضلع المنتظم الذي له 17 ضلعاً، قابل للإنشاء بالمسطرة والفرجار.  
ح. لكل عدد أولي  $p$ ، المضلع المنتظم الذي له  $p$  ضلعاً، قابل للإنشاء إذا وفقط إذا كان  $p$  عدد فيرما الأولي.  
ط. الأعداد الصحيحة كلها على الشكل  $2^{(2^k)} + 1$ ، حيث  $k$  عدد صحيح غير سالب، هي أعداد فيرما الأولية.  
ي. أعداد فيرما الأولية كلها أعداد على الصورة  $2^{(2^k)} + 1$ ، حيث  $k$  عدد صحيح غير سالب.

## براهين

10. أثبت أنه إذا كان  $F$  حقلاً مميزه لا يقسم  $n$ ، فإن

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

في  $F[x]$ ، حيث الضرب على القواسم  $d$  لـ  $n$  كلها.

11. أوجد كثيرة الحدود الدورية  $\Phi_n(x)$  على  $\mathbb{Q}$  لـ  $n = 1, 2, 3, 4, 5, 6$ . [مساعدة: استخدم التمرين 10].
12. أوجد  $\Phi_{12}(x)$  في  $\mathbb{Q}[x]$ . [مساعدة: استخدم التمرينين 10 و 11].
13. أثبت أنه في  $\mathbb{Q}[x]$ ,  $\Phi_{2n}(x) = \Phi_n(-x)$ , لكل عدد صحيح فردي  $n > 1$ . [مساعدة: إذا كانت  $\zeta$  جذراً بدائياً من الرتبة  $n$  الفردية للواحد، فما رتبة  $\zeta^{-1}$ ؟].
14. لتكن  $n, m \in \mathbb{Z}^+$  أولية نسبياً. أثبت أن حقل الانشطار في  $\mathbb{C}$  لـ  $x^{nm} - 1$  على  $\mathbb{Q}$  هو نفسه حقل الانشطار في  $\mathbb{C}$  لـ  $(x^n - 1)(x^m - 1)$  على  $\mathbb{Q}$ .
15. لتكن  $n, m \in \mathbb{Z}^+$  أولية نسبياً. أثبت أن زمرة  $\mathbb{Q}[x]$   $(x^{nm} - 1) \in \mathbb{Q}[x]$  على  $\mathbb{Q}$  تماثل الضرب المباشر لزمرتي  $(x^n - 1) \in \mathbb{Q}[x]$  و  $(x^m - 1) \in \mathbb{Q}[x]$  على  $\mathbb{Q}$ . [مساعدة: مستخدماً مبرهنة جالوا، أثبت أن زمرتي  $x^n - 1$  و  $x^m - 1$  كليهما يمكن أن تُعدا زمرتين جزئيتين من زمرة  $x^{nm} - 1$ . ثم استخدم التمرينين 50 و 51 في الفصل 11].

## الفصل 56

## المشكلة

## عدم قابلية حل المعادلة من الدرجة الخامسة للحلّ

نحن معتادون على حقيقة أنّ كثيرة الحدود من الدرجة الثانية  $f(x) = ax^2 + bx + c, a \neq 0$  ذات المعاملات الحقيقية لها  $(-b \pm \sqrt{b^2 - 4ac} / 2a)$  بوصفها أصفارًا في  $\mathbb{C}$ . في الحقيقة، هذا صحيح لـ  $f(x) \in F[x]$  حيث  $F$  أي حقل مميزه  $2 \neq$  والأصفار في  $\bar{F}$ . سيطلب منا في التمرين 4 إثبات هذا. وهكذا، وعلى سبيل المثال:

$$(x^2 + 2x + 3) \in \mathbb{Q}[x] \text{ أصفارها في } \mathbb{Q}(\sqrt{-2}).$$

## امتدادات بالجذور

قد تتساءل ما إذا كانت أصفار كثيرة حدود من الدرجة الثالثة على  $\mathbb{Q}$ ، يمكن دائمًا التعبير عنها باستخلاص الجذور، والجواب نعم بالتأكيد، وحتى أصفار كثيرة حدود من الدرجة 4 على  $\mathbb{Q}$ ، يمكن التعبير عنها باستخلاص الجذور، وبعد أن حاول الرياضيون سنوات إيجاد "صيغة" باستخلاص الجذور. لأصفار كثيرة الحدود من الدرجة 5، فقد كان نصرًا، عندما أثبت "أبل" أنّ المعادلة الخامسة لا تحلّ بالضرورة باستخلاص الجذور، سيكون عملنا الأول الوصف الدقيق لما يعنيه هذا، وسيستخدم في المناقشة المقبلة قدر كبير من الجبر الذي طوّره.

يسمى الامتداد  $K$  للحقل  $F$  امتدادًا لـ  $F$  بالجذور. (extension of  $F$  by radicals). إذا

وجدت عناصر  $\alpha_1, \dots, \alpha_r \in K$  وأعداد صحيحة موجبة

$n_1, \dots, n_r$ ، بحيث إنّ  $\alpha_i^{n_i} \in F$ ،  $K = F(\alpha_1, \dots, \alpha_r)$ ، و  $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$  لكل

$1 < i \leq r$  حيث كثيرة الحدود  $f(x) \in F[x]$  قابلة للحلّ باستخلاص الجذور على  $F$  (Solv-)

$F$  (able by radicals over  $F$ )، إذا كان حقل الانشطار  $E$  لـ  $f(x)$  على  $F$  محتوي في امتداد لـ

$F$  بالجذور.

■  
إنّ، تكون كثيرة الحدود  $f(x) \in F(x)$  قابلة للحلّ باستخلاص الجذور على  $F$ ، إذا كان بالإمكان الحصول على كل صفر لـ  $f(x)$  باستخدام سلسلة منتهية من عمليات الجمع، والطرح، والضرب، والقسمة، وأخذ الجذور  $n_i$  بدءًا بعناصر من  $F$ . الآن، قولنا: إنّ المعادلة من الدرجة الخامسة غير قابلة للحل في الحالة التقليدية - أي المميز  $0$  - لا يعني قولنا: إنه لا معادلة من الدرجة الخامسة قابلة للحلّ، كما يثبت المثال الآتي.

## 1.56 تعريف

■ نبذة تاريخية

كان أول نشر لصيغة حل المعادلة من الدرجة الثالثة باستخلاص الجذور عام 1545م في كتاب (*Ars Magna*) لجيرولامو كاردانو (*Girolamo Cardano*)، على الرغم من أن بداية اكتشاف الطريقة جزئياً يعود كذلك لسيبوني ديل فيرو، ونيكولو تارتاجليا (*Scipione del Ferro and Niccolo Tartaglia*). اكتشف تلميذ كاردانو، لودوفيكو فيراري (*Lodovico Ferrari*) طريقة لحل المعادلة من الدرجة الرابعة باستخلاص الجذور، التي ظهرت كذلك ضمن عمل كاردانو.

وبعد أن حاول كثير من الرياضيين حل المعادلة من الدرجة الخامسة بطرق مشابهة، كان جوزيف لويس لاجرانج (*Joseph Louis Lagrange*) عام 1770م أول من حاول بالتفصيل تحليل المبدأ العام وراء حلول كثيرات الحلول من الدرجة 3 و 4، وبرهن لماذا فشلت هذه الطرق في حل تلك المعادلات ذات الدرجات الأعلى، كان أساس فهمه العميق لهذه الطرق السابقة يقوم على وجود دوال نسبية للجذور، التي تأخذ قيمتين أو ثلاثة - على التوالي - تحت التباديل الممكنة للجذور كلها، وهكذا يمكن كتابة هذه الدوال النسبية بوصفها جذوراً لمعادلات ذات درجة أقل من الأصلية، لم تكن أي من هذه الدوال واضحة في المعادلات ذات الدرجات الأعلى.

كان أول رياضي يدعي عدم قابلية المعادلة من الدرجة الخامسة للحل هو باولو روفيني (*Paolo Ruffini* 1765-1822)، في كتابه في الجبر عام 1799م، وقد كان برهانه تبعاً لمقترحات لاجرانج، ففي الواقع، حدد الزمر الجزئية جميعها من  $S_5$ ، وأثبت كيف تؤثر هذه الزمر الجزئية في الدوال النسبية لجذور المعادلة، ولسوء الطالع، كان هناك كثير من الثغرات في النسخ المنشورة من البرهان، لقد كان نيلز هينريك أبل (*Niels Henrik Abel*) الذي نشر برهاناً كاملاً عامي 1824م و1826م، مغلقاً ثغرات روفيني جميعها، الذي حل سؤالاً عمره قرون.

2.56 مثال

كثيرة الحدود  $x^5 - 1$  قابلة للحل باستخلاص الجذور على  $\mathbb{Q}$ . حقل الانشطار  $K \supset \mathbb{Q}$  لـ  $x^5 - 1$  مولد بالجذر البدائي  $\zeta$  من الرتبة 5 للواحد، أي  $\zeta^5 = 1$  و  $K = \mathbb{Q}(\zeta)$ . وكذلك  $x^5 - 2$  قابلة للحل باستخلاص الجذور على  $\mathbb{Q}$ ؛ لأن حقل انشطارها مولد بـ  $\sqrt[5]{2}$  و  $\zeta$ ، حيث  $\sqrt[5]{2}$  هو الصفر الحقيقي لـ  $x^5 - 2$ . ▲

للقول: إن المعادلة من الدرجة الخامسة غير قابلة للحل في الحالة التقليدية، يعني أنه يوجد بعض كثيرات الحدود من الدرجة 5 معاملاتها أعداد حقيقية، ولا يمكن حلها باستخلاص الجذور. سنثبت ذلك، سوف نفترض أن الحقول المذكورة خلال هذا الفصل جميعها ذات مميز 0.

الخطوط العريضة للمناقشة هي كما يأتي، ومن النافع محاولة تذكرها.

1. سنثبت أن كثيرة الحدود  $f(x) \in F(x)$  قابلة للحل باستخلاص الجذور على  $F$ ، (إذا و) فقط إذا كان حقل انشطارها  $E$  على  $F$  له زمرة جالوا قابلة للحل.

تذكر أن الزمرة القابلة للحل، هي تلك التي يكون لها سلسلة تركيب مع خوارج إبدالية، ومع أن هذه المبرهنة صحيحة في الاتجاهين، فإننا لن نثبت جزء «إذا».

2. سوف نثبت أنه يوجد حقل جزئي  $F$  من الأعداد الحقيقية وكثيرة حدود  $f(x) \in F(x)$  من الدرجة 5 مع حقل انشطار  $E$  على  $F$ ، بحيث  $G(E/F) \simeq S_5$ ، زمرة التناظر على 5 حروف. تذكر أن سلسلة التركيب لـ  $S_5$  هي  $S_5 < A_5 < \{1\}$ ، ولأن  $A_5$  ليست إبدالية، نكون قد انتهينا.

التمهيدية الآتية تقوم بمعظم عمل الخطوة 1.

**3.56 تمهيدية** ليكن  $F$  حقلاً مميزه  $0$ ، وليكن  $a \in F$ ، فإذا كان  $K$  حقل انشطار  $x^n - a$  على  $F$ ، فإن  $G(K/F)$  زمرة قابلة للحل.

البرهان:

افترض أولاً أن  $F$  يحوي الجذور جميعها من الرتبة  $n$  للواحد، وبحسب النتيجة 6.23، تشكل الجذور من الرتبة  $n$  للواحد زمرة جزئية دورية من  $(F^*, \cdot)$  ليكن  $\zeta$  مولداً لهذه الزمرة الجزئية. (في الحقيقة، المولدات هي بالضبط الجذور البدائية من الرتبة  $n$  للواحد): إذن، الجذور من الرتبة  $n$  للواحد هي:

$$1, \zeta, \zeta^2, \dots, \zeta^{n-1}.$$

فإذا كان  $\beta \in \overline{F}$  صفراً لـ  $(x^n - a) \in F[x]$ ، فإن أصفار  $x^n - a$  هي:

$$\beta, \zeta\beta, \zeta^2\beta, \dots, \zeta^{n-1}\beta.$$

ولأن  $K = F(\beta)$ ، فإن أي تماثل ذاتي  $\sigma$  في  $G(K/F)$  يتحدد بقيمة  $\sigma(\beta)$  للتماثل الذاتي  $\sigma$  على  $\beta$ . الآن، إذا كان  $\sigma(\beta) = \zeta^i\beta$  و  $\tau(\beta) = \zeta^j\beta$ ، حيث  $\tau \in G(K/F)$ ، فإن:

$$(\tau\sigma)(\beta) = \tau(\sigma(\beta)) = \tau(\zeta^i\beta) = \zeta^i\tau(\beta) = \zeta^i\zeta^j\beta,$$

لأن  $\zeta^i \in F$  وبالمثل:

$$(\sigma\tau)(\beta) = \zeta^j\zeta^i\beta$$

إذن،  $\sigma\tau = \tau\sigma$ ، و  $G(F/K)$  إبدالية؛ ولذلك، فهي قابلة للحل.

الآن، افترض أن  $F$  لا يحوي الجذور البدائية من الرتبة  $n$  للواحد. ليكن  $\zeta$  مولداً للزمرة الدورية للجذور من الرتبة  $n$  للواحد مع عملية الضرب في  $\overline{F}$ . ليكن  $\beta$  مرة أخرى صفراً لـ  $x^n - a$ ، فلأن  $\beta$  و  $\zeta\beta$  كليهما في حقل الانشطار  $K$  لـ  $x^n - a$ ، فإن  $\zeta = (\zeta\beta)/\beta$  تقع في  $K$ . ليكن  $F' = F(\zeta)$ ، نحصل على  $F < F' \leq K$ . الآن،  $F'$  امتداد ناظمي على  $F$ ؛ لأن  $F'$  حقل انشطار  $x^n - 1$ ، ولأن  $F' = F(\zeta)$ ، فيتحدد التماثل الذاتي  $\eta$  من  $G(F'/F)$  بـ  $\eta(\zeta) = \zeta^i$ ، ويجب أن نحصل على  $\eta(\zeta) = \zeta^i$ ؛ لأن أصفار  $x^n - 1$  كلها هي قوى  $\zeta$ ، وإذا كان  $\mu(\zeta) = \zeta^j$ ، حيث  $\mu \in G(F'/F)$ ، إذن:

$$(\mu\eta)(\zeta) = \mu(\eta(\zeta)) = \mu(\zeta^i) = \mu(\zeta)^i = (\zeta^j)^i = \zeta^{ij}$$

وكذلك بالمثل،

$$(\eta\mu)(\zeta) = \zeta^{ij}.$$

إذن،  $G(F'/F)$  إبدالية. وبحسب المبرهنة الأساسية لمبرهنة جالوا،

$$\{i\} \leq G(K/F') \leq G(K/F)$$

سلسلة ناظرية؛ ولذلك فهي سلسلة تحت ناظرية من الزمر. أثبت الجزء الأول من البرهان أن  $G(K/F')$  إبدالية، وتخيرنا مبرهنة جالوا بأن  $G(K/F)/G(K/F')$  تماثل  $G(F'/F)$ ، وهي إبدالية، حيث يثبت التمرين 6، أنه إذا كان لزمرة سلسلة تحت ناظرية من الزمر الجزئية زمرة خارجة إبدالية، فإن أي تصفية لهذه السلسلة لها كذلك زمرة خارجة إبدالية؛ إذن، سلسلة التركيب لـ  $G(K/F)$  لها زمرة خارجة إبدالية، وهكذا، فإن  $G(K/F)$  قابلة للحل. ♦

ستكمل المبرهنة الآتية الخطوة 1 في برنامجنا.

#### 4.56 مبرهنة

ليكن  $F$  حقلاً مميزه صفر، وليكن  $F \leq E \leq K \leq \bar{F}$ ، حيث  $E$  امتداد ناظمي لـ  $F$  و  $K$  امتداد بالجزور لـ  $F$ ؛ إذن، زمرة  $G(E/F)$  زمرة قابلة للحل.

#### البرهان

سنثبت في البداية أن  $K$  محتوي في امتداد ناظمي منته  $L$  لـ  $F$  بالجزور، وأن الزمرة  $G(L/F)$  قابلة للحل. لأن  $K$  امتداد بالجزور،  $K = F(\alpha_1, \dots, \alpha_r)$ .

حيث  $\alpha_i^{n_i} \in F$  و  $1 < i \leq r$  و  $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ ، ولتكوين  $L$ ، نكوّن أولاً حقل الانشطار  $L_1$  لكثيرة الحدود  $f_1(x) = x^{n_1} - \alpha_1^{n_1}$  على  $F$ ؛ إذن،  $L_1$  امتداد ناظمي على  $F$ ، وتثبت التمهيدية 3.56 أن  $G(L_1/F)$  زمرة قابلة للحل. الآن،  $\alpha_2^{n_2} \in L_1$  ونكوّن كثيرة الحدود.

$$f_2(x) = \prod_{\sigma \in G(L_1/F)} \left[ (x^{n_2} - \sigma(\alpha_2))^{n_2} \right].$$

لأن كثيرة الحدود لا تتغير تحت تأثير أي  $\sigma$  في  $G(L_1/F)$ ، نرى أن  $f_2(x) \in F[x]$ . سنترك  $L_2$  ليكون حقل انشطار  $f_2(x)$  على  $L_1$ ؛ إذن،  $L_2$  حقل انشطار على  $F$  كذلك، وهو امتداد ناظمي على  $F$  بالجزور، نستطيع بناء  $L_2$  من  $L_1$  عن طريق خطوات متكررة كما في التمهيدية 3.56 مروراً إلى حقل انشطار  $x^{n_2} - \sigma(\alpha_2)^{n_2}$  بكل خطوة، وبحسب التمهيدية 3.56 وتمرين 7، نرى أن زمرة جالوا على  $F$  لكل امتداد جديد مكوّن تظل قابلة للحل، نستمر بهذه الخطوات بتكوين حقول انشطار على  $F$  بهذا الأسلوب: في المرحلة  $i$ ، نكوّن حقل انشطار لكثيرة الحدود

$$f_i(x) = \prod_{\alpha \in G(L_{i-1}/F)} \left[ (x^{n_i} - \sigma(\alpha_i))^{n_i} \right]$$

على  $L_{i-1}$ . نحصل أخيراً على الحقل  $L = L_r$ ، الذي يكون امتداداً ناظماً على  $F$  بالجزور، ونرى أن  $G(L/F)$  زمرة قابلة للحل، حيث نرى من خلال العمل أن  $K \leq L$ .

لنختم عملنا، نحتاج إلى أن نلاحظ أنه بحسب المبرهنة 6.53، يكون  $G(L/F) \simeq G(L/F)/G(L/E)$  زمرة عامل، وعليه، هي صورة تشاكل من  $G(L/F)$ . ولأن  $G(L/F)$  قابل للحل، فيثبت التميرين 29 في الفصل 35 أن  $G(E/F)$  قابل للحل. ♦

#### عدم قابلية المعادلة من الدرجة الخامسة للحل باستخلاص الجذور

بقي علينا إثبات وجود حقل جزئي  $F$  من الأعداد الحقيقية وكثيرة حدود  $f(x) \in F(x)$  من الدرجة الخامسة، بحيث إن حقل الانشطار  $E$  لـ  $f(x)$  على  $F$  له زمرة جالوا تماثل  $S_5$ .

