الوحدة السادسة

امتداد الحقول
Extension Fields

الفصل 29 مقدّمة لامتداد الحقول
Introduction to Extension Fields

الفصل 30 فضاء المتجهات
Vector Spaces

الفصل 31 الامتدادات الجبرية
Algebraic Extension

الفصل 32 إنشاءات هندسية [1]
Geometric Constructions

الفصل 33 الحقول المنتهية
Finite Fields

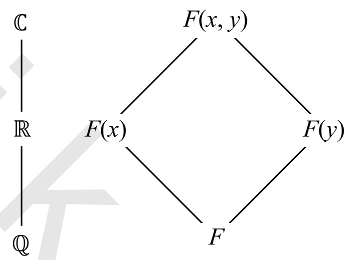
[1] الفصل 32 غير متطلب لباقي الكتاب

الفصل 29 مقدّمة لامتداد الحقول Introduction to Extension Fields

الهدف الأساسي المراد تحقيقه

إننا في الوضع الذي يمكننا من تحقيق **هدفنا الأساسي**، والذي يسعى بصورة مبسطة إلى إثبات أنّ لكل كثيرة حدود غير ثابتة صفرًا، وهذا ما ستنص عليه المبرهنة 3.29. سنقدم في البداية بعض التعريفات لأفكار سابقة.

1.29 تعريف يكون الحقل E **امتدادًا للحقل F (*Field Extension*)**، إذا كان $F \leq E$ ■



الشكل 2.29

لذا، فإنّ $\mathbb{R}$ امتداد للحقل $\mathbb{Q}$، و $\mathbb{C}$ امتداد للحقلين $\mathbb{R}$ و $\mathbb{Q}$.

وكما في دراسة الزمر، سيكون من المناسب دائمًا استخدام الرسم التخطيطي للحقول الجزئية لتوضيح امتدادات الحقول، حيث يكون الحقل الأكبر في الأعلى كما هو موضح في الشكل 2.29، ويسمى الشكل الذي يكون فيه عمود واحد من الحقول برج الحقول **(a tower of fields)**، كما هو موضح إلى اليسار في الشكل 2.29.

لنبدأ في تحقيق الهدف الأساسي، فهذه النتيجة المهمة والعظيمة تأتي بصورة سريعة وممتازة باستخدام الطرق التي باتت في متناول اليد.

3.29 مبرهنة (**مبرهنة كرونكر *Kronecker's Theorem*** (هدف: **أساسي**)، ليكن F حقلاً، ولتكن $f(x)$ كثيرة حدود غير ثابتة في $F[x]$ ، عندئذ، يوجد امتداد E للحقل F و $\alpha \in E$، حيث إنّ $f(\alpha)=0$.

البرهان بحسب المبرهنة 20.23، يمكن تحليل $f(x)$ في $F[x]$ إلى كثيرات حدود غير مختزلة على F، لتكن $p(x)$ إحدى كثيرات الحدود غير المختزلة في هذا التحليل، فمن الواضح أنه يكفينا أن نجد امتداد E للحقل F يحوي عنصرًا α، حيث إنّ $p(\alpha)=0$.

بحسب المبرهنة 25.27، $\langle p(x)\rangle$ مثالي أعظمي في $F[x]$، وبهذا يكون $F[x]/\langle p(x)\rangle$ حقلًا، يمكننا الادعاء أنّ F يطابق حقلًا جزئيًّا من $F[x]/\langle p(x)\rangle$ بطريقة طبيعية باستخدام الدالة $\psi: F \to F[x]/\langle p(x)\rangle$ المعرّفة بـ:

$$\psi(a) = a + \langle P(x) \rangle$$

حيث $a \in F$. هذه الدالة أحادية؛ لأنه إذا كان $\psi(a) = \psi(b)$، بمعنى أنّ $a + \langle P(x) \rangle = b + \langle P(x) \rangle$ حيث $a,b \in F$، فإنّ $(a-b) \in \langle P(x) \rangle$، وهكذا، فإنّ $(a-b)$ يجب أن تكون مضاعفًا لكثير الحدود $p(x)$، التي تكون درجتها ≤ 1.

الآن، $a, b \in F$ يؤدي إلى أنّ $a - b \in F$، وهكذا، فيجب أن يكون $a - b = 0$، أي $a = b$. نعرّف الجمع والضرب في $F[x]/\langle p(x) \rangle$ باختيار أيّ ممثلين، وهكذا يمكننا اختيار $a \in (a + \langle P(x) \rangle)$. إذن، ψ تمثل تشاكلاً يربط F بطريقة أحادية وغامرة بحقل جزئي من $F[x]/\langle p(x) \rangle$، ونطابق F مع $\{a + \langle p(x) \rangle \mid a \in F\}$ باستخدام الدالة ψ. وهكذا، نضع $E = F[x]/\langle p(x) \rangle$ بوصفه امتدادًا للحقل F، فنكون هكذا قد صنعنا الامتداد المطلوب E للحقل F، ويبقى علينا إثبات أنّ E يحوي صفر ألـ $p(x)$، لنعرّف

$$\alpha = x + \langle p(x) \rangle.$$

وهكذا، فإنّ $\alpha \in E$. باستخدام تشاكل التعويض $\phi_\alpha : F[x] \to E$ الذي سبق تعريفه في المبرهنة 4.22، إذا كانت $p(x) = a_0 + a_1 x + .. + a_n x^n$ حيث $a_i \in F$، فإن:

$$\phi_\alpha(p(x)) = a_0 + a_1(x + \langle p(x) \rangle) + \cdots + a_n(x + \langle p(x) \rangle)^n$$

■ نبذة تاريخية

عُرِفَ ليوبولد كرونكر بإصراره على بناء الإنشاءات الرياضية، فقد ذكر في ملاحظة له: "إنّ الله خلق الأعداد الصحيحة، وكل ما عداها هو من عمل الإنسان"؛ لهذا أراد أن ينشئ "مجالات نسبية" (حقول) بالاستعانة بتوافر الأعداد الصحيحة وغير المعينات.

لم يؤمن كرونكر في البداية بالأعداد الحقيقية أو المركبة، وذلك وبحسب تطلعاته بأنّ هذه الحقول لا يمكن تعيينها بطريقة إنشائية؛ لذلك، أنشأ في بحث له عام 1881م حقلاً ممتدًا بمنتهى البساطة، بأن ألحق بحقلٍ معطى الجذر α لكثيرة الحدود غير المختزلة من الدرجة n ، $p(x)$، أي إنّ حقله الجديد تكوّن من تعبيرات نسبية في عناصر الحقل الأصلي والجذر α مع الشرط أنّ $p(\alpha) = 0$.

إثبات المبرهنة المذكورة في الكتاب (مبرهنة 3.29) تمت كتابته في القرن العشرين، وقد أكمل كرونكر أطروحته للدكتوراة عام 1845م في جامعة برلين، وقام بعدها بإدارة أعمال العائلة سنين عدة، ثمّ اعتمد على نفسه ماليًّا، فعاد إلى برلين حيث انتخب في أكاديمية العلوم، وسُمِحَ له بأن يحاضر في الجامعة.

صار كرونكر في تقاعده أستاذًا في جامعة برلين، وأدار بمشاركة كارل وايرستراس (*Karl Weierstrass*) (1815 – 1897) ندوة رياضية غاية في التأثير.

في $E = F[x]/\langle p(x)\rangle$ ولكن يمكننا الحساب في $F[x]/\langle p(x)\rangle$؛ باختيار الممثلات وx هي الممثل للمجموعة المشاركة $\alpha = x + \langle p(x)\rangle$. وهكذا:

$$p(\alpha) = (a_0 + a_1 x + \ldots + a_n x^n) + \langle p(x)\rangle$$

$$= p(x) + \langle p(x)\rangle = \langle p(x)\rangle = 0$$

في $F[x]/\langle p(x)\rangle$ ، وهكذا نكون قد أوجدنا عنصر α في $E = F[x]/\langle p(x)\rangle$، بحيث إنّ $p(\alpha) = 0$، ما يعني أنّ $f(\alpha) = 0$. ♦

وإليك توضيح البناء الذي تمّ في إثبات المبرهنة 3.29 بهذين المثالين:

4.29 مثال ليكن $F = \mathbb{R}$، ولتكن $f(x) = x^2 + 1$ التي ليس لها أصفار في $\mathbb{R}$، وبهذا فهي غير مختزلة على $\mathbb{R}$ بحسب المبرهنة 10.23. إذن: $\langle x^2 + 1\rangle$ مثالي أعظمي في $\mathbb{R}[x]$، ما يؤدي إلى أن يكون $\mathbb{R}[x]/\langle x^2 + 1\rangle$ حقلاً. طابق بين $r \in \mathbb{R}$ و $r + \langle x^2 + 1\rangle$ في $\mathbb{R}[x]/\langle x^2 + 1\rangle$، يمكننا أن نعدّ $\mathbb{R}$ بوصفه حقلاً جزئيًا من $E = \mathbb{R}[x]/\langle x^2 + 1\rangle$، لتكن

$$\alpha = x + \langle x^2 + 1\rangle$$

بالحساب في $\mathbb{R}[x]/\langle x^2 + 1\rangle$، نجد أن:

$$\begin{aligned}\alpha^2 + 1 &= (x + \langle x^2 + 1\rangle)^2 + (1 + \langle x^2 + 1\rangle)\\ &= (x^2 + 1) + \langle x^2 + 1\rangle = 0.\end{aligned}$$

وهكذا، فإنّ α تمثل صفرًا لـ $x^2 + 1$، وسوف نطابق بين $\mathbb{R}[x]/\langle x^2 + 1\rangle$ و $\mathbb{C}$ في ختام هذا الفصل. ▲

5.29 مثال ليكن $F = \mathbb{Q}$، وخذ في الحسبان $f(x) = x^4 - 5x^2 + 6$، ففي هذه الحالة تتحلل $f(x)$ في $\mathbb{Q}[x]$ إلى $(x^2 - 2)(x^2 - 3)$، وكلا العاملين غير مختزلين على $\mathbb{Q}$، كما رأينا سابقًا. ويمكننا البدء مع $x^2 - 2$، وإنشاء امتداد E للحقل $\mathbb{Q}$ يحوي α، بحيث إنّ $\alpha^2 - 2 = 0$، أو يمكننا بناء امتداد K للحقل $\mathbb{Q}$ يحوي العنصر β، حيث $\beta^2 - 3 = 0$. الإنشاء في الحالتين هو تمامًا كما في المثال 4.29. ▲

العناصر الجبرية والمتسامية.

كما ذكرنا سابقًا، سنكرّس معظم بقية هذا الكتاب لدراسة أصفار كثيرات الحدود، حيث نستهل هذه الدراسة بوضع عناصر الامتداد E للحقل F ضمن أحد صنفين.

6.29 تعريف يكون العنصر α الذي ينتمي إلى الامتداد E للحقل F **جبريًا (algebraic)** على F، إذا كان $f(\alpha)=0$، حيث $f(x) \in F[x]$ كثيرة حدود غير صفرية، وإذا كانت α غير جبري على F، فإنّ α **متسامٍ (transcendental)** على F. ■

7.29 مثال $\mathbb{C}$ تمدد للحقل $\mathbb{Q}$، ولأنّ $\sqrt{2}$ صفر لـ $x^2 - 2$، فإنّ $\sqrt{2}$ عنصر جبري على $\mathbb{Q}$، وكذلك i عنصر جبري على $\mathbb{Q}$؛ لأنه صفر لـ $x^2 + 1$. ▲

8.29 مثال من المعروف (ولكن ليس من السهل إثبات) أنّ العددين الحقيقيين π و e متساميان على $\mathbb{Q}$، حيث e هي الأساس للوغاريتم الطبيعي. ▲

لا نتحدث ببساطة عن كثيرة حدود غير مختزلة، بل عن كثيرة حدود غير مختزلة على F، كذلك لا نتحدث ببساطة عن عنصر جبري، ولكن عن عنصر جبري على F. التوضيح الآتي يبيّن السبب في هذا.

9.29 مثال العدد الحقيقي π متسامٍ على $\mathbb{Q}$، كما ذكرنا في المثال 8.29، ولكن π جبري على $\mathbb{R}$؛ لأنه صفر لـ $(x-\pi) \in \mathbb{R}[x]$. ▲

10.29 مثال من السهل أن نرى أنّ العدد الحقيقي $\sqrt{1+\sqrt{3}}$ جبري على $\mathbb{Q}$؛ وذلك لأنه إذا كانت $\alpha = \sqrt{1+\sqrt{3}}$، فإنّ $\alpha^2 = 1+\sqrt{3}$، وهكذا فإنّ $\alpha^2 - 1 = \sqrt{3}$ و $(\alpha^2-1)^2=3$ إذن $\alpha^4 - 2\alpha^2 - 2 = 0$، وبهذا تكون α صفرًا لـ $x^4 - 2x^2 - 2$، التي تمثل عنصرًا في $\mathbb{Q}[x]$. ▲

للربط بين هذه الأفكار وتلك التي في نظرية الأعداد، نقدم التعريف الآتي:

11.29 تعريف يسمى العنصر الجبري في $\mathbb{C}$ على $\mathbb{Q}$ **عددًا جبريًا (*algebraic number*)**، **والعدد المتسامي (*transcendental number*)** هو عنصر في $\mathbb{C}$ متسامٍ على $\mathbb{Q}$. ■

هناك الكثير من الجمال في نظرية الأعداد الجبرية (انظر المراجع).

تعطي النظرية الآتية وصفًا مفيدًا للعناصر الجبرية والمتسامية على الحقل F في التمدد E، إضافة إلى أنها تبين أهمية تشاكل التعويض ϕ_α. لاحظ مرة أخرى أننا نصف مفاهيمنا باستخدام الدوال.

12.29 مبرهنة ليكن الحقل E تمددًا للحقل F، ولتكن $\alpha \in E$، ليكن $\phi_\alpha : F[x] \to E$ تشاكل التعويض من $F[x]$ إلى E، بحيث إنّ $\phi_\alpha(a) = a$ لكل $a \in F$ و $\phi_\alpha(x) = \alpha$، ويكون α متساميًا على F، إذا وفقط إذا كان ϕ_α تماثلًا من $F[x]$ مع مجال جزئي من E، بمعنى أنه إذا وفقط إذا كانت ϕ_α دالة أحادية.

البرهان يكون العنصر α متسامياً على F، إذا وفقط إذا كان $f(\alpha) \neq 0$ لكل كثير حدود غير صفري $f(x) \in F[x]$، الذي يكون صحيحًا (وبحسب التعريف) إذا وفقط إذا كان $\phi_\alpha(f(x)) \neq 0$ لكل كثير حدود غير صفري $f(x) \in F[x]$، الذي يكون صحيحًا إذا وفقط إذا كانت نواة ϕ_α تساوي $\{0\}$، أي إذا وفقط إذا كانت ϕ_α دالة أحادية. ♦

كثيرة الحدود غير المختزلة لـ α على F

ليكن التمدد $\mathbb{R}$ للحقل $\mathbb{Q}$، ونعلم أنّ $\sqrt{2}$ جبري على $\mathbb{Q}$؛ لأنه صفر لـ $x^2 - 2$، وبالطبع، فإنّ $\sqrt{2}$ صفر كذلك لـ $x^3 - 2x$ ولـ $x^4 - 3x^2 + 2 = (x^2 - 2)(x^2 - 1)$. كثيرتا الحدود هاتان – واللتان يكون $\sqrt{2}$ صفرًا لهما – من مضاعفات $x^2 - 2$. حيث تثبت النظرية الآتية أنّ هذا توضيح للحالة العامة، وستؤدي هذه النظرية دورًا محوريًّا في عملنا المقبل.

13.29 مبرهنة ليكن الحقل E تمددًا للحقل F، ولتكن $\alpha \in E$، حيث α جبرية على F، فإنه يوجد كثيرة حدود غير مختزلة $p(x) \in F[x]$ بحيث $p(\alpha) = 0$، كثيرة الحدود غير المختزلة $p(x)$ يمكن تحديدها بصورة وحيدة مع الضرب في عامل ثابت من F، وتكون كثيرة حدود من أصغر درجة ≤ 1 في $F[x]$، بحيث تكون α صفراً لها، فإذا كان $f(\alpha) = 0$، حيث $f(x) \in F[x]$ و $f(x) \neq 0$، فإن $p(x)$ تقسم $f(x)$.

البرهان ليكن ϕ_α تشاكل التعويض من $F[x]$ إلى E المعطى في المبرهنة 4.22، فتكون نواة ϕ_α مثاليًّا، وبحسب المبرهنة 24.27 يجب أن يكون مثالي رئيس متولد من عنصر $p(x) \in F[x]$. يتكوّن $\langle p(x) \rangle$ من تلك العناصر في $F[x]$، التي يكون α صفرًا لها، وهكذا، فإذا كان $f(\alpha) = 0$ و $f(x) \neq 0$، فإنّ $f(x) \in \langle p(x) \rangle$، ما يعني أنّ $p(x)$ تقسم $f(x)$. إذن، $p(x)$ كثيرة حدود من أصغر درجة ≤ 1، بحيث تكون α صفراً له، وكل كثيرة حدود تحقق هذا الشرط ومن درجة $p(x)$ نفسها، يجب أن تكون على الصورة $(a)\, p(x)$، حيث $a \in F$.

يبقى فقط أن نثبت أنّ $p(x)$ غير مختزلة، فإذا كان $p(x) = r(x)\, s(x)$ يمثل تحليلاً لـ $p(x)$ لكثيرات حدود من درجة أصغر، فإنّ $p(\alpha) = 0$ يؤدي إلى أنّ $r(\alpha)\, s(\alpha) = 0$، وهكذا، فإما أن يكون $r(\alpha) = 0$، أو $s(\alpha) = 0$؛ لأن E حقل، وهذا يناقض الحقيقة أنّ درجة $p(x)$ أصغر درجة ≤ 1 بحيث $p(\alpha) = 0$. وهكذا، فإنّ $p(x)$ غير مختزلة. ♦

بالضرب في ثابت مناسب من F، يمكننا الافتراض أنّ معامل أكبر قوة تظهر لـ x في $p(x)$ في المبرهنة 13.29 تساوي (1)، وتسمى كثيرة الحدود هذه، الذي يكون (1) معامل أكبر قوة تظهر لـ x فيها **كثيرة حدود أحادية** (***monic polynomial***).

14.29 تعريف ليكن الحقل E امتدادًا للحقل F، ولتكن $\alpha \in E$ جبرية على F، فتسمى كثيرة الحدود الأحادية الوحيدة $p(x)$ الذي تمتع بالصفات المذكورة في المبرهنة 13.29 **كثيرة الحدود غير المختزلة لـ α على F (*irreducible polynomial for* α *over F*)**، وسيرمز لها بالرمز $\operatorname{irr}(\alpha,F)$، وتسمى درجة $\operatorname{irr}(\alpha,F)$ **بدرجة α على F (*degree of* α *over F*)** ، وسيرمز لها بـ $\deg(\alpha, F)$. ■

15.29 مثال نعلم أنّ $\operatorname{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$، وبالعودة إلى المثال 10.29، نرى أنّ $\alpha = \sqrt{1+\sqrt{3}}$ عنصر في $\mathbb{R}$، و α صفر لـ $x^4 - 2x^2 - 2$ ، التي تقع في $\mathbb{Q}[x]$، ولأنّ $x^4 - 2x^2 - 2$ غير مختزلة على $\mathbb{Q}$ (بحسب أيزنستاين مع $p = 2$، أو بتطبيق طريقة مثال 14.23)، فإننا نرى أنّ:

$$\operatorname{irr}(\sqrt{1+\sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2$$

وبهذا، فإنّ $\sqrt{1+\sqrt{3}}$ جبري على $\mathbb{Q}$ من الدرجة 4. ▲

وكما يجب أن نتحدث عن α بوصفه عنصرًا جبريًّا على F وليس مجرد جبري، فيجب أن نتحدث عن درجة α على F وليس مجرد درجة α، وبوصفه توضيحًا بسيطًا، فإنّ $\sqrt{2} \in \mathbb{R}$ جبري من الدرجة 2 على $\mathbb{Q}$، ولكنه جبري من الدرجة 1 على $\mathbb{R}$؛ لأنّ $\operatorname{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$.

يعود التقدم السريع في النظرية هنا إلى تقنيات التشاكل ونظرية المثاليات، التي هي تحت تصرفنا الآن، لاحظ بصورة خاصة استخدامنا الثابت لتشاكل التعويض ϕ_α.

الامتدادات البسيطة

ليكن الحقل E امتدادًا للحقل F، ولتكن $\alpha \in E$، وليكن ϕ_α تشاكل التعويض من $F[x]$ إلى E، بحيث $\phi_\alpha(a) = a$ لكل $a \in F$ و $\phi_\alpha(x) = \alpha$، كما في المبرهنة 4.22 يمكن أن نعدّ حالتين، هما:

الحالة الأولى: افترض أنّ α جبري على F، فبحسب المبرهنة 13.29 تكون نواة ϕ_α تساوي $\langle \operatorname{irr}(\alpha,F)\rangle$، وبحسب المبرهنة 25.27 فإنّ $\langle \operatorname{irr}(\alpha,F)\rangle$ مثالي أعظمي في $F[x]$، وبهذا يكون $\phi_\alpha[F[x]]$ حقلاً متماثلاً مع الصورة $F[x]/\langle \operatorname{irr}(\alpha, F)\rangle$ في E، وهذا الحقل الجزئي $\phi_\alpha[F[x]]$ من E هو أصغر حقل جزئي من E يحوي كلًا من F و α، وسنرمز لهذا الحقل بـ $F(\alpha)$.

