المعهد العالي
للعلوم التطبيقية والتكنولوجيا

الدكتور عمران قوبا

الجبر

1

مبادئ الجبر المجرد

المنطق الرياضي والبنى الجبرية
الزمر والحلقات والحقول
الأعداد العقدية وكثيرات الحدود

الجبر

الجزء الأول

مبادئ الجبر المجرد

الطبعة الثانية

الدكتور عمران قوبا

منشورات المعهد العالي للعلوم التطبيقية والتكنولوجيا

2017

الجبر

الجزء الأول، الإصدار الأوّل، الطبعة الثانية

عمران قوبا

تصميم الغلاف: المؤلف

من منشورات المعهد العالي للعلوم التطبيقية والتكنولوجيا
الجمهورية العربية السورية، 2009.

Algebra

Volume 1, First Edition, Second Printing

Omran Kouba

Publications of the
Higher Institute for Applied Sciences and Technology (HIAST)
Syrian Arab Republic, 2017.

ISBN: 978-9933-9228-9-4

منشورات المعهد العالي للعلوم التطبيقية والتكنولوجيا

صدر حتى تاريخه:

- " الجبر، الجزء الأول، مبادئ الجبر المجرد"، للدكتور عمران قوبا، 2009.
- " التحليل، الجزء الأول"، للدكتور عمران قوبا، 2009.
- " كيمياء المحاليل المائية"، للدكتورة يمن الأتاسي، 2011.
- " الأنظمة الرادارية في مواجهة التشويش والخداع"، للدكتور علي طه، 2011.
- " ميكانيك النقطة المادية"، للدكتور مصطفى عليوي والدكتور هاني قوبا، الإصدار الثاني، 2015.
- " كيمياء المحاليل المائية"، للدكتورة يمن الأتاسي، الطبعة الثانية، 2016.
- " الجبر، الجزء الأول، مبادئ الجبر المجرد"، الطبعة الثانية، للدكتور عمران قوبا، 2017.
- " التحليل، الجزء الأول"، الطبعة الثانية، للدكتور عمران قوبا، 2017.
- " الجبر، الجزء الثاني، الجبر الخطي"، للدكتور عمران قوبا، 2017.
- " التحليل، الجزء الثاني"، للدكتور عمران قوبا، 2017.
- " المرجع في الرسم الصناعي، الجزء الثالث"، للدكتور محمد بدر قويدر، 2017.
- " مدخل إلى كيمياء المياه: تلوث- معالجة- تحليل"، للدكتور نصر الحايك، 2017.
- " مبادئ الترموديناميك"، للدكتور عقيل سلوم، 2017.
- " دليل الرسام الصناعي"، للدكتور مصطفى الجرف، 2017.

سيصدر قريباً:

- " التحليل، الجزء الثالث"، للدكتور عمران قوبا.
- " التحليل، الجزء الرابع"، للدكتور عمران قوبا.
- " التحليل، الجزء الخامس"، للدكتور عمران قوبا.

لمعلومات أوفى عن المنشورات وطلب نسخة ورقية أو تحميل
المتاح منها إلكترونياً، يمكن الاطلاع على موقع المعهد الإلكتروني:

www.hiast.edu.sy

المعهد العالي للعلوم التطبيقية والتكنولوجيا مؤسسة حكومية للتعليم العالي أحدثت بموجب المرسوم التشريعي رقم /24/ لعام 1983، وذلك بهدف إعداد أطر علمية متميزة من مهندسين وباحثين للإسهام الفاعل في عملية التطوير العلمي والتنمية في الجمهورية العربية السورية.
يمنح المعهد العالي درجة الإجازة في الهندسة في الاتصالات والمعلوماتية والنظم الإلكترونية والميكاترونيكس وعلوم وهندسة المواد وهندسة الطيران. يقبل المعهد العالي لدراسة هذه الاختصاصات شريحة منتقاة من المتفوقين في الشهادة الثانوية من الفرع العلمي. يتيح المعهد العالي أيضاً برامج ماجستير أكاديمي في نظم الاتصالات وفي التحكم والروبوتيك وفي نظم المعطيات الكبيرة ونظم المعلومات ودعم القرار وفي علوم وهندسة المواد وعلوم وهندسة البصريات. ويمنح المعهد العالي درجة الدكتوراه في الاتصالات والمعلوماتية ونظم التحكم والفيزياء التطبيقية. تُحدث في المعهد العالي اختصاصات جديدة بحسب متطلبات سوق العمل وتوجهات البحث والتطوير المحلية والعالمية.

يمتاز المعهد بأطره الكفوءة ذات التأهيل العالي وبمختبراته المجهزة تجهيزاً عالياً وببنيته التحتية الفريدة في القطر. إلى جانب النشاط التعليمي، يمارس المعهد العالي عبر جهود أطره وفعالياته العلمية المختلفة نشاطاً حثيثاً في البحث والتطوير، إذ ينفذ مشاريع متنوعة لصالح الجهات العامة والخاصة في القطر، كما يتعاون مع جهات خارج القطر في بعض المشاريع البحثية والتطويرية. يسعى المعهد أيضاً، عبر دورات تدريبية نظرية وعملية متاحة للقطاعين العام والخاص وللأفراد، إلى إفادة أوسع فئة من المهتمين من إمكانيات فريقه العلمي ومختبراته.

استكمالاً لدور المعهد العالي الرائد في مجال التعليم ونشر العلم، يحرص المعهد العالي على نشر كتب علمية عالية المستوى من نتاج أطره العلمية، منها ما هو تدريسي يوافق المناهج في المعهد العالي ويفيد شريحة واسعة من الطلاب الجامعيين عموماً، ومنها ما هو علمي ثقافي. يخضع الكتاب قبل نشره إلى عملية تقويم علمي من مجموعة منتقاة بعناية من أصحاب الاختصاص، إضافةً إلى تدقيق لغوي حفاظاً على سوية عالية للمنشورات باللغة العربية.

يتيح المعهد العالي للعلوم التطبيقية والتكنولوجيا بعضاً من منشوراته على موقعه على الشابكة تحت رخصة المشاع الإبداعي لتعميم الفائدة على شريحة واسعة من القراء.

للتواصل مع المعهد العالي والاطلاع على شروط النشر وآخر المنشورات وتحميل المتاح منها:

المعهد العالي للعلوم التطبيقية والتكنولوجيا، دمشق، ص.ب 31983
هاتف 00963115123819 - فاكس 00963112237710
بريد إلكتروني contact@hiast.edu.sy
موقع إلكتروني www.hiast.edu.sy

شكر

أتقدّم بالشكر العميق إلى جميع الزملاء الذين أغنوا بملاحظاتهم فحوى هذا الكتاب، وأسهموا في إعطائه شكله النهائي هذا.

وأخصُّ بالشكر المعلِّم الفاضل الأستاذ الدكتور موفق دعبول، والأستاذ الدكتور محمّد البغدادي والدكتور نبيه عودة قراءتهم المتمعّنة لهذا الكتاب وعلى الملاحظات القيّمة التي أبدوها عليه. وأخيراً، وليس آخراً، أتقدم بجزيل الشكر والامتنان إلى الأستاذ الدكتور مكّي الحسني الذي دقّق الكتاب لغوياً وأسهم بملاحظاته ومقترحاته في تحسين صياغة العديد من الفقرات.

محتوى الجزء الأوّل

مقدّمة

الفصل الأوّل
المجموعات والعلاقات وقوانين التشكيل

الفصل الثاني

حقل الأعداد العقديّة

الفصل الثالث

البنى الجبريّة

الفصل الرابع

كثيرات الحدود على حقل تبديلي

الفصل الخامس

الحقول

محتوى الجزء الثاني

مقدّمة

الفصل السادس
الفضاءات الشعاعيّة والتطبيقات الخطيّة

الفصل السابع
الفضاءات الشعاعية المنتهية البعد

الفصل الثامن
الثنويّة في الفضاءات الشعاعيّة

الفصل التاسع

المصفوفات

الفصل العاشر

المُحدِّدات وجمل المعادلات الخطّيّة

الفصل الحادي عشر

اختزال التطبيقات الخطّيّة

الفصل الثاني عشر
الفضاءات الشعاعيّة المزوَّدة بجداء سلّمي

مقدّمة

لم يتغيّر تعريف الرياضيات من حيث نهجها الاستنتاجيّ منذ أيام قدماء الإغريق، مروراً بالرياضيين العرب الكبار، وحتى أيامنا هذه، إذ تقوم الرياضيات ببناء نظريات بدءاً من مفاهيم أساسية معتمدة على المحاكمة المنطقية فقط. لقد كانت تتباين درجة وضوح وجلاء هذا المسعى باختلاف الأشخاص والأزمنة إلاّ أنها لم تتغير في طبيعتها. أمّا الموضوع الذي تقوم حوله أو تبنى عليه المحاكمة الرياضية فهو بحد ذاته كيفيّ، إذْ يكفي أن يتقبل هذا الموضوع المحاكمة المنطقية أسلوباً للمعالجة وأن يثير اهتمام الرياضيّ –أو من يعمل هذا الأخير لحسابه– حتى يولد فصل جديد في الرياضيات.

تبرّر النقطة السابقة استعمال الرياضيّات المتزايد في العلوم الأخرى، نظراً إلى سعي هذه الأخيرة وراء الدقة، و وراء بناء نظريات على أسس مُحكمة. هذا ولقد أصبح تصور العديد من الاتجاهات العلميّة خارج بيئتها الرياضيّة الطبيعية أمراً صعباً جداً بل مستحيلاً في عصرنا الراهن.

لقد بنينا كتاب الجبر هذا ليقدّم للقارئ بعض المعارف الأساسية في هذا العلم، وليطلعه على المفاهيم الجبرية اللازمة لدراسته اللاحقة، وذلك دون إسراف في التعمّق، ودون إجحاف بحق المادة المقدّمة. ومن ناحية أخرى، زوّدنا الكتاب بالعديد من التمارين التي نرى حلّ الطالب لها أمراً لا غنى عنه لضمان استيعابه للمادة، كما عرضنا مقترحات حلولٍ لهذه التمارين لعلّ الطالب يجد في ذلك فائدة.