ليكن  $y_1 \in \mathbb{R}$  متسامياً على  $\mathbb{Q}$ ،  $y_2 \in \mathbb{R}$  متسامياً على  $\mathbb{Q}(y_1)$ ، وهكذا، حتى نصل إلى  $y_5 \in \mathbb{R}$  متسامية على  $\mathbb{Q}(y_1, \dots, y_4)$ . بالإمكان برهنة وجود مثل هذه الأعداد الحقيقية المتسامية باستخدام مقاربة العد، فالأعداد المتسامية التي يمكن إيجادها بهذه الطريقة تسمى عناصر متسامية مستقلة على  $\mathbb{Q}$  (independent transcendental elements). ليكن  $E = \mathbb{Q}(y_1, \dots, y_5)$ ، ولتكن:

$$f(x) = \prod_{i=1}^5 (x - y_i).$$

إذن،  $f(x) \in E[x]$  الآن معاملات  $-f(x)$  ما عدا احتمال الإشارة - ضمن الدوال المتناظرة الابتدائية في  $y_i$ ، يعني:

$$\begin{aligned}
s_1 &= y_1 + y_2 + \dots + y_5, \\
s_2 &= y_1 y_2 + y_1 y_3 + y_1 y_4 + y_1 y_5 + y_2 y_3 \\
&\quad + y_2 y_4 + y_2 y_5 + y_3 y_4 + y_3 y_5 + y_4 y_5, \\
&\quad \cdot \\
&\quad \cdot \\
&\quad \cdot \\
s_5 &= y_1 y_2 y_3 y_4 y_5.
\end{aligned}$$

معامل  $x^i$  في  $f(x)$  هو  $\pm s_{5-i}$ . ليكن  $F = \mathbb{Q}(s_1, s_2, \dots, s_5)$ ؛ إذن،  $f(x) \in F[x]$  (انظر الشكل 5.56)؛ وعليه،  $E$  حقل انشطار على  $F$ .

لأن  $y_i$  تتصرف بوصفها غير معين على  $\mathbb{Q}$ ، فإن كل  $\sigma \in S_5$  زمرة التماثل على خمسة حروف - تولد تماثلاً ذاتياً على  $E$  معرّف بـ  $\sigma(a) = a$  لكل  $a \in \mathbb{Q}$  و  $\sigma(y_i) = y_{\sigma(i)}$  ولأن

$$\begin{aligned}
&\prod_{i=1}^5 (x - y_{\sigma(i)}) \text{ هي كثيرة الحدود نفسها، فنحصل على} \\
&\bar{\sigma}(s_i) = s_i
\end{aligned}$$

لكل  $i$ ، وهذا يؤدي إلى أن  $\bar{\sigma}$  تترك  $F$  ثابتة، وهكذا، فإن  $\bar{\sigma} \in G(E/F)$  الآن، رتبة  $S_5$  تساوي  $5!$ ، وعليه،

$$|G(E/F)| \geq 5!.$$

لأن درجة حقل الانشطار على  $F$  لكثيرة حدود من الدرجة 5 على  $F$ ، هي على الأكثر  $5!$ ، فنرى أن:

$$|G(E/F)| \leq 5!.$$

إذن،  $|G(E/F)| = 5!$ ، والتماثلات الذاتية  $\bar{\sigma}$  تصنع كامل زمرة جالوا  $G(E/F)$ .

لذلك،  $G(E/F) \simeq S_5$ ، وهذا يؤدي إلى أن  $G(E/F)$  غير قابلة للحل، هذا يكمل خطوطنا العريضة، ونلخص ذلك في مبرهنة.

لتكن  $y_1, \dots, y_5$  أعداداً حقيقية متسامية مستقلة على  $\mathbb{Q}$ . كثيرة الحدود

$$f(x) = \prod_{i=1}^5 (x - y_i)$$

غير قابلة للحل باستخلاص الجذور على  $F = \mathbb{Q}(s_1, s_2, \dots, s_5)$ ، حيث  $s_i$  هي الدالة المتناظرة الابتدائية  $i$  في  $y_1, \dots, y_5$ .

من الواضح أن تعميم هذه المناقشة يثبت (الهدف النهائي)، أن كثيرة الحدود من الدرجة  $n$  ليست بالضرورة قابلة للحل باستخلاص الجذور لـ  $n \geq 5$ .

وختاماً، نشير إلى أنه توجد كثيرات حدود من الدرجة 5 في  $\mathbb{Q}[x]$  غير قابلة للحل باستخلاص الجذور على  $\mathbb{Q}$ . يترك برهان هذا إلى التمارين (انظر التمرين 8).

$$\begin{array}{c}
E = \mathbb{Q}(y_1, \dots, y_5) \\
\hline
F = \mathbb{Q}(s_1, \dots, s_5) \\
\hline
\mathbb{Q}
\end{array}$$

الشكل 5.56

### 6.56 مبرهنة

## ■ تمارين 56

### مفاهيم

1. هل يمكن الحصول على حقل الانشطار  $K$  لـ  $x^2 + x + 1$  على  $\mathbb{Z}_2$  بإضافة جذر تربيعي لـ  $\mathbb{Z}_2$  لأحد عناصر  $\mathbb{Z}_2$ ؟ هل  $K$  امتداد بالجذور لـ  $\mathbb{Z}_2$ ؟
2. هل كل كثيرة حدود في  $F[x]$  على الصورة  $ax^8 + bx^6 + cx^4 + dx^2 + e$ ، حيث  $a \neq 0$ ، قابلة للحل باستخلاص الجذور على  $F$ ، إذا كان مميز  $F$  يساوي 0؟ لماذا نعم أو لا؟
3. ضع إشارة صح أو إشارة خطأ:
  - أ. \_\_\_\_\_ ليكن  $F$  حقلاً مميزه 0. كثيرة الحدود في  $F[x]$  قابلة للحل باستخلاص الجذور إذا وفقط إذا كان حقل انشطارها في  $\bar{F}$  محتوي في امتداد بالجذور لـ  $F$ .
  - ب. \_\_\_\_\_ ليكن  $F$  حقلاً مميزه 0. كثيرة الحدود في  $F[x]$  قابلة للحل باستخلاص الجذور إذا وفقط إذا كان حقل انشطارها في  $\bar{F}$  له زمرة جالوا قابلة للحل على  $F$ .
  - ج. \_\_\_\_\_ حقل انشطار  $5 - x^{17}$  على  $\mathbb{Q}$  له زمرة جالوا قابلة للحل.
  - د. \_\_\_\_\_ العدان  $\pi$  و  $\sqrt{\pi}$  متساميان مستقلان على  $\mathbb{Q}$ .
  - هـ. \_\_\_\_\_ زمرة جالوا لامتداد منته لحقل منته قابلة للحل.
  - و. \_\_\_\_\_ لا معادلة من الدرجة الخامسة قابلة للحل باستخلاص الجذور على أي حقل.
  - ز. \_\_\_\_\_ كل كثيرة حدود من الدرجة 4 على حقل مميزه 0، قابلة للحل باستخلاص الجذور.
  - ح. \_\_\_\_\_ أصفار كثيرة حدود تكعيبية على حقل  $F$  مميزه 0، يمكن دائماً الوصول إليها بسلسلة منتهية من عمليات الجمع، والطرح، والضرب، والقسمة، وأخذ الجذور التربيعية بدءاً من عناصر في  $F$ .
  - ط. \_\_\_\_\_ لا يمكن أبداً الوصول إلى أصفار كثيرة حدود تكعيبية على حقل  $F$  مميزه 0، بسلسلة منتهية من عمليات الجمع، والطرح، والضرب، والقسمة، وأخذ الجذور التربيعية بدءاً من عناصر في  $F$ .
  - ي. \_\_\_\_\_ أدت مبرهنة سلاسل الزمر تحت الناظرية دوراً مهماً في تطبيقات مبرهنة جالوا.

### براهين

4. ليكن  $F$  حقلاً، ولتكن  $f(x) = ax^2 + bx + c$  في  $F[x]$ ، حيث  $a \neq 0$ . أثبت أنه إذا كان مميز  $F$  لا يساوي 2، فإن حقل انشطار  $f(x)$  على  $F$  هو  $F(\sqrt{b^2 - 4ac})$ .  
[مساعدة: أكمل المربع، تماماً كما في عمل المدرسة العليا، لاستنتاج «القانون العام لحل المعادلة التربيعية»].
5. أثبت أنه إذا كان  $F$  حقلاً مميزه لا يساوي 2، و  $f(x) = ax^4 + bx^2 + c$ ، حيث  $a \neq 0$ ، فإن  $f(x)$  قابلة للحل باستخلاص الجذور على  $F$ .
6. أثبت أنه لزمره منتهية، كل تصفية لسلسلة تحت ناظرية مع خوارج إبدالية، لها كذلك خوارج إبدالية، وهكذا يكتمل إثبات التمهيدي 3.56. [مساعدة: استخدم المبرهنة 7.34].
7. أثبت أنه لزمره منتهية، يمكن تصفية سلسلة تحت ناظرية مع زمر خارجة قابلة للحل إلى سلسلة تركيب مع خوارج إبدالية، وهكذا يكتمل إثبات المبرهنة 4.56.  
[مساعدة: استخدم المبرهنة 7.34].

8. يقدم هذا التمرين كثيرة حدود من الدرجة 5 في  $\mathbb{Q}[x]$  غير قابلة للحلّ باستخلاص الجذور على  $\mathbb{Q}$ .
- أ. أثبت أنه إذا كانت  $H$  زمرة جزئية من  $S_5$ ، وتحتوي حلقة طولها 5 وحلقة طولها 2، فإن  $H = S_5$ . [مساعدة: أثبت أن  $H$  تحوي الحلقات الثنائية جميعها في  $S_5$ ، وطبق النتيجة 12.9. انظر التمرين 39، في الفصل 9].
- ب. أثبت أنه إذا كانت  $f(x)$  كثيرة حدود غير مختزلة في  $\mathbb{Q}[x]$  من الدرجة 5، ولها بالضبط صفران مركبان وثلاثة أصفار حقيقية في  $\mathbb{C}$ ، فإن زمرة  $f(x)$  على  $\mathbb{Q}$  تماثل  $S_5$ . [مساعدة: استخدم مبرهنة سيلو في إثبات أن الزمرة تحوي عنصرًا ترتبه 5. استخدم حقيقة أن  $f(x)$  له بالضبط صفران مركبان لإثبات أن الزمرة تحوي عنصرًا ترتبه 2، ثم طبق الفرع (أ)].
- ج. كثيرة الحدود  $f(x) = 2x^5 - 5x^4 + 5$  غير مختزلة في  $\mathbb{Q}[x]$  - بحسب معيار أيزنشتاين، حيث  $p = 5$ . استخدم تقنيات التفاضل والتكامل في إيجاد القيم العظمى والصغرى المحلية و"رسم دالة كثيرة الحدود  $f$ " : لمشاهدة أن  $f(x)$  يجب أن يكون لها بالضبط ثلاثة أصفار حقيقية في  $\mathbb{C}$ . استنتج من الفرع (ب) والمبرهنة 4.56، أن  $f(x)$  غير قابلة للحلّ باستخلاص الجذور على  $\mathbb{Q}$ .

## حلول التمارين ذات الأرقام الفردية

التي لا تسأل عن تعريفات أو براهين

### الفصل 0

$$1. \{-\sqrt{3}, \sqrt{3}\}$$

$$3. \{1, -1, 2, -2, 3, -3, 4, -4, 5, -5, 6, -6, 10, -10, 12, -12, 15, -15, 20, -20, 30, -30, 60, -60\}$$

5. ليست مجموعة (ليست حسنة التعريف). حالة يمكن عملها أيضاً للمجموعة الخالية  $\phi$

7. المجموعة  $\phi$

9. المجموعة  $\mathbb{Q}$

$$11. (a, 1), (a, 2), (a, c), (b, 1), (b, 2), (b, c), (c, 1), (c, 2), (c, c)$$

13. ارسم الخط المارّ خلال  $P$  و  $x$ ، ولتكن  $y$  هي نقطة تقاطعه مع القطعة المستقيمة  $CD$

17. مخمّنة:  $2^s = n(\mathcal{P}(A))$  (البراهين عادة تحذف من الحلول)

$$21. |\mathbb{R}| = 2^{\aleph_0} = 12^{\aleph_0} = 10^{\aleph_0}, 10^5, 10^2. [الأعداد  $x$  حيث  $0 \leq x \leq 1$  يمكن كتابتها للأساس 12 وللأساس 2 وأيضاً للأساس 10]$$

$$23. 1 \quad 25. 5 \quad 27. 52$$

29. ليست علاقة تكافؤ.

$$31. \bar{0} = \{0\}, \bar{a} = \{a, -a\} \text{ لأي عنصر غير صفري } a \in \mathbb{R}$$

33. علاقة تكافؤ:

$$\bar{1} = \{1, 2, \dots, 9\},$$

$$\bar{10} = \{10, 11, \dots, 99\},$$

$$\bar{100} = \{100, 101, \dots, 999\}, \text{ وبوجه عام}$$

$$\bar{10^n} = \{10^n, 10^n + 1, \dots, 10^{n+1} - 1\}$$

$$35. \text{ أ. } \{1, 3, 5, \dots\}, \{2, 4, 6, \dots\}$$

$$\text{ ب. } \{1, 4, 7, \dots\}, \{2, 5, 8, \dots\}, \{3, 6, 9, \dots\}$$

$$\text{ ج. } \{1, 6, 11, \dots\}, \{2, 7, 12, \dots\}, \{3, 8, 13, \dots\}, \{4, 9, 14, \dots\}, \{5, 10, 15, \dots\}$$

37. الاسم دالة اثنين إلى اثنين يقترح أن دالة  $f$  كهذه يجب أن تحمل كل زوج من النقاط المختلفة إلى نقطتين مختلفتين، دالة كهذه أحادية بالمعنى الاصطلاحي. (إذا كان في المجال عنصر واحد، فالدالة لا يمكن أن تفشل في أن تكون دالة اثنين إلى اثنين؛ لأن الطريقة الوحيدة التي يمكن أن تفشل فيها أن تكون دالة اثنين إلى اثنين هي أن تحمل نقطتين إلى نقطة واحدة، والمجموعة ليس فيها نقطتان)، في المقابل، كل دالة أحادية بالمعنى الاصطلاحي تحمل أي زوج من النقاط إلى نقطتين مختلفتين. وعليه، فمن الناحية الاصطلاحية، فإن الدوال التي تسمى أحادية هي بالضبط تلك التي تحمل أي نقطتين إلى نقطتين، وذلك باعتبار أن هذه الدوال وبصورة بديهية هي ذات طريق أحادي الاتجاه. أيضاً، الطريقة القياسية لإثبات أن الدالة أحادية، هي بالتحديد إثبات أنها لا تحمل نقطتين إلى نقطة واحدة فقط. وعليه، إثبات أن الدالة أحادية صار طبيعياً من خلال اصطلاح اثنين إلى اثنين.

### الفصل 1

$$-i.1 \quad -i.3 \quad 23 + 7i.5$$

$$17 - 15i.7 \quad -4 + 4i.9$$

$$2\sqrt{13}.11 \quad \sqrt{2}\left(-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i\right).13$$

$$\sqrt{34}\left(\frac{-3}{\sqrt{34}} + \frac{5}{\sqrt{34}}i\right).15$$

$$-\frac{1}{\sqrt{2}} \pm \frac{1}{\sqrt{2}}i, \frac{1}{\sqrt{2}} \pm \frac{1}{\sqrt{2}}i.17 \quad \pm \frac{3\sqrt{3}}{2} - \frac{3}{2}i, 3i.19$$

$$\sqrt{2}.27 \quad \frac{3}{8}.25 \quad 4.23 \quad -\sqrt{3} \pm i, \pm 2i, \sqrt{3} \pm i.21$$

$$7, 1.33 \quad 5.31 \quad 11.29$$

$$\zeta^0 \leftrightarrow 0, \zeta^3 \leftrightarrow 7, \zeta^4 \leftrightarrow 4, \zeta^5 \leftrightarrow 1, \zeta^6 \leftrightarrow 6, \zeta^7 \leftrightarrow 3.35$$

37. مع  $4 \leftrightarrow \zeta$  يجب أن يكون لدينا  $1 \leftrightarrow \zeta^2$ ،  $0 \leftrightarrow \zeta^3$ ، وأيضاً  $4 \leftrightarrow \zeta^4$ ، التي هي مستحيلة في التقابل الأحادي.

39. بالضرب، نحصل على:

$$z_1 z_2 = |z_1| |z_2| [(\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2) + (\cos\theta_1 \sin\theta_2 + \sin\theta_1 \cos\theta_2)i]$$

والنتيجة المطلوبة تنتج مباشرة من التمرين 38 ومن المعادلة  $|z_1 z_2| = |z_1| |z_2|$ .

## الفصل 2

1.  $a, b, e$  3.  $a, c$  ليست تجميعية

5. الصف الأول:  $d$  الصف الثاني:  $a$  الصف الرابع:  $b, c$

7. ليست تبديلية، ليست تجميعية.

9. تبديلية، تجميعية.

11. ليست تبديلية، ليست تجميعية.

13. 8, 729,  $n^{[n(n+1)/2]}$

17. لا، الشرط 2 يفشل 19. نعم

21. لا، الشرط 1 يفشل

23. أ. نعم ب. نعم

25. لتكن  $S = \{?, \Delta\}$ . عرّف  $*$  و  $'$  على  $S$  بـ  $a * b = ?$  و  $a * b = \Delta$  لكل  $a, b \in S$  (هناك حلول أخرى ممكنة).

27. صح. 29. صح

31. خطأ، افترض أن  $f(x) = x^2$ ،  $g(x) = x$ ، و  $h(x) = 2x + 1$ . عندئذ:

$$(f(x) - g(x)) - h(x) = x^2 - 3x - 1 \text{ لكن}$$

$$f(x) - (g(x) - h(x)) = x^2 - (-x - 1) = x^2 + x + 1$$

33. صح 35. خطأ، افترض أن  $*$  هي  $+$ ، وافترض أن  $'$  على  $\mathbb{Z}$

## الفصل 3

1. أ.  $\phi$  يجب أن يكون أحاديًا ب.  $\phi[S]$  يجب أن تكون جميع  $S'$

$$\text{ج. } \phi(a * b) = \phi(a) *' \phi(b) \text{ لكل } a, b \in S$$

3. لا؛ لأن  $\phi$  لا ترسل  $\mathbb{Z}$  بصورة غامرة إلى  $\mathbb{Z}'$ .  $\phi(n) \neq 1$  لكل  $n \in \mathbb{Z}$

5. نعم 7. نعم 9. نعم

11. لا؛ لأن  $\phi(x^2) = \phi(x^2 + 1)$

13. لا؛ لأن  $\phi(f) = x + 1$  ليس لها حل  $f \in F$

15. لا: لأن  $\phi(f) = 1$  ليس لها حل  $f \in F$

17. أ.  $m * n = mn - m - n + 2$ : العنصر المحايد 2

ب.  $m * n = mn + m + n$ : العنصر المحايد 0

19. أ.  $a * b = \frac{1}{3}(ab + a + b - 2)$ : العنصر المحايد 2

ب.  $a * b = 3ab - a - b + \frac{2}{3}$ : العنصر المحايد  $\frac{2}{3}$

25. لا، إذا كانت  $\langle S, * \rangle$  لها عنصر محايد أيسر  $e_L$  وعنصر محايد أيمن  $e_R$ ، فإن  $e_L = e_R$ . (من عادتنا حذف البراهين من الحلول).

#### الفصل 4

1. لا.  $\mathcal{G}_3$  تفشل 3. لا.  $\mathcal{G}_1$  تفشل 5. لا.  $\mathcal{G}_1$  تفشل

7. الزمرة  $\langle U_{1000}, \cdot \rangle$  لحلول المعادلة  $z^{1000} = 1$  في  $\mathbb{C}$  بالنسبة إلى الضرب فيها 1000 عنصر.

9. المعادلة على الصورة:  $x * x * x * x = e$  لها أربعة حلول في  $\langle U, \cdot \rangle$ ، حل واحد في  $\langle \mathbb{R}, + \rangle$ ، وحلان في  $\langle \mathbb{R}^*, \cdot \rangle$

11. نعم 13. نعم

15. لا. المصفوفة التي جميع مدخلاتها 0 هي مثلثية علوية، لكن ليس لها معكوس.

17. نعم

19. (البرهان محذوف) ج.  $-\frac{1}{3}$

21. 2، 3. (تصبح الإجابة صعبة في حالة أربعة عناصر، حيث إن الجواب ليس 4).