الحالة الثانية: افترض أنّ α متسام على F، فبحسب المبرهنة 12.29 يكون ϕ_α تماثلاً من $F[x]$ إلى مجال جزئي من E، وفي هذه الحالة لا يكون $\phi_\alpha[F[x]]$ حقلًا، وإنّما مجال صحيح، وسنرمز له بـ $F[\alpha]$، وبحسب النتيجة 8.21، فإنّ E يحتوي على حقل خوارج القسمة لـ $F[\alpha]$، الذي يكون أصغر حقل جزئي من E يحوي كلاً من F وα، وكما في الحالة الأولى، فسنرمز لهذا الحقل بـ $F(\alpha)$.

16.29 مثال لأنّ π متسام على $\mathbb{Q}$، فإنّ الحقل $\mathbb{Q}(\pi)$ متماثل مع الحقل $\mathbb{Q}(x)$ للدوال الكسرية على $\mathbb{Q}$ بغير المعين x، وهكذا ومن وجهة النظر الإنشائية، يتصرف العنصر المتسامي على الحقل F بوصفه غير معين على F. ▲

17.29 تعريف يسمى الامتداد E للحقل F **امتدادًا بسيطًا (simple extension)** لـ F، إذا كان $E = F(\alpha)$ حيث $\alpha \in E$. ■

ظهرت الكثير من النتائج المهمّة خلال هذا الفصل، وقد طوّرنا الكثير من الأساليب التي بدأت تؤتي ثمارها بصورة لافتة للنظر، حيث تعطي المبرهنة الآتية نظرة في العمق على طبيعة الحقل $F(\alpha)$، في حال كانت α جبرية على F.

18.29 مبرهنة ليكن E الامتداد البسيط $F(\alpha)$ للحقل F، ولتكن α جبرية على F، وافترض أنّ درجة $\operatorname{irr}(\alpha,F)$ تساوي $n \geq 1$، فإنّ كل عنصر β في $E = F(\alpha)$ يمكن كتابته بطريقة وحيدة على الصورة:

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

حيث b_i عنصر في F لكل i.

البرهان باستخدام العادي لتشاكل التعويض ϕ_α، فإنّ كل عنصر في

$$F(\alpha) = \phi_\alpha[F[x]]$$

يكون على الصورة $\phi_\alpha(f(x)) = f(\alpha)$ كثيرة حدود في α ومعاملات من F.

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

ما يعني أنّ $p(\alpha) = 0$، وهكذا، فإنّ

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$$

هذه المعادلة في $F(\alpha)$ يمكن أن تستخدم للتعبير عن أي وحيد الحد α^m، حيث $m \geq n$ باستخدام قوى α الأقل من n، على سبيل المثال:

$$\begin{aligned}\alpha^{n+1} = \alpha\alpha^n &= -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha \\ &= -a_{n-1}\left(-a_{n-1}\alpha^{n-1} - \cdots - a_0\right) - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha\end{aligned}$$

وهكذا، فإذا كانت $\beta \in F(\alpha)$، يمكن التعبير عن β بالصورة المطلوبة

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

لإثبات أنّ هذه الكتابة وحيدة، افترض أنّ:

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = b_0' + b_1'\alpha + \cdots + b_{n-1}'\alpha^{n-1}$$

حيث $b_i' \in F$ لكل i، وهكذا، فإنّ:

$$(b_0 - b_0') + (b_1 - b_1')x + \ldots + (b_{n-1} - b_{n-1}')x^{n-1} = g(x)$$

تمثل عنصرًا في $F[x]$ و $g(\alpha) = 0$، وكذلك فإنّ درجة $g(x)$ أقل من درجة $\mathrm{irr}(\alpha,F)$، ولأنّ $\mathrm{irr}(\alpha,F)$ كثيرة حدود غير صفرية ذات أقل درجة في $F[x]$، حيث تكون α صفراً لها، فإنه يجب أن يكون $g(x) = 0$، فنستنتج أنّ $b_i - b_i' = 0$، وهكذا، فإنّ $b_i = b_i'$، ما يبرهن أنّ b_i وحيدة.
♦

المثال الآتي لتوضيح المبرهنة 18.29 مثير للإعجاب.

19.29 مثال كثيرة الحدود $p(x) = x^2 + x + 1$ في $\mathbb{Z}_2[x]$ غير مختزلة على $\mathbb{Z}_2$، وذلك بحسب المبرهنة 10.23؛ لأن كلا عنصري $\mathbb{Z}_2$، 0 و 1 ليسا صفرين لـ $p(x)$.

باستخدام المبرهنة 3.29، نعلم أنه يوجد حقل E امتدادًا لـ $\mathbb{Z}_2$ يحوي صفرًا α لـ $x^2 + x + 1$، وبحسب المبرهنة 18.29، يحوي $\mathbb{Z}_2(\alpha)$ العناصر $0 + 0\alpha$، $0 + 1\alpha$، $1 + 0\alpha$ و $1 + 1\alpha$، أي 0، 1، α و $1 + \alpha$، وهذا يعطينا حقلاً جديدًا من أربعة عناصر!

جداول الجمع والضرب بهذا الحقل معطاة في الجدولين 20.29 و 21.29، على سبيل المثال: لحساب $(1 + \alpha)(1 + \alpha)$ في $\mathbb{Z}_2(\alpha)$، نلاحظ أنّه لأنّ $p(\alpha) = \alpha^2 + \alpha + 1 = 0$، فإنّ
$\alpha^2 = -\alpha - 1 = \alpha + 1$

وهكذا، فإنّ:

$$(1 + \alpha)(1 + \alpha) = 1 + \alpha + \alpha + \alpha^2 = 1 + \alpha^2 = 1 + \alpha + 1 = \alpha$$
▲

أخيرًا، نستطيع وباستخدام المبرهنة 18.29 أن نفي بالوعد في المثال 4.29، ونثبت أن $\mathbb{R}[x]/\langle x^2 + 1\rangle$ متماثل مع حقل الأعداد المركبة $\mathbb{C}$، فقد رأينا في المثال 4.29 أننا نستطيع أن نرى $\mathbb{R}[x]/\langle x^2 + 1\rangle$ بوصفه حقل امتداد لـ $\mathbb{R}$، لتكن:

$$\alpha = x + \langle x^2 + 1\rangle$$

الجدول 20.29

+	0	1	α	1 + α
0	0	1	α	1 + α
1	1	0	1 + α	α
α	α	1 + α	0	1
1 + α	1 + α	α	1	0

الجدول 21.29

	0	1	α	1 + α
0	0	0	0	0
1	0	1	α	1 + α
α	0	α	1 + α	1
1 + α	0	1 + α	1	α

إذن، $\mathbb{R}(\alpha) = \mathbb{R}[x]/\langle x^2 + 1\rangle$ وتتكون من العناصر جميعها على الصورة $a + b\alpha$ لكل $a,b \in \mathbb{R}$ بحسب مبرهنة 18.29، لكن لأنّ $\alpha^2 + 1 = 0$، فنجد أنّ α تؤدي دور $i \in \mathbb{C}$ ، و $a + b\,\alpha$ تؤدي دور $(a + bi) \in \mathbb{C}$؛ ولهذا $\mathbb{R}(\alpha) \simeq \mathbb{C}$، وهذه هي الطريقة الجبرية الممتازة لإنشاء $\mathbb{C}$ من $\mathbb{R}$.

■ تمارين 29

حسابات

في التمارين 1 إلى5، أثبت أنّ العدد المعطى $\alpha \in \mathbb{C}$ جبري على $\mathbb{Q}$، بإيجاد $f(x) \in \mathbb{Q}[x]$، حيث $f(\alpha) = 0$

1. $1+\sqrt{2}$ **2.** $\sqrt{2}+\sqrt{3}$ **3.** $1 + i$

4. $\sqrt{1+\sqrt[3]{2}}$ **5.** $\sqrt{\sqrt[3]{2}-i}$

في التمارين 6 إلى 8، أوجد $\operatorname{irr}(\alpha,\mathbb{Q})$ و $\deg(\alpha,\mathbb{Q})$ للعدد الجبري المعطى $\alpha \in \mathbb{C}$، وكن مستعدًا لتبرهن أنّ كثيرات الحدود غير مختزلة على $\mathbb{Q}$ إذا طلب منك ذلك.

6. $\sqrt{3-\sqrt{6}}$ **7.** $\sqrt{(\frac{1}{3})+\sqrt{7}}$ **8.** $\sqrt{2}+i$

في التمارين 9 إلى 16، صنّف العدد المعطى $\alpha \in \mathbb{C}$ إذا كان جبريًا أم متساميًا على الحقل المعطى F وإذا كان α جبريًا على F، فجد $\deg(\alpha,F)$.

9. $\alpha = i,\ F = \mathbb{Q}$ **10.** $\alpha = 1 + i,\ F = \mathbb{R}$

11. $\alpha = \sqrt{\pi},\ F = \mathbb{Q}$ **12.** $\alpha = \sqrt{\pi},\ F = \mathbb{R}$

13. $\alpha = \sqrt{\pi},\ F = \mathbb{Q}(\pi)$ **14.** $\alpha = \pi^2,\ F = \mathbb{Q}$

15. $\alpha = \pi^2,\ F = \mathbb{Q}(\pi)$ **16.** $\alpha = \pi^2,\ F = \mathbb{Q}(\pi^3)$

17. ارجع إلى المثال 19.29 في الكتاب. كثيرة الحدود $x^2 + x + 1$ لها صفر α في $\mathbb{Z}_2(\alpha)$؛ ولهذا يجب أن تتحلل إلى حاصل ضرب عوامل خطية في $(\mathbb{Z}_2(\alpha))[x]$. أوجد هذا التحليل. [مساعدة: قَسِّم $x^2 + x + 1$ على $x - \alpha$ قسمة طويلة باستخدام الحقيقة $\alpha^2 = \alpha + 1$].

18. أ. أثبت أنّ كثيرة الحدود $x^2 + 1$ غير مختزلة في $\mathbb{Z}_3[x]$.

ب. لتكن α صفرًا لـ $x^2 + 1$ في حقل ممتد لـ $\mathbb{Z}_3$. كما في المثال 19.29، فأعط جداول الضرب والجمع للعناصر التسعة في $\mathbb{Z}_3(\alpha)$ مكتوبة بحسب الترتيب 0، 1، 2، α، 2α، $1+\alpha$، $1+2\alpha$، $2+\alpha$ و $2+2\alpha$.

مفاهيم

في التمارين 19 إلى 22، صحّح تعريف الحدّ المكتوب بخط مائل دون الرجوع إلى الكتاب– إذا كانت هناك حاجة للتصحيح– بحيث يكون بصيغة قابلة للنشر.

19. يكون العنصر α من التمدد E للحقل F *جبريًا على F*، إذا وفقط إذا كان α صفرًا لكثيرة حدود.

20. يكون العنصر β من التمدد E للحقل F *متساميًا على F*، إذا وفقط إذا كان β ليس صفرًا لأيّ كثيرة حدود في $F[x]$.

21. *كثيرة الحدود الأحادية في $F[x]$* هي من كانت معاملاتها جميعها تساوي 1.

22. يكون الحقل E *امتدادًا بسيطًا للحقل الجزئي F*، إذا وفقط إذا توافرت $\alpha \in E$، حيث لا يوجد أيّ حقل جزئي فعلي من E يحتوي α.

21. ضع إشارة صح أو إشارة خطأ:

____ أ. العدد π متسامٍ على $\mathbb{Q}$.

____ ب. $\mathbb{C}$ امتداد بسيط لـ $\mathbb{R}$.

____ جـ. كل عنصر في الحقل F جبري على F.

____ د. $\mathbb{R}$ حقل ممتد لـ $\mathbb{Q}_2$.

____ هـ. $\mathbb{Q}$ حقل ممتد لـ $\mathbb{Z}_2$.

____ و. لتكن $\alpha \in \mathbb{C}$ جبريًا على $\mathbb{Q}$ من الدرجة n، إذا كانت $f(x) \in \mathbb{Q}[x]$ كثيرة حدود غير صفرية، و $f(\alpha) = 0$ تكون $n \geq$ (درجة $f(x)$).

____ ح. لتكن $\alpha \in \mathbb{C}$ جبريًا على $\mathbb{Q}$ من الدرجة n، إذا كانت $f(x) = 0$ للدالة غير الصفرية $f(x) \in \mathbb{R}[x]$، فإن $n \geq$(درجة $f(x)$)، أي أكبر أو تساوي n.

____ ط. كل كثيرة حدود غير ثابتة في $F[x]$ لها صفر في حقل ممتد لـ F.

____ ي. كل كثيرة حدود غير ثابتة في $F[x]$ لها صفر في الحقول الممتدة لـ F جميعها.

____ ك. إذا كان x غير معين، فإنّ $\mathbb{Q}[\pi] \simeq \mathbb{Q}[x]$.

24. ذكرنا من غير برهان أنّ π و e متساميان على $\mathbb{Q}$.

أ. أوجد حقلاً جزئيًا F من $\mathbb{R}$، حيث π جبري من الدرجة 3 على F.

ب. أوجد حقلاً جزئيًا E من $\mathbb{R}$، حيث إنّ e^2 جبري من الدرجة 5 على E.

25. أ. أثبت أنّ $x^3 + x^2 + 1$ غير مختزلة على $\mathbb{Z}_2$.

ب. لتكن a صفرًا لكثيرة الحدود $x^3 + x^2 + 1$ في الحقل الممتد من $\mathbb{Z}_2$، فأثبت أنّ $x^3 + x^2 + 1$ تتحلل إلى ثلاثة عوامل خطية في $(\mathbb{Z}_2(a))[x]$، وذلك بإيجاد هذه العوامل فعليًا. [مساعدة: كل عنصر من $\mathbb{Z}_2(\alpha)$ يكون على الصورة

$a_0 + a_1\,\alpha + a_2\,\alpha^2$، حيث $a_i = 0,1$ قَسِّم $x^3 + x^2 + 1$ على $x - a$ قسمة طويلة، وأثبت أنّ خارج القسمة له صفر أيضًا في $\mathbb{Z}_2(\alpha)$، وذلك بتجريب العناصر الثمانية بكل بساطة، ثمَّ أكمل التحليل].

26. ليكن الحقل E امتدادًا للحقل $\mathbb{Z}_2$ ، وليكن $\alpha \in E$ جبريًّا من الدرجة 3 على $\mathbb{Z}_2$. صنِّف الزمر $\langle \mathbb{Z}_2(\alpha), + \rangle$ و$\langle (\mathbb{Z}_2(\alpha))^*, \cdot \rangle$ تبعًا للمبرهنة الأساسية للزمر الإبدالية منتهية التولد، وكالمعتاد $(\mathbb{Z}_2(\alpha))^*$ هي مجموعة العناصر غير الصفرية لـ $\mathbb{Z}_2(\alpha)$.

27. ليكن الحقل E امتدادًا للحقل F، وليكن $\alpha \in E$ جبريًّا على F. حيث يُشار إلى كثيرة الحدود $\mathrm{irr}(\alpha, F)$ أحيانًا **بكثيرة الحدود الصغرى** ***(minimal polynomial for α over F)*** على F. لماذا يعدّ هذا الاسم ملائمًا؟

براهين مختصرة

28. أعطِ جملتين أو ثلاث جمل توجز إثبات المبرهنة 3.29.

براهين

29. ليكن الحقل E امتدادًا للحقل F، وليكن $\alpha, \beta \in E$، وافترض أنّ α متسامٍ على F وجبرية على $F(\beta)$، فأثبت أنّ β جبرية على $F(\alpha)$.

30. ليكن الحقل E امتدادًا للحقل المنتهي F، حيث F يحتوي على q عنصرًا، وليكن $\alpha \in E$ جبريًّا على F من الدرجة n. فأثبت أن $F(\alpha)$ يحتوي على q^n عنصرًا.

31. أ. برهن أنه توجد كثيرة حدود غير مختزلة من الدرجة الثالثة في $\mathbb{Z}_3[x]$.

ب. برهن باستخدام الفرع (أ) أنه يوجد حقل منتهٍ يتكوّن من 27 عنصرًا [مساعدة: استخدم تمرين 30].

32. ليكن الحقل الأولي $\mathbb{Z}_p$ ذا المميز $p \neq 0$.

أ. برهن أنه إذا كانت $p \neq 2$، فليس كل عنصر في $\mathbb{Z}_p$ مربعًا لعنصر في $\mathbb{Z}_p$. [مساعدة: $1^2 = (p-1)^2 = 1$ في $\mathbb{Z}_p$. استنتج النتيجة المطلوبة بالعد].

ب. استخدم الفرع (أ) لتبرهن أنه توجد حقول منتهية تتكوّن من p^2 عنصرًا لكل عدد أولي p في $\mathbb{Z}^+$.

33. ليكن الحقل E امتدادًا للحقل F ، وليكن $\alpha \in E$ متساميًّا على F. برهن أنّ كل عنصر في $F(\alpha)$ وليس في F ، يكون متساميًّا أيضًا على F.

34. برهن أنّ $\{a + b(\sqrt[3]{2}) + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$ حقل جزئي من $\mathbb{R}$ باستخدام الأفكار الواردة في هذا الفصل، وليس باستخدام التحقق العادي لمسلمات الحقل. [مساعدة: استخدم المبرهنة 18.29].

35. باستخدام النهج نفسه الوارد في تمرين 31، برهن أنه يوجد حقل من 8 عناصر، و 16 عنصرًا، و25 عنصرًا.

36. ليكن F حقلاً ذا مميز p. برهن أنّ كل عنصر من عناصر F جبري على حقل أولي $\mathbb{Z}_p \leq F$. [مساعدة: ليكن F^* مجموعة العناصر غير الصفرية في F، طبّق مبرهنة الزمر على الزمرة $\langle F^*, \cdot \rangle$؛ لتبرهن أنّ كل $\alpha \in F^*$ هي صفر لكثيرة حدود في $\mathbb{Z}_p[x]$ على الصورة $x^n - 1$].

37. استخدم التمرينين 30 و 36 لتبرهن أنّ عدد عناصر أي حقل منتهٍ يساوي إحدى قوى عدد أولي، أي إنه يحتوي عددًا من العناصر يساوي إحدى قوى عدد أولي.

الفصل 30 فضاء المتجهات Vector Spaces

قد تكـون مفاهيم فضاء المتجهات، والقياسيات، والمتجهات المستقلة والأساس مفاهيم معروفـة، وسنقـدم في هـذا الفصـل هـذه المفاهيم، حيـث تكون القياسيـات عناصـر في أي حقل، وسنستعمل الأحرف الإغريقية مثل α و β للمتجهات، وبحسب تطبيقاتنا ستكون المتجهات عناصر مـن حقل تمدد E للحقل F، وستكون أيضًـا البراهين مطابقة لتلك التي تعطى في العادة في المقرر الدراسي الأول للجبر الخطي، فإذا كانت هذه الأفكار معروفة، فنقترح دراسة الأمثلة 4.30، 11.30، 14.30و22.30، ثـمّ قراءة المبرهنة 23.30 وبرهـانها، وإذا كانـت الأمثلة والنظرية مفهومة، فحلّ بعض التمارين، ثم اذهب إلى الفصل الآتي.

التعريف والخصائص الأساسية

موضوع فضاء المتجهات هو حجر الزاوية في الجبر الخطي، ولأنّ الجبر الخطي ليس موضوع الدراسة في هذا الكتاب، فستكون معالجتنا لفضاء المتجهات مختصرة، ومصممة فقط لتطوير مفهومي الاستقلال الخطي والبعد، اللذين سنحتاج إليهما في نظرية الحقول.

إن مفهومي المتجه والقياسي ربما يكونان معروفين من التفاضل والتكامل، وستكون القياسيات هنا عناصر من أي حقل، وليس مجرد حقل الأعداد الحقيقية، إضافة إلى أننا سنطور النظرية باستخدام مسلمات، تمامًا كتلك التي درسناها للأنظمة الجبرية.

1.30 تعريف ليكن F حقلًا. **فضاء المتجهات على F** (***vector space over F***) يتكوّن من زمرة إبدالية V مع عملية الجمع وعملية ضرب بعدد قياسي لكل عنصر في V مع كل عنصر من F من اليسار، بحيث تتحقق الشروط الآتية لكل $a, b \in F$ و $\alpha, \beta \in V$:

$\mathscr{V}_1$: $a\alpha \in V$

$\mathscr{V}_2$: $a(b\alpha) = (ab)\alpha$

$\mathscr{V}_3$: $(a+b)\alpha = (a\alpha) + (b\alpha)$

$\mathscr{V}_4$: $a(\alpha + \beta) = (a\alpha) + (a\beta)$

$\mathscr{V}_5$: $1\alpha = \alpha$

تسمـى عناصـر V متجهـات وعناصـر F أعـدادًا قياسية، وعندمـا نناقش حقـلاً واحدًا فقط F، فسنسقط الإشارة إلى F، ونشير إلى فضاء المتجهات. ■

لاحظ أنّ الضرب القياسي في فضاء المتجهات ليس عملية ثنائية على مجموعة واحدة بالمفهوم الذي عرفناه في الفصل 2، فهي تربط العنصر $a\alpha$ في V بالزوج المرتب (a,α) والمكوّن من العنصر a من F والعنصر α من V، وهكذا فإنّ الضرب القياسي هو دالة من $F\times V$ إلى V، وسيرمز للعنصر المحايد لعملية الجمع على V – المتجه 0 – والعنصر المحايد لعملية الجمع على F – العدد القياسي 0 – بالرمز 0.