ولقد قسمنا هذا الكتاب إلى جزأين، وخصّصنا الأوّل لتقديم المفاهيم الأساسية في الجبر المجرّد، وجعلنا الثاني يهتمّ بالجبر الخطّي، معتمدين في اختيار المادّة المقدمة على حاجات الطالب المتوقّعة، فهو سيحتاج إلى بعض طرائق العدّ في دراسته تعقيد الخوارزميات، وسيحتاج إلى بنى جبرية مهمّة مثل كثيرات الحدود على حقول منتهية في دراسته لنظرية المعلومات.

لنأتِ الآن إلى وصف فصول الجزء الأوّل:

- يحتوي الفصل الأول على تذكرة بالتعاريف والرموز الأساسيّة في لغة المنطق والمجموعات وقوانين التشكيل، إضافة إلى بعض طرائق العدّ المعروفة.
- ويتضمّن الفصل الثاني دراسة الأعداد العقديّة بوصفها بنية جبريّة أساسيّة إضافة إلى بعد تطبيقاتها في الهندسة المستويّة.
- ويحتوي الفصل الثالث على دراسة البنى الجبرية الأساسية، كالزمر والحلقات، ومجموعة الأعداد الصحيحة وهي مثال مهم.
- ويدرس الفصل الرابع جبر كثيرات الحدود على حقل تبديلي وهو بنية أساسية مُستهدفة في هذا الكتاب.
- أمّا الفصل الخامس فيُعَدُّ مقدّمة إلى دراسة الحقول إذ يدرس طرائق بناء الحقول، وأمثلة عليها كحقل الكسور العاديّة بمتحوّل واحد، وكذلك الحقول المنتهية، إذْ يجري إثبات وجود الحقول المنتهية $\mathbb{F}_{p^n}$ ووحدانيتها.

في الختام، أشكر جزيل الشكر كل الزملاء والأصدقاء الذين ساهموا في جعل هذا الكتاب يرى النور. وأشكر كذلك الزملاء والقرّاء على أي انتقاد بنّاء أو ملاحظة على هذا الكتاب.

كانون الثاني 2008 عمران قوبا

مقدمة الطبعة الثانية

في هذه الطبعة الثانية، جرى تنقيح العديد من الأخطاء المطبعية التي ظهرت في الطبعة الأولى.

تموز 2017 عمران قوبا

المجموعات والعلاقات وقوانين التشكيل

1. مبادئ المنطق

القضية مفهومٌ أوليٌّ لا يمكن تعريفه، ونكتفي بالقول إنها نصٌ غير محتوٍ على متحولات، ولا تأخذ إلا واحدة من قيمتين منطقيتين : صحيحة (T) أو خاطئة (F).

لتكن A و B قضيتين. تفيد الجداول التالية، التي نسميها **جداول الحقيقة**، في تعريف خمس قضايا جديدة انطلاقاً من القضيّتين A و B، هي $\neg A$ وتُقرأ «نفي A»، و $A \wedge B$ وتُقرأ «A و B»، و $A \vee B$ وتُقرأ «A أو B»، و $A \Rightarrow B$ وتُقرأ «A يقتضي B»، وأخيراً $A \Leftrightarrow B$ وهي تُقرأ «A يكافئ منطقياً B».

A	$\neg A$
T	F
F	T

و

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

يمكن تعميم ما سبق لبناء قضايا جديدة $P(A,B,C,\ldots)$ تسمى **قضايا مركّبة**، وذلك انطلاقاً من القضايا A و B و C و .... يمكن تحديد القيمة المنطقية للقضيّة $P(A,B,C,\ldots)$ باستعمال جداول الحقيقة وذلك بمجرّد معرفتنا للقيم المنطقية لكل من A و B و C و .... فإذا تطابقت جداول الحقيقة لقضيتين $P(A,B,C,\ldots)$ و $Q(A,B,C,\ldots)$ قلنا إنّهما متكافئتان وكتبنا

$$P(A,B,C,\ldots) \equiv Q(A,B,C,\ldots)$$

نترك للقارئ مهمة التوثُّق من صحة التكافؤات التالية، والمحقّقة مهما كانت القيم المنطقية للقضايا $A, B, C, \ldots.$

$$A \equiv \neg(\neg A);\ \ A \equiv A \vee A;\ \ A \equiv A \wedge A \tag{1}$$

$$A \wedge B \equiv B \wedge A;\ \ A \vee B \equiv B \vee A \tag{2}$$

$$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C);\ \ (A \vee B) \vee C \equiv A \vee (B \vee C) \tag{3}$$

$$A \Rightarrow B \equiv (\neg A) \vee B;\ \ A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A) \tag{4}$$

$$\neg(A \vee B) \equiv (\neg A) \wedge (\neg B);\ \ \neg(A \wedge B) \equiv (\neg A) \vee (\neg B) \tag{5}$$

وهنالك تكافؤان مهمّان جداً من الناحية العملية هما

$$\neg(A \Rightarrow B) \equiv A \wedge (\neg B) \quad \text{و} \quad A \Rightarrow B \equiv (\neg B) \Rightarrow (\neg A)$$

إذ يعتبر الأخير أساس ما نسميه الإثبات **بنقض الفرْض**. وتوجد بعض القضايا المركّبة التي تكون صحيحة بقطع النظر عن القيم المنطقية للقضايا التي تدخل في بنائها مثل

$$A \vee (\neg A) \quad \text{و} \quad \neg(A \wedge (\neg A))$$

$$\text{و} \quad [(A \Rightarrow B) \wedge (B \Rightarrow C)] \Rightarrow (A \Rightarrow C)$$

يمكن أن نقرن بكلِّ عددٍ حقيقي x قضيةً، مثل «x هو عدد صحيح فردي» نرمز إليها بالرمز $A(x)$. فتكون $A(-3)$ قضية صحيحة وتكون $A(\pi)$ قضية خاطئة. وبوجهٍ عام، نسمّي **قضية مفتوحة** كل نصٍ $A(x,y,\ldots)$ يحتوي على متحولات $x, y, \ldots$ على أن نحصل على قضية عند استبدال قيم من مرجع ما E بالمتحولات $x, y, \ldots.$

لتكن $A(x)$ قضية مفتوحة تابعة لمتحول x يأخذ قيمه من المرجع E. يمكننا أن نقرن بالقضية $A(x)$ القضيتين الآتيتين:

① القضيّة $\forall x,\ A(x)$، وتُقرأ «$A(x)$ صحيحة عند كل قيمة للمتحول x يأخذها من المرجع E».

② القضيّة $\exists x,\ A(x)$، وتُقرأ «توجد على الأقل قيمة للمتحول x يأخذها من المرجع E تكون عندها $A(x)$ صحيحة».

يسمّى الرمزان $\forall$ و $\exists$ **مُكمِّي الشمول و مُكمِّي الوجود** على التوالي، ومن المهمّ ملاحظة أنّ كلاًّ من القضيتين $\forall x,\ A(x)$ و $\exists x,\ A(x)$ غير محتوية على المتحول x، فيسمّى الرمز x في هذه الحالة **متحولاً أبكم**. لنذكر أخيراً بعض التكافؤات المفيدة:

$$\neg(\exists x,\ A(x)) \equiv \forall x,\ \neg A(x)$$
$$\neg(\forall x,\ A(x)) \equiv \exists x,\ \neg A(x)$$

وبوجه خاص نستعمل كثيراً التكافؤ

$$\neg[\forall x \quad (P(x) \Rightarrow Q(x))] \equiv \exists x \quad (P(x) \wedge (\neg Q(x))$$

إذ نثبتُ خطأ اقتضاءٍ بتقديم مثال معاكس.

كما نستعمل في بعض الأحيان القضية $\exists! x,\ A(x)$ التي تُقرأ «توجد قيمة، وقيمة وحيدة، للمتحول x يأخذها من المرجع E تكون عندها القضيّة $A(x)$ صحيحة».

لننظر في المثال التالي بوصفه تطبيقاً على الأفكار السابقة.

1-1. مثال. قصّة من جزيرة المنطق

جزيرة المنطق جزيرة واقعة في أحد بحار الأرض. تسكنها قبيلتان متحابّتان : قبيلة «آل–الحق» وهم لا يقولون إلاّ الحقيقة، وقبيلة «آل–الباطل» وهم كاذبون في كلِّ ما يدّعون.

❶ في يومٍ من الأيام التقى A و B وهما اثنان من سكّان الجزيرة فقال A: "واحدٌ منّا على الأقل ينتمي إلى قبيلة «آل–الباطل»". فإلى أيّ القبيلتين ينتمي كلٌ من A و B؟

❷ وفي يومٍ آخر راح اثنان من سكّان الجزيرة هما C و D يتناقشان بعنف. وسُمِع C يقول لزميله واثقاً: "إمّا أن أكون من قبيلة «آل–الباطل»، أو أن تكون أنت من قبيلة «آل–الحق»". فإلى أيّ القبيلتين ينتمي كلٌ من C و D؟

❸ التقى ثلاثة من سكان جزيرة المنطق، هم E و H و G فأكّد كلٌ من E و H قائلَين:

E : " نحن جميعاً ننتمي إلى قبيلة «آل–الباطل»".

H : " واحدٌ وواحدٌ فقط من بيننا ينتمي إلى قبيلة «آل–الحق»".

فإلى أي القبيلتين ينتمي كلٌّ من E و H و G؟

☜ ننصح القارئ أن يفكِّر قليلاً في الإجابة عن الأسئلة السابقة قبل متابعة القراءة.

تَظْهرُ الأحجيات السابقة كأنها لا علاقة لها بالرياضيّات، وهذا حال العديد من المسائل التي تساهم الرياضيّات في حلّها. الخطوة الأولى التي نبدأ فيها معالجة مثل هذه المسائل هي الانتقال إلى صياغة جديدة مُكافِئة وتقع ضمن إطار الرياضيات، ثُمَّ نستفيد من الأدوات الرياضيّة في الحل، وأخيراً نترجم النتائج التي حصلنا عليها إلى لغة المسألة التي انطلقنا منها.