25. أ. خطأ ج. صح هـ. خطأ ز. صح ط. خطأ

#### الفصل 5

1. نعم 3. نعم 5. نعم 7.  $\mathbb{Q}^+$  و  $\{\pi^2 \mid n \in \mathbb{Z}\}$  9. نعم

11. لا، ليست مغلقة بالنسبة إلى الضرب.

13. نعم

15. أ. نعم ب. لا، إنها ليست حتى مجموعة جزئية من  $\tilde{F}$

17. أ. لا، ليست مغلقة بالنسبة إلى الجمع ب. نعم

19. أ. نعم ب. لا، الدالة الثابتة الصفريّة ليست في  $\tilde{F}$

21. أ.  $-50, -25, 0, 25, 50$  ب.  $\frac{1}{4}, \frac{1}{2}, 1, 2, 4$  ج.  $1, \pi, \pi^2, 1/\pi, 1/\pi^2$

23. جميع المصفوفات  $n \in \mathbb{Z} \downarrow \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$

25. المصفوفات جميعها على الصورة:  $n \in \mathbb{Z} \downarrow \begin{bmatrix} 0 & -2^{2n+1} \\ -2^{2n+1} & 0 \end{bmatrix}$  أو  $\begin{bmatrix} 4^n & 0 \\ 0 & 4^n \end{bmatrix}$

3.35

2.33

4.31

3.29

4.27

ط. صح

ز. خطأ

هـ. خطأ

ج. صح

أ. صح

## الفصل 6

60.7

8.5

$q = -7, r = 6$  3.

$q = 4, r = 6$  1.

4.19

6.17

2.15

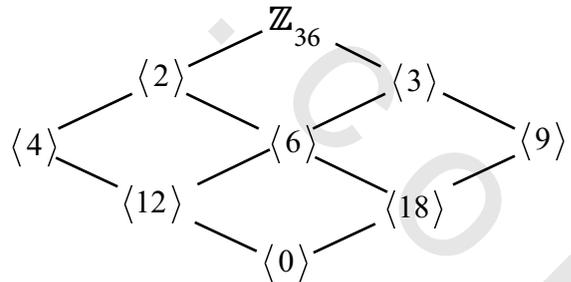
2.13

16.11

4.9

19. زمرة دورية لا نهائية

23.



17. 1. 29

12. 6. 4. 3. 2. 1. 27

6. 3. 2. 1. 25

$\mathbb{Z}_8$  37

33. زمرة كلاين الرباعية  $\mathbb{Z}_2$  35

39.  $\frac{1}{2}(1-i\sqrt{3})$  و  $\frac{1}{2}(1+i\sqrt{3})$

$$.41 \frac{1}{2}(-\sqrt{3}-i), \frac{1}{2}(-\sqrt{3}+i), \frac{1}{2}(\sqrt{3}-i), \frac{1}{2}(\sqrt{3}+i)$$

$$.51 (p-1)(q-1)$$

## الفصل 7

3. 0, 2, 4, 6, 8, 10, 12, 14, 16

1.1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

5. ..., -24, -18, -12, -6, 0, 6, 12, 18, 24, ...

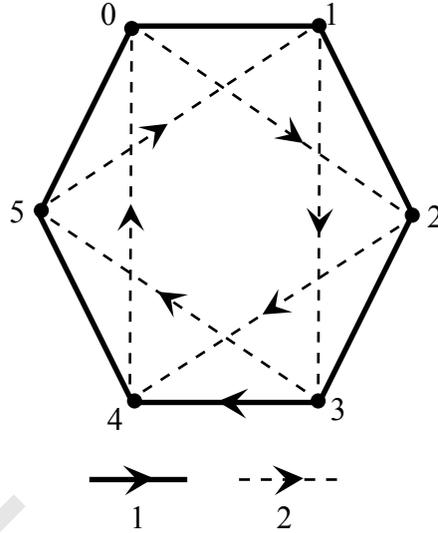
7. أ.  $a^3b$  ب.  $a^2$  ج.  $a^2$

9.

|     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|
|     | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
| $a$ | $a$ | $e$ | $c$ | $b$ | $f$ | $d$ |
| $b$ | $b$ | $d$ | $e$ | $f$ | $a$ | $c$ |
| $c$ | $e$ | $f$ | $a$ | $d$ | $e$ | $b$ |
| $d$ | $d$ | $b$ | $f$ | $e$ | $c$ | $a$ |
| $f$ | $f$ | $c$ | $d$ | $a$ | $b$ | $e$ |

11. اختر زوجًا من الحواف الموجّهة المولّدة، أطلق عليهما الاسمين  $arc1$  و  $arc2$ ، ابدأ من أيّ رأس لرسم موجه، وانظر فيما إذا كانت المتتالية  $arc1$  و  $arc2$  و  $arc1$  تؤدي إلى الرأس نفسه. (هذه تقابل السؤال فيما إذا كان المولدان المقابلان للزمرتين تبديليين). الزمرة تبديلية إذا وفقط إذا كانت هاتان المتسلسلتان تؤديان إلى الرأس نفسه لأيّ زوج من الحواف الموجّهة المولّدة.

13. إنها ليست واضحة؛ لأن رسم موجه لزمرة دورية يمكن أن يشكل باستخدام مجموعة مولدة من عنصرين أو أكثر، ليس أيّ منهما يولد الزمرة.



17. أ. البدء من أي رأس  $a$ ، أي مسار خلال البيان ينتهي عند الرأس  $a$  نفسه، يمثل ضرباً لمولدات أو لمعكوساتها، التي تساوي المحايد، وعليه، تعطي علاقة.

ب.  $a^4 = e, b^2 = e, (ab)^2 = e$

الفصل 8

3.  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}$

1.  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$

5.  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$

9.

2.7

13.  $\{1, 5\}$

11.  $\{1, 2, 3, 4, 5, 6\}$

15.  $\epsilon, \rho, \rho^2, \rho^3, \phi, \rho\phi, \rho^2\phi, \rho^3\phi$  حيث  $\phi$  هنا هي  $\mu_1$  خاصتنا. هذه تعطي عناصرنا على

الترتيب:  $\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \delta_1, \mu_2, \delta_2$

24.17

19. بالرجوع إلى الجدول 12.8، نجد أن:  $\langle \rho_0 \rangle = \{\rho_0\}$ ،  $\langle \rho_1 \rangle = \langle \rho_3 \rangle = \{\rho_0, \rho_1, \rho_2, \rho_3\}$

هي جميع الزمر الجزئية الدورية. الزمرة الجزئية التي تحوي واحدة من التباديل  $\delta_1, \mu_2, \mu_1$ ، أو  $\delta_2$  اللواتي "تعيد المربع" وتحوي أيضًا  $\rho_1$  أو  $\rho_3$  سوف تصف أوضاع المربع جميعها، وهكذا يجب أن تكون الزمرة  $D_4$  جميعها. بفحص الصف في الجدول المقابل لـ  $\mu_1$ ، نرى أن العناصر الأخرى الوحيدة التي يمكن أن تكون في زمرة جزئية فعلية مع  $\mu_1$  هي  $\rho_0, \rho_2, \mu_2$ . نفحص أن  $\{\rho_0, \rho_2, \mu_1, \mu_2\}$  مغلقة بالنسبة إلى الضرب، وفيما إذا كانت زمرة جزئية. بفحص الصف في الجدول المقابل لـ  $\mu_2$  يعطي الزمرة الجزئية نفسها، وبفحص الصفين في الجدول والمقابلين لـ  $\delta_1$  و  $\delta_2$  يعطي - باستخدام التفسير نفسه - الزمرة الجزئية  $\{\rho_0, \rho_2, \delta_1, \delta_2\}$  كاحتمال الوحيد المتبقي.

21. أ. هذه هي "مصفوفات التباديل البسيطة" التي تنتج عن تبديل صفوف مصفوفة الوحدة. عند ضرب مصفوفة أخرى  $A$  من اليسار بواحدة من هذه المصفوفات  $P$ ، فإن صفوف المصفوفة  $A$  تتبدل بالطريقة نفسها التي تبدلت فيها صفوف مصفوفة الوحدة من الدرجة  $3 \times 3$  لتنتج  $P$ ؛ ولأن احتمالات التباديل أ.د. 6 جميعها للمصفوف الثلاثة مُثلت، نرى أنها تؤثر كتأثير عناصر  $S_3$  في تبديل المدخلات 1, 2, 3 لمتجه العمود المعطى. وعليه، فإنها تشكل زمرة، وذلك؛ لأن  $S_3$  زمرة.

ب. زمرة التناظر  $S_3$  على ثلاثة أحرف.

25.  $D_4$

23.  $\mathbb{Z}_2$

$$27. \text{ لـ } \mathbb{Z}_4, \lambda_0 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}, \lambda_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}, \lambda_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}, \lambda_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix}$$

الجدول للتمثيل المنتظم الأيسر هو نفسه الجدول لـ  $\mathbb{Z}_4$  مع تبديل  $n$  بـ  $\lambda_n$ . لـ  $S_3$ .

$$\rho_1 = \begin{pmatrix} r_0 & r_1 & r_2 & m_1 & m_2 & m_3 \\ r_1 & r_2 & r_0 & m_2 & m_3 & m_1 \end{pmatrix}, \rho_0 = \begin{pmatrix} r_0 & r_1 & r_2 & m_1 & m_2 & m_3 \\ r_0 & r_1 & r_2 & m_1 & m_2 & m_3 \end{pmatrix}$$

التبديل  $\rho_\sigma$  يتكوّن من عناصر  $S_3$  بالترتيب الذي تظهر فيه من الأعلى إلى الأسفل في العمود تحت تأثير  $\sigma$  في الجدول

8.8. الجدول للتمثيل المنتظم الأيمن هو نفسه الجدول لـ  $S_3$  باستبدال  $\sigma$  بـ  $\rho_\sigma$ .

33. ليس تبديلاً

31. ليس تبديلاً

35. أ. صح ب. صح ج. خطأ د. خطأ

43. نعم

41. لا

37. مونويد



23. أ. خطأ ج. خطأ هـ. خطأ ز. صح ط. صح

### الفصل 10

$$1. \quad 4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

$$1 + 4\mathbb{Z} = \{\dots, -7, -3, 1, 5, 9, \dots\}$$

$$2 + 4\mathbb{Z} = \{\dots, -6, -2, 2, 6, 10, \dots\}$$

$$3 + 4\mathbb{Z} = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

$$3. \quad \langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}, \quad 1 + \langle 2 \rangle = \{1, 3, 5, 7, 9, 11\}$$

$$5. \quad \langle 18 \rangle = \{0, 18\}, \quad 1 + \langle 18 \rangle = \{1, 19\}, \quad 2 + \langle 18 \rangle = \{2, 20\}, \dots, \quad 17 + \langle 18 \rangle = \{17, 35\}$$

$$7. \quad \{\rho_0, \mu_2\}, \{\rho_1, \delta_1\}, \{\rho_2, \mu_1\}, \{\rho_3, m_2\} \text{ . ليست نفسها}$$

$$9. \quad \{\rho_0, \rho_2\}, \{\rho_1, \rho_3\}, \{\mu_1, \mu_2\}, \{\delta_1, \delta_2\}$$

11. نعم، نحصل على زمرة مجموعات مشاركة تماثل زمرة كلاين الرباعية  $V$

|            |            |            |            |            |            |            |            |            |
|------------|------------|------------|------------|------------|------------|------------|------------|------------|
|            | $\rho_0$   | $\rho_2$   | $\rho_1$   | $\rho_3$   | $\mu_1$    | $\mu_2$    | $\delta_1$ | $\delta_2$ |
| $\rho_0$   | $\rho_0$   | $\rho_2$   | $\rho_1$   | $\rho_3$   | $\mu_1$    | $\mu_2$    | $\delta_1$ | $\delta_2$ |
| $\rho_2$   | $\rho_2$   | $\rho_0$   | $\rho_3$   | $\rho_1$   | $\mu_2$    | $\mu_1$    | $\delta_2$ | $\delta_1$ |
| $\rho_1$   | $\rho_1$   | $\rho_3$   | $\rho_2$   | $\rho_0$   | $\delta_1$ | $\delta_2$ | $\mu_2$    | $\mu_1$    |
| $\rho_3$   | $\rho_3$   | $\rho_1$   | $\rho_0$   | $\rho_2$   | $\delta_2$ | $\delta_1$ | $\mu_1$    | $\mu_2$    |
| $\mu_1$    | $\mu_1$    | $\mu_2$    | $\delta_2$ | $\delta_1$ | $\rho_0$   | $\rho_2$   | $\rho_3$   | $\rho_1$   |
| $\mu_2$    | $\mu_2$    | $\mu_1$    | $\delta_1$ | $\delta_2$ | $\rho_2$   | $\rho_0$   | $\rho_1$   | $\rho_3$   |
| $\delta_1$ | $\delta_1$ | $\delta_2$ | $\mu_1$    | $\mu_2$    | $\rho_1$   | $\rho_3$   | $\rho_0$   | $\rho_2$   |
| $\delta_2$ | $\delta_2$ | $\delta_1$ | $\mu_2$    | $\mu_1$    | $\rho_3$   | $\rho_1$   | $\rho_2$   | $\rho_0$   |

24.15

3.13

ط. خطأ

ز. صح

هـ. صح

ج. صح

19. أ. صح

21.  $G = \mathbb{Z}_2$ ، الزمرة الجزئية  $H = \mathbb{Z}_2$

23. مستحيل، عدد الخلايا يجب أن يقسم رتبة الزمرة و12 لا يقسم 6

## الفصل 11

1.

| الرتبة | العنصر | الرتبة | العنصر |
|--------|--------|--------|--------|
| 2      | (0, 2) | 1      | (0, 0) |
| 2      | (1, 2) | 2      | (1, 0) |
| 4      | (0, 3) | 4      | (0, 1) |
| 4      | (1, 3) | 4      | (1, 1) |

الزمرة ليست دورية

60.7

9.5

2.3

9.  $\{(0,0), (0,1)\}, \{(0,0), (1,0)\}, \{(0,0), (1,1)\}$

$$\{(0,0), (0,1), (0,2), (0,3)\} \quad .11$$

$$\{(0,0), (0,2), (1,0), (1,2)\}$$

$$\{(0,0), (1,1), (0,2), (1,3)\}$$

$$\mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_4, \mathbb{Z}_{12} \times \mathbb{Z}_5, \mathbb{Z}_{15} \times \mathbb{Z}_4, \mathbb{Z}_{20} \times \mathbb{Z}_3 \quad .13$$

$$12.15$$

$$120.17$$

$$180.19$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_8 \quad .21$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_{16}, \mathbb{Z}_{32} \quad .23$$

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}, \mathbb{Z}_9 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}, \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{121}, \mathbb{Z}_9 \times \mathbb{Z}_{121} \quad .25$$

$$.1.29$$

|    |    |    |   |   |   |   |           |
|----|----|----|---|---|---|---|-----------|
| 8  | 7  | 6  | 5 | 4 | 3 | 2 | $n$       |
| 22 | 15 | 11 | 7 | 5 | 3 | 2 | عدد الزمر |

$$110 \text{ (iii)}$$

$$225 \text{ (ii)}$$

$$225 \text{ (i) ب.}$$

31. أ. إنها إبدالية، عندما تكون الأسهم على كلا المضلعين ذوي أُل  $n$  ضلعاً لها الاتجاه نفسه (مع عقارب الساعة أو عكس عقارب الساعة).

$$\mathbb{Z}_2 \times \mathbb{Z}_n \text{ ب.}$$

ج. عندما يكون  $n$  فردياً

د. الزمرة الزوجية  $D_n$

$$\mathbb{Z}_2 \text{ مثال على ذلك. } .33$$

$$S_3 \text{ مثال على ذلك. } .35$$

$$\{-1, 1\} \quad .41 \quad .37 \text{ الأعداد هي نفسها}$$

الفصل 12

1. أ. التقايسات الوحيدة من  $\mathbb{R}$  التي تترك العدد  $c$  مثبتاً، هي الانعكاس خلال  $c$ ، الذي يحمل  $x$  إلى  $c - x$  لكل  $x \in \mathbb{R}$ ، إضافة إلى الدالة المحايدة.

ب. التقايسات من  $\mathbb{R}^2$  التي تترك نقطة  $P$  مثبتة، هي الدورانات حول  $P$  خلال أيّ زاوية  $\theta$ ، حيث  $0 \leq \theta < 360^\circ$  بالإضافة إلى الانعكاسات عبر أيّ محور يمر خلال  $P$ .

ج. التقايسات الوحيدة من  $\mathbb{R}$  التي تحمل القطعة المستقيمة إلى نفسها هي الانعكاس خلال نقطة المنتصف للقطعة المستقيمة (انظر إجابة الفرع (أ)) إضافة إلى الدالة المحايدة.

د. التقايسات لـ  $\mathbb{R}^2$  التي تحمل القطعة المستقيمة إلى نفسها، هي تدوير بـ  $180^\circ$  حول نقطة المنتصف للقطعة المستقيمة، وانعكاس في المحور الذي يحوي القطعة المستقيمة، وانعكاس في المحور الذي يعامد القطعة المستقيمة في نقطة منتصفها، إضافة إلى الدالة المحايدة.

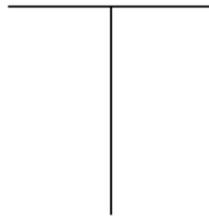
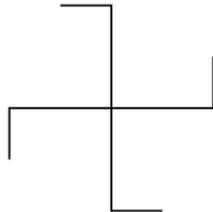
هـ. التقايسات لـ  $\mathbb{R}^3$  التي تحمل القطعة المستقيمة إلى نفسها تتضمن التدويرات خلال أيّ زاوية حول محور يحوي القطعة المستقيمة، والانعكاسات عبر أيّ مستوى يحوي القطعة المستقيمة، والانعكاس عبر المستوى العمودي على القطعة المستقيمة في نقطة منتصفها.

3.

|          | $\tau$      | $\rho$      | $\mu$       | $\gamma$    |
|----------|-------------|-------------|-------------|-------------|
| $\tau$   | $\tau$      | $\rho$      | $\mu\gamma$ | $\mu\gamma$ |
| $\rho$   | $\rho$      | $\rho\tau$  | $\mu\gamma$ | $\mu\gamma$ |
| $\mu$    | $\mu\gamma$ | $\mu\gamma$ | $\tau\rho$  | $\tau\rho$  |
| $\gamma$ | $\mu\gamma$ | $\mu\gamma$ | $\tau\rho$  | $\tau\rho$  |

7.

5.



9. انسحاب: الرتبة  $\infty$ دوران: الرتبة أي  $n \leq 2$  أو  $\infty$ 

انعكاس: الرتبة 2

انعكاس انحداري: الرتبة  $\infty$ 

11. دورانات 13. فقط المحايد والانعكاسات

17. نعم، الضرب لانسحابين هو انسحاب، ومعكوس الانسحاب هو انسحاب.

19. نعم، يوجد انعكاس واحد فقط  $\mu$  عبر خط معين  $L$ ، و  $\mu^2$  هو المحايد، وهكذا لدينا زمرة تماثل  $\mathbb{Z}_2$ 

21. فقط الانعكاسات والدورانات (والمحايد)؛ لأن الانسحابات والانعكاسات الانحدارية رتبها ليست منتهية في زمرة تقايسات المستوى جميعها.