مثال 2.30 لتكن الزمرة الإبدالية $\langle \mathbb{R}_n, + \rangle = \mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R}$ ، n من المرات، التي تتكوّن من المتعددات جميعها من الرتبة n مع الجمع. عرّف الضرب القياسي على القياسيات من $\mathbb{R}$ بالطريقة الآتية:

$$r\alpha = (ra_1, \ldots, ra_n)$$

■ **نبذة تاريخية**

بدأ تبلور المفهوم المجرد لفضاء المتجهات في أمثلة محددة في القرن التاسع عشرأو قبله، فعلى سبيل المثال: تعامل ويليام روان هاملتون (William Rowan Hamilton) مع الأعداد المركبة على نحو واضح بوصفها أزواجًا من الأعداد الحقيقية – كما ذُكر في الفصل 24– كذلك تعامل مع ثلاثي مرتب من الأعداد الحقيقية، وأخيرًا تعامل مع رباعي مرتب من الأعداد الحقيقية عندما ابتكر المرباعيات، وفي هذه الحالات أصبحت المتجهات كائنات يمكن جمعها وضربها في قياسي، وذلك باستخدام قوانين مناسبة لتلك العمليات، وهناك المزيد من الأمثلة على هذه الكائنات بما فيها الأشكال التفاضلية (مفاهيم مرتبطة بإشارات التكامل) والأعداد الصحيحة الجبرية، وعلى الرغم من أنّ هيرمان جراسمان ((Herman Grassman 1809 - 1877) نجح في استنباط مبرهنة مفصلة لفضاءات ذات البعد n ، في كتابه (Die lineale Ausdnungslehre) عامي 1844م و1862م، إلّا أنَّ أول رياضي أعطى تعريفًا مجرّدًا لفضاء المتجهات يكافئ التعريف 1.30 كان جوسبي بيانو (Giuseppe Peano 1858 – 1932)، في كتابه (Calcolo Geometrico) عام 1888م. كان بيانو يهدف في كتابه – كما يتضح من عنوان الكتاب – إلى تطوير تفاضل وتكامل هندسي، وتبعًا له، فإنّ مثل هذا التفاضل والتكامل يتكوّن من نظام من العمليات، يشبه تلك التي في التفاضل والتكامل الجبري، والفرق أنّ الكائنات التي تتم بها الحسابات هي كائنات هندسية بدلاً من الكائنات الجبرية، لكنّ الغريب في الأمر، أنّ عمل بيانو لم يكن له أي أثر في الساحة الرياضية، ومع أنّ هيرمان وايل (Herman Weyl 1885 – 1955) أعاد بصورة أساسية تعريف بيانو نفسه، حيث ورد ذلك في كتابه (Space – Time – Matter) عام 1918م، إلّا أنّ تعريف فضاء المتجهات لم يدخل حقل الرياضيات إلا عندما أُعلن عنه للمرة الثالثة من قبل ستيفان باناخ (Stefan Banach 1892 – 1945)، في رسالة للدكتوراة طُبعت عام 1922م، التي تعاملت مع ما نسميه اليوم فضاء المتجهات المعياري الكامل (Banach Spaces).

حيث $r \in \mathbb{R}$ و $\alpha = (a_1, \ldots, a_n) \in \mathbb{R}^n$، ومع هاتين العمليتين، تصبح $\mathbb{R}^n$ فضاء متجهات على $\mathbb{R}$، حيث يمكن التحقق من مسلمات فضاء المتجهات بسهولة، وبوجه خاص، يمكن النظر إلى $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ بوصفها فضاء متجهات على $\mathbb{R}$، الذي يتكون من المتجهات جميعها المنطلقة من نقطة الأصل، كما تدرس في العادة في مادة التفاضل والتكامل. ▲

مثال 3.30 لأيّ حقل F، يمكن أن نعدّ $F[x]$ فضاء متجهات على F، حيث جمع المتجهات هو الجمع الاعتيادي لكثيرات الحدود في $F[x]$، والضرب القياسي $a\alpha$ لعنصر من $F[x]$ مع عنصر من F هو الضرب العادي لعناصر $F[x]$، **حيث** يمكن التوصل إلى مسلمات فضاء المتجهات $\mathscr{V}_1$ إلى $\mathscr{V}_5$ بسهولة، وذلك من حقيقة أنّ $F[x]$ يمثل حلقة لها عنصر محايد. ▲

مثال 4.30 ليكن الحقل E تمددًا للحقل F، يمكن أن نعدّ E فضاء متجهات على F، حيث جمع المتجهات هو الجمع العادي في E، والضرب القياسي $a\alpha$ هو الضرب العادي في الحقل E، حيث $a \in F$ و $\alpha \in E$، فتتحقق المسلمات هنا مباشرة من مسلمات الحقل E، وفي هذه الحالة حقل القياسيات هو في الحقيقة مجموعة جزئية من فضاء المتجهات.

هذا هو المثال المهم بالنسبة إلينا. ▲

لا نفترض أي شيء بالنسبة إلى فضاء المتجهات من عملنا السابق، وسنبرهن كل شيء نحتاج إليه باستخدام التعريف، على الرغم من أن النتائج قد تكون مألوفة من التفاضل والتكامل.

5.30 مبرهنة إذا كان V فضاء متجهات على F، فإنّ $0\alpha = 0$، $a0 = 0$ و $(-a)\alpha = a(-\alpha) = -(a\alpha)$ لكل $a \in F$ و $\alpha \in V$.

البرهان يجب أن تقرأ المعادلة $0\alpha = 0$ كالآتي-: "(المتجه 0) $= \alpha$ (القياسي 0)"، وكذلك $a0 = 0$ تقرأ: "(المتجه 0) $=$ (المتجه 0)a"، والبراهين هنا شبيهة بتلك في المبرهنة 8.18 على الحلقات، التي تعتمد بصورة مكثفة على قوانين التوزيع $\mathscr{V}_3$ و $\mathscr{V}_4$. الآن:

$$(0\alpha) = (0+0)\alpha = (0\alpha) + (0\alpha)$$

تمثل معادلة في الزمرة الإبدالية $\langle V, +\rangle$؛ وهكذا، وباستخدام قانون الحذف في الزمر، $0\alpha = 0$. وكذلك، فمن:

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

نستنتج أن $a0 = 0$. إذن:

$$0 = 0\alpha = (a + (-a))\alpha = a\alpha + (-a)\alpha,$$

وهكذا، فإنّ $(-a)\alpha = -(a\alpha)$. وبالمثل، فمن

$$0 = a0 = a(\alpha + (-\alpha)) = a\alpha + a(-\alpha),$$

نستنتج كذلك أنّ $a(-\alpha) = -(a\alpha)$. ♦

الاستقلال الخطي والأساس

6.30 تعريف ليكن V فضاء متجهات على F، فالمتجهات في المجموعة $S = \{\alpha_i \mid i \in I\}$ من V **تولد** V (***span or generate***) إذا كان لكل $\beta \in V$،

$$\beta = a_1\alpha_{i_1} + a_2\alpha_{i_2} + \dots a_n\alpha_{i_n}$$

بحيث $a_j \in F$ و $\alpha_{ij} \in S$، $j = 1, \dots, n$.
المتجه $\sum_{j=1}^{n} a_j\alpha_{i_j}$ **تركيب خطي (*linear combination*)** من α_{ij}. ■

7.30 مثال في فضاء المتجهات $\mathbb{R}^n$ على $\mathbb{R}$ في المثال 2.30 من الواضح أنّ المتجهات:

$$(1,0,\dots,0), (0,1,\dots,0), \dots, (0,0,\dots,1)$$

تولد $\mathbb{R}^n$؛ لأن

$$(a_1, a_2, \ldots, a_n) = a_1(1,0, \ldots, 0) + a_2\,(0,1, \ldots , 0) + \ldots + a_n\,(0,0, \ldots,1)$$

وكذلك أحاديات الحد x^m حيث $m \geq 0$ تولد $F[x]$ على F فضاء المتجهات في المثال 3.30. ▲

8.30 مثال ليكن F حقلاً، وليكن الحقل E امتدادًا لـ F، ولتكن $\alpha \in E$ جبرية على F، فإنّ $F(\alpha)$ فضاء متجهات على F بحسب المبرهنة 18.30، وهو يتولد من المتجهات $\{1, \alpha, \ldots, \alpha^{n-1}\}$، حيث $n = \deg(\alpha,F)$.

هذا مثال مهم لنا. ▲

9.30 تعريف يسمى فضاء المتجهات V على F فضاءً **منتهي البعد (finite dimensional)**، إذا توافرت مجموعة متجهات منتهية من V تولد V. ■

10.30 مثال يرينا المثال 7.30 أنّ $\mathbb{R}^n$ منتهي البعد، ولكن فضاء المتجهات $F[x]$ على F ليس منتهي البعد؛ لأنّ كثيرات الحدود ذوات الدرجات العليا لا يمكن أن تكون تركيبًا خطيًّا من عناصر أيّ مجموعة منتهية من كثيرات الحدود. ▲

11.30 مثال ليكن $F \leq E$، ولتكن $\alpha \in E$ جبرية على الحقل F، فيرينا المثال 8.30 أنّ فضاء المتجهات $F(\alpha)$ منتهي البعد على F. وهذا أكثر الأمثلة أهمية. ▲

12.30 تعريف تسمى المتجهات في المجموعة $S = \{\alpha_i | i \in I\}$ من فضاء المتجهات V **مستقلة خطيًّا (*linearly independent*)** على F، إذا كان لأي عناصر مختلفة $\alpha_{ij} \in S$ ومعاملات $a_j \in F$ و $n\in\mathbb{Z}^+$ يكون $\sum_{j=1}^{n} a_j\alpha_{i_j} = 0$ في V فقط إذا كان $a_j = 0$ لكل $j = 1,\ldots, n$؛ أمّا إذا كانت المتجهات ليست مستقلة خطيًّا على F، فإنها تسمى **مرتبطة خطيًّا** على F **(*linearly dependent*)**. ■

إذن، تكون المتجهات في $\{\alpha_i\colon i \in I\}$ مستقلة خطيًّا على F، إذا كانت الطريقة الوحيدة لكتابة المتجه 0 بوصفها تركيبًا خطيًّا من المتجهات α_i، هو لأنّ المعاملات القياسية جميعها تساوي 0، فإذا كانت المتجهات مرتبطة خطيًّا على F، فيوجد $a_j \in F$، حيث $j = 1,\ldots, n$ و $\sum_{j=1}^{n} a_j\alpha_{i_j} = 0$، وليس كل $a_j = 0$.

13.30 مثال لاحظ أنّ المتجهات التي تولد $\mathbb{R}^n$ المعطاة في المثال 7.30 مستقلة خطيًّا على $\mathbb{R}$، وكذلك المتجهات $\{x^m\colon m \geq 0\}$ مستقلة خطيًّا بوصفها متجهات من $F[x]$ على F، ولاحظ أنّ $(1,-1)$, $(2,1)$ و$(-3, 2)$ مرتبطة خطيًّا في $\mathbb{R}^2$ على $\mathbb{R}$؛ وذلك لأن:

$$7(1, -1) + (2,1) + 3(-3,2) = (0,0) = 0$$ ▲

14.30 مثال ليكن الحقل E امتدادًا للحقل F، ولتكن $\alpha \in E$ جبرية على F.

إذا كانت $deg(\alpha, F) = n$، فإن كل عنصر في $F(\alpha)$ وبحسب المبرهنة 18.29، يكتب بطريقة وحيدة على الصورة:

$$b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

حيث $b_i \in F$.

بوجه خاص، $0 = 0 + 0\alpha + \ldots + 0\alpha^{n-1}$ هي صورة وحيدة لـ 0، وهكذا، فإنّ العناصر $1, \alpha, \ldots, \alpha^{n-1}$ متجهات مستقلة خطيًّا في $F(\alpha)$ على الحقل F.

وهي كذلك تولد $F(\alpha)$، وهكذا وبحسب التعريف الآتي، فإنّ $1, \alpha, \ldots, \alpha^{n-1}$ تشكل أساسًا لـ $F(\alpha)$ على F، وهذا مثال مهم بالنسبة إلينا، وفي الحقيقة هذا هو سبب دراستنا لهذه المادة من فضاء المتجهات. ▲

15.30 تعريف إذا كان V فضاء متجهات على الحقل F، فإنّ متجهات المجموعة الجزئية $B = \{\beta_i | i \in I\}$ من V تشكل **أساسًا** لـ V على F (***basis***)، إذا كانت تولد V ومستقلة خطيًّا. ■

البعد

النتائج الوحيدة المتبقية التي نود برهنتها عن فضاء الاتجاهات، هي أنّ كل فضاء متجهات ذو بعد منته له أساس، وكل أساسين لفضاء متجهات منتهيتا البعد لهما عدد العناصر نفسه، هاتان النتيجتان كلتاهما صحيحتان دون اشتراط أنهما منتهيا البعد، ولكن البراهين تحتاج إلى المزيد من المعرفة بنظرية المجموعات بما يزيد على ما افترضناه، وحالة البعد المنتهي هي كل ما نحتاج إليه، وسنبدأ أولاً بتمهيدية سهلة.

16.30 تمهيدية ليكن V فضاء متجهات على الحقل F، ولتكن $\alpha \in V$، فإذا كانت α تركيبًا خطيًّا من المتجهات β_i في V ، حيث $i = 1, \ldots, m$ ، وكل β_i تركيب خطي من المتجهات γ_j في V، حيث $j = 1, \ldots, m$، فإنّ α تركيب خطي من γ_j.

البرهان لتكن $\alpha = \sum_{i=1}^{m} a_i \beta_i$، ولتكن $\beta_i = \sum_{j=1}^{n} b_{ij}\gamma_j$ ، حيث a_i و b_{ij} عناصر في F.

وهكذا، فإنّ:

$$\alpha = \sum_{i=1}^{m} a_i \left(\sum_{j=1}^{n} b_{ij}\gamma_j \right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_i b_{ij} \right) \gamma_j$$

و

$$\left(\sum_{i=1}^{m} a_i b_{ij}\right) \in F$$ ♦

مبرهنة 7.30 في فضاء متجهات منتهي البعد، كل مجموعة منتهية من المتجهات مولدة للفضاء تحوي مجموعة جزئية تشكل أساسًا.

البرهان ليكن V منتهي البعد على F، ولتكن المتجهات $\alpha_n ,\ldots, \alpha_i$ في V تولد V. ضع ألـ α_i في صف، واختبر من ثم كل α_i بادئًا من اليسار مع $i = 1$، واحذف أول α_j تكتب بوصفها تركيبًا خطيًّا من α_i السابق لها، حيث $i < j$، ثمّ أكمل بادئًا ب - α_{j+1}، ثم احذف α_k اللاحقة التي تكتب بوصفها تركيبًا خطيًّا من العناصر المتبقية السابقة لها، وهكذا. عندما نصل إلى α_n بعد عدد منته من الخطوات، فإنّ أي α_i متبقية في القائمة لا تكتب بوصفها تركيبًا خطيًّا من سابقاتها في القائمة المختصرة، أضف إلى ذلك، تبرهن التمهيدية 16.30 أنّ أي متجه يكتب بوصفه تركيبًا خطيًّا من المجموعة α_i الأصلية، يظل يكتب بوصفه تركيبًا خطيًّا من القائمة المختصرة – وربما الأصغر – التي لا يكتب فيها أي α_i بوصفه تركيبًا خطيًّا من المتجهات السابقة له، وهكذا فإنّ المتجهات في القائمة المختصرة لـ α_i تولد V كذلك.

في القائمة المختصرة، افترض أنّ:

$$a_1 \alpha_{i\,1} + \ldots + a_r \alpha_{ir} = 0$$

حيث $i_1 < i_2 < \ldots < i_r$ وبعض ألـ $a_j \neq 0$. يمكننا أن نفرض من المبرهنة 5.30 أنّ $a_r \neq 0$، أو أن نحذف $a_r \alpha_{ir}$ من يسار المعادلة، وهكذا وباستخدام المبرهنة 5.30 مرة ثانية، فإننا نحصل على:

$$\alpha_{i_r} = \left(-\frac{a_1}{a_r}\right)\alpha_{i_1} + \cdots + \left(-\frac{a_{r-1}}{a_r}\right)\alpha_{i_{r-1}},$$

الذي يثبت أنّ α_{i_r} تكتب بوصفها تركيبًا خطيًّا من سابقاتها، ما يناقض عملنا. إذن، المتجهات α_i في القائمة المختصرة تولد V ومستقلة خطيًّا، وهكذا فإنها تشكل أساسًا لـ V على F. ♦

18.30 نتيجة يكون لفضاء المتجهات منتهي البعد أساس منتهٍ.

البرهان بحسب التعريف، يكون لفضاء المتجهات منتهي البعد مجموعة مولدة منتهية من المتجهات.

المبرهنة 17.30 تكمل الإثبات. ♦

والمبرهنة الآتية هي أوج عملنا في فضاء المتجهات.

19.30 مبرهنة لتكن $S = \{\alpha_1, \cdots, \alpha_r\}$ مجموعة منتهية من المتجهات المستقلة خطيًّا في فضاء متجهات منتهي البعد V على الحقل F، ويمكن تكبير S لتصبح أساسًا لـ V على F، وأكثر من ذلك، إذا كانت $B = \{\beta_1, \cdots, \beta_n\}$ أساسًا لـ V على F، فإنّ $r \leq n$.

البرهان بحسب النتيجة 18.30، يوجد أساس $B = \{\beta_1, \cdots, \beta_n\}$ لـ V على F، لتكن المتتالية المنتهية من المتجهات.

$$\alpha_1, \cdots, \alpha_r, \beta_1, \cdots, \beta_n$$

هذه المتجهات تولد V؛ لأن B أساس، وباتباع الخطوات المستخدمة في المبرهنة 17.30 بحذف

كل متجه يكتب بوصفه تركيبًا خطيًّا من المتجهات السابقة له وبالترتيب من اليسار إلى اليمين، سنصل إلى أساس للفضاء V، لاحظ أنه لن يحذف أي α_i لأنها مستقلة خطيًّا، وهكذا يمكن تكبير S لتصبح أساسًا لـ V على F.

لإثبات الجزء الثاني من الاستنتاج، افترض المتتالية

$$\alpha_1, \beta_1, \cdots, \beta_n$$

هذه المتجهات ليست مستقلة خطيًّا على F؛ لأن α_i تكتب بوصفها تركيبًا خطيًّا

$$\alpha_1 = b_1\beta_1 + \cdots + b_n\beta_n$$

لأن β_i تمثل أساسًا، وهكذا فإنّ:

$$\alpha_1 + (-b_1)\beta_1 + \cdots + (-b_n)\beta_n = 0$$

المتجهات في هذه المتتالية تولد V، وإذا أوجدنا أساسًا بالعمل من اليسار إلى اليمين وحذف كل متجه يكتب بوصفه تركيبًا خطيًّا من المتجهات المتبقية السابقة له، فستحذف على الأقل β_i واحدة، ما يعطي الأساس.

$$\left\{\alpha_1, \beta_1^{(1)}, \cdots, \beta_m^{(1)}\right\}$$

حيث $m \le n$-1. وبتطبيق الخطوات نفسها على متتالية المتجهات

$$\alpha_1, \alpha_2, \beta_1^{(1)}, \cdots, \beta_m^{(1)}$$

نصل إلى أساس جديد

$$\left\{\alpha_1, \alpha_2, \beta_1^{(2)}, \cdots, \beta_s^{(2)}\right\}$$

حيث $s \le n-2$. ونستمر في العمل حتى نصل في النهاية للأساس

$$\left\{\alpha_1, \cdots, \alpha_r, \beta_1^{(r)}, \cdots, \beta_t^{(r)}\right\}$$

حيث $0 \le t \le n-r$. إذًا $r \le n$. ♦

20.30 نتيجة أي أساسين لفضاء متجهات منتهي البعد V على F لهما عدد العناصر نفسه.

البرهان لتكن $B = \{\beta_1, \cdots, \beta_n\}$، و $B' = \{\beta_1', \cdots, \beta_m'\}$ أساسين، وبحسب المبرهنة 19.30 وعدّ

B مجموعة مستقلة من المتجهات و B' بوصفها أساسًا، نرى أنّ $n \le m$ ، وبطريقة مماثلة نحصل على $m \le n$. إذن، $m = n$. ♦

21.30 تعريف إذا كان V فضاء متجهات منتهي البعد على الحقل F، فإنّ عدد عناصر أيّ أساس (بغض النظر عن اختيار الأساس، كما أثبتنا توًّا) يسمى **بعد V على F**. (***dimension of V over F***). ■

22.30 مثال ليكن الحقل E امتدادًا للحقل F و $\alpha \in E$، ويثبت المثال 14.30 أنه إذا كانت α جبرية على F و $\deg(\alpha, F) = n$، فإنّ بعد $F(\alpha)$ بوصفه فضاء متجهات على F يساوي n، وهذا أكثر مثال مهم لنا. ▲

تطبيق على نظرية الحقول

سنجمع النتائج حول نظرية الحقول الواردة في الأمثلة 4.30، 8.30، 11.30، 14.30 22.30 وندمجها في مبرهنة واحدة، حيث تعطي العبارة الأخيرة في هذه المبرهنة تطبيقًا إضافيًّا جميلاً لأفكار فضاء المتجهات على نظرية الحقول.

23.30 مبرهنة ليكن الحقل E امتدادًا للحقل F، ولتكن $\alpha \in E$ جبرية على F، فإذا كانت $\deg(\alpha,F)=n$، فإنّ $F(\alpha)$ يكون فضاء متجهات ذا بعد يساوي n على F مع الأساس $\{1, \alpha, \dots , \alpha^{n-1}\}$، وكذلك يكون كل عنصر β في $F(\alpha)$ جبريًّا على F و $\deg(\beta, F) \le \deg(\alpha, F)$.