لنبدأ إذن بإدخال الرمز الآتي: إذا كان X أحد سكّان الجزيرة فإننا نكتب الرمز $[X]$ للدلالة على القضية «X ينتمي إلى قبيلة آل–الحق» فتكون القضيّة المفتوحة $[X]$ صحيحة أي قيمتها المنطقيّة T، إذا انتمى X إلى قبيلة آل–الحق، وتكون خاطئة، أي قيمتها المنطقيّة F، إذا انتمى X إلى قبيلة آل–الباطل. فإذا ادّعى X صحّة قضيّة P استنتجنا أنّه إمّا أن تكون القضيّتان $[X]$ و P صحيحتين معاً أوخاطئتين معاً.ومن ثَمَّ فالقضيّة $(P \Leftrightarrow [X])$ صحيحة بقطع النظر عن انتماء X.

- ويمكن التعبير عن المقولة الواردة في ❶ بأن القيمة المنطقيّة للقضيّة P_1 التالية هي T:

$$P_1 \equiv ([A] \Leftrightarrow (\neg[A] \vee \neg[B]))$$

وبكتابة جدول الحقيقة لهذه القضيّة نجد

$[A]$	$[B]$	$\neg[A] \vee \neg[B]$	P_1
T	T	F	F
T	F	T	T
F	T	T	F
F	F	T	F

فنستنتج أنّ

$$P_1 \equiv [A] \wedge \neg[B]$$

وعليه تكون القضيّة $[A]$ صحيحة والقضيّة $[B]$ خاطئة. ونعود إلى لغة المسألة فنستنتج من ذلك أنّ :

A ينتمي إلى قبيلة آل–الحق، و B ينتمي إلى قبيلة آل–الباطل

- وكذلك يمكن التعبير عن المقولة الواردة في ❷ بأن القيمة المنطقيّة للقضيّة P_2 التالية هي T:

$$P_2 \equiv ([C] \Leftrightarrow (\neg[C] \vee [D]))$$

وباستعمال جدول الحقيقة، كما في الحالة السابقة، نجد أنّ

$[C]$	$[D]$	$\neg[C] \vee [B]$	P_2
T	T	T	T
T	F	F	F
F	T	T	F
F	F	T	F

ومن ثَمّ

$$P_2 \equiv [C] \wedge [D]$$

أي إن $[C]$ و $[D]$ صحيحتان. ونعود إلى لغة المسألة فنستنتج من ذلك أنّ :

$$\boxed{D \text{ و } C \text{ ينتميان إلى قبيلة آل–الحق}}$$

- وأخيراً يمكننا التعبير عن المقولة الواردة في ❸ بأن القيمة المنطقيّة للقضيّتين P_3 و P_4 التاليتين هي T:

$$P_3 \equiv ([E] \Leftrightarrow P)$$
$$P_4 \equiv ([H] \Leftrightarrow Q)$$

وقد عرّفنا

$$P = \neg([E] \vee [H] \vee [G])$$

و Q هي القضيّة

$$\Big([E] \wedge \neg[H] \wedge \neg[G]\Big) \vee \Big(\neg[E] \wedge [H] \wedge \neg[G]\Big) \vee \Big(\neg[E] \wedge \neg[H] \wedge [G]\Big)$$

علينا إيجاد القيمة المنطقيّة للقضيّة $P_3 \wedge P_4$ وتبيان متى تكون مساوية T. لذلك سنستفيد من جداول الحقيقة فنكتب ما يلي :

$[E]$	$[H]$	$[G]$	P	Q	$\underbrace{[E] \Leftrightarrow P}_{P_3}$	$\underbrace{[H] \Leftrightarrow Q}_{P_4}$	$P_3 \wedge P_4$
T	T	T	F	F	F	F	F
T	T	F	F	F	F	F	F
T	F	T	F	T	F	F	F
T	F	F	F	F	F	T	F
F	T	T	F	F	T	F	F
F	T	F	F	T	T	T	T
F	F	T	F	T	T	F	F
F	F	F	T	F	F	T	F

ومن ثَمّ فإن كوْن القيمة المنطقيّة للقضيّة $P_3 \wedge P_4$ هي T يعني أنّ القضيتين $[E]$ و $[G]$ خاطئتان وأنّ القضيّة $[H]$ صحيحة. ونعود إلى لغة المسألة فنستنتج من ذلك أنّ

$$\boxed{E \text{ و } G \text{ ينتميان إلى قبيلة آل–الباطل، وأنّ } H \text{ ينتمي إلى قبيلة آل–الحق}}$$

كان بالإمكان مناقشة الأحجية الأخيرة كما يأتي: يناقض قول E انتماءه إلى قبيلة آل–الحق، فلا بدّ أنه من آل–الباطل. وينتج من ذلك أنّ واحداً على الأقل من بين H و G ينتمي إلى قبيلة آل–الحق، فيناقض قول H انتماءه إلى قبيلة آل–الباطل، ولا بدّ أنّه من قبيلة آل–الحق، وأنّ G ينتمي إلى قبيلة آل–الباطل.

2. المجموعات والتطبيقات

لنذكِّر ببعض المفاهيم الأساسية في نظرية المجموعات وبالرموز المتعارفة، معتمدين في ذلك وجهة النظر الحسّية. **فالمجموعة** مفهوم أولي يدركه القارئ ولا يحتاج إلى تعريف، ونسمّي **عناصرَ مجموعةٍ** الأشياء التي تتألف منها هذه المجموعة. فإذا كانت A مجموعة، عنى الرمز $a \in A$ أنّ العنصر a **ينتمي** إلى A، ونستعمل الرمز $a \notin A$ للدلالة على عدم انتماء العنصر a إلى A. أي $a \notin A \Leftrightarrow \neg(a \in A)$. أمّا **المجموعة الخالية**، أي التي لا تحتوي على عناصر، فنرمز إليها بالرمز $\varnothing$.

إذا كانت A و B مجموعتين، فإننا نستعمل الرمز $B \supset A$ (أو $A \subset B$) للدلالة على أنّ كل عنصر ينتمي إلى B ينتمي أيضاً إلى A، ونقول في هذه الحالة إنّ B **محتواة في** A أو إنّ B **مجموعة جزئية** من A. ونقول إنّ $A = B$ إذا وفقط إذا كان $(B \subset A)$ و $(A \subset B)$. وأخيراً إذا كانت Ω مجموعة فإننا نرمز بالرمز $P(\Omega)$ إلى مجموعة أجزائها أي

$$(A \in P(\Omega)) \Leftrightarrow (A \subset \Omega)$$

إذا كانت A و B مجموعتين، واستطعنا أن نقرن بكل عنصر a من A عنصراً وحيداً $f(a)$ ينتمي إلى B، وذلك وفق قاعدة محدّدة تماماً، قلنا إننا قد عرّفنا **تطبيقاً** f **منطلقه** A **ومستقره** B، ونكتب

$$f : A \to B, a \mapsto f(a).$$

ونعرّف **الصورة المباشرة** $f(X)$ لمجموعة $X \subset A$ على الوجه الآتي:

$$f(X) = \left\{b \in B : \exists a \in X, b = f(a)\right\}$$

ونعرّف **الصورة العكسية** $f^{-1}(Y)$ لمجموعة $Y \subset B$ بالصيغة الآتية:

$$f^{-1}(Y) = \{a \in A : f(a) \in Y\}$$

يكون التطبيق $f : A \to B, a \mapsto f(a)$ **متبايناً** إذا وفقط إذا

$$\forall x_1 \in A, \forall x_2 \in A, \quad (f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2)$$

ويكون **غامراً** إذا وفقط إذا كان $f(A) = B$، وأخيراً يكون **تقابلاً** إذا كان متبايناً وغامراً في آن معاً، وفي هذه الحالة يمكننا أنّ نعرّف **التقابل العكسي** الذي نرمز إليه بالرمز f^{-1}.

إذا كان $f : A \to B$ و $g : B \to C$ تطبيقين فإننا نعرّف ناتج **تركيب التطبيقين** f **ثُمّ** g بأنّه التطبيق

$$g \circ f : A \to C, x \mapsto g(f(x))$$

ونقرأ $g \circ f$ بالقول «g يلي f». إنّ ناتج تركيب تطبيقات متباينة تطبيقٌ متباين، وناتج تركيب تطبيقات غامرة تطبيقٌ غامر.

إذا كانت A و X مجموعتين، فإننا نسمّي كل تطبيق منطلقه A ومستقره X وقاعدة ربطه $a \mapsto x_a$، **جماعة من عناصر** X **مجموعة أدلّتها** A، ونكتب $(x_a)_{a \in A}$.

لنذكّر الآن بالعمليات الأساسية على المجموعات. لتكن Ω مجموعة ولتكن $P(\Omega)$ مجموعة أجزائها. ولنتأمّل جماعة $(X_a)_{a\in A}$ من عناصر $P(\Omega)$ مجموعة أدلّتها A، نسمّي **اجتماع** الجماعة $(X_a)_{a\in A}$، ونكتب $\bigcup_{a\in A} X_a$ مجموعة عناصر Ω التي ينتمي كل منها إلى واحدة على الأقل من المجموعات X_a. أي

$$x \in \bigcup_{a\in A} X_a \;\Leftrightarrow\; \exists b \in A, x \in X_b$$

ونسمّي **تقاطع** هذه الجماعة ونكتب $\bigcap_{a\in A} X_a$ مجموعة عناصر Ω التي ينتمي كل منها إلى جميع المجموعات X_a. أي

$$x \in \bigcap_{a\in A} X_a \;\Leftrightarrow\; \forall b \in A, x \in X_b$$

ونسمّي **الجداء الديكارتي** لهذه الجماعة، ونكتب $\prod_{a\in A} X_a$، مجموعة الجماعات $(x_a)_{a\in A}$ من عناصر Ω التي مجموعة أدلّتها A، والتي تحقّق الشرط $\forall b \in A, x_b \in X_b$.