25. أ. لا ب. لا ج. نعم د. لا هـ.  $D_\infty$
27. أ. نعم ب. لا ج. لا د. لا هـ.  $D_\infty$
29. أ. لا ب. لا ج. لا د. نعم هـ.  $\mathbb{Z}$
31. أ. نعم.  $90^\circ, 180^\circ$  ب. نعم ج. لا
33. أ. لا ب. لا ج. لا
35. أ. نعم.  $180^\circ$  ب. نعم ج. لا
37. أ. نعم.  $120^\circ$  ب. نعم ج. لا
39. أ. نعم.  $90^\circ, 180^\circ$  ب. نعم ج. لا د.  $(-1, 1)$  و  $(1, 1)$
41. أ. نعم.  $120^\circ$  ب. نعم ج. لا د.  $(0, 1)$  و  $(1, \sqrt{3})$

## الفصل 13

1. نعم 3. نعم 5. لا
7. نعم 9. نعم
11. نعم 13. نعم 15. لا

17.  $\phi(25) = 2 : \text{Ker}(\phi) = 7\mathbb{Z}$ 19.  $\phi(20) = (1, 2, 7)(4, 5, 6) : \text{Ker}(\phi) = 6\mathbb{Z}$

$$21. \phi(14) = (1, 6)(4, 7) : \text{Ker}(\phi) = \{0, 4, 8, 12, 16, 20\}$$

$$23. \phi(4, 6) = (2, 18) : \text{Ker}(\phi) = \{(0, 0)\}$$

$$29. \text{ لكل } g \in G \quad 2.27 \quad 2.25$$

33. لا يوجد تشاكل غير تافه. المبرهنة 12.13 تبين أن الصورة لـ  $\phi$  يجب أن تكون زمرة جزئية من  $\mathbb{Z}_5$ ، وعليه، لتشاكل غير تافه  $\phi$ ، ستكون الصورة لـ  $\phi$  هي  $\mathbb{Z}_5$  جميعها. لكن عدد مجموعات المشاركة لزمرة جزئية من زمرة منتهية هو قاسم لرتبة الزمرة، و 5 لا تقسم 12.

$$35. \text{ ليكن } (m, n) \in \mathbb{Z}_2 \times \mathbb{Z}_4 \quad \phi(m, n) = (m, 0)$$

$$37. \text{ ليكن } \phi(n) = \rho_n \quad n \in \mathbb{Z}_3 \quad \text{مستخدمًا رموزنا في الكتاب لعناصر } S_3$$

$$39. \text{ ليكن } \phi(m, n) = 2m$$

41. بالنظر إلى  $D_4$  بوصفها زمرة تباديل، ليكن  $\phi(\sigma) = (1, 2)$  لكل  $\sigma \in D_4$  فردية و  $\phi(\sigma)$  هو المحايد لكل  $\sigma \in D_4$  زوجية.

43. ليكن  $\phi(\sigma) = (1, 2)$  لكل  $\sigma \in S_4$  فردية و  $\phi(\sigma)$  هو المحايد لكل  $\sigma \in S_4$  زوجية.

51. الصورة لـ  $\phi$  هي  $\langle a \rangle$  و  $\text{Ker}(\phi)$  يجب أن تكون زمرة جزئية ما  $n\mathbb{Z}$  من  $\mathbb{Z}$ .

$$53. \quad hk = kh \quad 55. \text{ يجب أن يكون المحايد } e \text{ في } G.$$

## الفصل 14

$$1. \quad 3 \quad 3 \quad 4 \quad 5 \quad 2$$

$$9. \quad 4 \quad 11 \quad 3 \quad 13 \quad 4 \quad 15 \quad 1$$

21. أ. عند العمل مع زمرة العامل  $G/H$ ، يمكنك جعل  $a$  و  $b$  عنصرين في  $G$ ، ليسا في  $G/H$ . من المحتمل أن الطالب لا يدرك صورة العناصر في  $G/H$ ، ولا يستطيع كتابة شيء منطقي متعلق بهم.

ب. يجب أن نثبت أن  $G/H$  إبدالية. ليكن  $aH$  و  $bH$  عنصرين في  $G/H$

$$23. \quad \text{أ. صح} \quad \text{ب. صح} \quad \text{ج. صح} \quad \text{د. صح} \quad \text{هـ. صح} \quad \text{ز. صح} \quad \text{ط. صح}$$

$$29. \quad \{\rho_0, \mu_1\}, \{\rho_0, \mu_2\}, \text{ و } \{\rho_0, \mu_3\}$$

35. مثال: لتكن  $G = N = S_3$ ، ولتكن  $H = \{\rho_0, \mu_1\}$ . عندئذٍ  $N$  ناظرية في  $G$ ، لكن  $H \cap N = H$  ليست ناظرية في  $G$ .

## الفصل 15

$$\mathbb{Z}_3 \times \mathbb{Z} \times \mathbb{Z}_4 \quad .9 \quad \mathbb{Z} \quad .7 \quad \mathbb{Z}_4 \times \mathbb{Z}_8 \quad .5 \quad \mathbb{Z}_4 \quad .3 \quad \mathbb{Z}_2 \quad .1$$

$$\mathbb{Z}(D_4) = C = \{\rho_0, \rho_2\} \quad .13 \quad \mathbb{Z}_2 \times \mathbb{Z} \quad .11$$

$$Z(S_3 \times D_4) = \{(\rho_0, \rho_0), (\rho_0, \rho_2)\} \quad .15 \quad \text{مستخدمًا الرموز الواردة في الفصل 8 لهذه الزمر-}$$

$$C = A_3 \times \{\rho_0, \rho_2\}$$

$$.19 \quad \text{أ. صح} \quad \text{ب. خطأ} \quad \text{ج. خطأ} \quad \text{د. خطأ} \quad \text{هـ. خطأ} \quad \text{ط. صح}$$

$$.21 \quad \{f \in F^* \mid f(0) = 1\}$$

.23 نعم. ليكن  $f(x) = 1$  لـ  $0 \leq x$  و  $f(x) = -1$  لـ  $x > 0$ . عندئذٍ،  $f(x)f(x) = 1$  لكل  $x$ ، وهكذا  $f^2 \in K^*$  لكن  $f$  ليس في  $K^*$ ، وعليه،  $fK^*$  رتبته 2 في  $F^*/K^*$

$$.25 \quad U$$

.27 زمرة الضرب  $U$  للأعداد المركبة ذات القيمة المطلقة 1

.29 لتكن  $G = \mathbb{Z}_2 \times \mathbb{Z}_4$ . عندئذٍ  $H = \langle (1, 0) \rangle$  تماثل  $K = \langle (0, 2) \rangle$ ، لكن  $G/H$  تماثل  $\mathbb{Z}_4$ ، بينما  $G/K$  تماثل  $\mathbb{Z}_2 \times \mathbb{Z}_2$

$$.31 \quad \text{أ. } \{e\} \quad \text{ب. الزمرة جميعها}$$

## الفصل 16

$$.1 \quad X_{\rho_0} = X, \quad X_{\rho_1} = \{C\}, \quad X_{\rho_2} = \{m_1, m_2, d_1, d_2, C\}, \quad X_{\rho_3} = \{C\}$$

$$, \quad X_{\mu_1} = \{s_1, s_3, m_1, m_2, C, P_1, P_3\}, \quad X_{\mu_2} = \{s_2, s_4, m_1, m_2, C, P_2, P_4\}$$

$$, \quad X_{\delta_1} = \{2, 4, d_1, d_2, C\}, \quad X_{\delta_2} = \{1, 3, d_1, d_2, C\}$$

$$.3 \quad \{1, 2, 3, 4\}, \quad \{s_1, s_2, s_3, s_4\}, \quad \{m_1, m_2\}, \quad \{d_1, d_2\}, \quad \{C\}, \quad \{P_1, P_2, P_3, P_4\}$$

.7 مجموعة  $G$ -المتعدية لها مدار واحد فقط.

$$.9 \quad \text{أ. } \{s_1, s_2, s_3, s_4\} \quad \text{و} \quad \{P_1, P_2, P_3, P_4\}$$

.13 ب. مجموعة النقاط على الدائرة التي مركزها نقطة الأصل، وتمر في النقطة  $P$

$$\text{ج. الزمرة الجزئية الدورية } \langle 2\pi \rangle \text{ من } G = \mathbb{R}$$

$$.17 \quad \text{أ. } K = g_0 H g_0^{-1}$$

ب. مخمّنة:  $H$  و  $K$  يجب أن تكونا زمرتين جزئيتين مترافقتين من  $G$

19. يوجد أربعة منها:  $Z, Y, X$  و  $\mathbb{Z}_6$

|   | $X$ | $Y$ | $Z$ |
|---|-----|-----|-----|
|   | $a$ | $a$ | $b$ |
|   | $a$ | $b$ | $c$ |
| 0 | $a$ | $a$ | $b$ |
| 1 | $a$ | $b$ | $a$ |
| 2 | $a$ | $a$ | $b$ |
| 3 | $a$ | $b$ | $a$ |
| 4 | $a$ | $a$ | $b$ |
| 5 | $a$ | $b$ | $a$ |

### الفصل 17

1. 5  
2. 3  
3. 45 أ.  
4. 90 أ.  
5. 11, 712  
6. 231 ب.  
7. 6, 246 ب.

### الفصل 18

1. 0  
2. 1  
3. 3  
4. 5  
5. (1, 6)  
6. لا.  
7. حلقة إبدالية، لا يوجد محايد، ليست حقلاً.  
8. حلقة إبدالية مع عنصر محايد، ليست حقلاً.  
9. حلقة إبدالية مع عنصر محايد، ليست حقلاً.  
10. لا.  $\{ri \mid r \in \mathbb{R}\}$  ليست مغلقة بالنسبة إلى الضرب.

11. 15. (1, 1), (1, -1), (-1, 1), (-1, -1)

19. 1, 3

17. جميع الأعداد غير الصفرية  $q \in \mathbb{Q}$

21. لتكن  $\mathbb{R} = \mathbb{Z}$  مع عنصر محايد 1 و  $R' = \mathbb{Z} \times \mathbb{Z}$  مع العنصر المحايد  $1' = (1,1)$ . ليكن  $\phi: R \rightarrow R'$  معرف بـ  $\phi(n) = (n, 0)$ . عندئذٍ:  $\phi(1) = (1,0) \neq 1'$

23.  $\phi_1: \mathbb{Z} \rightarrow \mathbb{Z}$  حيث  $\phi_1(n) = 0$ ،  $\phi_2: \mathbb{Z} \rightarrow \mathbb{Z}$  حيث  $\phi_2(n) = n$

25.  $\phi_1: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  حيث  $\phi_1(n, m) = 0$ ،  $\phi_2: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  حيث  $\phi_2(n, m) = n$

$\phi_3: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  حيث  $\phi_3(n, m) = m$ .

27. التفسير غير صحيح؛ لأن الضرب  $(X - I_3)(X + I_3)$  لمصفوفتين يمكن أن يكون المصفوفة الصفرية 0 دون أن يكون أي من المصفوفتين مصفوفة صفرية. مثال مناقض:

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^2 = I_3$$

31.  $a = 2, b = 3$  في  $\mathbb{Z}_6$

33. أ. صح ج. خطأ هـ. صح ز. صح ط. صح

## الفصل 19

1. 0, 3, 5, 8, 9, 11, 3. لا توجد حلول 5. 0 7. 0 9. 12

$$a^4 + 2a^2b^2 + b^4 \quad 13. a^6 + 2a^3b^3 + b^6$$

17. أ. خطأ ج. خطأ هـ. صح ز. خطأ ط. خطأ

19. 1.  $\text{Det}(A) = 0$  2. متجهات الأعمدة لـ  $A$  غير مستقلة (تابعة).

3. متجهات الصفوف لـ  $A$  غير مستقلة (تابعة). 4. الصفر هو قيمة ذاتية لـ  $A$

5.  $A$  ليس لها معكوس.

## الفصل 20

1. 3 أو 5 3. أي من 3, 5, 6, 7, 10, 11, 12 أو 14 5. 2

$$\varphi(1) = 1 \quad \varphi(7) = 6 \quad \varphi(13) = 12 \quad \varphi(19) = 18 \quad \varphi(25) = 20$$

$$\varphi(2) = 1 \quad \varphi(8) = 4 \quad \varphi(14) = 6 \quad \varphi(20) = 8 \quad \varphi(26) = 12$$

$$\varphi(3) = 2 \quad \varphi(9) = 6 \quad \varphi(15) = 8 \quad \varphi(21) = 12 \quad \varphi(27) = 18$$

$$\varphi(28)=12 \quad \varphi(22)=10 \quad \varphi(16)=8 \quad \varphi(10)=4 \quad \varphi(4)=2$$

$$\varphi(29)=28 \quad \varphi(23)=22 \quad \varphi(17)=16 \quad \varphi(11)=10 \quad \varphi(5)=4$$

$$\varphi(30)=8 \quad \varphi(24)=8 \quad \varphi(18)=6 \quad \varphi(12)=4 \quad \varphi(6)=2$$

13. لا توجد حلول

$$3+4\mathbb{Z}, 1+4\mathbb{Z}.11$$

$$9. (p-1)(q-1)$$

15. لا توجد حلول.

$$3+65\mathbb{Z}, 16+65\mathbb{Z}, 29+65\mathbb{Z}, 42+65\mathbb{Z}, 55+65\mathbb{Z}.17$$

$$9. 21 \quad 1. 19$$

23. أ. خطأ ج. صح هـ. صح ز. خطأ ط. خطأ

## الفصل 21

$$1. \{q_1 + q_2 i \mid q_1, q_2 \in \mathbb{Q}\}$$

15. إنها تماثل حلقة جميع الأعداد النسبية  $D$ ، التي يمكن أن يعبر عنها بوصفها خارج قسمة أعداد صحيحة مقامها قوة  $2$ .

17. سنقع في مشكلة عند محاولتنا إثبات خاصية التعدي في التمهيدية 2.21؛ لأن الحذف في الضرب من الممكن ألا يتحقق. لـ  $R = \mathbb{Z}_6$  و  $T = \{1, 2, 4\}$  لدينا  $(1, 2) \sim (2, 4)$ ؛ لأن  $(1)(2) = 4 = (2)(2)$  و  $(1)(4) = (2)(1)$  و  $(2, 4) \sim (2, 1)$ ؛ لأن  $(2)(1) = (4)(2)$  و  $(2, 1) \sim (1, 2)$ ؛ لأن  $(2)(1) \neq (1)(1)$  في  $\mathbb{Z}_6$  وفي الأحوال كلها،  $(1, 2)$  لا تكافئ  $(2, 1)$ ؛ لأن  $(2)(1) \neq (1)(1)$  في  $\mathbb{Z}_6$ .

## الفصل 22

$$1. f(x)g(x) = 6x^2 + 4x + 6, f(x) + g(x) = 2x^2 + 5$$

$$3. f(x)g(x) = x^3 + 5x, f(x) + g(x) = 5x^2 + 5x + 1$$

$$4, 2, 0. 15 \quad 3, 2. 13 \quad 0. 11 \quad 2. 9 \quad 7. 7 \quad 16. 5$$

$$3, 2, 1, 0. 17$$

21.  $0, x - 5, 2x - 10, x^2 - 25, x^2 - 5x, x^4 - 5x^3$  (هناك حلول أخرى ممكنة).

23. أ. صح ج. صح هـ. خطأ ز. صح ط. صح

25. أ. إنها عناصر الوحدة في  $D$  ب. 1، -1 ج. 1، 2، 3، 4، 5، 6

27. ب.  $F$  ج.  $F[x]$  31. أ. 4، 27 ب.  $\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

### الفصل 23

1.  $q(x) = x^4 + x^3 + x^2 + x - 2, r(x) = 4x + 3$

3.  $q(x) = 6x^4 + 7x^3 + 2x^2 - x + 2, r(x) = 4$

5، 2، 3، 7، 10، 11، 14، 12، 6

9.  $(x-1)(x+1)(x-2)(x+2)$

11.  $(x-3)(x+3)(2x+3)$

13. نعم. إنها من الدرجة 3، وليس لها أصفار في  $\mathbb{Z}_5$

$2x^3 + x^2 + 2x + 2$

15. إجابة مختصرة:  $g(x)$  غير مختزلة على  $\mathbb{R}$ ، لكنها مختزلة على  $\mathbb{C}$

19. نعم.  $p = 3$  21. نعم.  $p = 5$

25. أ. صح ج. صح هـ. صح ز. صح ط. صح

27.  $x^2 + x + 1$

29.  $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2, 2x^2 + 2, 2x^2 + x + 1, 2x^2 + 2x + 1$

31.  $p(p-1)^2 / 2$

### الفصل 24

1.  $1e + 0a + 3b$  3.  $2e + 2a + 2b$  5.  $j$  7.  $(1/50)j - (3/50)k$

9.  $\mathbb{R}^*$ ، أي إن،  $\{a_1 + 0i + 0j + 0k \mid a_1 \in \mathbb{R}, a_1 \neq 0\}$

11. أ. خطأ ج. خطأ هـ. خطأ ز. صح ط. صح

ج. إذا كان  $|A| = 1$ ، فإن  $\text{End}(A) = \{0\}$  هـ.  $0 \in \text{End}(A)$  ليس في  $\text{Iso}(A)$

$$19. \text{ أ. } K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

ب. نرمز بالرمز  $B$  للمصفوفة ذات المعامل  $b$ ، ونرمز بالرمز  $C$  للمصفوفة ذات المعامل  $c$ ، ونرمز للمصفوفة الوحدة من الدرجة  $2 \times 2$  بالرمز  $I$ ، يجب علينا فحص أن:

$$B^2 = -I, C^2 = -I, K^2 = -I$$

$$CK = B, KB = C, CB = -K, KC = -B, BK = -C$$

ج. يجب علينا فحص أن  $\phi$  أحادي

### الفصل 25

$$1. \dots < x^n < \dots < x^3 < x^2 < x < a \text{ لأي } a \in R$$

$$3. \sqrt{2}m + n \text{ موجب إذا كان } m > 0 \text{ و } n < 0 \text{، أو إذا كان } m > 0 \text{ و } m^2 > 2n^2 \text{، أو إذا كان } n < 0 \text{ و } 2n^2 > m^2$$

$$5. \text{ i. أ ج ه د ب ii. ه ج ب أ د}$$

$$7. \text{ i. د أ ب ج ه ii. د ج ه أ ب}$$

$$9. \text{ i. ج أ ه د ب ii. ه ج ب أ د}$$

$$11. \text{ د ب أ ه ج 13. د ه ب أ ج}$$

$$15. \text{ أ. صح ج. خطأ ه. صح ز. صح ط. خطأ}$$

## الفصل 26

1. هناك تسعة احتمالات فقط:

$$\phi(0, 1) = (0, 1) \text{ أو } \phi(0, 1) = (0, 0) \text{ بينما } \phi(1, 0) = (1, 0)$$

$$\phi(0, 1) = (1, 0) \text{ أو } \phi(0, 1) = (0, 0) \text{ بينما } \phi(1, 0) = (0, 1)$$

$$\phi(0, 1) = (0, 0) \text{ بينما } \phi(1, 0) = (1, 1)$$

$$\phi(0, 1) = (1, 1) \text{ أو } \phi(0, 1) = (0, 0) \text{ أو } \phi(0, 1) = (1, 0) \text{ أو } \phi(0, 1) = (0, 1) \text{ بينما } \phi(1, 0) = (0, 0) \text{ و}$$

$$\langle 0 \rangle = \{0\}, \mathbb{Z}_{12} / \langle 0 \rangle \simeq \mathbb{Z}_{12} \quad \mathbf{3.}$$

$$\langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}, \mathbb{Z}_{12} / \langle 1 \rangle \simeq \{0\}$$

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}, \mathbb{Z}_{12} / \langle 2 \rangle \simeq \mathbb{Z}_2$$

$$\langle 3 \rangle = \{0, 3, 6, 9\}, \mathbb{Z}_{12} / \langle 3 \rangle \simeq \mathbb{Z}_3$$

$$\langle 4 \rangle = \{0, 4, 8\}, \mathbb{Z}_{12} / \langle 4 \rangle \simeq \mathbb{Z}_4$$

$$\langle 6 \rangle = \{0, 6\}, \mathbb{Z}_{12} / \langle 6 \rangle \simeq \mathbb{Z}_6$$

$$\mathbf{9.} \text{ لتكن } \phi: \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z} \text{ معطاة بـ } \phi(n) = (n, 0) \text{ لـ } n \in \mathbb{Z}.$$

11.  $R/R$  و  $R/\{0\}$  ليست ذات أهمية فعلية؛ لأن  $R/R$  هي الحلقة التي تحوي العنصر صفر فقط، و  $R/\{0\}$  تماثل  $R$ .