البرهان برهنا كل شيء في الأمثلة السابقة عدا النتيجة المهمة المذكورة في العبارة الأخيرة في هذه المبرهنة، لتكن $\beta \in F(\alpha)$، حيث α جبرية على F من الدرجة n، لتكن العناصر

$$1, \beta, \beta^2, \dots , \beta^n$$

لا يمكن لـ $n + 1$ عنصر في $F(\alpha)$ أن تكون مختلفة ومستقلة خطيًّا على F؛ لأنه وبحسب المبرهنة 19.30، أي أساس لـ $F(\alpha)$ على F يجب أن يحوي على الأقل عددًا مماثلاً لأي مجموعة من المتجهات المستقلة خطيًّا على F، وفي كل حال، فإنّ الأساس $\{1,\alpha, \dots, \alpha^{n-1}\}$ يحوي n عنصرًا فقط، فإذا كانت $\beta^i = \beta^j$، فإنّ $\beta^i - \beta^j = 0$، وهكذا وفي أي حالة يوجد $b_i \in F$، بحيث إنّ

$$b_0 + b_1\beta + b_2\beta^2 + \cdots + b_n\beta^n = 0$$

وليس كل $b_i = 0$. إذن، $f(x) = b_n x^n + \dots + b_1 x + b_0$ تعطي عنصرًا لا يساوي الصفر في $F[x]$ بحيث $f(\beta) = 0$، وهكذا فإنّ β جبرية على F و $\deg(\beta, F)$ على الأكثر n. ♦

■ تمارين 30

حسابات

1. أوجد ثلاثة أساسات لـ $\mathbb{R}^2$ على $\mathbb{R}$، بحيث لا يكون لأي اثنين منهما متجه مشترك.

في التمرينين 2 و 3، حدّد إذا كانت مجموعة المتجهات المعطاة تشكل أساسًا لـ $\mathbb{R}^3$ على $\mathbb{R}$.

2. $\{(1,1,0), (1,0,1), (0,1,1)\}$ **3.** $\{(-1,1,2), (2,-3,1), (10, -14,0)\}$

في التمارين 4 إلى 9، أعطِ أساسًا لفضاء المتجه المعيّن على الحقل.

4. $\mathbb{Q}(\sqrt{2})$ على $\mathbb{Q}$ **5.** $\mathbb{R}(\sqrt{2})$ على $\mathbb{R}$

6. $\mathbb{Q}(\sqrt[3]{2})$ على $\mathbb{Q}$ **7.** $\mathbb{C}$ على $\mathbb{R}$

8. $\mathbb{Q}(i)$ على $\mathbb{Q}$ **9.** $\mathbb{Q}(\sqrt[4]{2})$ على $\mathbb{Q}$

10. تبعًا للمبرهنة 23.30، العنصر $\alpha + 1$ من $\mathbb{Z}_2(\alpha)$ في المثال 19.29 جبري على $\mathbb{Z}_2$. أوجد كثيرة الحدود غير المختزلة لـ $\alpha + 1$ في $\mathbb{Z}_2[x]$.

مفاهيم

في التمارين 11 إلى 14، صحّح التعريفات للفقرات المكتوبة بخط مائل، دون الرجوع إلى الكتاب – إذا كانت هناك حاجة للتصحيح – وذلك حتى تصبح في شكل قابل للنشر.

11. المتجهات في مجوعة جزئية S من فضاء المتجهات V على الحقل F يولد V، إذا وفقط إذا كان كل $\beta \in V$ يمكن التعبير عنها بصورة وحيدة بوصفها تركيبًا خطيًّا من متجهات S.

12. المتجهات في المجموعة الجزئية S من فضاء المتجه V على الحقل F مستقلة خطيًّا على F، إذا وفقط إذا كان المتجه الصفر لا يمكن أن يكون تركيبًا خطيًّا من متجهات في S.

13. البعد على F لفضاء متجهات منتهي البعد V على الحقل F، هو أصغر عدد مطلوب من المتجهات ليولد V.

14. الأساس لفضاء المتجهات على الحقل F، هو مجموعة متجهات في V تولد V وتكون مرتبطة خطيًّا.

15. ضع إشارة صح أو إشارة خطأ:

ـــــــــ أ. مجموع متجهين يكون متجهًا.

ـــــــــ ب. مجموع قياسيين يكون متجهًا.

ـــــــــ جـ. حاصل ضرب قياسيين يكون قياسيًا.

ـــــــــ د. حاصل ضرب قياسي في متجه يكون متجهًا.

ـــــــــ هـ. كل فضاء متجهات له أساس منتهٍ.

ـــــــــ و. المتجهات في أساس تكون مرتبطة خطيًا.

ـــــــــ ز. متجه الصفر يمكن أن يكون جزءًا من أساس.

ـــــــــ ح. إذا كان $F \leq E$ و $\alpha \in E$ جبريًا على الحقل F، فإنّ α^2 جبري على F.

ـــــــــ ط. إذا كان $F \leq E$ و $\alpha \in E$ جبريًا على الحقل F، فإنّ $\alpha + \alpha^2$ جبري على F.

ـــــــــ ي. كل فضاء متجهات له أساس.

التمارين الآتية تتناول دراسات مستقبلية لفضاء المتجهات، وفي كثير من الحالات نكون مطالبين بأن نعرّف بعض المفاهيم لفضاء المتجهات مشابهة لتلك التي تمّت دراستها لبنى جبرية أخرى، ستطور هذه التمارين قدراتنا لنتعرّف حالات متوازية ومرتبطة بالجبر.

لا يعتمد أي من التمارين الآتية على المفاهيم المعرفة في التمارين السابقة.

16. ليكن V فضاء متجهات على الحقل F.

أ. عرِّف فضاءً جزئيًا لفضاء متجهات V على F.

ب. برهن على أنّ تقاطع فضاءات جزئية من V هو أيضًا فضاء جزئي من V على F.

17. ليكن V فضاء متجهات على الحقل F، ولتكن $S = \{\alpha_i \mid i \in I\}$ مجموعة غير خالية من المتجهات في V.

أ. باستخدام التمرين (16 ب)، عرّف الفضاء الجزئي من V المتولد بـ S.

ب. برهن على أنّ المتجهات في الفضاء الجزئي من V المتولد بـ S هي بالتحديد التراكيب الخطية (المنتهية) للمتجهات في S. (قارن بالمبرهنة 6.7).

18. لتكن $V_1, \ldots, V_n$ فضاءات متجهات على الحقل F نفسه. عرِّف الجمع المباشر $V_1 \oplus \ldots \oplus V_n$ لفضاءات المتجهات V_i لكل $i = 1, \ldots, n$، وأثبت أنّ الجمع المباشر هو أيضًا فضاء متجهات على F.

19. عمِّم المثال 2.30 لتحصل على فضاء المتجهات F^n لمتعددات مرتبة من الرتبة n لعناصر من F على الحقل F، ما الأساس لـ F^n؟

20. عرِّف تماثلًا لفضاء المتجهات V على الحقل F مع فضاء متجهات V' على الحقل F نفسه.

براهين

21. برهن على أنه إذا كان V فضاء متجهات منتهي البعد على الحقل F، فإنّ المجموعة الجزئية $\{\beta_i, \beta_2, \ldots \beta_n\}$ من V هي أساس لـ V على F، إذا وفقط إذا كان كل متجه في V يمكن التعبير عنه بصورة وحيدة بوصفه تراكيب خطية من β_i.

22. ليكن F أيّ حقل. خذ في الحسبان النظام المكوّن من m معادلة خطية آنية تحتوي على n من المجاهيل:

$$\begin{aligned}
a_{11}X_1 + a_{12}X_2 + \cdots + a_{1n}X_n &= b_1,\\
a_{21}X_1 + a_{22}X_2 + \cdots + a_{2n}X_n &= b_2,\\
&\vdots\\
a_{m1}X_1 + a_{m2}X_2 + \cdots + a_{mn}X_n &= b_m,
\end{aligned}$$

حيث $a_{ij}, b_j \in F$

أ. برهن على أنّ النظام «له حل»، أي إنه توجد $X_1, \ldots, X_n \in F$ تحقق الـ m معادلة، إذا وفقط إذا كان المتجه $\beta = (b_1, \cdots, b_m)$ من F^m هو تركيب خطي للمتجهات $\alpha_j = (a_{1j}, \cdots, a_{mj})$، (هذه النتيجة يمكن برهنتها مباشرة؛ لأنها عمليًّا تعريف للحل، لكن يجب أن تعد النظرية الأساسية لتوافر حل آني لنظام المعادلات الخطية).

ب. من الجزء (أ). برهن على أنه إذا كان $n = m$ و $\{\alpha_j \mid j = 1, \cdots, n\}$ هي أساس لـ F^n، فإنّ النظام يكون له دائمًا حل وحيد.

23. برهن على أنّ كل فضاء متجهات V منتهي البعد، وله البعد n على الحقل F يماثل فضاء المتجهات F^n في التمرين 19.

24. ليكن V و V' فضائي متجهات على الحقل F نفسه، فالدالة $\phi : V \rightarrow V'$ هي **تحويل خطي (linear transformation)** من V إلى V'، إذا تحققت الشروط الآتية لكل $\alpha, \beta \in V$ و $a \in F$:

$$\phi\ (\alpha + \beta) = \phi\ (\alpha) + \phi\ (\beta)$$

$$\phi\ (a\alpha) = a\ (\phi(\alpha))$$

أ. إذا كانت $\{\beta_i \mid i \in I\}$ أساسًا لـ V على F، فبرهن على أنّ التحويل الخطي $\phi : V \rightarrow V'$ يتعين كليًّا بالمتجهات $\phi\ (\beta_i) \in V'$

ب. ليكن $\{\beta_i \mid i \in I\}$ أساسًا لـ V، وليكن $\{\beta_i' \mid i \in I\}$ أي مجموعة من المتجهات من V' – التي ليست بالضرورة مختلفة – برهن على أنه يوجد تحويل خطي وحيد $\phi : V \rightarrow V'$، حيث إنّ $\phi\ (\beta_i) = \beta_i'$.

25. ليكن V', V فضائي متجهات على الحقل F نفسه، وليكن $\phi : V \rightarrow V'$ تحويلًا خطيًّا.

أ. ما المفهوم الذي سبق أن درسناه للبنية الجبرية للزمر والحلقات، ويطابق مفهوم التحويل الخطي؟

ب. عرّف النواة (*kernel*) أو الفضاء الصفري (*nullspace*) لـ ϕ، وبرهن على أنه فضاء جزئي من V.

26. ليكن V فضاء متجهات على الحقل F، وليكن S فضاءً جزئيًّا من V، فعرّف فضاء خارج القسمة V / S (*quotient space*)، وبرهن على أنه فضاء متجهات على F.

27. ليكن V، V' فضائي متجهات على الحقل F نفسه ، وليكن V منتهي البعد على F، وليكن $\dim(V)$ البعد لفضاء المتجهات V على F، ولتكن $\phi : V \rightarrow V'$ تحويلًا خطيًّا.

أ. برهن على أنّ $\phi\ (V)$ فضاء جزئي من V'.

ب. برهن على أنّ $\dim\ (\phi\ [V]) = \dim\ (V) - \dim\ (Ker(\phi))$. [مساعدة: اختر الأساس المناسب لـ V باستخدام المبرهنة 19.30، على سبيل المثال: وسّع أساسًا لـ $\mathrm{Ker}\ (\phi)$ إلى أساس لـ $[V]$.

الفصل 31 الامتدادات الجبرية Algebraic Extensions

الامتدادات المنتهية

رأينا في المبرهنة 23.30 أنه إذا كان الحقل E امتدادًا للحقل F، وكان $\alpha \in E$ جبريًّا على F، فإنّ كل عنصر في $F(\alpha)$ يكون جبريًّا على F، وفي دراستنا لأصفار كثيرات الحدود في $F[x]$، سنكون مهتمين وبصورة حصرية تقريبًا بامتدادات F التي تحوي عناصر جبرية عليه.

1.31 تعريف يسمى الامتداد E للحقل F **امتدادًا جبريًّا على F** **(algebraic extension)**، إذا كان كل عنصر في E جبريًّا على F. ■

2.31 تعريف إذا كان الامتداد E للحقل F ذا بعد منتهٍ n بوصفه فضاء متجهات على F، فإنّ E امتداد منتهٍ من الدرجة n على F **(finite extension of degree n)**. سوف ندع $[E : F]$ لتكون الدرجة n لـ E على F. ■

عندما نقول: إنّ الحقل E امتداد منتهٍ على الحقل F، فإنّ هذا لا يعني أنّ E حقل منتهٍ، إنه يؤكد فقط أنّ E فضاء متجهات منتهي البعد على F، بمعنى أنّ $[E : F]$ منتهٍ.

سنستعمل غالبًا حقيقة أنه إذا كان E امتدادًا منتهيًا لـ F، فإنّ $[E : F] = 1$ إذا وفقط إذا كان $E = F$، ونحتاج فقط إلى أن نلاحظ أنه وبحسب المبرهنة 19.30، يمكن دائمًا توسيع $\{1\}$ لتصبح أساسًا لـ E على F. وهكذا، $[E : F] = 1$ إذا وفقط إذا كان $E = F(1) = F$.

دعونا نعيد النقاش في المبرهنة 23.30، لنثبت أنّ أيّ امتداد منتهٍ E للحقل F يجب أن يكون امتدادًا جبريًّا على F.

3.31 مبرهنة يكون الامتداد المنتهي E للحقل F امتدادًا جبريًّا على F.

البرهان يجب أن نثبت أنه إذا كانت $\alpha \in E$، فإنّ α جبرية على F، وبحسب المبرهنة 1930، إذا كان $[E : F] = n$، فإنّ العناصر

$$1, \alpha, \ldots, \alpha^n$$

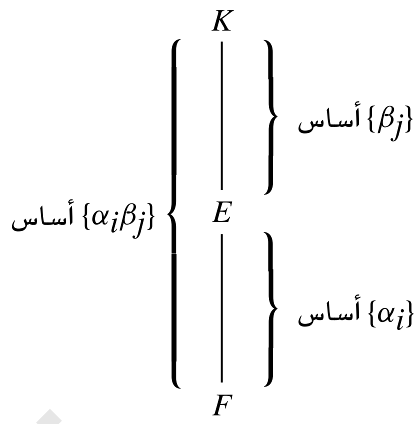
لا يمكن أن تكون عناصر مستقلة خطيًّا. إذن، يوجد $a_i \in F$ بحيث:

$$a_n \alpha^n + \ldots + a_1 \alpha + a_0 = 0$$

وليس كل $a_i = 0$. وهكذا فإنّ $f(x) = a_n x^n + \cdots + a_1 x + a_0$ كثيرة حدود غير صفرية في $F[x]$ و $f(\alpha) = 0$. إذن، α جبرية على F. ♦

لا نغالي عندما نؤكد أهمية المبرهنة الآتية، فهي تؤدي دورًا في نظرية الحقول مشابهًا للدور الذي أدته نظرية لاجرانج في نظرية الزمر، بينما يتمّ برهانها بسهولة باستخدام عملنا الموجز في فضاء المتجهات، فإنها أداة ذات قوة لا تصدق، وبوصفه تطبيقًا رائعًا لها في الفصل المقبل يبرهن استحالة أداء بعض الإنشاءات الهندسية باستخدام المسطرة والفرجار؛ لذا لا تقلل من قيمة المبرهنة التي تعد شيئًا.

4.31 مبرهنة إذا كان الحقل E امتدادًا منتهيًا للحقل F، وكان الحقل K امتدادًا منتهيًا للحقل E، فإنّ K امتداد منتهٍ لـ F، و $[K:F]=[K:E][E:F]$



الشكل 5.31

البرهان لتكن $\{\alpha_i \mid i=1,\cdots,n\}$ أساسًا لـ E بوصفها فضاء متجهات على F، ولتكن المجموعة $\{\beta_j \mid j=1,\cdots,m\}$ أساسًا لـ K بوصفها فضاء متجهات على E، حيث تُثبت المبرهنة إذا أثبتنا أنّ ألـ mn عنصر $\alpha_i\beta_j$ تشكل أساسًا لـ K بوصفها فضاء متجهات على F. (انظر الشكل5.31).

ليكن γ أي عنصر في K، ولأنّ β_j تشكل أساسًا لـ K على E، فإنّ:

$$\gamma=\sum_{j=1}^{m} b_j\beta_j$$

حيث $b_j\in E$، لأنّ α_i تشكل أساسًا لـ E على F، فإنّ:

$$b_j=\sum_{i=1}^{n} a_{ij}\alpha_i$$

حيث $a_{ij}\in F$، إذن:

$$\gamma=\sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{ij}\alpha_i\right)\beta_j=\sum_{i,j} a_{ij}(\alpha_i\beta_j)$$

وهكذا، فإنّ ألـ mn متجه $\alpha_i\beta_j$ تولد K على F.

تبقى علينا أن نثبت أنّ ألـ mn عنصر $\alpha_i\beta_j$ مستقلة على F. افترض أنّ $\Sigma_{i,j}c_{ij}(\alpha_i\beta_j)=0$، حيث $c_{ij}\in F$. إذن:

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{n} c_{ij}\alpha_i\right)\beta_j=0$$

و $\left(\sum_{i=1}^{n} c_{ij}\alpha_i\right)\in E$ لأنّ العناصر β_j مستقلة على E، فإننا نحصل على:

$$\sum_{i=1}^{n} c_{ij}\alpha_i = 0$$

لكل j. ولكن α_i الآن مستقلة على F، وهكذا، فإنّ $\sum_{i=1}^{n} c_{ij}\alpha_i = 0$ تقتضي أنّ $c_{ij} = 0$.
وهكذا، فإنّ $\alpha_i\beta_j$ لا تولد فقط K على F، ولكنها كذلك مستقلة على F. إذن، هي تشكل أساسًا لـ K على F. ♦

لاحظ أننا أثبتنا هذه المبرهنة في الحقيقة بإيجاد أساس، ومن الجدير بالتذكر أنه إذا كانت $\{\alpha_i \mid i = 1, \cdots, n\}$ أساسًا لـ E على F، وكانت $\{\beta_j \mid j = 1, \cdots, m\}$ أساسًا لـ K على E، للحقول $F \le E \le K$، فإنّ المجموعة $\{\alpha_i\beta_j\}$ من حواصل الضرب ألـ mn تشكل أساسًا لـ K على F، يعطي الشكل (5.31) توضيحًا لهذه الحالة، وسوف نوضحه أكثر.

6.31 نتيجة إذا كانت F_i حقولًا، حيث $i = 1, \ldots, r$، وكان F_{i+1} امتدادًا منتهيًا لـ F_i، فإنّ F_r امتداد منتهٍ لـ F_1، و

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \ldots [F_2 : F_1]$$

7.31 نتيجة إذا كان الحقل E امتدادًا للحقل F، وكانت $\alpha \in E$ جبرية على F و $\beta \in F(\alpha)$، فإنّ $\deg(\beta, F)$ تقسم $\deg(\alpha, F)$.

البرهان بحسب المبرهنة 23.30، $\deg(\alpha, F) = [F(\alpha) : F]$ و $\deg(\beta, F) = [F(\beta) : F]$، ولكن $F \le F(\beta) \le F(\alpha)$. إذن وبحسب المبرهنة 4.31، فإنّ $[F(\beta) : F]$ تقسم $[F(\alpha) : F]$. ♦

يوضح المثال الآتي الطريقة التي تتبع عادة باستخدام المبرهنة 4.31. أو إحدى نتائجها.

8.31 مثال بحسب النتيجة 7.31، لا يحوي $\mathbb{Q}(\sqrt{2})$ صفرًا لـ $x^3 - 2$. لاحظ أنّ $\deg(\sqrt{2}, \mathbb{Q}) = 2$، بينما صفر $x^3 - 2$ من الدرجة 3 على $\mathbb{Q}$، ولكن 3 لا تقسم 2. ▲

ليكن الحقل E امتدادًا للحقل F، ولتكن α_1 و α_2 عنصرين في E – ليسا بالضرورة جبريين على F –، وبحسب التعريف، $F(\alpha_1)$ هو أصغر امتداد للحقل F في E ويحوي α_1، وكذلك يمكن أن تُعدّ $(F(\alpha_1))(\alpha_2)$ أصغر امتداد للحقل F في E يحوي كلًّا من α_1 و α_2. كذلك بالإمكان وبصورة مكافئة البداية بـ α_2، إذن: $(F(\alpha_1))(\alpha_2) = (F(\alpha_2))(\alpha_1)$، سنرمز لهذا الحقل بـ $F(\alpha_1, \alpha_2)$، كذلك إذا كان $\alpha_i \in E$، فإنّ $F(\alpha_1, \cdots, \alpha_n)$ هو أصغر امتداد للحقل F في E ويحوي α_i كلها، حيث $i = 1, \ldots, n$، ونحصل على الحقل $F(\alpha_1, \cdots, \alpha_n)$ من الحقل F **بإضافة العناصر** α_i من E إلى F، يثبت التمرين 49 في الفصل 18 – بصورة مماثلة لتقاطع زمر جزئية محتواة في زمرة – أنّ تقاطع حقول جزئية من الحقل E هو كذلك حقل جزئي من E. وهكذا، فإنه يمكن أن تُعدّ $F(\alpha_1, \cdots, \alpha_n)$ بوصفها تقاطع الحقول الجزئية كلها من E، التي تحوي F والعناصر α_i جميعها، حيث $i = 1, \ldots, n$.