إذا كانت $A = \{1,2,\ldots,n\}$ فإننا نعبّر عن اجتماع الجماعة $(X_a)_{a\in A}$ أو تقاطعها أو جدائها الديكارتي بالرموز المكافئة

$$\begin{aligned}
\bigcup_{k=1}^{n} X_k &= X_1 \cup X_2 \cup \cdots \cup X_n,\\
\bigcap_{k=1}^{n} X_k &= X_1 \cap X_2 \cap \cdots \cap X_n,\\
\prod_{k=1}^{n} X_k &= X_1 \times X_2 \times \cdots \times X_n
\end{aligned}$$

ولقد جرت العادة أنّ نكتب $(x_1, x_2, \ldots, x_n)$ عوضاً عن $(x_k)_{k\in\{1,2,\ldots,n\}}$.

نقول إنّ المجموعتين A و B **منفصلتان** إذا وفقط إذا كان $A \cap B = \varnothing$. ونقول إنّ الجماعة $(X_a)_{a\in A}$ من عناصر $P(\Omega)$ التي مجموعة أدلّتها A، **منفصلة مثنى مثنى** إذا وفقط إذا كان

$$\forall (a_1, a_2) \in A \times A,\;\; a_1 \neq a_2 \Rightarrow X_{a_1} \cap X_{a_2} = \varnothing$$

وأخيراً نقول إنّ الجماعة $(X_a)_{a\in A}$ من عناصر $P(\Omega)$ تؤلّف **تجزئة** للمجموعة Ω إذا وفقط إذا كان

① $\forall a \in A, X_a \neq \varnothing;$

② $\forall (a_1, a_2) \in A\times A, \quad a_1 \neq a_2 \Rightarrow X_{a_1} \cap X_{a_2} = \varnothing;$

③ $\Omega = \bigcup\limits_{a\in A} X_a.$

إذا كانت A و B مجموعتين، فإننا نستعمل الرمز $A\backslash B$ ونقرؤه «A **فرق** B» دلالة على مجموعة العناصر التي تنتمي إلى A ولا تنتمي إلى B. ونستعمل الرمز $A\Delta B$ الذي نسميه **الفرق التناظري** للمجموعتين A و B دلالة على اجتماع المجموعتين $A\backslash B$ و $B\backslash A$.

2-1. مثال. لتكن A و B مجموعتين غير خاليتين، وليكن التطبيق $f : A \to B$. نفترض أنّه يوجد تطبيق $g : B \to A$ يُحقّق

$$g\circ f = I_A \quad \text{و} \quad f\circ g = I_B$$

حيث I_A و I_B هما التطبيقان المطابقان في A و B على التوالي. سنثبت أنّ التطبيق f تقابلٌ وأنّ $f^{-1} = g$.

لنثبت أوّلاً أنّ التطبيق f متباينٌ. ليكن x_1 و x_2 عنصرين من A. عندئذ

$$\begin{aligned} f(x_1) = f(x_2) \quad &\Rightarrow \quad g\circ f(x_1) = g(f(x_1)) = g(f(x_2)) = g\circ f(x_2) \\ &\Rightarrow \quad I_A(x_1) = I_A(x_2) \Rightarrow x_1 = x_2 \end{aligned}$$

ومن جهة أخرى، إنّ التطبيق f غامرٌ. لأنّه أياً كان y من B يوجدْ عنصرٌ $x = g(y)$ من A يُحقّق

$$f(x) = f(g(y)) = f\circ g(y) = I_B(y) = y$$

نستنتج إذن أنّ التطبيق f تقابلٌ. ليكن f^{-1} تقابله العكسيّ. عندئذ

$$f^{-1} = f^{-1}\circ I_B = f^{-1}\circ(f\circ g) = (f^{-1}\circ f)\circ g = I_A\circ g = g$$

وبذلك يكتمل الإثبات.

تطبيقاً على ذلك، لتكن Ω مجموعةً غير خالية، ولتكن Γ مجموعة جزئية منها. نعرّف التطبيق

$$\Psi : P(\Omega) \to P(\Gamma) \times P(\Omega \backslash \Gamma), X \mapsto (X \cap \Gamma, X \cap (\Omega \backslash \Gamma))$$

وكذلك نعرِّف التطبيق

$$\Phi : P(\Gamma) \times P(\Omega \backslash \Gamma) \to P(\Omega), (A, B) \mapsto A \cup B$$

عندئذ نتحقق بسهولة صحةَ المساواتين

$$\Psi \circ \Phi = I_{P(\Gamma) \times P(\Omega \backslash \Gamma)} \quad \text{و} \quad \Phi \circ \Psi = I_{P(\Omega)}$$

وهذا يُثبتُ أنّ Φ و Ψ تقابلان، وأنّ أيّاً منهما هو التقابل العكسيّ للآخر.

3. العلاقات الثنائية

لتكن E مجموعة. نسمي **علاقة ثنائية** على المجموعة E الزوج $\mathcal{R} = (E, \Gamma)$ حيث Γ مجموعة جزئية من الجداء الديكارتي $E \times E$ نسميها بيان العلاقة $\mathcal{R}$. ونقول إنّ عنصرين x و y من E مرتبطان وفق العلاقة $\mathcal{R}$ ونكتب $x\mathcal{R}y$ إذا وفقط إذا كان $(x, y) \in \Gamma$.

لتكن $\mathcal{R}$ علاقة ثنائية على المجموعة E. نقول عن $\mathcal{R}$ إنها

- **انعكاسية** إذا وفقط إذا $\forall x \in E,\ \ x\mathcal{R}x$.
- **تناظرية** إذا وفقط إذا $\forall (x, y) \in E \times E,\ \ x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
- **تخالفية** إذا وفقط إذا $\forall (x, y) \in E \times E,\ \ (x\mathcal{R}y) \wedge (y\mathcal{R}x) \Rightarrow y = x$.
- **متعدّية** إذا وفقط إذا $\forall (x, y, z) \in E^3,\ \ (x\mathcal{R}y) \wedge (y\mathcal{R}z) \Rightarrow x\mathcal{R}z$.

3-1. علاقات التكافؤ

لتكن $\mathcal{R}$ علاقة ثنائية على المجموعة E. نقول إنّ $\mathcal{R}$ علاقة **تكافؤ** إذا وفقط إذا كانت انعكاسية وتناظرية ومتعدّية، في هذه الحالة نكتب $x = y \bmod \mathcal{R}$، عوضاً عن $y\mathcal{R}x$، ونقرأ «x يساوي y بالقياس $\mathcal{R}$». وإذا كان x عنصراً من E فإننا نسمّي المجموعة

$$[x] = \left\{ y \in E : y\mathcal{R}x \right\}$$

صف تكافؤ العنصر x.

ونسمّي مجموعة صفوف التكافؤ **مجموعة خارج قسمة** E **بالقياس** $\mathcal{R}$ ونرمز إليها بالرمز $E/\mathcal{R}$. كما نسمّي أي عنصر من صف تكافؤ ممثّلاً عن هذا الصف. وأخيراً نسمّي التطبيق $Q : E \to E/\mathcal{R}, x \mapsto [x]$ **الغمر القانوني**.

3-1-1. **مبرهنة**. لتكن $\mathcal{R}$ علاقة تكافؤ على المجموعة E . تكوّنُ مجموعةُ صفوف التكافؤ بالقياس $\mathcal{R}$ تجزئة للمجموعة E . وبالعكس، تعرّف كلُّ تجزئة للمجموعة E علاقة تكافؤ صفوفها هي عناصر التجزئة نفسها.

الإثبات

– لمّا كان $x \in [x]$ ، فإن صفوف التكافؤ ليست خالية، ثُمّ إنّ

$$E = \bigcup_{x \in E} \{x\} \subset \bigcup_{x \in E} [x] \subset E$$

ومن ناحية أخرى إذا وُجد y ينتمي إلى $[x] \cap [z]$ كان

$$x = y \bmod \mathcal{R} \quad \text{و} \quad z = y \bmod \mathcal{R}$$

ومن ثَمّ $x = z \bmod \mathcal{R}$ ، ومنه

$$u \in [x] \Leftrightarrow u = x \bmod \mathcal{R} \underset{x\mathcal{R}y}{\Leftrightarrow} u = z \bmod \Re \Leftrightarrow u \in [z] \,.$$

إذن $[z] = [x]$. فصفوف التكافؤ منفصلة مثنى مثنى، وتكوّن تجزئة للمجموعة E .

– إذا كانت $(X_a)_{a \in A}$ تجزئة للمجموعة E ، فإننا نعرّف العلاقة الثنائية $\mathcal{R}$ على E كما يلي:

$$x \mathcal{R} y \Leftrightarrow \exists a \in A, (x \in X_a) \wedge (y \in X_a)$$

ونترك للقارئ مهمة التوثُّق من كوْن العلاقة $\mathcal{R}$ علاقة تكافؤ على المجموعة E محققة للشرط

$$E/\mathcal{R} = \{ X_a : a \in A \}$$

وهي النتيجة المرجوّة. ❐

3-2. علاقات الترتيب

لتكن $\mathcal{R}$ علاقة ثنائية على المجموعة E . نقول إنّ $\mathcal{R}$ علاقة **ترتيب** إذا وفقط إذا كانت انعكاسية وتخالفية ومتعدّية، ونرمز عادة بالرمز $\leq$ إلى علاقة ترتيب، ونقول إنّ $(E, \leq)$ **مجموعة مرتّبة**. يكون عنصران x و y من E قابلين للمقارنة إذا وفقط إذا كان $y \leq x$ أو $x \leq y$.

ونقول إنّ $(E, \leq)$ **مرتَّبة كليّاً** إذا كانت جميع عناصرها قابلة للمقارنة مثنى مثنى.

لتكن $(E,\leq)$ مجموعة مرتّبة، ولتكن A مجموعة جزئية غير خالية من E.

- نقول إنّ X من E عنصر **راجح** على A إذا وفقط إذا

$$\forall a \in A,\ \ a \leq X$$

- نقول إنّ x من E عنصر **قاصر** عن A إذا وفقط إذا

$$\forall a \in A,\ \ x \leq a$$

- نقول إنّ M من E هو **أكبر عنصر** في A إذا وفقط إذا

$$(\forall a \in A,\ \ a \leq M) \wedge (M \in A)$$

ونرمز إلى هذا العنصر إن وُجِدَ بالرمز $\max(A)$.