13.  $\mathbb{Z}$  حلقة تامة.  $\mathbb{Z}/4\mathbb{Z}$  تماثل  $\mathbb{Z}_4$ ، التي لها قاسم 2 لـ 0.

15.  $\{(n, n \mid n \in \mathbb{Z})\}$  (هناك إجابات أخرى محتملة).

31. متلاشي الجذر لـ  $\mathbb{Z}_{12}$  هو  $\{0, 6\}$ . متلاشي الجذر لـ  $\mathbb{Z}$  هو  $\{0\}$ ، ومتلاشي الجذر لـ  $\mathbb{Z}_{32}$  هو  $\{0, 2, 4, 6, 8, \dots, 30\}$ .

35. أ. لتكن  $R = \mathbb{Z}$ ، ولتكن  $N = 4\mathbb{Z}$ ، عندئذ يكون  $\sqrt{N} = 2\mathbb{Z} \neq 4\mathbb{Z}$ .

ب. لتكن  $R = \mathbb{Z}$ ، ولتكن  $N = 2\mathbb{Z}$ ، عندئذ يكون  $\sqrt{N} = N$ .

الفصل 27

1.  $\{0, 2, 4\}$  و  $\{0, 3\}$  كلاهما أولي وأعظمي.

3.  $\{(0, 0), (1, 0)\}$  و  $\{(0, 0), (0, 1)\}$  كلاهما أولي وأعظمي.

1.5 2.7 9.1 4. 15.  $2\mathbb{Z} \times \mathbb{Z}$  17.  $4\mathbb{Z} \times \{0\}$

19. نعم.  $x^2 - 6x + 6$  غير مختزل على  $\mathbb{Q}$  بالاعتماد على آيزنشتاين مع  $p=2$ .

21. نعم.  $\mathbb{Z}_2 \times \mathbb{Z}_3$

23. لا. بتكبير المجال إلى حقل خوارج، يجب أن يكون لديك حقل يحوي حقلين أوليين مختلفين  $\mathbb{Z}_p$  و  $\mathbb{Z}_q$ ، وهذا مستحيل.

الفصل 28

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

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

5.  $2z^5y^3x - 5z^3yx^2 + 7zy^2x^2 - 3x^3$

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

9.  $1 < z < y < x < z^2 < yz < y^2 < xz < xy < x^2 < z^3 < yz^2 < y^2z < y^3 < xz^2 < xyz < xy^2 < x^2z < x^2y < x^3 < \dots$

13.  $3yz^3 - 8xy - 4xz + 2yz + 38$

11.  $3y^2z^5 - 8z^7 + 5y^3z^3 - 4x$

17.  $\langle y^2z^3 + 3, -3y - 2z, y^2z^2 + 3 \rangle$

15.  $\langle y^5 + y^3, y^3 + z, x - y^4 \rangle$

21.  $\{x - 1\}$

19.  $\{1\}$

23.  $\{2x + y - 5, y^2 - 9y + 18\}$

المتنوعة الجبرية هي  $\{(1, 3), (-\frac{1}{2}, 6)\}$ .

25.  $\{x + y, y^3 - y + 1\}$

تتكون المتنوعة الجبرية من نقطة واحدة  $(a, -a)$ ، حيث  $a \approx 1.3247$ .

27. أ. صح ج. صح هـ. صح ز. صح ط. خطأ

## الفصل 29

1.  $x^2 - 2x - 1$  3.  $x^2 - 2x + 2$

5.  $x^{12} + 3x^8 - 4x^6 + 3x^4 + 12x^2 + 5$

7.  $\text{Irr}(\alpha, \mathbb{Q}) = x^4 - \frac{2}{3}x^2 - \frac{62}{9}; \text{deg}(\alpha, \mathbb{Q}) = 4$

9. جبري،  $\text{deg}(\alpha, F) = 2$

11. متسام

13. جبري،  $\text{deg}(\alpha, F) = 2$

15. جبري،  $\text{deg}(\alpha, F) = 1$

17.  $x^2 + x + 1 = (x - \alpha)(x + 1 + \alpha)$

23. أ. صح ج. صح هـ. خطأ ز. خطأ ط. خطأ

25. ب.  $x^3 + x^2 + 1 = (x - \alpha)(x - \alpha^2)[x - (1 + \alpha + \alpha^2)]$

27. هي كثيرة الحدود الواحدة في  $F[x]$  ذات الدرجة الأصغر، التي  $\alpha$  صفر لها.

## الفصل 30

1.  $\{(0, 1), (1, 0)\}, \{(1, 1), (-1, 1)\}, \{(2, 1), (1, 2)\}$ . (هناك إجابات أخرى محتملة).

3. لا.  $2(-1, 1, 2) - 4(2, -3, 1) + (10, -14, 0) = (0, 0, 0)$

5.  $\{1\}$  7.  $\{1, i\}$  9.  $\{1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3\}$

15. أ. صح ج. صح هـ. خطأ ز. خطأ ط. صح

17. أ. الفضاء الجزئي من  $V$  المولد بـ  $S$  هو تقاطع جميع الفضاءات الجزئية من  $V$  التي تحوي  $S$ .

19. جواب جزئي: أساس لـ  $F^n$  هو  $\{(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)\}$  حيث 1 هو المحايد الضربي لـ  $F$ .

25. أ. تشاكل

ب. جواب جزئي: النواة (kernel) (أو الفضاء الصفري (nullspace)) لـ  $\phi$  هو  $\{\alpha \in V \mid \phi(\alpha) = 0\}$ .

ج.  $\phi$  تماثل من  $V$  إلى  $V'$  إذا كان  $\text{Ker}(\phi) = \{0\}$ ، و  $\phi$  ترسل  $V$  بصورة غامرة إلى  $V'$ .

### الفصل 31

$$1. \{1, \sqrt{2}\}, 2. \{1, \sqrt{3}, \sqrt{2}, \sqrt{6}\}, 3.$$

$$4. \{1, \sqrt{6}\}, 5. \{1, \sqrt{2}, \sqrt[3]{2}, \sqrt{2}(\sqrt[3]{2})^2, (\sqrt[3]{2})^2, \sqrt{2}(\sqrt[3]{2})^2\}, 6.$$

$$7. \{1, \sqrt{6}\}, 8. \{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt[3]{3}, \sqrt[3]{6}, \sqrt[3]{12}, \sqrt[3]{9}, \sqrt[3]{18}, \sqrt[3]{36}\}, 9.$$

$$10. \{1, \sqrt{2}\}, 11. \{1, \sqrt{2}\}, 12.$$

$$13. \{1, \sqrt{2}\}, 14. \text{أ. خطأ ج. خطأ هـ. خطأ ز. خطأ ط. خطأ}$$

15. جواب جزئي: يتم الحصول على امتدادات من الدرجة  $2^n$  لـ  $n \in \mathbb{Z}^+$ .

### الفصل 32

الأسئلة جميعها ذات الأرقام الفردية تحتاج إلى براهين، وهي ليست مسرودة هنا.

### الفصل 33

$$1. \text{نعم} \quad 2. \text{نعم} \quad 3. \text{نعم} \quad 4. 0.7 \quad 5. 6.5$$

## الفصل 34

$$1. \text{ أ. } K = \{0, 3, 6, 9\}$$

$$\text{ب. } 0 + K = \{0, 3, 6, 9\}, 1 + K = \{1, 4, 7, 10\}, 2 + K = \{2, 5, 8, 11\}$$

$$\text{ج. } \mu(0 + K) = 0, \mu(1 + K) = 2, \mu(2 + K) = 1$$

$$3. \text{ أ. } HN = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22\}, H \cap N = \{0, 12\}$$

$$\text{ب. } 0 + N = \{0, 6, 12, 18\}, 2 + N = \{2, 8, 14, 20\}, 4 + N = \{4, 10, 16, 22\}$$

$$\text{ج. } 0 + (H \cap N) = \{0, 12\}, 4 + (H \cap N) = \{4, 16\}, 8 + (H \cap N) = \{8, 20\}$$

$$\text{د. } \phi(0 + N) = 0 + (H \cap N), \phi(2 + N) = 8 + (H \cap N), \phi(4 + N) = 4 + (H \cap N)$$

$$5. \text{ أ. } 0 + H = \{0, 4, 8, 12, 16, 20\}, 1 + H = \{1, 5, 9, 13, 17, 21\}$$

$$2 + H = \{2, 6, 10, 14, 18, 22\}, 3 + H = \{3, 7, 11, 15, 19, 23\}$$

$$\text{ب. } 0 + K = \{0, 8, 16\}, 1 + K = \{1, 9, 17\}, 2 + K = \{2, 10, 18\}$$

$$3 + K = \{3, 11, 19\}$$

$$4 + K = \{4, 12, 20\}, 5 + K = \{5, 13, 21\}, 6 + K = \{6, 14, 22\}$$

$$7 + K = \{7, 15, 23\}$$

$$\text{ج. } 0 + K = \{0, 8, 16\}, 4 + K = \{4, 12, 20\}$$

$$\text{د. } (0 + K) + (H/K) = H/K = \{0 + K, 4 + K\} = \{\{0, 8, 16\}, \{4, 12, 20\}\}$$

$$(1 + K) + (H/K) = \{1 + K, 5 + K\} = \{\{1, 9, 17\}, \{5, 13, 21\}\}$$

$$(2 + K) + (H/K) = \{2 + K, 6 + K\} = \{\{2, 10, 18\}, \{6, 14, 22\}\}$$

$$(3 + K) + (H/K) = \{3 + K, 7 + K\} = \{\{3, 11, 19\}, \{7, 15, 23\}\}$$

$$\text{هـ. } \phi(0 + H) = (0 + K) + (H/K), \phi(1 + H) = (1 + K) + (H/K)$$

$$\phi(2 + H) = (2 + K) + (H/K), \phi(3 + H) = (3 + K) + (H/K)$$

1. التصنيفات  $\{0\} < 10\mathbb{Z} < \mathbb{Z} \perp \{0\} < 250\mathbb{Z} < 25\mathbb{Z} < \mathbb{Z}$  و  $\{0\} < 25\mathbb{Z} < \mathbb{Z} \perp \{0\} < 250\mathbb{Z} < 10\mathbb{Z} < \mathbb{Z}$  متماثلة.
3. المتسلسلات المعطاة متماثلة.
5. التصنيفات  $\{0, 0\} < (4800\mathbb{Z}) \times \mathbb{Z} < (240\mathbb{Z}) \times \mathbb{Z} < (60\mathbb{Z}) \times \mathbb{Z} < (10\mathbb{Z}) \times \mathbb{Z} < \mathbb{Z} \times \mathbb{Z}$  للمتسلسلة الأولى، و  $\{0, 0\} < \mathbb{Z} \times (4800\mathbb{Z}) < \mathbb{Z} \times (480\mathbb{Z}) < \mathbb{Z} \times (80\mathbb{Z}) < \mathbb{Z} \times (20\mathbb{Z}) < \mathbb{Z} \times \mathbb{Z}$  للمتسلسلة الثانية هي تصنيفات متماثلة.

$$7. \{0\} < 16 < 8 < 4 < 2 < \mathbb{Z}_{48}$$

$$\{0\} < \langle 24 \rangle < \langle 8 \rangle < \langle 4 \rangle < \langle 2 \rangle < \mathbb{Z}_{48}$$

$$\{0\} < \langle 24 \rangle < \langle 12 \rangle < \langle 4 \rangle < \langle 2 \rangle < \mathbb{Z}_{48}$$

$$\{0\} < \langle 24 \rangle < \langle 12 \rangle < \langle 6 \rangle < \langle 2 \rangle < \mathbb{Z}_{48}$$

$$\{0\} < \langle 24 \rangle < \langle 12 \rangle < \langle 6 \rangle < \langle 3 \rangle < \mathbb{Z}_{48}$$

$$9. \{(\rho_0, 0)\} < A_3 \times \{0\} < S_3 \times (0) < S_3 \times \mathbb{Z}_2$$

$$\{(\rho_0, 0)\} < \{(\rho_0)\} \times \mathbb{Z}_2 < A_3 \times \mathbb{Z}_2 < S_3 \times \mathbb{Z}_2$$

$$\{(\rho_0, 0)\} < A_3 \times \{0\} < A_3 \times \mathbb{Z}_4 < S_3 \times \mathbb{Z}_2$$

$$11. \{(\rho_0)\} \times \mathbb{Z}_4 \quad 13. \{(\rho_0)\} \times \mathbb{Z}_4 \leq \{(\rho_0)\} \times \mathbb{Z}_4 \leq \dots$$

$$17. \text{أ. صح ج. خطأ هـ. خطأ ز. خطأ ط. صح}$$

ط. تطبيق مبرهنة جوردن-هولدر على الزمر  $\mathbb{Z}_n$  يضمن المبرهنة الأساسية للحساب.

19. نعم.  $D_4 < \{(\rho_0, \rho_1, \rho_2, \rho_3)\} < \{(\rho_0, \rho_2)\} < \{(\rho_0)\}$  هي متسلسلة تركيب (فعلياً رئيسية) وزمر العامل جميعها تماثل  $\mathbb{Z}_2$ ، وعليه، فهي إبدالية.

$$21. \text{سلسلة (3)} \quad \text{سلسلة (4)}$$

$$\{0\} \leq \langle 12 \rangle \leq \langle 12 \rangle \leq \langle 12 \rangle \quad \{0\} \leq \langle 12 \rangle \leq \langle 12 \rangle \leq \langle 6 \rangle$$

$$\leq \langle 12 \rangle \leq \langle 12 \rangle \leq \langle 4 \rangle \quad \leq \langle 6 \rangle \leq \langle 6 \rangle \leq \langle 3 \rangle$$

$$\leq \langle 2 \rangle \leq \mathbb{Z}_{24} \leq \mathbb{Z}_{24} \quad \leq \langle 3 \rangle \leq \mathbb{Z}_{24} \leq \mathbb{Z}_{24}$$

## التماثلات

$$\begin{aligned} \langle 12 \rangle / \langle 12 \rangle &\simeq \langle 6 \rangle / \langle 6 \rangle = \{0\} & \langle 12 \rangle / \{0\} &\simeq \langle 12 \rangle / \{0\} = \mathbb{Z}_4 \\ \langle 12 \rangle / \langle 12 \rangle &\simeq \langle 12 \rangle / \langle 12 \rangle = \{0\} & \langle 12 \rangle / \langle 12 \rangle &\simeq \langle 3 \rangle / \langle 3 \rangle = \{0\} \\ \langle 4 \rangle / \langle 12 \rangle &\simeq \mathbb{Z}_{24} / \langle 3 \rangle = \mathbb{Z}_3 & \langle 12 \rangle / \langle 12 \rangle &\simeq \langle 6 \rangle / \langle 6 \rangle = \{0\} \\ \mathbb{Z}_{24} / \langle 2 \rangle &\simeq \langle 3 \rangle / \langle 6 \rangle = \mathbb{Z}_2 & \langle 2 \rangle / \langle 4 \rangle &\simeq \langle 6 \rangle / \langle 12 \rangle = \mathbb{Z}_2 \\ \mathbb{Z}_{24} / \mathbb{Z}_{24} &\simeq \mathbb{Z}_{24} / \mathbb{Z}_{24} = \{0\} \end{aligned}$$

## الفصل 36

3. 1. 3

3. 1

5. زمر سيلو الجزئية من النوع 3 هي:  $\langle (1, 2, 3) \rangle$ ،  $\langle (1, 2, 4) \rangle$ ،  $\langle (1, 3, 4) \rangle$ ، و  $\langle (2, 3, 4) \rangle$ .  
كذلك  $\langle (1, 2, 4) \rangle = \langle (1, 2, 3) \rangle \langle (3, 4) \rangle$ ، إلى آخره.

## الفصل 37

1. أ. صفوف الترافق هي:  $\{\rho_0\}$ ،  $\{\rho_2\}$ ،  $\{\rho_1, \rho_3\}$ ،  $\{\mu_1, \mu_2\}$ ،  $\{\delta_1, \delta_2\}$ .

ب.  $8 = 2 + 2 + 2 + 2$

3. أ. صح ج. خطأ هـ. صح ز. صح ط. خطأ

هـ. هذا يُعدّ إلى حدّ ما وجهة نظر.

9.  $24 = 1 + 6 + 3 + 8 + 6$

### الفصل 38

1.  $\{(1, 1, 1), (1, 2, 1), (1, 1, 2)\}$

3. لا.  $n(2, 1) + m(4, 1)$  لا يمكن أن تؤدي إلى عدد فردي للإحداثي الأول.

7.  $\mathbb{Z} < \mathbb{Z}$ ، المرتبة  $r = 1$

### الفصل 39

1. أ.  $a^2b^2a^3c^3b^{-2}$ ،  $b^2c^{-3}a^{-3}b^{-2}a^{-2}$  ب.  $a^{-1}b^3a^4c^6a^{-1}$ ،  $ac^{-6}a^{-4}b^{-3}a$

3. أ. 16 ب. 36 ج. 36

5. أ. 16 ب. 36 ج. 18

11. أ. جواب جزئي:  $\{1\}$  هو أساس لـ  $\mathbb{Z}_4$ . ج. نعم

13. ج. زمرة بلوب على  $S$  تماثل الزمرة الحرة  $F[S]$  على  $S$ .

### الفصل 40

1.  $(a : a^4 = 1)$ ؛  $(a, b : a^4 = 1, b = a^2)$ ؛  $(a, b, c : a = 1, b^4 = 1, c = 1)$ . (هناك إجابات أخرى محتملة).