مثال 9.31 اعتبر $\mathbb{Q}(\sqrt{2})$، حيث تثبت المبرهنة 23.30 أنّ $\{1, \sqrt{2}\}$ تشكل أساسًا لـ $\mathbb{Q}(\sqrt{2})$ على $\mathbb{Q}$، وباستخدام الخطوات التي عرضت في المثال 10.29، يمكننا اكتشاف أنّ $\sqrt{3} + \sqrt{2}$ صفر لـ $x^4 - 10x^2 + 1$، وباستخدام الطريقة التي عرضت في المثال 14.23، يمكننا إثبات أنّ كثيرة الحدود هذه غير مختزلة في $\mathbb{Q}[x]$، إذن:

$\operatorname{irr}(\sqrt{2}+\sqrt{3}, \mathbb{Q}) = x^4 - 10x^2 + 1$، وهكذا، فإنّ $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$. إذًا $(\sqrt{2}+\sqrt{3}) \notin \mathbb{Q}(\sqrt{2})$، ما يعني أنّ $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$؛ لذلك $\{1, \sqrt{3}\}$ تشكل أساسًا لـ $(\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ على $\mathbb{Q}(\sqrt{2})$. إثبات المبرهنة 4.31 – انظر الملاحظة الآتية للمبرهنة – يرينا أنّ $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ يشكل أساسًا لـ $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ على $\mathbb{Q}$. ▲

مثال 10.31 ليكن $2^{\frac{1}{3}}$ الجذر التكعيبي الحقيقي لـ 2 و $2^{\frac{1}{2}}$ الجذر التربيعي الموجب لـ 2، إذن: $2^{\frac{1}{2}} \notin \mathbb{Q}(2^{\frac{1}{3}})$؛ لأن $\deg(2^{\frac{1}{2}}, \mathbb{Q}) = 2$ و2 ليست من قواسم $3 = \deg(2^{\frac{1}{3}}, \mathbb{Q})$، وهكذا $[\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}(2^{\frac{1}{3}})] = 2$، ما يعني أنّ $\{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}\}$ تشكل أساسًا لـ $\mathbb{Q}(2^{\frac{1}{3}})$ على $\mathbb{Q}$ و $\{1, 2^{\frac{1}{2}}\}$ تشكل أساسًا لـ $\mathbb{Q}(2^{\frac{1}{3}}, 2^{\frac{1}{2}})$ على $\mathbb{Q}(2^{\frac{1}{3}})$، إضافة إلى ذلك، وبحسب المبرهنة 4.31

– انظر الملاحظة الآتية للمبرهنة –

$$\left\{1,\ 2^{\frac{1}{2}},\ 2^{\frac{1}{3}},\ 2^{\frac{5}{6}},\ 2^{\frac{2}{3}},\ 2^{\frac{7}{6}}\right\}$$

تشكل أساسًا لـ $\mathbb{Q}(2^{\frac{1}{3}}, 2^{\frac{1}{2}})$ على $\mathbb{Q}$، ولأنّ $2(2^{\frac{1}{6}}) = 2^{\frac{7}{6}}$، نحصل على أنّ $2^{\frac{1}{6}} \in \mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}})$.

الآن، $2^{\frac{1}{6}}$ يمثل صفرًا لـ $x^6 - 2$، وهي غير مختزلة على $\mathbb{Q}$ – بحسب معيار أيزنستاين – حيث

$p = 2$. إذن:

$$\mathbb{Q} \leq \mathbb{Q}(2^{\frac{1}{6}}) \leq \mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}})$$

وبحسب المبرهنة 4.31

$$6 = [\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}] = [\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}(2^{\frac{1}{6}})]\ [\mathbb{Q}(2^{\frac{1}{6}}) : \mathbb{Q}]$$

$$= [\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}(2^{\frac{1}{6}})]\,(6)$$

لذلك يجب أن نحصل على:

$$\left\{\mathbb{Q}\left(2^{\frac{1}{2}}, 2^{\frac{1}{3}}\right) : \mathbb{Q}\left(2^{\frac{1}{6}}\right)\right\} = 1$$

وهكذا، فإنّ $\mathbb{Q}\left(2^{\frac{1}{2}}, 2^{\frac{1}{3}}\right) = \mathbb{Q}\left(2^{\frac{1}{6}}\right)$، بحسب التعليق السابق للمبرهنة 3.31. ▲

يثبت المثال 10.31 أنه من الممكن للامتداد $F(\alpha_1, \ldots, \alpha_n)$ على الحقل F أن يكون في الحقيقة امتدادًا بسيطًا، حتى لو كانت $n > 1$.

لنصف امتدادات F من الصورة $F(\alpha_1, \ldots, \alpha_n)$ في حالة أنّ ألـ α_i كلها جبرية على F.

مبرهنة 11.31 ليكن الحقل E امتدادًا جبريًّا للحقل F. فإنه يوجد عدد منته من العناصر $\alpha_1, \cdots, \alpha_n$ في E بحيث $E = F(\alpha_1, \cdots, \alpha_n)$، إذا وفقط إذا كان E فضاء متجهات ذا بعد منتهٍ على F، بمعنى أنه إذا وفقط إذا كان E امتدادًا منتهيًا لـ F.

البرهان افترض أنّ $E = F(\alpha_1, \cdots, \alpha_n)$، ولأنّ E امتداد جبري لـ F، وكل α_i جبرية على F؛ لذلك كل α_i جبرية على كل حقل امتداد لـ F في E ، وهكذا، فإنّ $F(\alpha_1)$ جبري على F، وبوجه عام $F(\alpha_1, \ldots, \alpha_j)$ جبري على $F(\alpha_1, \ldots, \alpha_{j-1})$ لكل $j = 2, \ldots, n$. لتطبيق النتيجة 6.31 على متتالية الامتدادات المنتهية

$$F,\ F(\alpha_1),\ F(\alpha_1, \alpha_2), \cdots, F(\alpha_1, \cdots, \alpha_n) = E$$

هذا يثبت أنّ E امتداد منتهٍ لـ F.

في المقابل، افترض أنّ E امتداد جبري منته على F، فإذا كان $[E : F] = 1$، فإنّ $E = F(1) = F$، وبذلك نكون قد انتهينا، وإذا كان $E \neq F$، لتكن $\alpha_1 \in E$، بحيث $\alpha_1 \notin F$.

ثم $[F(\alpha_1) : F] > 1$. إذا كان $F(\alpha_1) = E$ ، نكون قد انتهينا، أمّا إذا لم يكن كذلك فلتكن $\alpha_2 \in E$، بحيث $\alpha_2 \notin F(\alpha_1)$، وبالاستمرار بهذا العمل، نرى من المبرهنة 4.31 ولأنّ $[E : F]$ منتهٍ، فيجب أن نصل إلى α_n بحيث:

$$F(\alpha_1, \cdots, \alpha_n) = E$$ ♦

الحقول المغلقة جبريًا والإغلاق الجبري

لم نلاحظ بعد أنه إذا كان الحقل E امتدادًا للحقل F ، وكانت $\alpha, \beta \in E$ جبرية على F،

فكذلك الحال مع $\alpha + \beta, \alpha\beta, \alpha - \beta$ و $\frac{\alpha}{\beta}$ إذا كانت $\beta \neq 0$، ينتج هذا عن المبرهنة 3.31، وكذلك فإنه متضمن في المبرهنة الآتية:

مبرهنة 12.31 ليكن الحقل E امتدادًا لـ F. فإنّ:

$$\overline{F}_E = \{\alpha \in E \mid \text{جبرية على } F\ \alpha\}$$

تشكل حقلاً جزئيًا من E، ويسمى **الإغلاق الجبري لـ F في E (algebraic closure)**.

البرهان لتكن $\alpha, \beta \in \bar{F}_E$، تثبت المبرهنة 11.31 أنّ $F(\alpha, \beta)$ امتداد منته على F، وبحسب المبرهنة 3.31، كل عنصر في $F(\alpha, \beta)$ جبري على F، بمعنى أن $F(\alpha, \beta) \subseteq \bar{F}_E$، وهكذا يحوي $\bar{F}_E$ كلاً من $\alpha + \beta, \alpha\beta, \alpha - \beta$، وكذلك يحوي $\dfrac{\alpha}{\beta}$ إذا كانت $\beta \neq 0$، إذن: $\bar{F}_E$ حقل جزئي من E. ♦

13.31 نتيجة مجموعة الأعداد الجبرية تشكل حقلًا.

البرهان برهان هذه النتيجة مباشر من المبرهنة 12.31؛ لأن مجموعة الأعداد الجبرية هي الإغلاق الجبري لـ $\mathbb{Q}$ في $\mathbb{C}$. ♦

إنه من المعلوم أنّ الأعداد المركبة تتمتع بخاصية أنّ كلّ كثيرة حدود غير ثابتة في $\mathbb{C}[x]$ لها صفر في $\mathbb{C}$، وهذا معروف بأنه النظرية الأساسية في الجبر، فهناك إثبات تحليلي لهذه النظرية معطًى في المبرهنة 18.31، ونقدّم الآن تعريفًا يعمّم هذا المفهوم المهم للحقول الأخرى.

14.31 تعريف يسمّى الحقل F **مغلقًا جبريًا (algebraically closed)** إذا كانت كل كثيرة حدود غير ثابتة في $F[x]$ لها صفر في F. ■

لاحظ أنّ الحقل F قد يكون إغلاقًا جبريًا للحقل F في امتداد E ومن غير أن يكون F مغلقًا جبريًا، على سبيل المثال: $\bar{\mathbb{Q}}$ هو الإغلاق الجبري لـ $\mathbb{Q}$ في $\mathbb{Q}(x)$، ولكن $\bar{\mathbb{Q}}$ ليس مغلقًا جبريًا؛ لأن $x^2 + 1$ لا جذور لها في $\mathbb{Q}$.

تثبت المبرهنة الآتية حقيقة مفهوم أنّ الحقل مغلق جبريًا يمكن أن يعرّف باستخدام تحليل كثيرات الحدود على الحقل.

15.31 مبرهنة يكون الحقل F مغلقًا جبريًا إذا وفقط إذا كانت كل كثيرة حدود غير ثابتة في $F[x]$، يمكن تحليلها في $F[x]$ إلى عوامل خطية.

البرهان ليكن F مغلقًا جبريًا، ولتكن $f(x)$ كثيرة حدود غير ثابتة في $F[x]$. إذن $f(x)$ لها صفر $a \in F$، فبحسب النتيجة 3.23، $x - a$ عامل من عوامل $f(x)$، وهكذا، فإنّ $f(x) = (x - a)\, g(x)$، وإذا كانت $g(x)$ غير ثابتة، فإنّ لها صفرًا $b \in F$، وهكذا نحصل على: $f(x) = (x - a)(x - b)h(x)$، وبالاستمرار نحصل على تحليل $f(x)$ في $F[x]$ إلى عوامل خطية.

في المقابل، افترض أنّ كل كثيرة حدود غير ثابتة في $F[x]$ تحلل إلى عوامل خطية، فإذا كان $ax - b$ عاملًا خطيًا لـ $f(x)$، فإنّ $\dfrac{a}{b}$ صفر لـ $f(x)$، إذن: F مغلق جبريًا. ♦

16.31 نتيجة الحقل المغلق جبريًا F لا يوجد له امتداد جبري فعلي، بمعنى أنه لا يوجد امتداد جبري E، بحيث $F < E$.

البرهان ليكن E امتدادًا جبريًا لـ F، إذن: $F \leq E$، فإذا كانت $\alpha \in E$، فإنّ $\text{irr}\,(\alpha, F) = x - \alpha$ بحسب المبرهنة 15.31؛ لأن F مغلق جبريًا، إذن: $\alpha \in F$، ويجب أن تكون $F = E$. ♦

سنبرهن على أنه كما يوجد امتداد جبري مغلق $\mathbb{C}$ للأعداد الحقيقية $\mathbb{R}$، فلكل حقل F يوجد كذلك امتداد جبري $\bar{F}$ لـ F مع خاصية أنّ $\bar{F}$ مغلق جبريًا، ببساطة، لإيجاد $\bar{F}$، سنقوم بالآتي: إذا كانت كثيرة الحدود $f(x)$ في $F[x]$ لا أصفار لها في F، فأضف صفر α لـ $f(x)$ إلى F، وهكذا الحصول على الحقل $F(\alpha)$. حيث تستعمل المبرهنة 3.29 – مبرهنة كرونكر –بقوة هنا بالطبع، فإذا كان $F(\alpha)$ لا يزال غير مغلق جبريًا، فاستمر في هذا العمل أكثر.

المشكلة هنا – وخلافًا لحالة الإغلاق الجبري $\mathbb{C}$ لـ $\mathbb{R}$، قد نحتاج إلى عمل هذا – ربما – عدد لا نهائي من المرات، من الممكن إثبات (انظر التمرين 33 و 36) أنّ $\overline{\mathbb{Q}}$ متماثل مع حقل الأعداد الجبرية، ولا يمكننا الحصول على $\overline{\mathbb{Q}}$ من $\mathbb{Q}$ بإضافة عدد منته من الأعداد الجبرية، ويجب علينا في البداية أن نناقش بعض آليات نظرية المجموعات – تمهيدية زورن – لنصبح قادرين على التعامل مع هذه الحالة، هذه الآلية معقدة بعض الشيء، لذلك سنضع البرهان تحت عنوان مستقل، إضافة إلى أنّ نظرية توافر $\overline{F}$ مهمة جدًّا، وسنذكرها هنا؛ لكي نعرف هذه الحقيقة، حتى لو لم ندرس برهانها.

17.31 مبرهنة يوجد **إغلاق جبري** لكل حقل F، أي امتداد جبري $\overline{F}$ الذي يكون مغلقًا جبريًّا.

إنه من المعلوم أن $\mathbb{C}$ مغلق جبريًّا، وسنذكر برهانًا تحليليًّا للطلاب الذين درسوا مادة الدوال ذات المتغيرات المركبة، حيث توجد براهين جبرية، إلّا أنها أطول.

18.31 مبرهنة (**النظرية الأساسية في الجبر**) حقل الأعداد المركبة $\mathbb{C}$ مغلق جبريًّا.

البرهان لتكن كثيرة الحدود $f(z) \in \mathbb{C}[z]$ بلا أصفار في $\mathbb{C}$، ما يؤدي إلى أن تكون $\frac{1}{f(z)}$ دالة صحيحة، بمعنى أنّ $\frac{1}{f}$ تحليلية في كل مكان، وكذلك إذا كان $f \notin \mathbb{C}$، فإنّ $\lim_{|z|\to\infty} |f(z)| = \infty$، إذن: $\lim_{|z|\to\infty} \left|\frac{1}{f(z)}\right| = 0$، وهكذا، فإنّ $\frac{1}{f}$ يجب أن تكون محدودة في المستوى، إذن، وبحسب مبرهنة ليوفيل في نظرية الدوال المركبة، فإنّ $\frac{1}{f}$ ثابتة، ما يؤدي إلى أن تكون f ثابتة، وهكذا، فإنّ أي كثيرة حدود غير ثابتة في $\mathbb{C}[z]$ يجب أن يكون لها صفر في $\mathbb{C}$، إذن، $\mathbb{C}$ مغلقة جبريًّا. ♦

إثبات وجود الإغلاق الجبري

سنثبت أنه يوجد امتداد جبري لكل حقل، بحيث يكون مغلقًا جبريًّا، يتعيّن أن تكون لطالب الرياضيات الفرصة برؤية بعض البراهين التي تتضمن مسلمة الاختيار قبل إنهاء دراسته الجامعية، وهذا مكان طبيعي لمثل هذا البرهان، سنستخدم التكافؤ بين تمهيدية زورن ومسلمة الاختيار، ولعرض تمهيدية زورن، يجب علينا إعطاء تعريف من نظرية المجموعات.

19.31 تعريف **الترتيب الجزئي للمجموعة S (*partial order*)** يعطى بالعلاقة $\leq$ المعرفة على بعض الأزواج المرتبة لعناصر من S، بحيث تتحقق الشروط الآتية:

1. $a \leq a$ لكل $a \in S$ **علاقة انعكاسية** (***Reflexive***).

2. إذا كان $a \leq b$ و $b \leq a$، فإنّ $a = b$ **علاقة قطرية التناظر** (***Antisymmetric***).

3. إذا كان $a \leq b$ و $b \leq c$، فإنّ $a \leq c$ **علاقة متعدية** (***Transitive***). ■

علاقة الترتيب الجزئي، ليس بالضرورة أن يكون كل عنصرين **قابلين للمقارنة (*Comparable*)**، بمعنى أنّه إذا كان $a, b \in S$، فليس بالضرورة أن يكون $a \leq b$ أو $b \leq a$، وكالعادة، $a < b$ تعني $a \leq b$ ولكن $a \neq b$.

تسمى المجموعة الجزئية T من مجموعة مرتبة جزئيًّا S **سلسلة (*Chain*)** إذا كان بالإمكان المقارنة بين أي عنصرين a و b في T، بمعنى أنّ $a \leq b$ أو $b \leq a$ (أو كليهما)، ويكون العنصر $u \in S$ **حدًّا أعلى للمجموعة الجزئية** A **(*upper bound*)** من مجموعة مرتبة جزئيًّا S إذا كان $a \leq u$ لكل $a \leq A$. أخيرًا، يكون العنصر m من مجموعة مرتبة جزئيًّا S **أعظميًّا (*maximal*)** إذا لم يوجد $s \in S$، بحيث $m < s$.

20.31 مثال مجموعة المجموعات الجزئية جميعها من مجموعة ما تشكل مجموعة مرتبة جزئيًّا مع العلاقة $\leq$ المعطاة بـ $\subseteq$، على سبيل المثال: إذا كانت المجموعة كاملة $\mathbb{R}$، فإنّ $\mathbb{Z} \subseteq \mathbb{Q}$، لاحظ – على أيّ حال – أنه لـ $\mathbb{Z}$ و $\mathbb{Q}^+$، فليس صحيحًا أنّ $\mathbb{Z} \subseteq \mathbb{Q}^+$ أو $\mathbb{Q}^+ \subseteq \mathbb{Z}$. ▲

21.31 تمهيدية **تمهيدية زورن (*Zorn's Lemma*)**: إذا كانت S مجموعة مرتبة جزئيًّا، بحيث إنّ كل سلسلة في S لها حد أعلى في S، فإنّ S تحوي على الأقل عنصرًا أعظميًّا.

لا يوجد سؤال عن برهان تمهيدية زورن، فالتمهيدية مكافئة لمسلمة الاختيار، وهكذا، فإننا في الحقيقة نأخذ تمهيدية زورن هنا بوصفها مسلمة في نظرية المجموعات. ارجع إلى المصادر لمعرفة نصّ مسلمة الاختيار وبرهان أنها مكافئة لتمهيدية زورن. (ارجع إلى [47]Edgerton).

تكون تمهيدية زورن في العادة مفيدة عندما نريد إثبات توافر عنصر كبير أو أعظمي في بناء من نوع ما، وإذا كان الحقل F له امتداد جبري $\overline{F}$ ، فبالتأكيد سيكون امتدادًا جبريًّا أعظميًّا لـ F؛ لأن $\overline{F}$ مغلق جبريًّا، فلن يكون له امتداد جبري حقيقي.

إنّ فكرة إثباتنا للمبرهنة 17.31 بسيطة جدًا، فإذا أُعطينا الحقل F، فسوف نصف في البداية مجموعة من الامتدادات الجبرية لـ F، بحيث تكون كبيرة جدًّا لدرجة أنها تحوي (تبعًا للتماثل) أي امتداد جبري معقول لـ F، ثم نعرف ترتيبًا جزئيًّا – الترتيب العادي للحقول الجزئية – في هذه المجموعة، ثم نثبت أنّ فرضيات تمهيدية زورن متحققة، حيث إنه بحسب تمهيدية زورن، سيكون هناك امتداد جبري أعظمي $\overline{F}$ لـ F في هذه المجموعة، ومن ثم سنناقش بأنه بوصفه عنصرًا أعظميًّا، فإن هذا الامتداد $\overline{F}$ لن يكون له امتداد جبري فعلي، وهكذا، فإنه يجب أن يكون مغلقًا جبريًّا.

يختلف برهاننا قليلاً عن البراهين المتوافرة في الكثير من الكتب، ونفضله لأنه لا يستخدم من الجبر أكثر من ذلك المستنتج من المبرهنتين 3.29 و 4.31. وهكذا، فهي تعتمد بقدر كبير ومريح على قوة كل من مبرهنة كرونكر وتمهيدية زورن، يبدو البرهان طويلاً، وذلك فقط لأننا نكتب كل خطوة، أمّا للرياضيين المحترفين، فبناء البرهان من المعلومات في الفقرة السابقة يُعدّ مسألة روتينية، وقد اقتُرح هذا البرهان على المؤلف أيام دراسته العليا من زميل دراسته نورمان شابيرو (Norman Shapiro) الذي كان يفضله كثيرًا كذلك.

■ **نبذة تاريخية**

على الرغم من أنّ مسلمة الاختيار استُخدمت بصورة ضمنية في عامي 1870م و 1880م، إلّا أنها أُعلنت صراحة على يد إرنست زيرملو (Ernst Zermelo) عام 1904م، مرتبطة ببرهانه لنظرية الترتيب الحسن التي نصت على أنّ لأي مجموعة A، توجد علاقة ترتيب $<$ ، حيث كلّ مجموعة جزئية غير خالية B من A تحتوي عنصرًا أصغر بحسب العلاقة $<$، وتؤكد مسلمة الاختيار لزيرملو أنّ لأي مجموعة M والمجموعة S المكوّنة من جميع المجموعات الجزئية من M، توجد دائمًا دالة "اختيار" $f : S \to M$، حيث $f(M') \in M'$ لكل M' في S.

في الحقيقة، لاحظ زيرملو أنّ هذا المبدأ المنطقي لا يمكن ... أن يختزل إلى صورة أبسط، ولكنه يستخدم بلا تردد في الاستنتاج الرياضي في كل مكان.

وبعد بضع سنوات لاحقة قام بتضمين مسلمته مع مجموعة مسلماته الخاصة بنظرية المجموعات، وقد عُدّلت هذه المجموعة قليلاً عام 1930م، لتشكل ما يُعرف الآن بنظرية المجموعات الخاصة بزيرملو – فرانكل (Zermelo – Frankel)، عمومًا نظام المسلمات يُعمل به اليوم بوصفه أساسًا لتلك النظرية.