- نقول إنّ m من E هو **أصغر عنصر** في A إذا وفقط إذا

$$(\forall a \in A,\ \ m \leq a) \wedge (m \in A)$$

ونرمز إلى هذا العنصر إن وُجِدَ بالرمز $\min(A)$.

- نقول إنّ S من E هو **الحد الأعلى** للمجموعة الجزئيّة A إذا وفقط إذا كان S أصغر العناصر الراجحة على A. ونرمز إلى هذا العنصر إن وُجِدَ بالرمز $\sup(A)$.

- نقول إنّ I من E هو **الحد الأدنى** للمجموعة الجزئيّة A إذا وفقط إذا كان I أكبر العناصر القاصرة عن A. ونرمز إلى هذا العنصر إن وُجِدَ بالرمز $\inf(A)$.

- نقول إنّ α من A **عنصر أعظمي** في A إذا وفقط إذا

$$\forall b \in A,\ \ \alpha \leq b \Rightarrow \alpha = b$$

- نقول إنّ β من A **عنصر أصغري** في A إذا وفقط إذا

$$\forall b \in A,\ \ b \leq \beta \Rightarrow \beta = b$$

لتكن $(E,\prec)$ و $(F,\leq)$ مجموعتين مرتّبتين، وليكن التطبيق $f:E\to F$.

- نقول إنّ f **متزايد** إذا وفقط إذا

$$\forall (x,y)\in E\times E,\quad x\prec y \Rightarrow f(x)\leq f(y)$$

- نقول إنّ f **متناقص** إذا وفقط إذا

$$\forall (x,y)\in E\times E,\quad x\prec y \Rightarrow f(y)\leq f(x)$$

- نقول إنّ f **متزايد تماماً** إذا وفقط إذا

$$\forall (x,y)\in E\times E,\quad (x\prec y)\wedge(x\neq y) \Rightarrow f(x)< f(y)$$

- نقول إنّ f **متناقص تماماً** إذا وفقط إذا

$$\forall (x,y)\in E\times E,\quad (x\prec y)\wedge(x\neq y) \Rightarrow f(y)< f(x)$$

- نقول إنّ f **مطّردٌ** إذا كان متزايداً أو متناقصاً.

حيث رمزنا، كما جرت العادة، $a<b$ للدلالة على $(a\leq b)\wedge(a\neq b)$.

3-2-1. **مثال**. لتكن $E=\mathbb{R}^2=\mathbb{R}\times\mathbb{R}$، و $\mathbb{R}$ هي مجموعة الأعداد الحقيقيّة. ولنعرّف على E العلاقة الثنائيّة:

$$(x_1,y_1)\prec(x_2,y_2)\Leftrightarrow (x_1\leq x_2)\wedge(y_1\leq y_2)$$

نترك القارئ يتحقّق كوْنَ $(E,\prec)$ مجموعة مرتّبة.

وإذا تأمّلنا المجموعة الجزئيّة التالية :

$$A=\left\{(x,y)\in E: x^2+y^2\leq 1\right\}$$

وجدنا أنّ عناصرَ المجموعة:

$$\tilde{A}=\left\{(x,y)\in E:(x^2+y^2=1)\wedge(x\geq 0)\wedge(y\geq 0)\right\}$$

هي العناصر الأعظميّة في A، وأنّ $\sup A=(1,1)$ وهو لا ينتمي إلى المجموعة A.

أمّا إذا تأمّلنا المجموعة الجزئيّة

$$B=\left\{(x,y)\in E: x^2+y^2< 1\right\}$$

فلا نجد فيها عناصر أعظميّة، مع أنّ $\sup B=(1,1)$.

4. المجموعات المنتهية

4-1. مجموعة الأعداد الطبيعية $\mathbb{N}$

سنكتفي بإعطاء فكرة عن الخطوط العريضة لبناء الأعداد الطبيعية. نعتبر **موضوعةً أساسيةً** أنه توجد مجموعة مرتبة وغير خالية وحيدة $\mathbb{N}$ تحقق الخواص التالية :

$\mathcal{N}_1$ – في كل مجموعة جزئية غير خالية من $\mathbb{N}$ أصغر عنصر.

$\mathcal{N}_2$ – إذا وُجِدَ لمجموعة جزئية غير خالية من $\mathbb{N}$ عنصر راجح عليها ففيها أكبر عنصر.

$\mathcal{N}_3$ – ليس في المجموعة $\mathbb{N}$ أكبر عنصر.

☞ نقصد بالوحدانية أنّه إذا وُجِدَت مجموعة أخرى تحقق الخواص السابقة فيوجد تقابل متزايد وحيد بين تلك المجموعة والمجموعة $\mathbb{N}$.

- نجد بناءً على الخاصة $\mathcal{N}_1$ أصغر عنصر في كل مجموعة جزئية مؤلّفة من عنصرين محتواة في $\mathbb{N}$. نستنتج من ذلك أنّ المجموعة $\mathbb{N}$ مرتبة كلياً. سنرمز فيما يلي بالرمز $\leq$ إلى علاقة الترتيب على $\mathbb{N}$، وسنكتب $x < y$ دلالة على أنّ $(x \leq y) \wedge (x \neq y)$.

- إذا كان a عنصراً من $\mathbb{N}$ كانت المجموعة $\{n \in \mathbb{N} : a < n\}$ غير خالية استناداً إلى $\mathcal{N}_3$، فهي تحتوي على أصغر عنصر، بناءً على $\mathcal{N}_1$، نرمز إليه عادة بالرمز $a+1$. نلاحظ أنّ $a < a+1$ وأن المجموعة $\{n \in \mathbb{N} : a < n < a+1\}$ خالية. نسمّي $a+1$ العنصر اللاحق للعنصر a. جرت العادةُ أن نرمز إلى أصغر عنصر من المجموعة $\mathbb{N}$ بالرمز 0، وإلى العناصر اللاحقة للعناصر $0,1,2,\ldots$ بالرموز $1,2,3,\ldots$ على التوالي. وأن نستعمل الرمز $\mathbb{N}^*$ دلالة على $\mathbb{N}\backslash\{0\}$.

- إذا كان a عنصراً من $\mathbb{N}^*$ كانت المجموعة $\{n \in \mathbb{N} : n < a\}$ غير خالية لأنّها تحوي 0، والعنصر a راجح عليها فهي، بمقتضى $\mathcal{N}_2$، تحتوي على أكبر عنصر نرمز إليه عادة بالرمز $a-1$، ونسمّيه العنصر السابق للعنصر a. نلاحظ أنّ $a-1 < a$ وأن المجموعة $\{n \in \mathbb{N} : a-1 < n < a\}$ خالية.

نستنتج مما سبق أنّ التطبيقين

$$p : \mathbb{N}^* \to \mathbb{N}, a \mapsto a-1 \quad \text{و} \quad s : \mathbb{N} \to \mathbb{N}^*, a \mapsto a+1$$

تقابلان متزايدان، وكلٌّ منهما هو التطبيق العكسي للآخر.

1-1-4. **مبرهنة**. لتكن A مجموعة جزئية من $\mathbb{N}$. نفترض أنّ

$$(0 \in A) \wedge \Big(\forall n \in \mathbb{N}, \quad (n \in A) \Rightarrow (n+1 \in A)\Big)$$

إذن $A = \mathbb{N}$.

الإثبات

لنفترض أنّ المجموعة $B = \mathbb{N} \backslash A$ ليست مجموعة خالية، إذن لا بد أن فيها أصغر عنصر وليكن b. ولكن 0 لا ينتمي إلى B إذن $b \in \mathbb{N}^*$. ليكن $p(b) = a$ عندئذ $a+1 = b$. وبناءً على تعريف b يكون $a \notin B$ أي $a \in A$. واستناداً إلى الفرْض يجب أن يكون $b = a+1 \in A$، وهذا يناقض كوْن $b \in B$. ❐

2-1-4. **مبرهنة**. لتكن $\mathcal{P}(n)$ قضية مفتوحة على المجموعة المرجعية $\mathbb{N}$. نفترض أنّ :

① $\mathcal{P}(0)$ صحيحة.

② $\forall n \in \mathbb{N}, \quad \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$.

عندئذ تكون $\mathcal{P}(n)$ صحيحةً أيّاً كان n من $\mathbb{N}$.

الإثبات

نرى بسهولة أنّ المجموعة $A = \{n \in \mathbb{N} : \text{صحيحة } \mathcal{P}(n)\}$ تُحقّق شروطَ المبرهنة السابقة. وهذا يُثبت الخاصّة المطلوبة. ❐

نسمّي هذه المبرهنة مبدأ **الإثبات بالتدريج**. ويمكننا أن نستبدل بالشرط ① الشرطَ $\mathcal{P}(n_0)$ صحيحة، وبالشرط ② الشرطَ $\forall n \geq n_0, \quad \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$، فنثبت أنّ $\mathcal{P}(n)$ صحيحة أيّاً كان $n_0 \leq n$.

2-4. المجموعات المنتهية، رئيس مجموعة

ليكن n عنصراً من $\mathbb{N}$، نرمز إلى المجموعة $\{k \in \mathbb{N} : 1 \leq k \leq n\}$ بالرمز $\mathbb{N}_n$. وبوجه خاص $\mathbb{N}_0 = \varnothing$. ونثبت بسهولة أنه إذا وُجِدَ تطبيق متباين منطلقه $\mathbb{N}_n$ ومستقره $\mathbb{N}_m$ كان $n \leq m$، و منه إذا وُجِدَ تقابل بين $\mathbb{N}_n$ و $\mathbb{N}_m$ كان $n = m$.