3. الزمرة الثمانية:

|                  | 1                | a                | a <sup>2</sup>   | a <sup>3</sup>   | b                | ab               | a <sup>2</sup> b | a <sup>3</sup> b |
|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| 1                | 1                | a                | a <sup>2</sup>   | a <sup>3</sup>   | b                | ab               | a <sup>2</sup> b | a <sup>3</sup> b |
| a                | a                | a <sup>2</sup>   | a <sup>3</sup>   | 1                | ab               | a <sup>2</sup> b | a <sup>3</sup> b | b                |
| a <sup>2</sup>   | a <sup>2</sup>   | a <sup>3</sup>   | 1                | a                | a <sup>2</sup> b | a <sup>3</sup> b | b                | ab               |
| a <sup>3</sup>   | a <sup>3</sup>   | 1                | a                | a <sup>2</sup>   | a <sup>3</sup> b | b                | ab               | a <sup>2</sup> b |
| b                | b                | a <sup>3</sup> b | a <sup>2</sup> b | ab               | 1                | a <sup>3</sup>   | a <sup>2</sup>   | a                |
| ab               | ab               | b                | a <sup>3</sup> b | a <sup>2</sup> b | a                | 1                | a <sup>3</sup>   | a <sup>2</sup>   |
| a <sup>2</sup> b | a <sup>2</sup> b | ab               | b                | a <sup>3</sup> b | a <sup>2</sup>   | a                | 1                | a <sup>3</sup>   |
| a <sup>3</sup> b | a <sup>3</sup> b | a <sup>2</sup> b | ab               | b                | a <sup>3</sup>   | a <sup>2</sup>   | a                | 1                |

الزمرة الرباعية: جدول الزمرة الثمانية نفسه ما عدا الـ 16 مدخلاً في الزاوية اليمنى السفلى، فتكون:

|       |       |       |       |
|-------|-------|-------|-------|
| $a^2$ | $a$   | 1     | $a^2$ |
| $a^3$ | $a^2$ | $a$   | 1     |
| 1     | $a^3$ | $a^2$ | $a$   |
| $a$   | 1     | $a^3$ | $a^2$ |

5.  $\mathbb{Z}_{21}.(a, b : a^7 = 1, b^3 = 1, ba = a^2 b)$

## الفصل 41

$$2P_1P_3 - 3P_1P_4 + P_1P_6 - 3P_2P_3 + 3P_2P_4 - 5P_3P_4 + 4P_3P_6 - 5P_4P_6 \text{ أ. 1}$$

ب. لا ج. نعم

$$0 \text{ الدورة-} P \text{ وتتولد من } Z_0(P) \simeq \mathbb{Z} . B_0(P) = 0 . i > 0 \perp C_i(P) = Z_i(P) = B_i(P) = H_i(P) = 0 \text{ 3}$$

$$H_0(P) \simeq \mathbb{Z} \text{ (0-cycle)}$$

$$P_2 - P_1 \text{ (0-chain) 0- وتتولد من السلسلة-} B_0(x) \simeq \mathbb{Z} . i > 0 \perp C_i(X) = Z_i(X) = B_i(X) = H_i(X) = 0 \text{ 5}$$

$Z_0(X) \simeq \mathbb{Z} \times \mathbb{Z}$  ، وتتولد من الدورتين-0 (two 0-cycles)  $P_2$  و  $P_1$  : لأن  $Z_0(X)/B_0(X)$  "تطابق  $P_1$  مع  $P_2$ " ،  
 $H_0(X) \simeq \mathbb{Z}$  ، وتولدت من مجموعة المشاركة  $P_1 + B_0(X)$

$$P_1P_2 \dots P_{n+1} \text{ مرتبة } n \text{ هو متتالية مرتبة 7 أ. مبسّط موجّه من الرتبة } n$$

ب. الحدود لـ  $P_1P_2 \dots P_{n+1}$  تعطي بـ

$$\partial_n (P_1P_2 \dots P_{n+1}) \sum_{i=1}^{n+1} (-1)^{i+1} P_1P_2 \dots P_{i-1}P_{i+1} \dots P_{n+1}.$$

ج. كل مجموع مفرد من حدود مبسّط موجّه من الرتبة  $n$  هو وجه للمبسط

$$\delta^{(n)} \left( \sum_i m_i \sigma_i \right) = \sum_i m_i \delta^{(n)}(\sigma_i) \text{ أ. 11}$$

$$H^{(n)}(X) = Z^{(n)}(X)/B^{(n)}(X) \text{ 13}$$

$$H^{(0)}(S) \simeq \mathbb{Z} \text{ وتتولد من } \{0\} + (P_1 + P_2 + P_3 + P_4)$$

$$H^{(2)}(S) \simeq \mathbb{Z} \text{ وتتولد من } P_1P_2P_3 + B^{(2)}(S)$$

## الفصل 42

$$n > 1 \perp H_0(X) \simeq \mathbb{Z} . H_1(X) \simeq \mathbb{Z} \times \mathbb{Z} . H_n(X) = 0 \text{ 1}$$

$$n > 2 \perp H_0(X) \simeq \mathbb{Z} \times \mathbb{Z} . H_1(X) \simeq \mathbb{Z} . H_2(X) \simeq \mathbb{Z} . H_n(X) = 0 \text{ 3}$$

$$n > 2 \perp H_0(X) \simeq \mathbb{Z} . H_1(X) \simeq \mathbb{Z} . H_2(X) \simeq \mathbb{Z} . H_n(X) = 0 \text{ 5}$$

7 أ. صح ج. خطأ هـ. صح ز. صح ط. خطأ

$$n > 2 \perp H_0(X) \simeq \mathbb{Z} . H_1(X) \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} . H_2(X) \simeq \mathbb{Z} \times \mathbb{Z} . H_n(X) = 0 \text{ 9}$$

$$n > 2 \perp H_0(X) \simeq \mathbb{Z}. H_1(X) \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}. H_2(X) \simeq \mathbb{Z}. H_n(X) = 0 \quad 11$$

### الفصل 43

$$1. \chi(X) = I \text{ أن يبين أن } \chi(X) = I$$

3. ستتحقق للمنطقة المربعة؛ لأن منطقة كهذه تماثل  $E^2$ . من الواضح أنها لا تتحقق لخليتين منفصلتين من الرتبة 2، لأن كلاهما يمكن أن ترسل بصورة متصلة وغامرة إلى الأخرى، ومثل هذه الدالة ليس لها نقاط مثبتة.

$$n > 1 \perp H_0(X) \simeq \mathbb{Z} \times \mathbb{Z}. H_1(X) \simeq \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}_2. H_n(X) = 0 \quad 5$$

$$2 - 2n \quad 7$$

$$n > 1 \perp H_0(X) \simeq \mathbb{Z}. H_1(X) \simeq \underbrace{\mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z} \times \mathbb{Z}_2}_{(q-1) \text{ عامل}}. H_n(X) = 0 \quad 9$$

(q-1) عامل

11. ليكن  $Q$  رأساً لـ  $b$ ، وليكن  $c$  متسلسلة 2- (2-chain) تتكوّن من جميع المبسطات (2-simplexes) لـ  $X$ ، موجهة بالطريقة نفسها، بحيث تكون  $c \in Z_2(X)$

$$أ.  $f_{*0}(Q + B_0(X)) = Q + B_0(b)$  معطى بـ$$

$$f_{*1}((ma + nb) + B_1(X)) = nb + B_1(b) \text{ معطى بـ}$$

$$f_{*2}(c + B_1(X)) = 0 \text{ معطى بـ}$$

ب.  $f_{*0}$  كما في (أ)

$$f_{*1}((ma + nb) + B_1(X)) = 2nb + B_1(b) \text{ معطى بـ}$$

$f_{*2}$  كما في (أ)

13. ليكن  $Q$  رأساً لـ  $b$ ،

$$f_{*0}(Q + B_0(X)) = Q + B_0(b) \text{ معطى بـ}$$

$$f_{*1} \text{ معطى بـ } f_{*1}((ma + nb) + B_1(X)) = nb + B_1(b) \text{ حيث } m = 0, 1$$

$$f_{*2} \text{ تافه؛ لأن كلاً من } H_2(X) \text{ و } H_2(b) \text{ هو } 0.$$

الفصل 44

5. للمبرهنة 4.44، الشرط  $f_k \partial_k = \partial_k f_{k-1}$  يؤدي إلى  $f_{k-1}(B_{k-1}(A)) \subseteq B_{k-1}(A')$

عندئذ التمرين 39.14 يبين أن  $f_{k-1}$  ينشئ تشاكلاً طبيعياً من  $Z_{k-1}(A)/B_{k-1}(A)$  إلى  $Z_{k-1}(A')/B_{k-1}(A')$ . هذه هي الطريقة الصحيحة للنظر إلى المبرهنة 4.44.

7.44، إذا استخدمنا التمرين 39.14، الحقيقة أن  $\partial_k(A'_k) \subseteq A'_{k-1}$  تبين أن  $\partial_k$  ينشئ تشاكلاً طبيعياً  $\bar{\partial}_k : (A'_k/A'_k) \rightarrow (A'_{k-1}/A'_{k-1})$

7. متتالية الشباه المضبوطة هي

$$\begin{aligned} [H_2(a) = 0] &\xrightarrow{i_{*2}} [H_2(X) = \mathbb{Z}] \xrightarrow{j_{*2}} [H_2(X, a) = \mathbb{Z}] \xrightarrow{\partial_{*2}} [H_1(a) = \mathbb{Z}] \\ &\xrightarrow{i_{*1}} [H_1(X) = \mathbb{Z} \times \mathbb{Z}] \xrightarrow{j_{*1}} [H_1(X, a) = \mathbb{Z}] \xrightarrow{\partial_{*1}} [H_0(a) = \mathbb{Z}] \\ &\xrightarrow{i_{*0}} [H_0(X) = \mathbb{Z}] \xrightarrow{j_{*0}} [H_0(X, a) = 0] \end{aligned}$$

$j_{*2}$  ترسل المولد  $c + B_2(X)$  في  $H_2(X)$  بصورة غامرة إلى المولد

$$(c + C_2(a)) + B_2(X, a)$$

في  $H_2(X, a)$  وهي تماثل. وعليه،  $(\text{image } i_{*2}) = (\text{kernel } j_{*2}) = 0$ .

$\partial_{*2}$  ترسل كل شيء بصورة غامرة إلى 0، وهكذا  $(\text{kernel } \partial_{*2}) = (\text{image } j_{*2}) = \mathbb{Z}$ .

$i_{*1}$  ترسل المولد  $a + B_1(a)$  بصورة غامرة إلى  $(a + 0b) + B_1(X)$ ، وهكذا  $i_{*1}$  هي تماثل إلى،

$$(\text{kernel } i_{*1}) = (\text{image } \partial_{*2}) = 0$$

$j_{*1}$  ترسل  $(ma + nb) + B_1(X)$  بصورة غامرة إلى  $(nb + C_1(a)) + B_1(X, a)$ ، وهكذا  $(\text{kernel } j_{*1}) = (\text{image } i_{*1}) = \mathbb{Z}$ .

$\partial_{*1}$  ترسل  $(nb + C_1(a)) + B_1(X, a)$  بصورة غامرة إلى 0، وهكذا  $(\text{kernel } \partial_{*1}) = (\text{image } j_{*1}) = \mathbb{Z}$ .

لرأس  $Q$  لـ  $i_{*0}$  ترسل  $Q + B_0(a)$  بصورة غامرة إلى  $Q + B_0(X)$ ، وهكذا  $i_{*0}$  تماثل، و  $(\text{kernel } i_{*0}) = (\text{image } \partial_{*1}) = 0$ .

$j_{*0}$  ترسل  $Q + B_0(X)$  بصورة غامرة إلى  $Q + B_0(X, a)$  من  $H_0(X, a)$ ، وهكذا  $(\text{kernel } j_{*0}) = (\text{image } i_{*0}) = \mathbb{Z}$ .

9. الحل بصورة منهجية مماثل لذلك في التمرين 44.7

11. إجابة جزئية: متتالية الشباه المضبوطة هي

$$\begin{aligned}
[H_2(Y) = 0] &\xrightarrow{i_{*2}} [H_2(X) = 0] \xrightarrow{j_{*2}} [H_2(X, Y) \simeq \mathbb{Z}] \xrightarrow{\partial_{*2}} [H_1(Y) \simeq \mathbb{Z} \times \mathbb{Z}] \\
&\xrightarrow{i_{*1}} [H_1(X) \simeq \mathbb{Z}] \xrightarrow{j_{*1}} [H_1(X, Y) \simeq \mathbb{Z}] \xrightarrow{\partial_{*1}} [H_0(Y) \simeq \mathbb{Z} \times \mathbb{Z}] \\
&\xrightarrow{i_{*0}} [H_0(X) \simeq \mathbb{Z}] \xrightarrow{j_{*0}} [H_0(X, Y) = 0]
\end{aligned}$$

يترك لك التحقق من أنها مضبوطة. لاحظ أن الحافة  $P_1Q_1$  في الشكل 11.42 تنشئ مولدًا لـ  $H_1(X, Y)$ . بالبدء بـ  $\partial_{*2}$  تلك الدوال ممتعة

## الفصل 45

1. نعم 3. لا 5. لا 7. نعم

9. في  $\mathbb{Z}[x]$ : فقط  $2x - 7, -2x + 7$

في  $\mathbb{Q}[x]$ :  $4x - 14, x - \frac{7}{2}, 6x - 21, -8x + 28$

في  $\mathbb{Z}_{11}[x]$ :  $2x - 7, 10x - 2, 6x + 1, 3x - 5, 5x - 1$

11. 26. -26 13. 198. -198

15. إنها "كثيرة حدود بدائية": لأن كل عنصر غير صفري في  $\mathbb{Q}$  هو عنصر وحدة. في الواقع  $18ax^2 - 12ax + 48a$  كثيرة حدود بدائية لكل  $a \in \mathbb{Q}, a \neq 0$

17.  $2ax^2 - 3ax + 6a$  كثيرة حدود بدائية لكل  $a \neq 0$  في  $\mathbb{Z}_7$ : لأن كل عنصر  $a$  مثل هذا هو عنصر محايد في  $\mathbb{Z}_7$ .

21. أ. صح ج. صح هـ. صح ز. خطأ ط. خطأ

ط. أما  $p$  أو إحدى مرافقاتها (associates) فيجب أن تظهر في كل تحليل إلى غير مختزلات.

23.  $2x + 4$  غير مختزل في  $\mathbb{Q}[x]$  لكن ليس في  $\mathbb{Z}[x]$

31. إجابة جزئية:  $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$

### الفصل 46

1. نعم 3. لا (1) لا يتحقق 5. نعم

7. 61  $x^3 + 2x - 1$  11. 66

13. أ. ص ب. ص ج. ص د. ص هـ. ص ز. ص ط. ص

23. إجابة جزئية: المعادلة  $ax = b$  لها حل في  $\mathbb{Z}_n$  للعناصر غير الصفرية  $a, b \in \mathbb{Z}_n$  إذا كان فقط إذا كان gcd الموجب لـ  $a$  و  $n$  في  $\mathbb{Z}$  يقسم  $b$ .

### الفصل 47

1.  $5 = (1 + 2i)(1 - 2i)$  3.  $4 + 3i = (1 + 2i)(2 - i)$

5.  $6 = (2)(3) = (-1 + \sqrt{-5})(-1 - \sqrt{-5})$  7.  $7 - i$

15. ج. i) الرتبة 9، المميز 3 ii) الرتبة 2، المميز 2 iii) الرتبة 5، المميز 5

### الفصل 48

1.  $\sqrt{2}, -\sqrt{2}$  3.  $3 + \sqrt{2}, 3 - \sqrt{2}$  5.  $\sqrt{2} + i, \sqrt{2} - i, -\sqrt{2} + i, -\sqrt{2} - i$

7.  $\sqrt{1 + \sqrt{2}}, -\sqrt{1 + \sqrt{2}}, \sqrt{1 - \sqrt{2}}, -\sqrt{1 - \sqrt{2}}$  9.  $\sqrt{3}$

11.  $-\sqrt{2} + 3\sqrt{5}$  13.  $-\sqrt{2} + \sqrt{45}$

15. أ.  $\mathbb{Q}$  ب.  $\mathbb{Q}(\sqrt{6})$  ج.  $\mathbb{Q}$

17.  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$  19.  $\mathbb{Q}(\sqrt{3}, \sqrt{10})$  21.  $\mathbb{Q}$

25. أ.  $3 - \sqrt{2}$  ب. إنهما الدالة نفسها

27.  $\sigma_3(0) = 0, \sigma_3(1) = 1, \sigma_3(2) = 2, \sigma_3(a) = -a, \sigma_3(2a) = -2a$

$$\sigma_3(1 + a) = 1 - a, \sigma_3(1 + 2a) = 1 - 2a, \sigma_3(2 + a) = 2 - a.$$

$$\sigma_3(2 + 2a) = 2 - 2a, \mathbb{Z}_3(a)\{\sigma_3\} = \mathbb{Z}_3.$$

29. أ. خطأ ج. صح ه. خطأ ز. صح ط. صح

37. نعم

## الفصل 49

1. الدالة المحايدة من  $E$  وبصورة غامرة إلى  $E$

$$\tau \text{ المعطاة بـ } \tau(\sqrt{2}) = \sqrt{2}, \tau(\sqrt{3}) = -\sqrt{3}, \tau(\sqrt{5}) = -\sqrt{5}$$

$$\tau_1 \text{ المعطاة بـ } \tau_1(\sqrt{2}) = \sqrt{2}, \tau_1(\sqrt{3}) = \sqrt{3}, \tau_1(\sqrt{5}) = -\sqrt{5} \quad 3.$$

$$\tau_2 \text{ المعطاة بـ } \tau_2(\sqrt{2}) = \sqrt{2}, \tau_2(\sqrt{3}) = -\sqrt{3}, \tau_2(\sqrt{5}) = \sqrt{5}$$

$$\tau_3 \text{ المعطاة بـ } \tau_3(\sqrt{2}) = -\sqrt{2}, \tau_3(\sqrt{3}) = \sqrt{3}, \tau_3(\sqrt{5}) = \sqrt{5}$$

$$\tau_4 \text{ المعطاة بـ } \tau_4(\sqrt{2}) = -\sqrt{2}, \tau_4(\sqrt{3}) = -\sqrt{3}, \tau_4(\sqrt{5}) = -\sqrt{5}$$

5. الدالة المحايدة من  $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$  إلى نفسها:

$$\tau_1 \text{ المعطاة بـ } \tau_1(\alpha_1) = \alpha_1, \tau_1(\sqrt{3}) = -\sqrt{3} \text{ حيث } \alpha_1 = \sqrt[3]{2}$$

$$\tau_2 \text{ المعطاة بـ } \tau_2(\alpha_1) = \alpha_2, \tau_2(\sqrt{3}) = \sqrt{3} \text{ حيث } \alpha_2 = \sqrt[3]{2}(-1 + i\sqrt{3})/2$$

$$\tau_3 \text{ المعطاة بـ } \tau_3(\alpha_1) = \alpha_2, \tau_3(\sqrt{3}) = -\sqrt{3}$$

$$\tau_4 \text{ المعطاة بـ } \tau_4(\alpha_1) = \alpha_3, \tau_4(\sqrt{3}) = \sqrt{3} \text{ حيث } \alpha_3 = \sqrt[3]{2}(-1 - i\sqrt{3})/2$$

$$\tau_5 \text{ المعطاة بـ } \tau_5(\alpha_1) = \alpha_3, \tau_5(\sqrt{3}) = -\sqrt{3}$$

$$7. \text{ أ. } \mathbb{Q}(\pi^2) \text{ ب. } \tau_1 \text{ المعطاة بـ } \tau_1(\sqrt{\pi}) = i\sqrt{\pi}, \tau_2 \text{ المعطاة بـ } \tau_2(\sqrt{\pi}) = -i\sqrt{\pi}$$

الفصل 50

2.1    4.3    2.5    1.7    2.9    13.  $1 \leq [E : F] \leq n!$

15. ليكن  $F = \mathbb{Q}$  و  $E = \mathbb{Q}(\sqrt{2})$ . عندئذٍ، يكون لـ

$$f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$$

صفر في  $E$ ، لكنه لا ينشطر في  $E$ .

23. أ. 6

الفصل 51

1.  $\alpha = \sqrt[6]{2} = 2/(\sqrt[3]{2}\sqrt{2})$ .  $\sqrt{2} = (\sqrt[6]{2})^3$ ,  $\sqrt[3]{2} = (\sqrt[6]{2})^2$ . (هناك إجابات أخرى محتملة).

3.  $\alpha = \sqrt{2} + \sqrt{3}$ .  $\sqrt{2} = (\frac{1}{2})\alpha^3 - (\frac{9}{2})\alpha$ ,  $\sqrt{3} = (\frac{11}{2})\alpha - (\frac{1}{2})\alpha^3$ . (هناك إجابات أخرى محتملة).

7.  $f(x) = x^4 - 4x^2 + 4 = (x^2 - 2)^2$ . هنا  $f(x)$  ليست كثيرة حدود غير مختزلة. كل عامل غير مختزل لـ  $f(x)$  له أصفار تكررهما 1 فقط.

15. ب. الحقل  $F$ . ج.  $F[x^p]$

الفصل 52

1.  $\mathbb{Z}_3(y^3, z^9)$     3.  $\mathbb{Z}_3(y^4, z^2)$

5. أ. خطأ    ج. خطأ    هـ. خطأ    ز. صح    ط. صح

الفصل 53

8.1    8.3    4.5    2.7

9. للزمرة عنصران، التماثل الذاتي المحايد 1 لـ  $\mathbb{Q}(i)$  و  $\sigma$ ، بحيث إن  $\sigma(i) = -i$ .

11. أ. ليكن  $\alpha_1 = \sqrt[3]{2}$ ،  $\alpha_2 = \sqrt[3]{2} \frac{-1 + i\sqrt{3}}{2}$  و  $\alpha_3 = \sqrt[3]{2} \frac{-1 - i\sqrt{3}}{2}$ .