قدّم ماكس زورن (Max Zorn 1906 – 1993) تمهيدية زورن عام 1935م، على الرغم من إدراكه أنها تكافئ نظرية الترتيب الحسن (التي تكافئ بدورها مسلمة الإختيار)، وادعى أنّ استخدام تمهيديته في الجبر طبيعي أكثر؛ لأن نظرية الترتيب الحسن كانت بصورة أو بأخرى مبدأً "متساميًا"، وفي الحال وافق الرياضيون الآخرون على تعليله، حيث ظهرت التمهيدية عام 1939م في المجلد الأول لنيكولس بورباكي

(Nicols Bourbaki's Eléments de Mathématique: les structures fondamentales de I'Analyse)

لقد استُخدمت بصورة ثابتة في ذلك العمل، وأصبحت سريعًا جزءًا أساسيًّا من أدوات الرياضيين.

إننا مستعدون الآن لإثبات المبرهنة 17.31. التي سنعيد هنا صياغتها.

22.31 إعادة صياغة المبرهنة 17.31 لكل حقل F إغلاق جبري $\bar{F}$.

البرهان يمكن الإثبات في نظرية المجموعات أنه لأي مجموعة معطاة، توجد مجموعة تحوي عناصر أكثر تمامًا. افترض أننا شكّلنا المجموعة:

$$A = \{\omega_{f,i} \mid f \in F[x]; i = 0, \cdots, (\text{degree } f)\}$$

التي تحوي عنصرًا لكل صفر محتمل لكل $f(x) \in F[x]$، لتكن Ω مجموعة تحوي عدد عناصر أكثر تمامًا من عناصر A، وباستبدال $\Omega \cup F$ بدلاً من Ω عند الضرورة، يمكننا أن نفترض أنّ $F \subset \Omega$. لتكن الحقول جميعها الممكنة بوصفها امتدادات جبرية لـ F ، التي تكون – بوصفها مجموعات – مكوّنة من عناصر من Ω، فأحد هذه الامتدادات الجبرية هي F نفسها، فإذا كان الحقل E أيّ امتداد $F[\gamma]$، وإذا كانت $\gamma \in E$ هي صفر لـ $F[x]$ $f(x) \in$ و $\gamma \notin F$ و $\deg(\gamma, F) = n$، فإنه وبإعادة تسمية γ بـ ω حيث $\omega \in \Omega$ و $\omega \notin F$، وإعادة تسمية العناصر $a_0 + a_1\gamma + \cdots + a_{n-1}\gamma^{n-1}$ من $F(\gamma)$ بعناصر مختلفة من Ω والعناصر a_i بعناصر من F، فيمكننا أن نعدّ $F(\gamma)$ بعد إعادة تسميته بوصفها امتدادًا جبريًّا $F(\omega)$ لـ F، بحيث $F(\omega) \subseteq \Omega$ و $f(\omega) = 0$. تحوي المجموعة Ω عناصر كافية لتكوين $F(\omega)$؛ لأن Ω فيها عناصر أكثر من كافية لتزويدنا بـ n من الأصفار المختلفة لكل عنصر من كل درجة n في أي مجموعة

جزئية من $F[x]$.

امتدادات الحقول الجبرية كلها E_j لـ F، حيث $E_j \subseteq \Omega$ تشكل المجموعة

$$S = \{E_j \mid j \in J\}$$

التي تكون مرتبة جزئيًّا مع علاقة الاحتواء العادية للحقول الجزئية$\leq$. أحد عناصر S هو F نفسه، والفقرات السابقة تثبت أنه إذا كان F غير مغلق جبريًّا، فسيكون هناك الكثير من الحقول E_j في S.

لتكن $T = \{E_{jk}\}$ أي سلسلة في S، ولتكن $W = \cup_k E_{j_k}$، سنصنع من W حقلاً، فلتكن $\alpha, \beta \in W$، فيوجد $E_{j1}, E_{j2} \in S$، بحيث $\alpha \in E_{j1}$ و $\beta \in E_{j2}$، ولأنّ T سلسلة، فإنّ أحد الحقلين E_{j1} و E_{j2} حقل جزئي من الآخر، وليكن $E_{j1} \leq E_{j2}$، إذن: $\alpha, \beta \in E_{j2}$.

سنستخدم عمليات الحقل E_{j2} لنعرّف جمع α وβ في W كـ $(\alpha + \beta) \in E_{j2}$ وبالمثل حاصل الضرب $(\alpha\beta) \in E_{j2}$، فهاتان العمليتان حسنتا التعريف في W، وهما مستقلتان عن تعريفنا لـ E_{j2}؛ لأنه إذا كانت $\alpha, \beta \in E_{j3}$ كذلك حيث E_{j3} عنصر في T، فإنّ أحد الحقلين E_{j2} و E_{j3} يكون حلقة جزئية من الآخر؛ لأن T سلسلة، إذن، صارت عمليتا الجمع والضرب معرفتين لدينا على W.

تتحقق الآن مسلمات الحقل كلها في W مع هاتين العمليتين، باستخدام حقيقة أنهما معرفتان باستخدام الجمع والضرب في الحقول، وهكذا، وعلى سبيل المثال: $1 \in F$ يؤدي دور العنصر المحايد للضرب في W؛ لأنه لكل $\alpha \in W$، إذا كان $1,\alpha \in E_{j1}$ فإنّ $1\alpha = \alpha$ في E_{j1}، وهكذا $1\alpha = \alpha$ في W، بحسب تعريف الضرب في W، ولمزيد من التوضيح، نتحقق من قوانين التوزيع، لتكن $\alpha, \beta, \gamma \in W$، ولأنّ T سلسلة، فيمكننا إيجاد حقل واحد في T يحوي العناصر الثلاثة α، β وγ، حيث تتحقق في هذا الحقل خاصية التوزيع على α، وβ، وγ، وبهذا، فهي تتحقق في W، وهكذا يمكننا أن نعدّ W حقلاً، ومن خلال الإنشاء، $E_{jk} \leq W$ لكل $E_{jk} \in T$.

فإذا تمكنّا من إثبات أنّ W جبري على F، فإنّ $W \in S$ ستكون حدًّا أعلى لـ T، ولكن إذا كان $\alpha \in W$، فإنّ $\alpha \in E_{j1}$ لأحد العناصر E_{j1} في T، وهكذا، فإنّ α جبرية على F، إذن، W امتداد جبري لـ F وحدّ أعلى لـ T.

تتحقق فرضيات تمهيدية زورن، وهكذا، فإنه يوجد عنصر أعظمي $\bar{F}$ في S، فندّعي أنّ $\bar{F}$ مغلق جبريًّا، ولتكن $f(x) \in \bar{F}[x]$، حيث $f(x) \notin \bar{F}$، وافترض أنّ $f(x)$ لا أصفار لها في $\bar{F}$، ولأنّ Ω تحوي عناصر أكثر من تلك التي تحويها $\bar{F}$، فيمكننا أن نأخذ $\omega \in \Omega$، بحيث $\omega \notin \bar{F}$، ونكوّن الحقل $\bar{F}(\omega) \subseteq \Omega$ وω صفر لـ $f(x)$، كما رأينا في الفقرة الأولى من هذا البرهان، لتكن β في $\bar{F}(\omega)$، وبحسب المبرهنة 23.30. تكون β صفرًا لكثيرة حدود.

$$g(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_n x^n$$

في $\bar{F}[x]$ وبحيث $\alpha_i \in \bar{F}$، وهكذا، فإنّ α_i جبرية على F، إذن وبحسب المبرهنة 11.31. يكون الحقل $F(\alpha_0, \dots, \alpha_n)$ امتدادًا منتهيًا على F، ولأنّ β جبرية على $F(\alpha_0, \dots, \alpha_n)$، فبإمكاننا أن نرى أنّ $F(\alpha_0, \dots, \alpha_n, \beta)$ امتداد منته على F، إذن وبحسب المبرهنة 3.31 β جبرية على F، وهكذا، فإنّ $\bar{F}(\omega) \in S$ و $\bar{F} < \bar{F}(\omega)$، ما يناقض اختيار $\bar{F}$ بوصفها عنصرًا أعظميًّا في S، إذن، يجب أن يكون لـ $f(x)$ صفر في $\bar{F}$ ، إذن، $\bar{F}$ مغلق جبريًّا. ♦

تبدو الخطوات في البرهان السابق عادية للرياضي المحترف، ولأنها المرة الأولى التي نرى فيها استخدام تمهيدية زورن في البرهان، فقد كتبنا البرهان بالتفصيل.

■ تمارين 31

حسابات

في التمارين 1 إلى 13،أوجد الدرجة والأساس للامتداد الحقلي المعطى، وكن مستعدًا لتبرير إجابتك.

1. $\mathbb{Q}(\sqrt{2})$ على $\mathbb{Q}$

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

3. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$ على $\mathbb{Q}$

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

5. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ على $\mathbb{Q}$

6. $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ على $\mathbb{Q}$

7. $\mathbb{Q}(\sqrt{2}\sqrt{3})$ على $\mathbb{Q}$

8. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ على $\mathbb{Q}$

9. $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{6}, \sqrt[3]{24})$ على $\mathbb{Q}$

10. $\mathbb{Q}(\sqrt{2}, \sqrt{6})$ على $\mathbb{Q}(\sqrt{3})$

11. $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ على $\mathbb{Q}(\sqrt{3})$

12. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ على $\mathbb{Q}(\sqrt{2} + \sqrt{3})$

13. $\mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10})$ على $\mathbb{Q}(\sqrt{3} + \sqrt{5})$

مفاهيم

في التمارين 14 إلى 17، صحّح تعريف الحدّ المكتوب بخط مائل دون الرجوع إلى الكتاب – إن كانت هناك حاجة للتصحيح – بحيث يكون بصيغة قابلة للنشر.

14. *الامتداد الجبري* للحقل F، هو الحقل $F(\alpha_1, \alpha_2, \cdots, \alpha_n)$، حيث α_i كلها أصفار لكثيرة حدود في $F[x]$.

15. *الامتداد المنتهي* للحقل F، هو ذلك الذي يمكن الحصول عليه بإضافة عدد منتهٍ من العناصر لـ F.

16. *الإغلاق الجبري* $\overline{F_E}$ للحقل F في الامتداد E للحقل F، هو المكون من عناصر E الجبرية جميعها على F.

17. الحقل F *مغلق جبريًا*، إذا وفقط إذا كانت كل كثيرة حدود لها صفر في F.

18. أثبت بمثال أنّ للامتداد الفعلي E للحقل F، الإغلاق الجبري لـ F في E ليس بالضرورة مغلقًا جبريًا.

19. ضع إشارة صح أو إشارة خطأ:

______ أ. إذا كان الحقل E امتدادًا منتهيًا للحقل F، فإن E حقل منتهٍ.

______ ب. كل امتداد منتهٍ للحقل هو امتداد جبري.

______ جـ. كل امتداد جبري للحقل هو امتداد منتهٍ.

______ د. الحقل الأعلى لبرج منتهٍ لامتداد منتهٍ من الحقول، هو امتداد منتهٍ للحقل في أسفل البرج.

______ هـ. $\mathbb{Q}$ هي الإغلاق الجبري لنفسها في $\mathbb{R}$، أي إنّ $\mathbb{Q}$ مغلقة جبريًا في $\mathbb{R}$.

______ و. $\mathbb{C}$ مغلقة جبريًا في $\mathbb{C}(x)$، حيث x غير معين.

______ ز. $\mathbb{C}(x)$ مغلقة جبريًا، حيث x غير معين.

______ ح. الحقل $\mathbb{C}(x)$ ليس له إغلاق جبري؛ لأن $\mathbb{C}$ تحوي فعليًا الأعداد الجبرية كلها.

______ ط. الحقل المغلق جبريًا يجب أن يكون مميزه 0.

______ ي. إذا كان E امتدادًا مغلقًا جبريًا للحقل F، فإن E امتداد جبري لـ F.

براهين مختصرة

20. أعطِ برهانًا مختصرًا من جملة واحدة للمبرهنة 3.31.

21. أعطِ برهانًا مختصرًا من جملة واحدة للمبرهنة 4.31.

براهين

22. ليكن $(a + bi) \in \mathbb{C}$، حيث $a, b \in \mathbb{R}$ و $b \neq 0$. أثبت أنّ $\mathbb{C} = \mathbb{R}(a + bi)$.

23. أثبت أنه إذا كان E امتدادًا منتهيًا للحقل F وكان $[E : F]$ عددًا أوليًا، فإنّ E امتداد بسيط لـ F وفي الحقيقة $E = F(\alpha)$ لكل $\alpha \in E$، ولا تنتمي إلى F.

24. برهن على أنّ $x^2 - 3$ غير مختزلة على $\mathbb{Q}(\sqrt[3]{2})$.

25. ما درجة امتدادات الحقول التي يمكن الحصول عليها بإضافة جذر تربيعي لعنصر من F ليس مربعًا كاملاً في F، ثمّ جذر تربيعي لعنصر ليس مربعًا كاملاً في هذا الحقل الجديد، وهكذا؟ مستخدمًا ذلك ناقش العبارة: إنّ أي صفر لكثيرة الحدود $x^{14} - 3x^2 + 12$ على $\mathbb{Q}$ لا يمكن التعبير عنه بوصفه دالة نسبية لجذور تربيعية لدالة نسبية لجذور تربيعية – وهكذا – لعناصر في $\mathbb{Q}$.

26. ليكن E امتدادًا منتهيًا للحقل F، وليكن D حلقة تامة، حيث $F \subseteq D \subseteq E$. أثبت أنّ D حقل.

27. برهن بالتفصيل على أنّ $\mathbb{Q}(\sqrt{3} + \sqrt{7}) = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.

28. عمِّم تمرين 27، وأثبت أنه إذا كان $\sqrt{a} + \sqrt{b} \neq 0$، فإنّ $\mathbb{Q}(\sqrt{a} + \sqrt{b}) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ لكل a وb في $\mathbb{Q}$ [مساعدة: احسب $(a - b)/(\sqrt{a} + \sqrt{b})$].

29. ليكن E امتدادًا منتهيًا للحقل F، ولتكن $p(x) \in F[x]$ غير مختزلة على F ودرجتها لا تقسم $[E : F]$. أثبت أنه لا توجد أصفار لـ $p(x)$ في E.

30. ليكن E امتدادًا للحقل F، ولتكن $\alpha \in E$ جبرية ذات درجة فردية على F. أثبت أنّ α^2 جبرية لها درجة فردية على F و $F(\alpha) = F(\alpha^2)$.

31. أثبت أنه إذا كانت F, وE و K حقولاً، حيث $F \leq E \leq K$، فإنّ K جبري على F، إذا وفقط إذا كان E جبريًا على F و K جبريًا على E. (يجب ألّا تفترض أنّ الامتدادات منتهية).

32. ليكن E امتدادًا للحقل F. برهن على أنَّ كل $\alpha \in E$ وليست في الإغلاق الجبري $\overline{F_E}$ لـ F في E متسامٍ على $\overline{F_E}$.

33. ليكن E امتدادًا مغلقًا جبريًّا للحقل F. أثبت أنّ الإغلاق الجبري $\overline{F_E}$ لـ F في E مغلق جبريًّا. (بتطبيق هذا المثال على $\mathbb{C}$ و$\mathbb{Q}$ نرى أنّ الحقل المكون من الأعداد الجبرية جميعها مغلق جبريًّا).

34. أثبت أنه إذا كان E امتدادًا جبريًّا للحقل F ويحتوي الأصفار جميعها في $\overline{F}$ لكل $f(x) \in F[x]$، فإن E حقل مغلق جبريًّا.

35. أثبت أنه لا يوجد حقل منتهٍ ذو مميز فردي مغلق جبريًّا. (في الواقع، لا يوجد حقل منتهٍ مميزه 2 مغلق جبريًّا). [مساعدة: بالعدّ أثبت أنه لمثل هذا الحقل المنتهي F، بعض كثيرات الحدود $x^2 - a$، حيث $a \in F$، ليس لها صفر في F. انظر تمرين 32 الفصل 29].

36. برهن على أنّ – كما تمّ التأكيد في الكتاب – الإغلاق الجبري لـ $\mathbb{Q}$ في $\mathbb{C}$ ليس امتدادًا منتهيًا لـ $\mathbb{Q}$.

37. ناقش العبارة: كل امتداد منتهٍ للحقل $\mathbb{R}$، إما $\mathbb{R}$ نفسها أو يماثل $\mathbb{C}$.

38. استخدم تمهيدية زورن لتثبت أنّ كل مثالي فعلي في حلقة R تحوي عنصرًا محايدًا، يكوّن محتوًى في مثالي أعظمي.

الفصل 32 إنشاءات هندسية[1] Geometric Constructions

في هذا الفصل سنحيد قليلاً عن خطنا لنعطي تطبيقًا يوضّح قوة المبرهنة 4.31 لدراسة أكثر تفصيلاً للإنشاءات الهندسية، ارجع إلى كتاب كورنت وروبنس (Courant and Robbins) [44، الوحدة الثالثة].

ينصب اهتمامنا على أنواع الأشكال التي يمكن بناؤها باستخدام الفرجار والمسطرة، كما في الهندسة الإقليدية التقليدية، وسنناقش استحالة تثليث زوايا معينة وغيرها من الأسئلة التقليدية الأخرى.

الأعداد القابلة للإنشاء

لنتخيل أننا أُعطينا قطعة مستقيمة واحدة فقط، التي سنعرفها بأنها وحدة طول واحدة.

يُسمى العدد الحقيقي α عددًا **قابلاً للإنشاء (*Constructible*)**، وذلك إذا تمكنّا من إنشاء قطعة مستقيمة طولها $|\alpha|$ بعدد منتهٍ من الخطوات من القطعة المعطاة، التي طولها وحدة طول، وذلك باستخدام المسطرة والفرجار.

إنّ قوانين اللعبة صارمة جدًّا، فنفترض أننا أُعطينا نقطتين فقط في هذه اللحظة، ولتكونا طرفي القطعة المستقيمة ذات وحدة الطول، ولنفترض أنهما تقابلان النقطتين $(0, 0)$ و $(1, 0)$ في المستوى الإقليدي، حيث يُسمح لنا الآن أن نرسم خطًّا باستعمال المسطرة فقط، وذلك بين النقطتين اللتين تمّ تعيينهما، وهكذا يمكننا البدء باستعمال المسطرة ورسم الخط المار بـ $(0, 0)$ و $(1, 0)$، ويُسمح لنا بأن نفتح الفرجار مسافة تساوي ما بين النقطتين فقط، دعونا الآن نركز رأس الفرجار في النقطة $(1, 0)$، ونرسم دائرة بنصف قطر 1، التي تمر بالنقطة $(2, 0)$، وهكذا نكون قد عيّنا نقطة ثالثة $(2, 0)$، وبالاستمرار بهذه الطريقة نستطيع تعيين النقاط $(3, 0)$، $(4, 0)$، $(-1, 0)$ $(-2, 0)$ وهكذا...، الآن نفتح الفرجار مسافة تساوي البعد بين $(0, 0)$ و$(2, 0)$، ثمّ نضع رأس الفرجار في النقطة $(1, 0)$، ونرسم دائرة بنصف قطر 2، ونكرر العمل مع النقطة $(-1, 0)$، وبذلك نكون قد أوجدنا نقطتين جديدتين، وذلك حيث تتقاطع الدائرتان وحيث نستطيع أن نضع المسطرة عليهما، ونرسم ما يُسمى بمحور الصادات، ثمَّ نفتح الفرجار مسافة تساوي ما بين $(0, 0)$ و$(1, 0)$، ونرسم دائرة مركزها $(0, 0)$، ونعيّن النقطة $(0, 1)$ حيث تتقاطع الدائرة مع محور الصادات، وبالاستمرار في العمل على النمط نفسه، نستطيع تعيين النقاط (x, y) جميعها ذات الإحداثيات الصحيحة في أي مستطيل يحوي النقطة $(0, 0)$، ودون الخوض في مزيد من التفاصيل، نستطيع أن نثبت أنه بالإمكان إقامة عمود على خطٍّ معطًى من نقطة معلومة على الخط.

كذلك نستطيع إيجاد خط يمر من خلال نقطة معلومة وموازٍ لخطٍّ معطى، نتيجتنا الأولى هي المبرهنة الآتية:

مبرهنة 1.32 إذا كان α وβ عددين حقيقيين قابلين للإنشاء، فإنّ $\alpha + \beta$، $\alpha - \beta$، $\alpha\beta$ و α / β كلها أعداد حقيقية قابلة للإنشاء، إذا كان $\beta \neq 0$.

[1] لن يتم استخدام هذا الفصل في بقية هذا الكتاب.

البرهان أُعطينا α و β قابلين للإنشاء؛ لذلك توجد قطع مستقيمة بطول $|\alpha|$ و $|\beta|$، إذا كانت $\alpha, \beta > 0$، فمدّ قطعة مستقيمة بطول α بالمسطرة، ابدأ بأحد طرفي القطعة الأصلية بطول α، وخذ على الامتداد الطول β باستخدام الفرجار، هذا يُنشئ قطعة مستقيمة بطول $\alpha + \beta$؛ كذلك $\alpha - \beta$ يمكن إنشاؤها بالطريقة نفسها (انظر الشكل 2.32)، وإذا كان α و β ليس كلاهما موجبًا، فمن الواضح أنه يمكن تقسيم البرهان إلى حالات تبعًا لإشارتيهما، وإثبات أنّ $\alpha + \beta$ و $\alpha - \beta$ لا تزال قابلة للإنشاء.