نقول عن مجموعة غير خالية A إنها **منتهية** إذا وفقط إذا وُجِدَ عدد طبيعي n وتقابل بين A و $\mathbb{N}_n$. بالطبع هذا العدد وحيد في حال وجوده ونسمّيه **رئيس المجموعة** A أو عدد عناصرها ونرمز إليه بالرمز $\mathrm{card}(A)$، ونصطلح أنّ $\mathrm{card}(\varnothing) = 0$. أمّا إذا لم تكن المجموعة A منتهية فنقول إنّها **لانهائية**. لنذكر الآن بعض خواص المجموعات المنتهية دون إثبات نظراً إلى سهولتها:

- تكون كلُّ مجموعة جزئية F من مجموعة منتهيةٍ E منتهيةً و $\mathrm{card}(E) \geq \mathrm{card}(F)$.
- تقاطع جماعة من المجموعات المنتهية مجموعةٌ منتهية.
- لتكن E مجموعة منتهية، وليكن $f : E \to F$ تطبيقاً. عندئذ تكون $f(E)$ مجموعة منتهية، و $\mathrm{card}(E) \geq \mathrm{card}(f(E))$. وتتحقق المساواة إذا وفقط إذا كان التطبيق f متبايناً.
- لتكن E مجموعة منتهية، وليكن $f : E \to F$ تطبيقاً غامراً.عندئذ تكون F منتهية و $\mathrm{card}(E) \geq \mathrm{card}(F)$. وتتحقق المساواة إذا وفقط إذا كان f تقابلاً.
- ليكن $f : E \to F$ تطبيقاً متبايناً. إذا كانت المجموعة $f(E)$ منتهية كانت المجموعة E منتهية وكان $\mathrm{card}(E) = \mathrm{card}(f(E))$.
- ليكن $f : E \to F$ تطبيقاً بين مجموعتين منتهيتين E و F لهما عدد العناصر نفسه، هناك تكافؤ بين الخواص الآتية: f متباين، و f غامر، و f تقابل.

نعرّف، أيّاً كان العددان الطبيعيان n و m، العمليتين

$$n + m = \mathrm{card}\big((\{1\} \times \mathbb{N}_n) \cup (\{0\} \times \mathbb{N}_m)\big)$$
$$nm = \mathrm{card}(\mathbb{N}_n \times \mathbb{N}_m)$$

فنحصل على قوانين التشكيل المعروفة في مجموعة الأعداد الطبيعية. ولن نطيل في بحث خواص هاتين العمليتين التي نعتبرها معروفة للقارئ.

4-3. التحليل التوافقي

يؤول العديد من المسائل في الرياضيات، وغيرها من العلوم إلى حساب عدد عناصر مجموعة منتهية. سنذكر في هذه الفقرة بعض طرائق العدّ أو التحليل التوافقي. نقول إنّ للمجموعتين E و F القدرة نفسها إذا وفقط إذا وُجِدَ تقابل بينهما. يمكننا بسهولة أن نثبت أنّ رئيس اجتماع مجموعتين منتهيتين ومنفصلتين لا يتغيّر إذا استبدلنا بأحدهما مجموعةً لها القدرة نفسها. وكذلك فإن رئيس الجداء الديكارتي لمجموعتين منتهيتين لا يتغيّر إذا استبدلنا بأحدهما مجموعةً لها القدرة نفسها. مما يتيح لنا وضع الخاصتين التاليتين :

(D_1) إذا كانت A و B مجموعتين منتهيتين منفصلتين كانت المجموعة $A \cup B$ مجموعة منتهية وكان $$\operatorname{card}(A \cup B) = \operatorname{card}(A) + \operatorname{card}(B)$$

(D_2) إذا كانت A و B مجموعتين منتهيتين كان $A \times B$ مجموعة منتهية وكان $$\operatorname{card}(A \times B) = \operatorname{card}(A) \cdot \operatorname{card}(B)$$

ويمكن تعميم هاتين الخاصتين على عددٍ منتهٍ من المجموعات.

4-3-1. أجزاء مجموعة منتهية

① **المجموعة** $P^{(n)}$.

لنذكّر أنّ $P(E)$ هي مجموعة أجزاء E. نرمز بالرمز $P^{(n)}$ إلى المجموعة $P(\mathbb{N}_n)$ تسهيلاً. فما هو عدد عناصر $P^{(n)}$ ؟

من الواضح أنّ

$$P^{(2)} = \{\varnothing, \{1\}, \{2\}, \{1,2\}\} \text{ و } P^{(1)} = \{\varnothing, \{1\}\} \text{ و } P^{(0)} = \{\varnothing\}$$

ومن ثَمّ

$$\operatorname{card}(P^{(2)}) = 4 \text{ و } \operatorname{card}(P^{(1)}) = 2 \text{ و } \operatorname{card}(P^{(0)}) = 1$$

لنأتِ إذن إلى الحالة العامّة، لتكن $n \geq 1$ ولنرمز بالرمز $A^{(n)}$ إلى مجموعة أجزاء $\mathbb{N}_n$ التي تحوي العنصر n، وبالرمز $B^{(n)}$ إلى مجموعة أجزاء $\mathbb{N}_n$ التي لا تحوي العنصرَ n. من الواضح أنّ $\left\{A^{(n)}, B^{(n)}\right\}$ تجزئة للمجموعة $P^{(n)}$.

الملاحظة الأولى هي أنّ $B^{(n)}$ هي نفسها المجموعة $P^{(n-1)}$. أمّا الملاحظة الثانية فهي أنّه يوجد تقابل بسيط بين $A^{(n)}$ و $P^{(n-1)}$ معرّف كما يلي

$$\varphi : P^{(n-1)} \rightarrow A^{(n)}, T \mapsto T \cup \{n\}$$

نستنتج أنّ

$$\operatorname{card}(P^{(n-1)}) = \operatorname{card}(A^{(n)}) = \operatorname{card}(B^{(n)})$$

ومن ثَمّ

$$\operatorname{card}(P^{(n)}) = \operatorname{card}(A^{(n)}) + \operatorname{card}(B^{(n)}) = 2\operatorname{card}(P^{(n-1)})$$

وهذا ما يتيح لنا أن نثبت بالتدريج أنّ $\operatorname{card}(P^{(n)}) = 2^n$. ومنه :

(D_3) إذا كانت E مجموعة منتهية كانت مجموعة أجزائها $P(E)$ منتهية وكان $\operatorname{card}(P(E)) = 2^{\operatorname{card}(E)}$.

② المجموعة $P_k^{(n)}$.

إذا كان k عنصراً من $\mathbb{N}$، رمزنا بالرمز $P_k^{(n)}$ إلى مجموعة أجزاء $\mathbb{N}_n$ التي عدد عناصر كل منها يساوي k. أي

$$P_k^{(n)} = \left\{A \subset \mathbb{N}_n : \operatorname{card}(A) = k\right\}$$

نضع بالتعريف $C_n^k = \operatorname{card}(P_k^{(n)})$.

هنالك جزء وحيد في $\mathbb{N}_n$ يحوي 0 عنصراً، وآخر وحيد يحوي n عنصراً، ومن ثَمّ يكون $C_n^n = C_n^0 = 1$ أيّاً كان العدد n من $\mathbb{N}$. ولا يوجد في $\mathbb{N}_n$ أجزاء عدد عناصرها أكبر تماماً من n، ومن ثَمّ $C_n^k = 0$ في حالة $k > n$.

أياً كان $1 \leq n$ و $1 \leq k$، نرمز بالرمز $A_k^{(n)}$ إلى مجموعة أجزاء $\mathbb{N}_n$ التي تحوي العنصرَ n والتي عدد عناصر كل منها k. ونرمز بالرمز $B_k^{(n)}$ إلى مجموعة أجزاء $\mathbb{N}_n$ التي لا تحوي العنصرَ n والتي عدد عناصر كل منها k.

من الواضح أنّ $\left\{A_k^{(n)}, B_k^{(n)}\right\}$ تجزئة للمجموعة $P_k^{(n)}$. مما يثبت أنّ

$$C_n^k = \operatorname{card}(A_k^{(n)}) + \operatorname{card}(B_k^{(n)})$$

وهنا يمكننا، مجدّداً، ملاحظة ما يلي:

- المجموعة $B_k^{(n)}$ هي نفسها $P_k^{(n-1)}$.
- هنالك تقابل بين $A_k^{(n)}$ و $P_{k-1}^{(n-1)}$ معطى بالعلاقة

$$\varphi : P_{k-1}^{(n-1)} \to A_k^{(n)},\ \ T \mapsto T \cup \{n\}$$

إذن $C_{n-1}^k = \operatorname{card}(B_k^{(n)})$ و $C_{n-1}^{k-1} = \operatorname{card}(A_k^{(n)})$. وهذا ما يتيح لنا استنتاج العلاقة التالية:

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$$

أو

$$(1) \qquad \forall (n,k) \in \mathbb{N} \times \mathbb{N}, \quad C_{n+1}^{k+1} = C_n^k + C_n^{k+1}$$

تفيد هذه العلاقة في حساب القيم غير المعدومة للأعداد C_n^k، كما هو موضّح فيما يلي

$n \backslash k$	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1

$$\begin{array}{ccc} C_n^k & + & C_n^{k+1} \\ & \to & \\ & \downarrow & \| \\ & & C_{n+1}^{k+1} \end{array}$$

سنحاول الآن البحث عن صيغة أخرى لحساب الأعداد C_n^k.