الدوال هي

$\rho_0$ ، حيث  $\rho_0$  هي الدالة المحايدة:

$\rho_1$ ، حيث  $\rho_1(\alpha_1) = \alpha_2$  و  $\rho_1(i\sqrt{3}) = i\sqrt{3}$

$\rho_2$ ، حيث  $\rho_2(\alpha_1) = \alpha_3$  و  $\rho_2(i\sqrt{3}) = i\sqrt{3}$

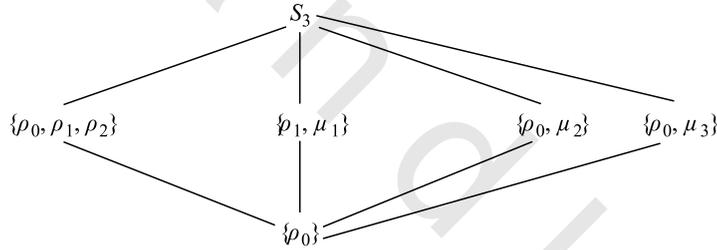
$\mu_1$ ، حيث  $\mu_1(\alpha_1) = \alpha_1$  و  $\mu_1(i\sqrt{3}) = -i\sqrt{3}$

$\mu_2$ ، حيث  $\mu_2(\alpha_1) = \alpha_3$  و  $\mu_2(i\sqrt{3}) = -i\sqrt{3}$

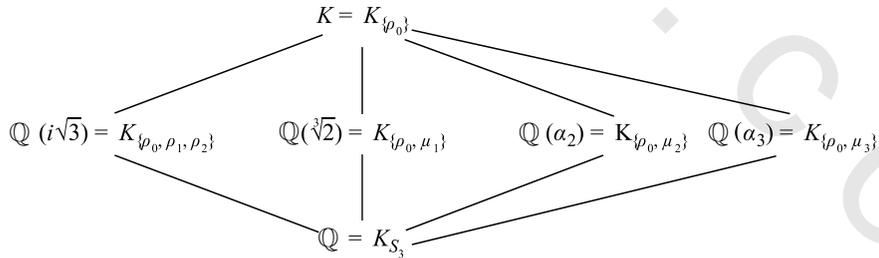
$\mu_3$ ، حيث  $\mu_3(\alpha_1) = \alpha_2$  و  $\mu_3(i\sqrt{3}) = -i\sqrt{3}$

ب.  $S_3$ . تم اختيار الرموز في (أ) لتتطابق مع الرموز لـ  $S_3$  في المثال 7.8.

جـ



مخطط الزمرة



مخطط الحقل

13. حقل الانشطار لـ  $(x^3 - 1) \in \mathbb{Q}[x]$  هو  $\mathbb{Q}(i\sqrt{3})$ ، والزمرة دورية من الرتبة 2 وعناصرها:  $\sigma$ ، حيث  $\sigma$  هي الدالة

المحايدة لـ  $\mathbb{Q}(i\sqrt{3})$ ، و  $\sigma$ ، حيث  $\sigma(i\sqrt{3}) = -i\sqrt{3}$ .

15. أ. خطأ ج. صح هـ. صح ز. خطأ ط. خطأ

25. جواب جزئي:  $G(K/(E \vee L)) = G(K/E) \cap G(K/L)$

الفصل 54

3.  $\mathbb{Q}(\sqrt[4]{2}, i): \sqrt[4]{2} + i, x^8 + 4x^6 + 2x^4 + 28x^2 + 1;$

$\mathbb{Q}(\sqrt[4]{2}): \sqrt[4]{2}, x^4 - 2;$

$\mathbb{Q}(i(\sqrt[4]{2})): i(\sqrt[4]{2}), x^4 - 2;$

$\mathbb{Q}(\sqrt{2}, i): \sqrt{2} + i, x^4 - 2x^2 + 9;$

$\mathbb{Q}(\sqrt[4]{2} + i(\sqrt[4]{2})): \sqrt[4]{2} + i(\sqrt[4]{2}), x^4 + 8;$

$\mathbb{Q}(\sqrt[4]{2} - i(\sqrt[4]{2})): \sqrt[4]{2} - i(\sqrt[4]{2}), x^4 + 8;$

$\mathbb{Q}(\sqrt{2}): \sqrt{2}, x^2 - 2;$

$\mathbb{Q}(i): i, x^2 + 1;$

$\mathbb{Q}(i\sqrt{2}): i\sqrt{2}, x^2 + 2;$

$\mathbb{Q}: 1, x - 1$

5. الزمرة دورية من الرتبة 5، وعناصرها هي:

|                           | $\iota$       | $\sigma_1$           | $\sigma_2$             | $\sigma_3$             | $\sigma_4$             |
|---------------------------|---------------|----------------------|------------------------|------------------------|------------------------|
| $\sqrt[5]{2} \rightarrow$ | $\sqrt[5]{2}$ | $\zeta(\sqrt[5]{2})$ | $\zeta^2(\sqrt[5]{2})$ | $\zeta^3(\sqrt[5]{2})$ | $\zeta^4(\sqrt[5]{2})$ |

حيث  $\sqrt[5]{2}$  هو الجذر الحقيقي الخامس لـ 2.

7. حقل الانشطار لـ  $x^8 - 1$  على  $\mathbb{Q}$  هو حقل الانشطار نفسه لـ  $x^4 + 1$  على  $\mathbb{Q}$ ، وعليه، فهناك وصف كامل ضمن المثال 7.54. (هذه أسهل طريقة للإجابة عن السؤال).

9. أ.  $s_1^2 - 2s_2$  ب.  $\frac{s_1s_2 - 3s_3}{s_3}$

## الفصل 55

3. أ. 16 ب. 400 ج. 2160

5. 3°

7.  $\phi_3(x)$  على  $\mathbb{Z}_2$  هي  $x^2 + x + 1$ 8.  $\phi_8(x)$  على  $\mathbb{Z}_3$  هي  $(x^2 + x + 2)(x^2 + 2x + 2)$  هي  $x^4 + 1$ .

9. أ. صح ب. خطأ ج. خطأ هـ. صح ز. صح ط. خطأ

$$\phi_1(x) = x - 1$$

$$\phi_2(x) = x + 1$$

$$\phi_3(x) = x^2 + x + 1$$

$$\phi_4(x) = x^2 + 1$$

$$\phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

$$\phi_6(x) = x^2 - x + 1$$

## الفصل 56

1. لا. نعم،  $K$  امتداد لـ  $\mathbb{Z}_2$  بالجذور

3. أ. صح ب. صح ج. صح هـ. صح ز. خطأ ط. خطأ

(تعطى مثالاً مناقضاً)  $x^3 - 2x$  على  $\mathbb{Q}$ 

ملحق

$$\begin{bmatrix} -3 + 2i & -1 - 4i \\ 2 & -i \\ 0 & -i \end{bmatrix}.3$$

$$\begin{bmatrix} 2 & 1 \\ 2 & 7 \end{bmatrix}.1$$

$$\begin{bmatrix} 1 & -i \\ 4 - 6i & -2 - 2i \end{bmatrix}.7$$

$$\begin{bmatrix} 5 & 16 & -3 \\ 0 & -18 & 24 \end{bmatrix}.5$$

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.11$$

$$\begin{bmatrix} 8 & -8i \\ 8i & 8 \end{bmatrix}.9$$

-48.13

## ملحق: جبر المصفوفات

نعطي هنا ملخصاً مختصراً لجبر المصفوفات. تظهر المصفوفات في أمثلة لبعض وحدات الكتاب، كما ضُمَّت في كثير من التمارين.

المصفوفة (matrix) هي ترتيب على صورة مستطيل لصفوفٍ من الأعداد، على سبيل المثال:

$$(1) \quad \begin{bmatrix} 2 & -1 & 4 \\ 3 & 1 & 2 \end{bmatrix}$$

مصفوفة لها صفان وثلاثة أعمدة. مصفوفة لها  $m$  صفاً و  $n$  عموداً، هي مصفوفة من الدرجة  $m \times n$ ، وهكذا المصفوفة (1) هي مصفوفة من الدرجة  $2 \times 3$ ، إذا كان  $m = n$ ، فإننا نقول: إن المصفوفة مربعة (square).

يمكن أن تكون مدخلات المصفوفة من أي نوع من الأعداد - صحيحة، أو نسبية، أو حقيقية، أو مركبة، وقد جعلنا  $M_{m \times n}(\mathbb{R})$  ترمز لمجموعة جميع المصفوفات من الدرجة  $m \times n$  بمدخلات حقيقية، فإذا كان  $m = n$ ، فيختصر الرمز إلى  $M_n(\mathbb{R})$ ، ويمكننا بصورة مشابهة أن نعد  $M_n(\mathbb{Z})$ ،  $M_{2 \times 3}(\mathbb{C})$ ، ... إلخ.

مصفوفتان لهما عدد الصفوف نفسه  $m$ ، وعدد الأعمدة نفسه  $n$ ، يمكن جمعها بطريقة واضحة: نجمع المدخلات في المواقع المتقابلة.

مثال A1 في  $M_{2 \times 3}(\mathbb{Z})$ ، لدينا

$$\begin{bmatrix} 2 & -1 & 4 \\ 3 & 1 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 & -3 \\ 2 & -7 & 1 \end{bmatrix} = \begin{bmatrix} 3 & -1 & 1 \\ 5 & -6 & 3 \end{bmatrix}$$

سوف نستخدم الأحرف الكبيرة لترمز للمصفوفات، فإذا كانت  $A$ ، و  $B$  و  $C$  مصفوفات من الدرجة  $m \times n$ ، فمن السهل رؤية أن  $A + B = B + A$  و  $A + (B + C) = (A + B) + C$ .

ضرب المصفوفات،  $AB$ ، مُعرَّف فقط إذا كان عدد أعمدة  $A$  يساوي عدد صفوف  $B$ ، أي إنه إذا كانت  $A$  مصفوفة من الدرجة  $m \times n$ ، فإن  $B$  يجب أن تكون مصفوفة من الدرجة  $n \times s$  لعدد ما صحيح  $s$ ، ونبدأ على النحو الآتي بتعريف الضرب  $AB$ ، حيث  $A$  مصفوفة من الدرجة  $1 \times n$  و  $B$  مصفوفة من الدرجة  $n \times 1$ :

$$AB = [a_1 \quad a_2 \quad \dots \quad a_n] \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = a_1 b_1 + a_2 b_2 + \dots + a_n b_n. \quad (2)$$

لاحظ أنّ النتيجة عدد. (لن نميز بين العدد والمصفوفة من الدرجة  $1 \times 1$  التي لها هذا العدد بوصفه مدخلتها الوحيدة)، يمكنك تمييز هذا الضرب على أنه الضرب النقطي لمتجهين. المصفوفات التي لها صف واحد فقط أو عمود واحد فقط، هي متجهات صف (row vectors) أو متجهات عمود (column vectors)، على الترتيب.

نجد أنّ:

A2 مثال

$$[3 \quad -7 \quad 2] \begin{bmatrix} 1 \\ 4 \\ 5 \end{bmatrix} = (3)(1) + (-7)(4) + (2)(5) = -15$$

لتكن  $A$  مصفوفة من الدرجة  $m \times n$ ، ولتكن  $B$  مصفوفة من الدرجة  $n \times s$ . لاحظ أنّ العدد  $n$  للمدخلات في كل صف من  $A$  هو العدد نفسه  $n$  للمدخلات في كل عمود من  $B$ . الضرب  $C = AB$  هو مصفوفة  $m \times s$ ، أمّا المدخلة في الصف ذي الترتيب  $i$  والعمود ذي الترتيب  $j$  في  $AB$ ، فهي الضرب للصف ذي الترتيب  $i$  من  $A$  بالعمود ذي الترتيب  $j$  من  $B$ ، كما عرّف من خلال المعادلة (2)، ووضّح في المثال A2.

احسب

A3 مثال

$$AB = \begin{bmatrix} 2 & -1 & 3 \\ 1 & 4 & 6 \end{bmatrix} \begin{bmatrix} 3 & 1 & 2 & 1 \\ 1 & 4 & 1 & -1 \\ -1 & 0 & 2 & 1 \end{bmatrix}$$

لاحظ أنّ  $A$  من الدرجة  $2 \times 3$ ، و  $B$  من الدرجة  $3 \times 4$ . وعليه،  $AB$  ستكون من الدرجة  $2 \times 4$ ، والمدخلة في صفها الثاني وعمودها الثالث، هي:

الحل

$$(A \text{ الصف الثاني}) (B \text{ العمود الثالث}) = [1 \quad 4 \quad 6] \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix} = 2 + 4 + 12 = 18.$$

بحساب المدخلات الثمانية جميعها لـ  $AB$  بهذا الأسلوب، نحصل على:

$$AB = \begin{bmatrix} 2 & -2 & 9 & 6 \\ 1 & 17 & 18 & 3 \end{bmatrix}$$

الضرب

A4 مثال

$$\begin{bmatrix} 2 & -1 & 3 \\ 1 & 4 & 6 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 5 & 4 \end{bmatrix}$$

غير مُعرّف؛ لأنّ عدد المدخلات في صفّ للمصفوفة الأولى لا يساوي عدد المدخلات في عمود للمصفوفة الثانية.

لمصفوفتين مربعيتين من الدرجة نفسها، الجمع والضرب كلاهما دائماً مُعرَّفان. يسألنا التمرين 10 أن نوضح الحقيقة الآتية:

ضرب المصفوفات غير إبدالي.

أي إن  $AB$  ليس بالضرورة تساوي  $BA$ ، حتى عندما يكون كلا الضربين مُعرَّفًا، كما لـ  $A, B \in M_n(\mathbb{Z})$ . يمكن إثبات أن  $A(BC) = (AB)C$  و  $A(B+C) = AB + AC$  متى كانت هذه التعابير معرفة.

جعلنا  $I_n$  لتكون المصفوفة من الدرجة  $n \times n$ ، مع المدخلات 1 على القطر من الزاوية اليسرى العليا إلى الزاوية اليمنى السفلى والمدخلات 0 في الأماكن الأخرى.

على سبيل المثال:

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

من السهل رؤية أنه إذا كانت  $A$  أي مصفوفة من الدرجة  $n \times s$  و  $B$  أي مصفوفة من الدرجة  $r \times n$ ، فإن  $I_n A = A$  و  $B I_n = B$ ، أي إن المصفوفة  $I_n$  تعمل كما يعمل العدد 1 للضرب عندما يكون الضرب بـ  $I_n$  مُعرَّفًا.

لتكن  $A$  مصفوفة من الدرجة  $n \times n$ ، وافترض معادلة مصفوفات على الصورة  $AX = B$ ، حيث  $A$  و  $B$  معلومتان لكن  $X$  غير معلومة، فإذا استطعنا إيجاد مصفوفة  $A^{-1}$  من الدرجة  $n \times n$ ، بحيث إن  $A^{-1}A = AA^{-1} = I_n$ ، فإننا نستطيع استنتاج أن:

$$A^{-1}(AX) = A^{-1}B, \quad (A^{-1}A)X = A^{-1}B, \quad I_n X = A^{-1}B, \quad X = A^{-1}B$$

وقد وجدنا المصفوفة  $X$  المطلوبة. مصفوفة مثل  $A^{-1}$  تعمل مثل مقلوب العدد:  $A^{-1}A = I_n$  و  $(1/r)r = 1$ . هذا هو سبب الرمز  $A^{-1}$ .

إذا كانت  $A^{-1}$  موجودة، فنقول: إن المصفوفة المربعة  $A$  لها معكوس (invertible)، و  $A^{-1}$  هو معكوس (inverse)  $A$ ، إما إذا كانت  $A^{-1}$  غير موجودة، فإن  $A$  يقال عنها: منفردة (singular). يمكن إثبات أنه إذا وجدت مصفوفة  $A^{-1}$  بحيث إن  $A^{-1}A = I_n$ ، فإن  $AA^{-1} = I_n$ ، إضافة إلى ذلك، توجد مصفوفة واحدة فقط  $A^{-1}$  لها هذه الخاصية.

## A5 مثال

لتكن

$$A^{-1} = \begin{bmatrix} -4 & 9 \\ 1 & -2 \end{bmatrix}.$$

يمكننا فحص أن

$$\begin{bmatrix} -4 & 9 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 2 & 9 \\ 1 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 9 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} -4 & 9 \\ 1 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

وعليه،

$$A^{-1} = \begin{bmatrix} -4 & 9 \\ 1 & -2 \end{bmatrix}.$$

نترك مسائل تحديد وجود  $A^{-1}$  وحسابها إلى مقرر دراسي في الجبر الخطي.

يتوافق مع كل مصفوفة مربعة  $A$  من الدرجة  $n \times n$  عدد يسمى المحددة لـ  $A$ ، ويرمز له بـ  $\det(A)$ ، ويمكن حساب هذا العدد بوصفه جمعاً وطرحاً لضروب معينة للأعداد التي تظهر في المصفوفة  $A$ ، على سبيل المثال: المحددة للمصفوفة  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  من الدرجة  $2 \times 2$  هي  $ad - bc$ . لاحظ أن مصفوفة من الدرجة  $n \times 1$  مدخلاتها أعداد حقيقية، يمكن النظر إليها بوصفها إعطاء إحداثيات نقطة في الفضاء الإقليدي  $\mathbb{R}^n$  ذي البعد  $n$ ، ويضرب مصفوفة عمود واحد كهذه من اليسار بمصفوفة حقيقية  $A$  من الدرجة  $n \times n$ ، تنتج مصفوفة عمود واحد تقابل نقطة في  $\mathbb{R}^n$ ، وهذا الضرب من اليسار بـ  $A$  يعطي دالة من  $\mathbb{R}^n$  إلى نفسها، ومن الممكن إثبات أن قطعة من  $\mathbb{R}^n$  حجمها  $V$  تُرسل من خلال هذا الضرب بـ  $A$  إلى قطعة حجمها  $|\det(A)| \cdot V$ . هذا أحد أسباب أهمية المحددات.

الخصائص الآتية للمحددات لمصفوفتين  $A$  و  $B$  من الدرجة  $n \times n$  ذات أهمية في هذا الكتاب:

1.  $\det(I_n) = 1$
2.  $\det(AB) = \det(A) \det(B)$
3.  $\det(A) \neq 0$ ، إذا وفقط إذا كانت  $A$  مصفوفة لها معكوس.
4. إذا نتجت  $B$  عن  $A$  بتبديل صفين (أو عمودين) من  $A$ ، فإن  $\det(B) = -\det(A)$
5. إذا كانت كل مدخلة لـ  $A$  صفراً فوق القطر الرئيس من الزاوية اليسرى العليا إلى الزاوية اليمنى السفلى، فإن  $\det(A)$  هو ضرب مدخلات هذا القطر. النتيجة نفسها صحيحة إذا كانت المدخلات كلها تحت القطر الرئيس أصفاراً.

## ■ التمارين أ

في التمارين من 1 إلى 9، احسب العبارات الجبرية للمصفوفات المعطاة إذا كانت العملية معرفة.

$$1. \begin{bmatrix} -2 & 4 \\ 1 & 5 \end{bmatrix} + \begin{bmatrix} 4 & -3 \\ 1 & 2 \end{bmatrix}$$

$$2. \begin{bmatrix} 1+i & -2 & 3-i \\ 4 & i & 2-i \end{bmatrix} + \begin{bmatrix} 3 & i-1 & -2+i \\ 3-i & 1+i & 0 \end{bmatrix}$$

$$3. \begin{bmatrix} i & -1 \\ 4 & 1 \\ 3 & -2i \end{bmatrix} - \begin{bmatrix} 3-i & 4i \\ 2 & 1+i \\ 3 & -i \end{bmatrix}$$

$$5. \begin{bmatrix} 3 & 1 \\ -4 & 2 \end{bmatrix} \begin{bmatrix} 1 & 5 & -3 \\ 2 & 1 & 6 \end{bmatrix}$$

$$4. \begin{bmatrix} 1 & -1 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ -1 & 3 \end{bmatrix}$$

$$7. \begin{bmatrix} i & 1 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 3i & 1 \\ 4 & -2i \end{bmatrix}$$

$$6. \begin{bmatrix} 4 & -1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 7 \\ 3 & 7 \end{bmatrix}$$

$$9. \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}^4$$

$$8. \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}^4$$

10. أعطِ مثالاً في  $M_2(\mathbb{Z})$  يبيِّن أن ضرب المصفوفات ليس إبدالياً.