إنشاء $\alpha\beta$ موضح في الشكل 3.32، لتكن القطعة المستقيمة $\overline{OA}$ من النقطة O إلى النقطة A، ولتكن $|\overline{OA}|$ طول هذه القطعة المستقيمة، فإذا كان $\overline{OA}$ بطول $|\alpha|$، فأنشئ الخط l من خلال O ولا يحوي $\overline{OA}$ (ربما إذا كان O عند $(0, 0)$، و A عند $(a, 0)$، تستخدم الخط المار من خلال $(0, 0)$ و $(4, 2)$)، ثم أوجد النقاط P و B على l، حيث $\overline{OP}$ بطول 1 و $\overline{OB}$ بطول $|\beta|$، ارسم $\overline{PA}$، وأنشئ l' من خلال B موازٍ لـ $\overline{PA}$ ويقطع $\overline{OA}$ في امتداده عند Q. باستخدام المثلثات المتشابهة نجد أنّ:

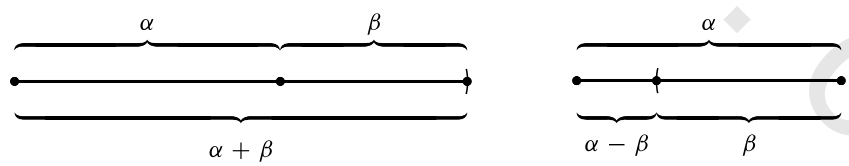
$$\frac{1}{|\alpha|} = \frac{|\beta|}{|\overline{OQ}|}$$

لذلك، $\overline{OQ}$ بطول $|\alpha\beta|$.

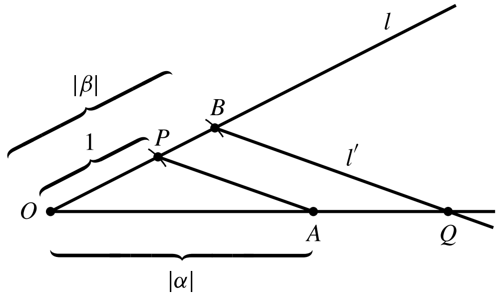
أخيرًا، يبين الشكل 4.32 أنّ α / β قابل للإنشاء، إذا كان $\beta \neq 0$، ليكن $\overline{OA}$ بطول $|\alpha|$، أنشئ l من خلال O ولا يحوي OA، ثمّ أوجد B و P على l، حيث $\overline{OB}$ بطول $|\beta|$ و $\overline{OP}$ بطول 1، ارسم BA، وأنشئ l' من خلال P موازٍ لـ $\overline{BA}$ ويقطع $\overline{OA}$ عند Q، مرة أخرى باستخدم تشابه المثلثات تجد أنّ:

$$\frac{|\overline{OQ}|}{1} = \frac{|\alpha|}{|\beta|}$$

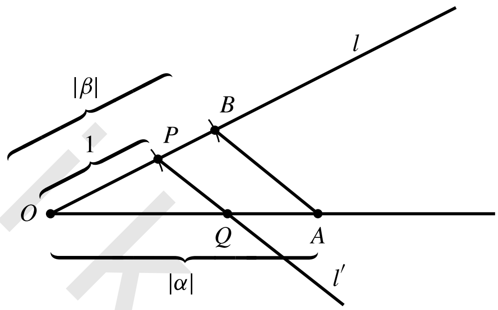
لذلك، $\overline{OQ}$ بطول $|\alpha/\beta|$.



الشكل 2.32



الشكل 3.32



الشكل 4.32

5.32 نتيجة مجموعة الأعداد الحقيقية القابلة للإنشاء تكوّن حقلاً جزئيًّا F من حقل الأعداد الحقيقية.

البرهان برهان هذه النتيجة مباشر من المبرهنة 1.32. ♦

وهكذا، فإنّ الحقل F المكون من الأعداد الحقيقية جميعها القابلة للإنشاء، يحوي $\mathbb{Q}$− حقل الأعداد النسبية − نظرًا لأن $\mathbb{Q}$ هو أصغر حقل جزئي من $\mathbb{R}$.

من الآن فصاعدًا سنتابع بالطرق التحليلية، حيث نستطيع إنشاء أي عدد نسبي، فيما يتعلق بالقطعة المستقيمة

$$0 \underline{\qquad\qquad} 1$$

بطول 1 بوصفها وحدة أساسية على محور السينات، نستطيع أن نعيّن أي نقطة (q_1, q_2) في المستوى بإحداثييها النسبيين، حيث إنّ أي نقطة أخرى في المستوى التي نستطيع تعيينها باستخدام الفرجار والمسطرة، يمكن إيجادها باستخدام إحدى الطرق الثلاث الآتية:

1. بوصفها تقاطع خطين يمرّ كلاهما من خلال نقطتين معلومتين وإحداثياتهما نسبية.

2. بوصفها تقاطع خط يمر من خلال نقطتين، لهما إحداثيات نسبية ودائرة مركزها إحداثياته نسبية ونصف قطرها نسبي.

3. بوصفها تقاطع دائرتين إحداثيات مركزيهما نسبية وأنصاف أقطارها نسبية.

معادلات الخطوط والدوائر من الأنواع المذكورة في 1، و2 و3 هي على الصورة:

$$ax + by + c = 0$$

و

$$x^2 + y^2 + dx + ey + f = 0$$

حيث a ,bو ,c ,dو ,e و f جميعها في $\mathbb{Q}$ ، ولأنّ الحالة 3 تقاطع الدائرتين ذوات المعادلتين:

$$x^2 + y^2 + d_1x + e_1y + f_1 = 0$$

و

$$x^2 + y^2 + d_2x + e_2y + f_2 = 0$$

هو تقاطع الدائرة الأولى نفسه التي معادلتها:

$$x^2 + y^2 + d_1x + e_1y + f_1 = 0$$

والخط (الوتر المشترك) الذي معادلته:

$$(d_1 - d_2)x + (e_1 - e_2)y + f_1 - f_2 = 0$$

كما نرى، فإنّ الحالة 3 يمكن اختزالها إلى الحالة 2، وبالنسبة إلى الحالة الأولى، فحل مشترك للمعادلتين الخطيتين ذواتي المعاملات النسبية، يمكن أن ينتج عنه قيم نسبية لكل من x وy، وهذا لا يعطينا نقاطًا جديدة، ولكن إيجاد حلّ مشترك لمعادلة خطية ذات معاملات نسبية مع معادلة تربيعية ذات معاملات نسبية – كما في الحالة 2 – يؤدي بالتعويض إلى معادلة تربيعية، وعند حلّ مثل هذه المعادلة بالصيغة التربيعية، يمكن أن يكون لها حلول تتضمن جذورًا تربيعية لأعداد ليست مربعات كاملة في $\mathbb{Q}$.

حيث لم نتطرق في النقاش السابق للحديث عن $\mathbb{Q}$، إلاّ فيما يختص بمسلمات الحقول، فإذا كان H هو أصغر حقل يحوي هذه الأعداد الحقيقية المنشأة حتى الآن، فيظهر النقاش أنّ "العدد الجديد الآتي" الذي تمَّ إنشاؤه يقع في الحقل $H(\sqrt{\alpha})$، حيث $\alpha \in H$، و $\alpha > 0$، وبهذا نكون برهنا نصف النظرية الآتية.

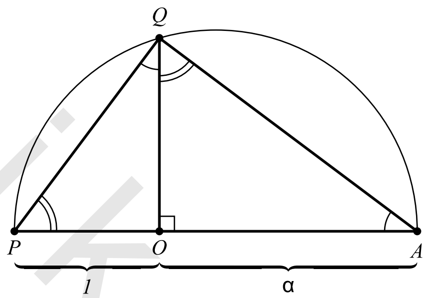
مبرهنة 6.32 الحقل F من الأعداد الحقيقية القابلة للإنشاء، يتكوّن تحديدًا من الأعداد الحقيقية جميعها، التي نستطيع الحصول عليها من $\mathbb{Q}$، بأخذ الجذور التربيعية للأعداد الموجبة بعدد منتهٍ من المرات، وتطبيق عددٍ منته من عمليات الحقول.

البرهان وضّحنا أنّ F لا يحوي سوى الأعداد التي نحصل عليها من $\mathbb{Q}$، بأخذ عدد منته من الجذور التربيعية للأعداد الموجبة، وتطبيق عدد منتهٍ من عمليات الحقول، لكن إذا كان $\alpha > 0$ قابلًا للإنشاء، فإنّ الشكل 7.32 يبيّن أنّ $\sqrt{\alpha}$ قابل للإنشاء، ليكن $\overline{OA}$ بطول α، عيّن p على امتداد $\overline{OA}$ بحيث $\overline{OP}$ بطول 1، وأوجد منتصف $\overline{PA}$، وارسم نصف دائرة يكون $\overline{PA}$ قطرًا لها، ثمّ أقم عمودًا على $\overline{PA}$ من النقطة O، حيث يقطع نصف الدائرة في النقطة Q، إذن، المثلثان OPQ وOQA متشابهان، ويكون

$$\frac{\left|\overline{OQ}\right|}{\left|\overline{OA}\right|}=\frac{\left|\overline{OP}\right|}{\left|\overline{OQ}\right|}$$

و $\left|\overline{OQ}\right|^2 = 1\alpha = \alpha$. إذن، طول $\overline{OQ}$ يساوي $\sqrt{\alpha}$، وبهذا، فإنّ الجذور التربيعية للأعداد القابلة للإنشاء تكون قابلة للإنشاء.

تظهر المبرهنة 1.32 أنّ عمليات الحقول ممكنة بالإنشاء. ♦



الشكل 7.32

8.32 نتيجة إذا كان γ قابلًا للإنشاء و $\gamma \notin \mathbb{Q}$، فتوجد متتالية منتهية من الأعداد الحقيقية $\gamma = \alpha_1,..,\alpha_n$ حيث $\mathbb{Q}\left(\alpha_1, \ldots, \alpha_i\right)$ هو امتداد لـ $\mathbb{Q}$ من الدرجة الثانية، وبشكل خاص، $\left[\mathbb{Q}(\gamma):\mathbb{Q}\right]=2^r$، حيث r عدد صحيح، $r \geq 0$.

البرهان إثبات توافر α_i مباشر من مبرهنة 6.32؛ ولذلك:

$$\begin{aligned} 2^n &= [\mathbb{Q}(\alpha_1,\cdots,\alpha_n):\mathbb{Q}] \\ &= [\mathbb{Q}(\alpha_1,\cdots,\alpha_n):\mathbb{Q}(\gamma)][\mathbb{Q}(\gamma):\mathbb{Q}] \end{aligned}$$

باستخدام المبرهنة 4.32، وهذا ينهي البرهان. ♦

استحالة إنشاءات محددة

سنثبت الآن استحالة إنشاءات هندسية محددة.

مبرهنة 9.32 مضاعفة مكعب مستحيلة، أي إنه إذا أُعطينا ضلعًا من مكعب، فليس بالإمكان دائمًا استخدام المسطرة والفرجار في إنشاء ضلع مكعب له ضعف حجم المكعب الأصلي.

البرهان ليكن للمكعب المعطى ضلع بطول 1، وبذلك يكون حجمه 1، والمكعب الذي نبحث عنه يجب أن يكون حجمه *2*، وعليه، طول ضلعه $\sqrt[3]{2}$، ولكن $\sqrt[3]{2}$ هو صفر لكثيرة الحدود غير المختزلة على $\mathbb{Q}$، $x^3 - 2$، ولذلك:

$$\left[\mathbb{Q}\ \sqrt[3]{2} : \mathbb{Q}\right] = 3$$

تبين النتيجة 8.32 أنه لمضاعفة هذا المكعب ذي الحجم *1*، نحتاج إلى أن يكون لدينا $2^r = 3$، حيث r عدد صحيح، ولكن مثل هذا العدد غير متوافر. ♦

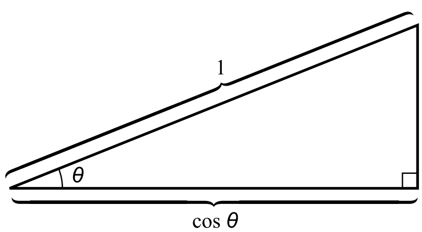
مبرهنة 10.32 تربيع الدائرة مستحيل، أي إنه إذا أُعطينا دائرة، فليس بالإمكان دائمًا استخدام المسطرة والفرجار في إنشاء مربع له مساحة تساوي مساحة الدائرة المعطاة.

البرهان ليكن نصف قطر الدائرةيساوي 1؛ ولذلك تكون مساحتها تساوي π، نحن في حاجة إلى إنشاء مربع ضلعه يساوي $\sqrt{\pi}$، ولكن π متسامٍ على $\mathbb{Q}$؛ ولذلك $\sqrt{\pi}$ متسامٍ على $\mathbb{Q}$ أيضًا. ♦

مبرهنة 11.32 تثليث الزاوية مستحيل، أي إنه توجد زاوية لا يمكن تثليثها باستخدام المسطرة والفرجار.

البرهان يبين الشكل 12.32 أنّ الزاوية θ تكون قابلة للإنشاء إذا وفقط إذا أمكننا إنشاء قطعة بطول $|\cos\theta|$، الآن، الزاوية $60°$ قابلة للإنشاء، وسنبين أنها غير قابلة للتثليث، لاحظ أنّ:

$$\begin{aligned}
\cos 3\theta &= \cos(2\theta + \theta) \\
&= \cos 2\theta \cos\theta - \sin 2\theta \sin\theta \\
&= (2\cos^2\theta - 1)\cos\theta - 2\sin\theta\cos\theta\sin\theta \\
&= (2\cos^2\theta - 1)\cos\theta - 2\cos\theta(1 - \cos^2\theta) \\
&= 4\cos^3\theta - 3\cos\theta.
\end{aligned}$$



الشكل 21.32

[نلاحظ أنّ الكثير من الطلاب اليوم لم يشاهدوا المتطابقات المثلثية التي استخدمناها

تـوًّا، فالتمريـن 1 يعيـد التمريـن 40 الـوارد في الفصـل الأول، ويطلـب إليـك إثبـات المتطابقـة $cos\ 3\theta = 4\ cos^3\theta - 3\ cos\ \theta$ باستخدام صيغة أويلر (*Euler's Formula*)].

لتكن $\theta = 20°$، وبـذلـك، فـإنّ $cos\ 3\theta = \frac{1}{2}$، ولتكن $\alpha = \cos 20°$، مـن المتطابقة $4\ cos^3\ \theta - 3\ cos\ \theta = cos\ 3\theta$ نجد أنّ

$$4\alpha^3 - 3\alpha = \frac{1}{2}$$

وبذلك، فإنّ α صفر لكثيرة الحدود $8x^3 - 6x - 1$، وكثيرة الحدود هذه غير مختزلة في $\mathbb{Q}[x]$ لأنه باستخدام المبرهنة 11.23 يكفي أن نثبت أنها لا تتحلل إلى عوامل في $\mathbb{Z}[x]$، ولكن التحليل إلى عوامل في $\mathbb{Z}[x]$ يستلزم عاملًا خطيًّا على الصورة $(8x \pm 1)$، $(4x \pm 1)$، $(2x \pm 1)$ أو $(x \pm 1)$، حيث نستطيع التحقق سريعًا من أنّ أيًّا من الأعداد $\pm\frac{1}{8}$، $\pm\frac{1}{4}$، $\pm\frac{1}{2}$ و ± 1 ليس صفرًا لكثيرة الحدود $8x^3 - 6x - 1$ ؛ ولذلك:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

وباستخدام النتيجة 8.32، فإنّ α غير قابلة للإنشاء، وبناءً عليه، فإن $60°$ لا يمكن تثليثها. ♦

■ نبذة تاريخية

بالعودة إلى القرن الرابع قبل الميلاد، نجد أنّ الرياضيين اليونان حاولوا دون نجاح أن يجدوا إنشاءات هندسية باستخدام المسطرة والفرجار لتثليث الزاوية، ومضاعفة المكعب وتربيع الدائرة، وعلى الرغم من أنهم لم يستطيعوا إثبات استحالة مثل هذه الإنشاءات، إلّا أنهم نجحوا في بناء حلول لهذه المعضلات باستخدام أدوات أخرى تشمل المقاطع المخروطية.

وفي بداية القرن التاسع عشر قام كارل جاوس (*Carl Gauss*) بدراسة تفصيلية لقابلية الإنشاء، وذلك فيما يتعلق بحله لمعادلات أولية العدد (*cyclotomic equations*)، والمعادلات التي على الصورة $x^p - 1 = 0$، حيث p عدد أولي جذورها رؤوس المضلع المنتظم الذي عدد أضلاعه p، وقد أثبت أنه على الرغم من أنّ هذه المعادلات جميعها تحلّ باستخدام الجذور إذا كان $p-1$ ليس من قوى 2، فإنّ الحلول يجب أن تتضمن جذورًا أعلى من الثاني، في الحقيقة، أكّد جاوس أنّ كل من يحاول أن يجد إنشاءً هندسيًّا للمضلع ذي الأضلاع p، حيث $p-1$ ليس من قوى 2، فسيضيع وقته هباءً، وكان الشيء المشوق أنّ جاوس لم يبرهن ما أكده من أنّ مثل هذه الإنشاءات مستحيلة، وهذا ما تمّ إنجازه عام 1837م على يد بيري وانتزل (*Pierre Wantzel* 1814- 1848)، حيث برهن النتيجة 8.32، وأقام الدليل على صحّة المبرهنة 9.32 والمبرهنة 11.32، ومن ناحية أخرى، فإنّ إثبات المبرهنة 10.32 يتطلب إثبات أنّ π متسامٍ، وهذا ما تمّ تحقيقه عام *1882*م على يد فيردناند ليندمان (*Ferdinand Lindemann* 1852- 1839).

لاحظ أنّ المضلع المنتظم الذي له عدد n من الأضلاع قابل للإنشاء عندما $n \geq 3$، إذا وفقط إذا كانت الزاوية $2\pi/n$ قابلة للإنشاء.

وهذه الحالة تتحقق إذا وفقط إذا كانت القطعة المستقيمة بطول $cos\left(2\pi/n\right)$، قابلة للإنشاء.

■ تمارين 32

حسابات

1. أثبت المتطابقة المثلثية $cos 3\theta = 4 cos^3 \theta - 3 cos \theta$ من صيغة أويلر

$e^{i\theta} = cos\theta + i \, sin\theta$.

مفاهيم

2. ضع إشارة صح أو إشارة خطأ:

______ أ. من المستحيل مضاعفة أي مكعب له ضلع قابل للإنشاء باستخدام المسطرة والفرجار.

______ ب. من المستحيل مضاعفة كل مكعب له ضلع قابل للإنشاء باستخدام المسطرة والفرجار.

______ جـ. من المستحيل تربيع دائرة لها نصف قطر قابل للإنشاء باستخدام المسطرة والفرجار.

______ د. من المستحيل تثليث زاوية قابلة للإنشاء باستخدام المسطرة والفرجار.

______ هـ. كل عدد قابل للإنشاء هو من الدرجة 2^r على $\mathbb{Q}$، حيث r عدد صحيح، $r \geq 0$.

______ و. لقد أثبتنا أن كل عدد حقيقي من الدرجة 2^r على $\mathbb{Q}$، حيث r عدد صحيح، $r \geq 0$ يكون قابلاً للإنشاء.

______ ز. حقيقة أنّ تحليل عدد صحيح موجب إلى حاصل ضرب عددين أوليين وحيد (دون اعتبار الترتيب)، استُخدمت بقوة في خاتمة المبرهنتين 9.32 و 11.32.

______ ح. البرهان بالعدّ هو إلى حدّ بعيد أداة قوية من أدوات الرياضيين.

______ ط. نستطيع إيجاد أي عدد قابل للإنشاء بعدد منتهٍ من الخطوات، وذلك بالبدء بقطعة بطول الوحدة وباستخدام المسطرة والفرجار.

______ ي. نستطيع إيجاد المجموع الكلي للأعداد القابلة للإنشاء جميعها بعدد منتهٍ من الخطوات، وذلك بالبدء بقطعة بطول الوحدة وباستخدام المسطرة والفرجار.

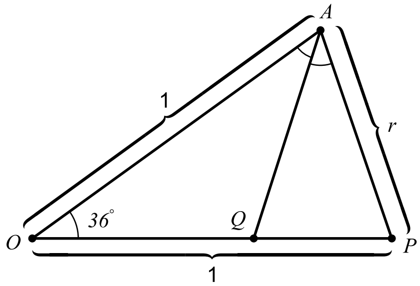
نظرية

3. باستخدام إثبات المبرهنة 11.32، أثبت أنّ المضلع المنتظم الذي له 9 أضلاع غير قابل للإنشاء.

4. أثبت جبريًا أنه يمكن إنشاء زاوية $30°$.

5. بالرجوع إلى الشكل 13.32 حيث $\overline{AQ}$ ينصف الزاوية OAP، أثبت أنّ المضلع المنتظم الذي له 10 أضلاع قابل للإنشاء، (ولذلك يكون الخماسي المنتظم قابلًا للإنشاء أيضًا). [مساعدة: المثلث OAP يشابه المثلث APQ. أثبت جبريًا أنّ r قابل للإنشاء].

في التمارين 6 إلى 9 استخدم نتائج تمرين 5 عند الحاجة؛ لتثبت أنّ العبارة صحيحة:



الشكل 13.32

6. المضلع المنتظم الذي له 20 ضلعًا قابل للإنشاء.

7. المضلع المنتظم الذي له 30 ضلعًا قابل للإنشاء.

8. من الممكن تثليث الزاوية $72°$.

9. المضلع المنتظم الذي له 15 ضلعًا قابل للإنشاء.

10. افترض أنك تريد أن تشرح بصورة تقريبية بثلاث أو أربع جمل لمدرّس مرحلة ثانوية يدرّس الهندسة المستوية، ولم يدرس مقررًا دراسيًّا في الجبر المجرّد، فكيف يمكن إثبات أنه من المستحيل تثليث زاوية قياسها $60°$؟ اكتب ما ستقوله.

الفصل 33 الحقول المنتهية Finite Fields

الهدف من هذا الفصل تحديد بنية الحقول المنتهية كلها، وسنثبت أنه لكل عدد أولي p وعدد صحيح موجب n، يوجد بالضبط حقل واحد (تبعًا للتماثل) عدد عناصره p^n، حيث يسمّى هذا الحقل $\mathrm{GF}(p^n)$ بالعادة **حقل جالوا من الرتبة p^n (*Galois field of order p^n*)**. سنستخدم بعض معلوماتنا عن الزمر الدورية، والبراهين بسيطة ورائعة.