لنعرّف، أياً كان العدد n من $\mathbb{N}$، المقدار

$$G_n(x) = C_n^0 + C_n^1 x + C_n^2 x^2 + \cdots + C_n^n x^n = \sum_{k\geq 0} C_n^k x^k$$

فمثلاً

$$G_0(x) = 1 \text{ و } G_1(x) = 1 + x \text{ و } G_2(x) = 1 + 2x + x^2 = (1+x)^2$$

لنضرب إذن طرفيّ العلاقة (1) بالمقدار x^{k+1} ولنجمع العلاقات الناتجة والموافقة لجميع قيم k فنجد

$$\sum_{k\geq 0} C_{n+1}^{k+1} x^{k+1} = \sum_{k\geq 0} C_n^k x^{k+1} + \sum_{k\geq 0} C_n^{k+1} x^{k+1}$$

وبإصلاح هذه العلاقة نجد:

$$G_{n+1}(x) - C_{n+1}^0 = x\,G_n(x) + G_n(x) - C_n^0$$

أو

$$G_{n+1}(x) = (1+x)G_n(x)$$

مما يتيح لنا أن نثبت بالتدريج صحة العلاقة الآتية

$$G_n(x) = (1+x)^n$$

ونحصل من ثَمّ على المتطابقة التالية المعروفة باسم دستور الكرخي–نيوتن

$$C_n^0 + C_n^1 x + C_n^2 x^2 + \cdots + C_n^n x^n = \sum_{k\geq 0} C_n^k x^k = (1+x)^n$$

ليكن p عدداً طبيعياً يُحقّق $0 < p < n$. باشتقاق طرفي العلاقة السابقة p مرّةً بالنسبة إلى المتحول x، ثُمّ تعويض 0 بالمتحول x نجد

$$n \times (n-1) \times \cdots \times (n-p+1) = p \times (p-1) \times \cdots \times 2 \times 1 \cdot C_n^p$$

ومنه العلاقة

$$C_n^p = \frac{n \times (n-1) \times \cdots \times (n-p+1)}{p \times (p-1) \times \cdots \times 2 \times 1}, \quad 1 \leq p < n$$

يوحي لنا هذا بإدخال الرمز الجديد $p!$، الذي يُقرأ «p **عاملي**» ، دلالة على جداء الضرب : $p \times (p-1) \times \cdots \times 2 \times 1$. ونصطلح أنّ $0! = 1$.

وبذلك يمكننا أن نكتب :

$$C_n^p = \frac{n!}{p!(n-p)!} \quad \text{حين يكون} \quad 0 \le p \le n.$$

نكون إذن قد وصلنا إلى النتيجة التالية:

(D_4) إذا كانت E مجموعة منتهية عدد عناصرها n، و $P_k(E)$ مجموعة أجزاء E التي عدد عناصر كلٍ منها k، عندئذ $\text{card}(P_k(E)) = C_n^k$ حيث $$C_n^k = \begin{cases} 0 & : \quad n < k \\ \dfrac{n!}{k!(n-k)!} & : \quad 0 \le k \le n \end{cases}$$

ونترك للقارئ مهمة التيقّن من صحّة العلاقتين المهمّتين :

$$C_{a+b}^a = C_{a+b}^b \quad \text{و} \quad C_a^b = \frac{a}{b} C_{a-1}^{b-1}$$

4-3-2. التطبيقات بين مجموعتين منتهيتين

③ المجموعة $F(\mathbb{N}_n, \mathbb{N}_p)$.

هي مجموعة التطبيقات التي منطلقها $\mathbb{N}_n$ ومستقرها $\mathbb{N}_p$ حيث $(n,p) \in \mathbb{N}^{*2}$. لنرمز مؤقتاً بالرمز $c(n,p)$ إلى عدد عناصر هذه المجموعة.

من الواضح أنّ $c(n,1) = 1$ وأنّ $c(1,p) = p$. لنثبّت العددين $1 < n$ و p، ولنعرّف، أياً كان العدد k من $\mathbb{N}_p$، المجموعة

$$B_k = \{ f \in F(\mathbb{N}_n, \mathbb{N}_p) : f(n) = k \}$$

من الواضح أنّ $\{B_1, B_2, \ldots, B_p\}$ تكوّن تجزئة للمجموعة $F(\mathbb{N}_n, \mathbb{N}_p)$، ومن ثَمّ

$$c(n,p) = \sum_{k=1}^{p} \text{card}(B_k)$$

ولكن هنالك تقابل بين المجموعة B_k والمجموعة $F(\mathbb{N}_{n-1}, \mathbb{N}_p)$. هذا التقابل هو التطبيق الذي يقرن بالعنصر g من B_k مقصورَه $\tilde{g}$ على المجموعة $\mathbb{N}_{n-1}$ أي العنصر $\tilde{g}$ من المجموعة $F(\mathbb{N}_{n-1}, \mathbb{N}_p)$ المعرّف كما يلي: $\tilde{g} : \mathbb{N}_{n-1} \to \mathbb{N}_p, \ x \mapsto g(x)$. إذن

$$c(n-1, p) = \text{card}(B_k)$$

ومنه

$$c(n, p) = p \cdot c(n-1, p)$$

هذا ما يتيح لنا أن نثبت، بالتدريج، العلاقة $c(n, p) = p^n$. ومنه:

> (D_5) لتكن $F(A, B)$ مجموعة التطبيقات التي منطلقها مجموعة منتهية A عدد عناصرها n، ومستقرها مجموعة منتهية B عدد عناصرها p، حيث (n, p) من $\mathbb{N}^{*2}$. عندئذ يكون $\text{card}\, F(A, B) = p^n$.

④ المجموعة $F_{sc}(\mathbb{N}_n, \mathbb{N}_p)$

هي مجموعة التطبيقات المتزايدة تماماً التي منطلقها $\mathbb{N}_n$ ومستقرها $\mathbb{N}_p$ حيث $(n, p) \in \mathbb{N}^{*2}$. لمّا كان كلّ عنصر من $F_{sc}(\mathbb{N}_n, \mathbb{N}_p)$ تطبيقاً متبايناً بالضرورة، كانت المجموعة $F_{sc}(\mathbb{N}_n, \mathbb{N}_p)$ خالية في حالة $p > n$. لنفترض إذن أنّ $p \leq n$.

نترك للقارئ مهمة بسيطة هي التحقُّق من كوْن التطبيق :

$$\varphi : F_{sc}(\mathbb{N}_n, \mathbb{N}_p) \to P_n^{(p)}, \quad f \mapsto \text{Im}\, f = f(\mathbb{N}_n)$$

تقابلاً ، وهذا يقتضي أنّ $\text{card}\left(F_{sc}(\mathbb{N}_n, \mathbb{N}_p)\right) = C_p^n$. ومنه :

> (D_6) لتكن $F_{sc}(\mathbb{N}_n, \mathbb{N}_p)$ مجموعة التطبيقات المتزايدة تماماً التي منطلقها $\mathbb{N}_n$ ومستقرها $\mathbb{N}_p$ حيث $(n, p) \in \mathbb{N}^{*2}$. عندئذ يكون
>
> $$\text{card}\left(F_{sc}(\mathbb{N}_n, \mathbb{N}_p)\right) = C_p^n$$

⑤ المجموعة $F_c(\mathbb{N}_n,\mathbb{N}_p)$.

هي مجموعة التطبيقات المتزايدة التي منطلقها $\mathbb{N}_n$، ومستقرها $\mathbb{N}_p$ حيث p و n من $\mathbb{N}^*$.
سنستعمل لحساب عدد عناصر هذه المجموعة تقنية أصبحت الآن مألوفة لدينا، وهي مبنية على إيجاد تقابل بين هذه المجموعة ومجموعة أخرى معلوم لدينا عدد عناصرها.

ليكن f عنصراً من $F_c(\mathbb{N}_n,\mathbb{N}_p)$، ولنضع $\tilde{f}(k)=f(k)+k-1$، أياً كان k من $\mathbb{N}_n$. من الواضح أنّ

$$\tilde{f}(k+1)-\tilde{f}(k)=1+f(k+1)-f(k)\geq 1$$

فالتطبيق $\tilde{f}$ متزايد تماماً.

ومن ناحية أخرى

$$\tilde{f}(n)=f(n)+n-1\leq n+p-1 \quad \text{و} \quad \tilde{f}(1)=f(1)\geq 1$$

إذن لقد أثبتنا أنّ $\tilde{f}$ ينتمي إلى $F_{sc}(\mathbb{N}_n,\mathbb{N}_{n+p-1})$، ونكون قد عرّفنا تطبيقاً

$$\varphi : F_c(\mathbb{N}_n,\mathbb{N}_p)\to F_{sc}(\mathbb{N}_n,\mathbb{N}_{n+p-1}),\ f\mapsto \tilde{f}$$

يمكن للقارئ أن يثبت بسهولة أن التطبيق φ تقابل وأنّ تقابله العكسي هو التطبيق

$$\psi : F_{sc}(\mathbb{N}_n,\mathbb{N}_{n+p-1})\to F_c(\mathbb{N}_n,\mathbb{N}_p),\ g\mapsto \hat{g}$$

حيث $\hat{g}(k)=g(k)-k+1$.

نستنتج من ذلك الخاصة التالية :

> (D_7) لتكن $F_c(\mathbb{N}_n,\mathbb{N}_p)$ مجموعة التطبيقات المتزايدة التي منطلقها المجموعة $\mathbb{N}_n$ ومستقرها $\mathbb{N}_p$ حيث p و n من $\mathbb{N}^*$. عندئذ
>
> $$\operatorname{card}\big(F_c(\mathbb{N}_n,\mathbb{N}_p)\big)=C^n_{n+p-1}$$

⑥ المجموعة $F_i(\mathbb{N}_n,\mathbb{N}_p)$

هي مجموعة التطبيقات المتباينة التي منطلقها $\mathbb{N}_n$ ومستقرها $\mathbb{N}_p$ مع p و n من $\mathbb{N}^*$. إنّ هذه المجموعة خالية إذا كان $p<n$.

سنترك للقارئ مهمة إثبات الخاصة التالية :

(D_8) لتكن $F_i(\mathbb{N}_n,\mathbb{N}_p)$ مجموعة التطبيقات المتباينة التي منطلقها المجموعة $\mathbb{N}_n$ ومستقرها $\mathbb{N}_p$ مع p و n من $\mathbb{N}^*$ و $p \geq n$. عندئذ $\operatorname{card}\big(F_i(\mathbb{N}_n,\mathbb{N}_p)\big) = p\times\cdots\times(p-n+1) = \dfrac{p!}{(p-n)!}$

⑦ المجموعة $\mathcal{S}(\mathbb{N}_n)$

هي مجموعة التقابلات أو التباديل على المجموعة $\mathbb{N}_n$. من الواضح أنّ

$$F_i(\mathbb{N}_n,\mathbb{N}_n) = \mathcal{S}(\mathbb{N}_n)$$

ونحصل من ثَمّ على الخاصة التالية :

(D_9) لتكن $\mathcal{S}(A)$ مجموعة التقابلات على مجموعة منتهية A عدد عناصرها $1 \leq n$. عندئذ $\operatorname{card}\big(\mathcal{S}(A)\big) = n!$.