11. أوجد  $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^{-1}$  ، بالتجريب إذا لزم.

12. أوجد  $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & -1 \end{bmatrix}^{-1}$  ، بالتجريب إذا لزم.

13. إذا كانت  $A = \begin{bmatrix} 3 & 0 & 0 \\ 10 & -2 & 0 \\ 4 & 17 & 8 \end{bmatrix}$  ، فأوجد  $\det(A)$ .

14. أثبت أنه إذا كانت  $A, B \in M_n(\mathbb{C})$  لهما معكوس، فإن  $AB$  و  $BA$  لهما معكوس أيضًا.

---

## قائمة المراجع

### Classic Works

أعمال كلاسيكية

1. N. Bourbaki, *Eléments de Mathématique*, Book II of Part I, *Algèbre*. Paris: Hermann, 1942–58.
2. N. Jacobson, *Lectures in Abstract Algebra*. Princeton, N.J.: Van Nostrand, vols. I, 1951, II, 1953, and III, 1964.
3. O. Schreier and E. Sperner, *Introduction to Modern Algebra and Matrix Theory* (English translation), 2nd Ed. New York: Chelsea, 1959.
4. B. L. van der Waerden, *Modern Algebra* (English translation). New York: Ungar, vols. I, 1949, and II, 1950.

### General Algebra Texts

كتب في الجبر العام

5. M. Artin, *Algebra*. Englewood Cliffs, N.J.: Prentice-Hall, 1991.
6. A. A. Albert, *Fundamental Concepts of Higher Algebra*. Chicago: University of Chicago Press, 1956.
7. G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, 3rd Ed. New York: Macmillan, 1965.
8. J. A. Gallian, *Contemporary Abstract Algebra*, 2nd Ed. Lexington, Mass.: D. C. Heath, 1990.
9. I. N. Herstein, *Topics in Algebra*. New York: Blaisdell, 1964.
10. T. W. Hungerford, *Algebra*. New York: Springer, 1974.
11. S. Lang, *Algebra*. Reading, Mass.: Addison-Wesley, 1965.
12. S. MacLane and G. Birkhoff, *Algebra*. New York: Macmillan, 1967.
13. N. H. McCoy, *Introduction to Modern Algebra*. Boston: Allyn and Bacon, 1960.
14. G. D. Mostow, J. H. Sampson, and J. Meyer, *Fundamental Structures of Algebra*. New York: McGraw-Hill, 1963.
15. W. W. Sawyer, *A Concrete Approach to Abstract Algebra*. San Francisco: Freeman, 1959.

### Group Theory

مبرهنة الزمرة

16. W. Burnside, *Theory of Groups of Finite Order*, 2nd Ed. New York: Dover, 1955.
17. H. S. M. Coxeter and W. O. Moser, *Generators and Relations for Discrete Groups*, 2nd Ed. Berlin: Springer, 1965.
18. M. Hall, Jr., *The Theory of Groups*. New York: Macmillan, 1959.
19. A. G. Kurosh, *The Theory of Groups* (English translation). New York: Chelsea, vols. I, 1955, and II, 1956.
20. W. Ledermann, *Introduction to the Theory of Finite Groups*, 4th rev. Ed. New York: Interscience, 1961.
21. J. G. Thompson and W. Feit, "Solvability of Groups of Odd Order." *Pac. J. Math.*, **13** (1963), 775–1029.
22. M. A. Rabin, "Recursive Unsolvability of Group Theoretic Problems." *Ann. Math.*, **67** (1958), 172–194.

**Ring Theory**

مبرهنة الحلقة

23. W. W. Adams and P. Loustanaun, *An Introduction to Gröbner Bases* (Graduate Studies in Mathematics, vol. 3). Providence, R.I.: American Mathematical Society, 1994.
24. E. Artin, C. J. Nesbitt, and R. M. Thrall, *Rings with Minimum Condition*. Ann Arbor: University of Michigan Press, 1944.
25. N. H. McCoy, *Rings and Ideals* (Carus Monograph No. 8). Buffalo: The Mathematical Association of America; LaSalle, Ill.: Open Court, 1948.
26. N. H. McCoy, *The Theory of Rings*. New York: Macmillan, 1964.

**Field Theory**

مبرهنة الحقل

27. E. Artin, *Galois Theory* (Notre Dame Mathematical Lecture No. 2), 2nd Ed. Notre Dame, Ind.: University of Notre Dame Press, 1944.
28. O. Zariski and P. Samuel, *Commutative Algebra*. Princeton, N.J.: Van Nostrand, vol. I, 1958.

**Number Theory**

مبرهنة الأعداد

29. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th Ed. Oxford: Clarendon Press, 1960.
30. S. Lang, *Algebraic Numbers*. Reading, Mass.: Addison-Wesley, 1964.
31. W. J. LeVeque, *Elementary Theory of Numbers*, Reading, Mass.: Addison-Wesley, 1962.
32. W. J. LeVeque, *Topics in Number Theory*. Reading, Mass.: Addison-Wesley, 2 vols., 1956.
33. T. Nagell, *Introduction to Number Theory*. New York: Wiley, 1951.
34. I. Nivin and H. S. Zuckerman, *An Introduction to the Theory of Numbers*. New York: Wiley, 1960.
35. H. Pollard, *The Theory of Algebraic Numbers* (Carus Monograph No. 9). Buffalo: The Mathematical Association of America; New York: Wiley, 1950.
36. D. Shanks, *Solved and Unsolved Problems in Number Theory*. Washington, D.C.: Spartan Books, vol. I, 1962.
37. B. M. Stewart, *Theory of Numbers*, 2nd Ed. New York: Macmillan, 1964.
38. J. V. Uspensky and M. H. Heaslet, *Elementary Number Theory*. New York: McGraw-Hill, 1939.
39. E. Weiss, *Algebraic Number Theory*. New York: McGraw-Hill, 1963.

**Homological Algebra**

الجبر الشباهي

40. J. P. Jans, *Rings and Homology*. New York: Holt, 1964.
41. S. MacLane, *Homology*. Berlin: Springer, 1963.

**Other References**

مراجع إضافية

42. A. A. Albert (ed.), *Studies in Modern Algebra* (MAA Studies in Mathematics, vol. 2). Buffalo: The Mathematical Association of America; Englewood Cliffs, N.J.: Prentice-Hall, 1963.
43. E. Artin, *Geometric Algebra*. New York: Interscience, 1957.
44. R. Courant and R. Robbins, *What Is Mathematics?* Oxford University Press, 1941.
45. H. S. M. Coxeter, *Introduction to Geometry*, 2nd Ed. New York: Wiley, 1969.
46. R. H. Crowell and R. H. Fox, *Introduction to Knot Theory*. New York: Ginn, 1963.
47. H. B. Edgerton, *Elements of Set Theory*. San Diego: Academic Press, 1977.
48. C. Schumacher, *Chapter Zero*. Reading, Mass.: Addison-Wesley, 1996.

| الرموز   |  |
|--|--|
| $\in, a \in S$   | 1، انتماء  |
| $\emptyset$  | 1، مجموعة خالية  |
| $\notin, a \notin S$                                     | 1، عدم انتماء  |
| $\{x P(x)\}$   | 1، مجموعة كل $x$ بحيث إن $P(x)$  |
| $B \subseteq A$  | 2، احتواء مجموعات  |
| $B \subset A$  | 2، مجموعة جزئية $B \neq A$   |
| $A \times B$   | 3، ضرب ديكارتي لمجموعات  |
| $\mathbb{Z}$   | 3، الأعداد الصحيحة   |
| $\mathbb{Q}$   | 3، الأعداد النسبية   |
| $\mathbb{R}$   | 3، الأعداد الحقيقية  |
| $\mathbb{C}$   | 3، الأعداد المركبة   |
| $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$               | 3، العناصر الموجبة من $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$                 |
| $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ | 3، العناصر غير الصفرية من $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ |
| $\mathcal{P}$  | 3، علاقة   |
| $ A $  | 50، بوصفها رتبة زمرة: 4، عدد العناصر في $A$                                |
| $\phi: A \rightarrow B$                                  | 4، دالة $\phi$ من $A$ إلى $B$  |
| $\phi(a)$  | 4، صورة العنصر $a$ تحت تأثير $\phi$  |
| $\phi[A]$  | 4، صورة المجموعة $A$ تحت تأثير $\phi$                                      |
| $\leftrightarrow$  | 4، تقابل أحادي   |
| $\phi^{-1}$  | 5، معكوس الدالة $\phi$   |
| $\aleph_0$   | 5، عدد عناصر $\mathbb{Z}^+$  |
| $\bar{x}$  | 6، خلية تحوي $x \in S$ في تجزئة لـ $S$                                     |
| $\equiv n, a \equiv b \pmod{n}$                          | 7، تطابق مقياس $n$   |
| $\mathcal{P}(A)$   | 9، مجموعة القوى لـ $A$   |
| $U$  | 15، مجموعة كل $z \in \mathbb{C}$ بحيث إن $ z  = 1$                         |
| $\mathbb{R}_c$   | 16، مجموعة كل $x \in \mathbb{R}$ بحيث إن $0 \leq x < c$                    |
| $+_c$  | 16، جمع مقياس $c$  |
| $U_n$  | 18، زمرة الجذور ذات الرتبة $n$ للواحد                                      |
| $\mathbb{Z}_n$   | $\{0, 1, 2, \dots, n-1\}$ ، 18   |
|  | 54، الزمرة الدورية $\{0, 1, \dots, n-1\}$ بالنسبة إلى الجمع مقياس $n$      |
|  | 137، زمرة صفوف الرواسب مقياس $n$   |
|  | 169، الحلقة $\{0, 1, \dots, n-1\}$ بالنسبة إلى الجمع والضرب مقياس $n$      |
| $*, a*b$   | 20، عملية ثنائية   |
| $\circ, f \circ g, \sigma \tau$                          | 22، 76، تركيب دوال   |

|  |   |
|--|---|
| $\langle S, * \rangle$                   | بنية ثنائية ، 29  |
| $\simeq, S \simeq S'$                    | تماثل بني ، 30  |
| $e$                                      | عنصر محايد ، 32   |
| $M_{m \times n}(S)$                      | مصفوفات من الدرجة $m \times n$ بمدخلات من $S$ ، 477 ، 40    |
| $M_n(S)$                                 | مصفوفات من الدرجة $n \times n$ بمدخلات من $S$ ، 477 ، 40    |
| $GL(n, \mathbb{R})$                      | زمرة خطية عامة من الدرجة $n$ ، 40                           |
| $\det(A)$                                | محددة المصفوفة المربعة $A$ ، 479 ، 46                       |
| $a^{-1}, -a$                             | معكوس أو نظير $a$ ، 49                                      |
| $H \leq G; K \leq L$                     | احتواء بنية جزئية؛ 50 ، احتواء زمرة جزئية                   |
| $H < G; K < L$                           | بنية جزئية $K \neq L$ ؛ 50 ، زمرة جزئية $H \neq G$          |
| $\langle a \rangle$                      | زمرة جزئية دورية مولدة بـ $a$ ، 54                          |
| $n\mathbb{Z}$                            | مثالي رئيس مولد بـ $a$ ، 250                                |
| $\gcd$                                   | زمرة جزئية من $\mathbb{Z}$ مولدة بـ $n$ ، 54                |
| $\bigcap_{i \in I} S_i$                  | حلقة جزئية (مثالي) من $\mathbb{Z}$ مولدة بـ $n$ ، 250 ، 169 |
| $S_1 \cap S_2 \cap \dots \cap S_n$       | قاسم مشترك أعظم ، 395 ، 258 ، 62                            |
| $S_A$                                    | تقاطع مجموعات ، 69  |
| $\iota$                                  | زمرة تبديلات $A$ ، 77                                       |
| $S_n$                                    | دالة محايدة ، 77  |
| $n!$                                     | زمرة التناظر على $n$ حرف ، 78                               |
| $D_n$                                    | مضروب $n$ ، 78  |
| $A_n$                                    | زمرة زوجية من الدرجة $n$ ، 79                               |
| $aH, a + H$                              | زمرة متناوبة على $n$ حرف ، 93                               |
| $Ha, H + a$                              | مجموعة مشاركة يسرى لـ $H$ تحوي $a$ ، 97                     |
| $(G:H)$                                  | مجموعة مشاركة يمنى لـ $H$ تحوي $a$ ، 97                     |
| $\varphi$                                | دليل $H$ في $G$ ، 101                                       |
| $\prod_{i=1}^n S_i$                      | دالة-فاي لأويلر ، 187 ، 104                                 |
| $S_1 \times S_2 \times \dots \times S_n$ | ضرب ديكارتي لمجموعات ، 104                                  |
| $\prod_{i=1}^n G_i$                      | ضرب مباشر لزمرة ، 105 ، 104                                 |
| $\bigoplus_{i=1}^n G_i$                  | جمع مباشر لزمرة ، 105                                       |
| $\text{lcm}$                             | مضاعف مشترك أصغر ، 107                                      |
| $\bar{G}_i$                              | زمرة جزئية طبيعية من $\prod_{i=1}^n G_i$ ، 107              |
| $\phi_c$                                 | تشاكل تعويض ، 126   |
| $\pi_i$                                  | إسقاط على المركبة ذات الترتيب $i$ ، 127                     |
| $\phi^{-1}[B]$                           | صورة معكوسة للمجموعة $B$ تحت تأثير $\phi$ ، 128             |
| $\text{Ker}(\phi)$                       | نواة التشاكل $\phi$ ، 129                                   |

|                                   |  |
|-----------------------------------|--|
| $G/N; R/N$                        | 242 ، حلقة العامل؛ 137 ، زمرة العامل                               |
| $\gamma$                          | 139 ، 140 ، دالة صفوف البواقي القانونية                            |
| $i_g$                             | 141 ، تماثل ذاتي داخلي   |
| $Z(G)$                            | 150 ، مركز الزمرة $G$  |
| $C$                               | 150 ، زمرة المبدلات الجزئية  |
| $X_g$                             | 157 ، مجموعة جزئية مؤلفة من عناصر $X$ المثبتة بـ $g$               |
| $G_x$                             | 157 ، زمرة توحد الخصائص الجزئية المؤلفة من عناصر $G$ التي تثبت $x$ |
| $Gx$                              | 158 ، مدار $x$ تحت تأثير $G$                                       |
| $R[x]$                            | 200 ، حلقة كثيرات حدود بمعاملات من $R$                             |
| $F(x)$                            | 201 ، حقل خوارج القسمة لـ $F[x]$                                   |
| $F(x_1, \dots, x_n)$              | 201 ، حقل دوال نسبية في $n$ مجهول                                  |
| $\Phi_p(x)$                       | 216 ، 217 ، كثيرة حدود دورية من الدرجة $p - 1$                     |
| $End(A)$                          | 221 ، تشاكلات $A$ الداخلية   |
| $RG$                              | 223 ، حلقة الزمرة  |
| $FG$                              | 223 ، جبر الزمرة على الحقل $F$                                     |
| $\mathbb{H}$                      | 224 ، 225 ، مربعيات  |
| $R[[x]]$                          | 231 ، حلقة متسلسلات قوى شكلية في $x$ على $R$                       |
| $F((x))$                          | 231 ، حقل متسلسلات لورنت شكلية في $x$ على $F$                      |
| $F[\mathbf{x}]$                   | 255 ، حلقة كثيرات حدود في $x_1, \dots, x_n$ على $F$                |
| $V(S)$                            | 255 ، متنوع جبرية لكثيرات حدود في $S$                              |
| $\langle b_1, \dots, b_r \rangle$ | 255 ، مثالي مولد بالعناصر $b_1, \dots, b_r$                        |
| $lt(f)$                           | 260 ، حد أمامي لكثيرة الحدود $f$                                   |
| $lp(f)$                           | 260 ، ضرب قوى لـ $lt(f)$   |
| $irr(\alpha, F)$                  | 269 ، كثيرة حدود غير مختزلة لـ $\alpha$ على $F$                    |
| $deg(\alpha, F)$                  | 269 ، درجة $\alpha$ على $F$  |
| $F(\alpha)$                       | 270 ، حقل ناتج من ضم $\alpha$ إلى الحقل $F$                        |
| $[E : F]$                         | 283 ، درجة $E$ على $F$   |
| $F(\alpha_1, \dots, \alpha_n)$    | 285 ، حقل ناتج عن ضم $\alpha_1, \dots, \alpha_n$ إلى الحقل $F$     |
| $\overline{F}_E$                  | 286 ، إغلاق جبري لـ $F$ في $E$                                     |
| $\overline{F}$                    | 287 ، 288 ، إغلاق جبري لـ $F$                                      |
| $GF(p^n)$                         | 300 ، حقل جالوا من الرتبة $p^n$                                    |
| $HN$                              | 308 ، مجموعة ضرب   |
| $H \vee N$                        | 308 ، موصل زمر جزئية   |
| $N[H]$                            | 323 ، منظم $H$   |
| $F[A]$                            | 341 ، 342 ، زمرة حرة على $A$                                       |
| $(x_j : r_i)$                     | 348 ، تمثيل زمرة   |
| $\partial_n$                      | 357 ، تشاكل حدود   |

|                                    |  |
|------------------------------------|--|
| $C_n(X)$                           | $X$ ـل $n$ الرتبة من سلاسل ، 358                                       |
| $Z_n(X)$                           | $X$ ـل $n$ الرتبة من دورات ، 359                                       |
| $B_n(X)$                           | $X$ ـل $n$ الرتبة من حدود ، 359  |
| $H_n(X)$                           | $X$ ـل $n$ الرتبة ذات الترتيب ، 361                                    |
| $\delta^{(n)}$                     | تشاكل حدود مقابلة ، 363  |
| $C^{(n)}(X)$                       | $X$ ـل $n$ الرتبة من سلاسل مقابلة ، 363                                |
| $Z^{(n)}(X)$                       | $X$ ـل $n$ الرتبة من دورات مقابلة ، 363                                |
| $H^{(n)}(X)$                       | $X$ ـل $n$ الرتبة من حدود مقابلة ، 363                                 |
| $H^{(n)}(X)$                       | $X$ ـل $n$ الرتبة ذات الترتيب مقابلة ، 363                             |
| $S^n$                              | $n$ كرة من الرتبة ، 364  |
| $E^n$                              | $n$ خلية ذات البعد ، 364   |
| $\chi(X)$                          | $X$ مميز أويلر ـل ، 374  |
| $f_{*n}$                           | $f: X \rightarrow Y$ تشاكل شباه مولد من ، 375 ، 381                    |
| $\langle A, \partial \rangle$      | سلسلة مركبة ، 381  |
| $\bar{\partial}_k$                 | مؤثر حدود نسبي ، 382   |
| $H_k(A/A')$                        | زمرة شباهية نسبية ذات الترتيب $k$ للسلسلة المركبة $A$ مقياس $A'$ ، 383 |
| $H_k(X, Y)$                        | شبه نسبي ذو الترتيب $k$ لمركب المبسطات $X$ مقياس $Y$ ، 383             |
| $a   b$                            | $a$ تقسم ( $\div$ ) $b$ ، 389  |
| UFD                                | حلقة تامة وحيدة التحليل ، 390  |
| PID                                | حلقة المثاليات الرئيسة التامة ، 391                                    |
| $\bigcup_{i \in I} S_i$            | اتحاد مجموعات ، 391  |
| $S_1 \cup S_2 \cup \dots \cup S_n$ |  |
| $v$                                | معيار إقليدي ، 401   |
| $N(\alpha)$                        | $\alpha$ معيار ، 408 ، 410 ، 455                                       |
| $\psi_{\alpha, \beta}$             | تماثل ترافق ـل $F(\alpha)$ مع $F(\beta)$ ، 416                         |
| $E_{\{\sigma_i\}}, E_H$            | حقل جزئي من $E$ مثبت بكل $\sigma_i$ أو كل $\sigma \in H$ ، 419         |
| $G(E/F)$                           | زمرة التماثلات الذاتية ـل $E$ على $F$ ، 420                            |
| $\{E : F\}$                        | $E$ دليل على $F$ ، 428   |