بناء الحقل المنتهي

سنثبت أنّ عدد عناصر أي حقل منتهٍ يجب أن يكون على صورة قوة لعدد أولي.

1.33 مبرهنة ليكن الحقل E امتدادًا من الدرجة n على الحقل المنتهي F، فإذا كان لـ F q من العناصر، فإن لـ E q^n من العناصر.

البرهان لتكن $\{\alpha_1,\dots,\alpha_n\}$ أساسًا لـ E بوصفها فضاء متجهات على F، فبحسب التمرين 21 من الفصل 30، فإنّ كل $\beta \in E$ تكتب بصورة وحيدة على الهيئة:

$$\beta = b_1\alpha_1 + \dots + b_n\alpha_n$$

حيث $b_i \in F$، ولأنّ كل b_i يمكن أن تكون أيًا من ألـ q عنصر في F، فإنّ العدد الكلي للتراكيب الخطية المختلفة في α_i تساوي q^n. ♦

2.33 نتيجة إذا كان E حقلًا منتهيًا ذا مميز p، فإنّ E يحوي بالضبط p^n من العناصر، حيث n عدد صحيح موجب.

البرهان كل حقل منتهٍ هو امتداد منتهٍ لحقل أولي يماثل الحقل $\mathbb{Z}_p$، حيث p هو المميز لـ E. تثبت النتيجة مباشرة من المبرهنة 1.33. ♦

سنتوجه الآن لدراسة البناء الضربي للحقل المنتهي، حيث ترينا المبرهنة الآتية، أنّ أي حقل منتهٍ يمكن أن يُبنى من الحقل الجزئي الأولي.

3.33 مبرهنة ليكن E حقلاً يحوي p^n من العناصر ومحتوًى في الإغلاق الجبري $\overline{\mathbb{Z}}_p$ لـ $\mathbb{Z}_p$. إنّ عناصر E هي بالضبط الأصفار المحتواة في $\overline{\mathbb{Z}}_p$ لكثيرة الحدود $x^{p^n}-x$ في $\mathbb{Z}_p[x]$.

البرهان تشكل المجموعة E^* المؤلفة من العناصر غير الصفرية من E زمرة مع الضرب، ويكون عدد عناصرها p^n-1، فإذا كانت $\alpha \in E^*$، فإنّ رتبتها في هذه الزمرة تقسم رتبة الزمرة p^n-1، إذن، لكل $\alpha \in E^*$، فإن $\alpha^{p^n-1}=1$، وهذا يؤدي إلى $\alpha^{p^n}=\alpha$، ما يعني أنّ كل عنصر في E هو صفر لـ $x^{p^n}-x$، ولأنّ $x^{p^n}-x$ يمكن أن يكون لها على الأكثر p^n من الأصفار، فإننا نرى أنّ E يحوي بالضبط أصفار $x^{p^n}-x$ في $\overline{\mathbb{Z}}_p$. ♦

4.33 تعريف يسمى العنصر α من الحقل F **جذرًا من الرتبة n للواحد (*nth root of unity*)**، إذا كان $\alpha^n = 1$، ويسمى **جذرًا بدائيًا من الرتبة n للواحد (*primitive nth root of unity*)**، إذا كان

$\alpha^n = 1$ و $\alpha^m \neq 1$ لكل $0 < m < n$. ■

إذن، العناصر غير الصفرية في حقل منتهٍ يحوي p^n من العناصر، هي ألـ $(p^n - 1)$ من الجذور للواحد.

تذكر أننا أثبتنا في النتيجة 6.23 أنّ زمرة الضرب للعناصر غير الصفرية في حقل منتهٍ تكون زمرة دورية، وهذه حقيقة مهمّة جدًّا عن الحقول المنتهية؛ فقد تمّ في الحقيقة استخدامها في الترميز الجبري، ولإتمام الشرح في هذا الفصل، فسوف ننصّ عليها هنا، ونعطي نتيجة ونوضحها بمثال.

5.33 مبرهنة زمرة الضرب $\langle F^*, \cdot \rangle$ للعناصر غير الصفرية في حقل منتهٍ F، تكون زمرة دورية.

البرهان انظر النتيجة 6.23. ♦

6.33 نتيجة يكون أي امتداد منتهٍ E لحقل منتهٍ امتدادًا بسيطًا لـ F.

البرهان لتكن α مولدة للزمرة الدورية E^* المكوّنة من العناصر غير الصفرية في E، إذن: $E = F(\alpha)$. ♦

7.33 مثال في الحقل المنتهي $\mathbb{Z}_{11}$، وبحسب المبرهنة 5.33 $\langle \mathbb{Z}_{11}^*, \cdot \rangle$ زمرة دورية، لنحاول إيجاد مولد لـ $\mathbb{Z}_{11}^*$ بالمحاولة والخطأ، سنبدأ بتجريب 2، ولأنّ $|\mathbb{Z}_{11}^*| = 10$، فإنّ 2 هي عنصر من $\mathbb{Z}_{11}^*$ من رتبة تقسم 10، بمعنى أنها 2، 5 أو 10، الآن:

$$2^2 = 4\ ,\ 2^4 = 4^2 = 5 \quad \text{و} \quad 2^5 = (2)(5) = 10 = -1,$$

إذن، 2^2 و 2^5 لا تساويان 1، ولكن بالطبع $2^{10} = 1$، وهكذا، فإنّ 2 مولدة لـ $\mathbb{Z}_{11}^*$، بمعنى أنّ 2 جذر بدائي من الرتبة 10 للواحد في $\mathbb{Z}_{11}$.

بحسب نظرية الزمر الدورية، فإنّ مولدات $\mathbb{Z}_{11}^*$ كلّها – التي هي جذور بدائية من الرتبة 10 للواحد – على الصورة 2^n، حيث n عدد أولي نسبيًا لـ 10، وهي:

$$2^1 = 2, \quad 2^3 = 8, \quad 2^7 = 7, \quad 2^9 = 6$$

■ **نبذة تاريخية**

على الرغم من أنّ كارل ف. جاوس (*Carl F. Gauss*) أثبت أنّ مجموعة الرواسب قياس عدد أولي p تحقق خصائص الحقل، فإن إيفرست جالوا (*Evariste Galois* 1811 – 1832) هو أول من تعامل مع ما أسماه "الحلول غير المتكافئة" (*incommensurable solutions*) للتطابق $F(x) \equiv 0$ (مقياس p)، حيث $F(x)$ كثيرة حدود غير مختزلة من الدرجة n مقياس p ، فقد لاحظ في بحث له كتب عام 1830م، أنّ على المرء أن يعدّ جذور هذا التطابق بوصفه "تنوعًا من الرموز التخيلية"، التي يمكن استخدامها في الحسابات تمامًا، كما نستخدم $\sqrt{-1}$ ، وقد أثبت جالوا أنه إذا كانت α حلاً لـ $F(x) \equiv 0$ (مقياس p)، فإنّ التعبير $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}$ تأخذ بالضبط p^n قيمة مختلفة، وأثبت أخيرًا نتائج مكافئة للمبرهنتين 3.33 و 5.33 في هذا الكتاب.

كانت حياة جالوا قصيرة ومأساوية، وقد أظهر مهارة في الرياضيات مبكرًا، ونشر كثيرًا من الأبحاث قبل سن ألـ 20، وبصورة أساسية، وضع الأساس للأفكار الرئيسة في نظرية جالوا، إضافة إلى أنه كان نشيطًا في الثورة السياسية الفرنسية، التي تبعت ثورة يوليو عام 1830م، وقد اعتُقل في مايو عام 1831م؛ لتهديده حياة الملك لويس فيليب، وبعد تبرئته اعتقل ثانية؛ لمشاركته في الاحتجاج المسلح بكثافة للجمهوريين في يوم الباستيل في تلك السنة، وبعد شهرين من إطلاق سراحه من السجن في مارس المقبل قُتل في مبارزة "ضحية امرأة لعوب مغمورة واثنين من المغفلين"، وقد كتب في الليلة السابقة رسالة لصديق يوضح فيها بعض أعماله في نظرية المعادلات، وطالبًا دراستها من قبل رياضيين آخرين، ولم تنشر أهم أبحاثه قبل عام 1846م، وقد أصبح عمله منذ ذلك التاريخ ذا مكانة مرموقة.

الجذور البدائية من الرتبة 5 للواحد في $\mathbb{Z}_{11}$ تكون على الصورة 2^m، حيث 2 هو القاسم المشترك الأكبر بين m و 10، وهي:

$$2^2 = 4\ ,\ 2^4 = 5\ ,\ 2^6 = 9\ ,\ 2^8 = 3$$

الجذر التربيعي البدائي للواحد في $\mathbb{Z}_{11}$ هو $2^5 = 10 = -1$ ▲

وجود $\mathbf{GF}(p^n)$

نتحول الآن إلى السؤال عن وجود الحقل المنتهي من الرتبة p^r لكل قوة p^r للعدد الأولي حيث $r > 0$. سوف نحتاج إلى التمهيدية الآتية:

8.33 تمهيدية إذا كان F حقلاً ذا مميز p وإغلاق جبري $\overline{F}$، فإنّ $x^{p^n} - x$ لها p^n من الأصفار المختلفة في $\overline{F}$. ♦

البرهان لأنّ $\overline{F}$ مغلقة جبريًا، فإنّ $x^{p^n} - x$ تتحلل في هذا الحقل إلى حاصل ضرب عوامل خطية $x - \alpha$، وهكذا، فإنه يكفي أن نثبت أنّ أيًا من هذه العوامل لن يظهر أكثر من مرة في هذا التحليل.

ولأننا لم نقدم نظرية جبرية للمشتقات، فإننا سنفقد هذه الآلية الرائعة؛ ولذلك، سنكمل باستخدام القسمة الطويلة، لاحظ أنّ 0 هو أحد أصفار $x^{p^n} - x$، وهو ذو تكرار 1، افترض أنّ

$\alpha \neq 0$ هو صفر لـ $x^{p^n} - x$، وعليه، فهو صفر لـ $f(x) = x^{p^n-1} - 1$. إذًا $x - \alpha$، عامل لـ $f(x)$ في $\overline{F}[x]$، وباستخدام القسمة الطويلة نجد أنّ:

$$\frac{f(x)}{(x-\alpha)}=g(x)$$

$$=x^{p^{n-2}}+\alpha x^{p^{n-3}}+\alpha^2 x^{p^{n-4}}+\ldots+\alpha^{p^{n-3}}x+\alpha^{p^{n-2}}$$

الآن يحوي $g(x)$ p^n-1 من الحدود، وفي $g(\alpha)$، كل حد هو:

$$\alpha^{p^n-2}=\frac{\alpha^{p^n-1}}{\alpha}=\frac{1}{\alpha}.$$

إذن:

$$g(\alpha)=\left[(p^n-1).1\right]\frac{1}{\alpha}=-\frac{1}{\alpha}.$$

لأننا في حقل ذي مميز p، إذن، $g(\alpha)\neq 0$، وهكذا، فإنّ α صفر لـ $f(x)$ ، ذو تكرار 1.♦

9.33 تمهيدية إذا كان F حقلاً ذا مميز p، فإنّ $(\alpha+\beta)^{p^n}=\alpha^{p^n}+\beta^{p^n}$ لكل $\alpha, \beta\in F$ وكل عدد صحيح موجب n. ♦

البرهان لتكن $\alpha, \beta\in F$، وبتطبيق مبرهنة ذات الحدين على $(\alpha+\beta)^p$، نحصل على

$$\begin{aligned}(\alpha+\beta)^p&=\alpha^p+(p.1)\alpha^{p-1}\beta+\left(\frac{p(p-1)}{2}.1\right)\alpha^{p-2}\beta^2\\&+\ldots+(p.1)\alpha\beta^{p-1}+\beta^p\\&=\alpha^p+0\alpha^{p-1}\beta+0\alpha^{p-2}\beta^2+\ldots+0\alpha\beta^{p-1}+\beta^p\\&=\alpha^p+\beta^p.\end{aligned}$$

وبالاستمرار واستخدام الاستقراء الرياضي على n، افترض أننا حصلنا على ،

$$(\alpha + \beta)^{p^{n-1}} = \alpha^{p^{n-1}} + \beta^{p^{n-1}}$$

إذن:

$$(\alpha+\beta)^{p^n} = \left[(\alpha+\beta)^{p^{n-1}}\right]^p = (\alpha^{p^{n-1}} + \beta^{p^{n-1}})^p = \alpha^{p^n} + \beta^{p^n} \quad \blacklozenge$$

10.33 مبرهنة يوجد حقل منتهٍ $GF(p^n)$ يحوي p^n من العناصر لكل قوى عدد أولي p^n.

البرهان ليكن $\overline{\mathbb{Z}}_p$ إغلاقًا جبريًا لـ $\mathbb{Z}_p$، وليكن K مجموعة جزئية من $\overline{\mathbb{Z}}_p$ مكونة من أصفار $x^{p^n} - x$ في $\overline{\mathbb{Z}}_p$ جميعها، ليكن $\alpha, \beta \in K$، حيث تثبت التمهيدية 9.33 أنّ $\alpha + \beta \in K$، وتثبت المعادلة: $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$ أنّ $\alpha\beta \in K$، ومن $\alpha^{p^n} = \alpha$ نحصل على $(-\alpha)^{p^n} = (-1)^{p^n}\alpha^{p^n} = (-1)^{p^n}\alpha$، فإذا كان p عددًا أوليًا فرديًا، فإنّ $(-1)^{p^n} = -1$، وإذا كان $p = 2$، فإنّ $-1 = 1$، وهكذا، فإنّ $(-\alpha)^{p^n} = -\alpha$، ما يعني أنّ $-\alpha \in K$، ولكن 0 و 1 أصفار لـ $x^{p^n} - x$، فإذا كانت $\alpha \neq 0$ و $\alpha^{p^n} = \alpha$، فإنّ ذلك يؤدي إلى أنّ $\left(\frac{1}{\alpha}\right)^{p^n} = \frac{1}{\alpha}$، إذن: K حقل جزئي من $\overline{\mathbb{Z}}_p$، ويحوي $\mathbb{Z}_p$، إذن، K هو الحقل المطلوب الذي يحوي p^n من العناصر؛ لأن التمهيدية 8.33 أثبتت أنّ لـ $x^{p^n} - x$، p^n من الأصفار المختلفة في $\overline{\mathbb{Z}}_p$. $\blacklozenge$

11.33 نتيجة (إذا كان F حقلاً منتهيًا، فإنّه لكل عدد صحيح موجب n، توجد كثيرة حدود غير مختزلة في $F[x]$ من الدرجة n.

البرهان ليكن F يحوي $q = p^r$ من العناصر، حيث p هو المميز لـ F، فبحسب المبرهنة 10.33 يوجد حقل $K \leq \overline{F}$ يحوي $\mathbb{Z}_p$ (بحسب التماثل)، ويتكوّن أساسًا من أصفار $x^{p^m} - x$. نريد إثبات أنّ $F \leq K$، فكل عنصر في F هو صفر لـ $x^{p^r} - x$، تبعًا للمبرهنة 3.33. الآن $p^{rs} = p^r p^{r(s-1)}$ وبتطبيق هذه المعادلة بصورة متكررة على القوى، واستخدام حقيقة أنه إذا كان $\alpha \in F$، فإن $\alpha^{p^r} = \alpha$، فإنه يمكننا أن نرى أنه إذا كان $\alpha \in F$، فإن

$$\alpha^{p^{rn}} = \alpha^{p^{r(n-1)}} = \alpha^{p^{r(n-2)}} = \cdots = \alpha^{p^r} = \alpha$$

إذن، $F \leq K$. تثبت المبرهنة 1.33 أننا يجب أن نحصل على $[K : F] = n$، لقد رأينا أنّ K بسيط على F في النتيجة 6.33، وهكذا، فإنّ $K = F(\beta)$، حيث $\beta \in K$، وهذا يؤدي إلى أن $\mathrm{irr}(\beta ، \mathrm{F})$ يجب أن تكون من الدرجة n. $\blacklozenge$

12.33 مبرهنة ليكن p عددًا أوليًّا، ولتكن $n \in \mathbb{Z}^+$، فإذا كان E و E' حقلين من الرتبة p^n، فإنّ $E \simeq E'$.

البرهان $\mathbb{Z}_p$ هو الحقل الأولي لكل من E و E' تبعًا للتماثل، وبحسب النتيجة 6.33، فإنّ E امتداد بسيط لـ $\mathbb{Z}_p$ من الدرجة n، ما يعني توافر كثيرة حدود غير مختزلة $f(x)$ من الدرجة n، في $\mathbb{Z}_p[x]$، بحيث $E \simeq \mathbb{Z}_p[x]/\langle f(x)\rangle$؛ ولأن عناصر E أصفار لـ $x^{p^n} - x$، فإننا نرى كذلك أنّ $f(x)$ عامل من عوامل $x^{p^n} - x$ في $\mathbb{Z}_p[x]$.

ولأن E' كذلك تتكوّن من أصفار $x^{p^n} - x$، فإننا نرى كذلك أنّ E' تحوي أصفارًا لغير المختزلة $f(x)$ في $\mathbb{Z}_p[x]$. إذن، ولأنّ E' تحوي تمامًا p^n من العناصر، فإن E' متماثلة مع $\mathbb{Z}_p[x]/\langle f(x)\rangle$.
♦

استخدمت الحقول المنهية في الترميز الجبري. في بحث منشور في
"*American Mathematical Monthly* 77 (1970): 249–258" . صنع نورمان ليفنسون
ترميزًا خطيًّا يستطيع التصحيح لغاية ثلاثة أخطاء باستخدام حقل منتهٍ من الرتبة 16.

■ تمارين 33

حسابات

في التمارين 1 إلى 3، حدّد ما إذا كان يوجد حقل منتهٍ له هذا العدد من العناصر (قد تكون الآلة الحاسبة مفيدة).

1. 4096 **2.** 3127 **3.** 68,921

4. أوجد عدد الجذور البدائية من الرتبة 8 للواحد في GF(9).

5. أوجد عدد الجذور البدائية من الرتبة 18 للواحد في GF(19).

6. أوجد عدد الجذور البدائية من الرتبة 15 للواحد في GF(31).

7. أوجد عدد الجذور البدائية من الرتبة 10 للواحد في GF(23).

مفاهيم

8. ضع إشارة صح أو إشارة خطأ:

______ أ. العناصر غير الصفرية في أي حقل منتهٍ تشكل زمرة دورية مع الضرب.

______ ب. عناصر أي حقل منتهٍ تشكل زمرة إبدالية مع الجمع.

______ جـ. تشكل الأصفار في $\mathbb{C}$ لـ $(x^{28}-1) \in \mathbb{Q}[x]$ زمرة دورية مع الضرب.

______ د. يوجد حقل منتهٍ بـ 60 عنصرًا.

______ هـ. يوجد حقل منتهٍ بـ 125 عنصرًا.

______ و. يوجد حقل منتهٍ بـ 36 عنصرًا.

______ ز. العدد المركب i جذر بدائي من الرتبة 4 للواحد.

______ ح. توجد كثيرة حدود غير مختزلة من الدرجة 58 في $\mathbb{Z}_2[x]$.

______ ط. العناصر غير الصفرية في $\mathbb{Q}$ تشكل زمرة دورية $\mathbb{Q}^*$ مع الضرب.

______ ي. إذا كان F حقلاً منتهيًا، فإنّ كل تماثل غامر من F إلى حقل جزئي من الإغلاق الجبري $\overline{F}$ لـ F، يكون تماثلًا ذاتيًّا لـ F.

براهين

9. ليكن $\overline{\mathbb{Z}_2}$ إغلاقًا جبريًّا لـ $\mathbb{Z}_2$، ولتكن $\alpha, \beta \in \overline{\mathbb{Z}_2}$ أصفارًا لـ x^3+x^2+1 و x^3+x+1، على الترتيب. استخدم نتائج هذا الفصل لإثبات أنّ $\mathbb{Z}_2(\alpha)=\mathbb{Z}_2(\beta)$.

10. أثبت أنّ كل كثيرة حدود غير مختزلة في $\mathbb{Z}_p[x]$ تقسم $x^{p^n}-x$ ، حيث n عدد صحيح.

11. ليكن F حقلًا منتهيًا يحوي p^n من العناصر، ويحوي الحقل الأولي $\mathbb{Z}_p$. أثبت أنه إذا كانت

$\alpha \in F$ مولدة للزمرة الجزيئية $\langle F^*, .\rangle$ المكونة من العناصر غير الصفرية في F، فإنّ

$\deg(\alpha,\mathbb{Z}_p)=n$.

12. أثبت أنّ كل حقل من الرتبة p^n يحوي بالضبط حقلًا جزئيًّا واحدًا من الرتبة p^m لكل قاسم m لـ n.

13. أثبت أنّ $x^{p^n}-x$ هي حاصل ضرب كثيرات الحدود الأحادية جميعها غير المختزلة في $\mathbb{Z}_p[x]$ من الدرجة d التي تقسم n.

14. ليكن p عددًا أوليًّا فرديًّا.

أ. أثبت أنه لكل $a \in \mathbb{Z}$، حيث $a \not\equiv 0$ (مقياس p)، يكون هناك حل في $\mathbb{Z}$ للتطابق $x^2 \equiv a$ (مقياس p)، إذا وفقط إذا كان $a^{(p-1)/2} \equiv 1$ (مقياس p).

[مساعدة: أعد الصياغة باستخدام عبارة مكافئة عن الحقل المنتهي $\mathbb{Z}_p$، واستخدم نظرية الرمز الدورية].

ب. استخدم الفرع (أ) لتحديد ما إذا كانت كثيرة الحدود x^2-6 غير مختزلة $\mathbb{Z}_{17}[x]$.