4-3-3. مبدأ الاحتواء والاستثناء

لتكن A و B مجموعتين منتهيتين. لمّا كانت A هي اجتماع المجموعتين المنفصلتين $A\cap B$ و $A\backslash B$ استنتجنا أنّ :

$$\operatorname{card}(A) = \operatorname{card}(A\backslash B) + \operatorname{card}(A\cap B)$$

وكذلك

$$\operatorname{card}(B) = \operatorname{card}(B\backslash A) + \operatorname{card}(A\cap B)$$

ولكن $A\cap B$ و $A\backslash B$ و $B\backslash A$ تكوّن تجزئة للمجموعة $A\cup B$. إذن

$$\operatorname{card}(A\cup B) = \operatorname{card}(A\backslash B) + \operatorname{card}(A\cap B) + \operatorname{card}(B\backslash A)$$

ومنه

$$\operatorname{card}(A\cup B) = \operatorname{card}(A) + \operatorname{card}(B) - \operatorname{card}(A\cap B)$$

سنعمّم في المبرهنة التالية هذه العلاقة لحساب عدد عناصر اجتماع n مجموعة منتهية، نسمّي هذه العلاقة مبدأ الاحتواء والاستثناء.

مبرهنة : لتكن n عنصراً من $\mathbb{N}^*$. نرمز بالرمز $P_k^{(n)}$ إلى مجموعة أجزاء $\mathbb{N}_n$ التي عدد عناصر كلٍّ منها يساوي k. ولتكن $(A_k)_{1\le k\le n}$ جماعة من المجموعات المنتهية. عندئذ

$$\operatorname{card}\left(\bigcup_{k=1}^{n} A_k\right) = \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in P_k^{(n)}} \operatorname{card}\left(\bigcap_{i\in B} A_k\right)\right)$$

الإثبات

سنثبت هذا المبدأ بالتدريج على عدد المجموعات n. إنّ النتيجة واضحة حين يكون $n=1$، وقد أثبتنا صحتها عند $n=2$. لنفترض صحة العلاقة عند قيمة n. ولنتأمّل جماعة $(A_k)_{1\le k\le n+1}$ من المجموعات المنتهية. فإذا طبّقنا حالة $n=2$ على المجموعتين $A=A_{n+1}$ و $B=\bigcup_{k=1}^{n} A_k$ وجدنا

$$❶\quad \operatorname{card}\left(\bigcup_{k=1}^{n+1} A_k\right) = \operatorname{card}(A_{n+1}) + \underbrace{\operatorname{card}\left(\bigcup_{k=1}^{n} A_k\right)}_{\Delta_1} - \underbrace{\operatorname{card}\left(\bigcup_{k=1}^{n}(A_k\cap A_{n+1})\right)}_{\Delta_2}$$

وإذا استفدنا من فرْض التدريج لحساب Δ_2 وجدنا

$$\begin{aligned}
\Delta_2 &= \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in P_k^{(n)}} \operatorname{card}\left(\bigcap_{i\in B}(A_i\cap A_{n+1})\right)\right)\\
&= \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in P_k^{(n)}} \operatorname{card}\left(\bigcap_{i\in B\cup\{n+1\}} A_i\right)\right)\\
&= \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in A_{k+1}^{(n+1)}} \operatorname{card}\left(\bigcap_{i\in B} A_i\right)\right)
\end{aligned}$$

إذ كتبنا $A_{k+1}^{(n+1)}$ دلالة على مجموعة أجزاء $\mathbb{N}_{n+1}$ التي تحتوي على العنصر $n+1$، والتي عدد عناصر كل منها $k+1$. فإذا أجرينا تغييراً للدليل بوضع $k\mapsto(k+1)$ أصبح لدينا

$$\Delta_2 = -\sum_{k=2}^{n+1}(-1)^{k-1}\left(\sum_{B\in A_k^{(n+1)}} \operatorname{card}\left(\bigcap_{i\in B} A_i\right)\right)$$

أو

$$❷\quad \operatorname{card}(A_{n+1}) - \Delta_2 = \sum_{k=1}^{n+1}(-1)^{k-1}\left(\sum_{B\in A_k^{(n+1)}} \operatorname{card}\left(\bigcap_{i\in B} A_i\right)\right)$$

ومن ناحية أخرى، إذا كانت $B_k^{(n+1)}$ مجموعة أجزاء $\mathbb{N}_{n+1}$ التي لا تحتوي على العنصر $n+1$ والتي عدد عناصر كل منها k . فمن الواضح أنّ $B_k^{(n+1)} = P_k^{(n)}$ ومن ثَمّ فإن

$$\Delta_1 = \sum_{k=1}^{n} (-1)^{k-1} \left(\sum_{B \in B_k^{(n+1)}} \operatorname{card}\left(\bigcap_{i \in B} A_i \right) \right)$$

ولكن $\left\{ A_k^{(n+1)}, B_k^{(n+1)} \right\}$ تجزئة للمجموعة $P_k^{(n+1)}$ فإذا جمعنا العلاقة السابقة إلى العلاقة ❷ آخذين بعين الاعتبار العلاقة ❶ وجدنا

$$\operatorname{card}\left(\bigcup_{k=1}^{n+1} A_k \right) = \sum_{k=1}^{n+1} (-1)^{k-1} \left(\sum_{B \in P_k^{(n+1)}} \operatorname{card}\left(\bigcap_{i \in B} A_i \right) \right) \qquad \square$$

سنرى في التطبيق التالي مثالاً على استعمال العلاقة السابقة في حساب عدد التطبيقات الغامرة بين مجموعتين منتهيتين.

⑧ المجموعة $F_s(\mathbb{N}_n, \mathbb{N}_p)$

هي مجموعة التطبيقات الغامرة التي منطلقها $\mathbb{N}_n$ ومستقرها $\mathbb{N}_p$ مع p و n من $\mathbb{N}^*$. لنذكّر بأن الرمز $F(A,B)$ يمثل مجموعة التطبيقات من A إلى B .

لتكن k من $\mathbb{N}_p$ ، ولنرمز بالرمز A_k إلى مجموعة التطبيقات f من $F(\mathbb{N}_n, \mathbb{N}_p)$ التي تحقق $k \notin \operatorname{Im} f = f(\mathbb{N}_n)$. من الواضح عندئذ أنّ

$$F_s(\mathbb{N}_n, \mathbb{N}_p) = F(\mathbb{N}_n, \mathbb{N}_p) \backslash \left(\bigcup_{k=1}^{p} A_k \right)$$

سنستعمل مبدأ الاحتواء والاستثناء لحساب عدد عناصر $A_1 \cup A_2 \cup \cdots \cup A_p$. إذا كانت $U \subset \mathbb{N}_p$ رمزنا بالرمز A_U إلى مجموعة التطبيقات f من $F(\mathbb{N}_n, \mathbb{N}_p)$ التي تحقق الشرط $U \cap \operatorname{Im} f = \varnothing$ أو $\operatorname{Im} f \subset \mathbb{N}_p \backslash U$. من الواضح أنّ $A_k = A_{\{k\}}$ أياً كان k من $\mathbb{N}_p$ ، وأنّ $A_B = \bigcap_{i \in B} A_i$.

يتيح لنا ما سبق صياغة مبدأ الاحتواء والاستثناء كما يلي :

$$\operatorname{card}\left(\bigcup_{k=1}^{p} A_k \right) = \sum_{k=1}^{p} (-1)^{k-1} \left(\sum_{B \in P_k^{(p)}} \operatorname{card}(A_B) \right)$$

ولكن $F(\mathbb{N}_n, \mathbb{N}_p \setminus B) = A_B$ ، إذن لدينا $\text{card}(A_B) = (p - \text{card}(B))^n$ ، فالعلاقة السابقة تكافئ

$$\begin{aligned}\text{card}\left(\bigcup_{k=1}^{p} A_k\right) &= \sum_{k=1}^{p}(-1)^{k-1}\left(\sum_{B\in P_k^{(p)}}(p-\text{card}(B))^n\right)\\ &= \sum_{k=1}^{p}(-1)^{k-1}C_p^k(p-k)^n\end{aligned}$$

ومنه

$$\begin{aligned}\text{card}\left(F_s(\mathbb{N}_n,\mathbb{N}_p)\right) &= p^n + \sum_{k=1}^{p}(-1)^k C_p^k (p-k)^n\\ &= \sum_{k=0}^{p}(-1)^k C_p^k(p-k)^n\end{aligned}$$

نكون بذلك قد أثبتنا الخاصّة التالية :

(D_{10}) لتكن $F_s(\mathbb{N}_n, \mathbb{N}_p)$ مجموعة التطبيقات الغامرة التي منطلقها المجموعة $\mathbb{N}_n$ ومستقرها $\mathbb{N}_p$ مع $(n,p) \in \mathbb{N}^{*2}$. عندئذ

$$\text{card}\left(F_s(\mathbb{N}_n,\mathbb{N}_p)\right) = \sum_{k=0}^{p}(-1)^k C_p^k(p-k)^n$$

5. قوانين التشكيل والبنى الجبريّة

لتكن A و B و C ثلاث مجموعات. نسمّي **قانون تشكيل** معرف على $A \times B$ ويأخذ قيمه في C كلّ تطبيق f منطلقه $A \times B$ و مستقره C . لقد جرت العادة أن نكتب $z = x * y$ (أو $z = x \bullet y$ أو $z = x \oplus y$ ...)، عوضاً عن $z = f(x,y)$ ، عندما ينتمي (x,y,z) على $A \times B \times C$. و نقول إنّ z هو ناتج تشكيل x مع y وفق $*$.

إذا كان $A \neq B = C$ قلنا إنّ القانون $*$ **قانون تشكيل خارجي** على B مجموعة مؤثراته هي A . أمّا إذا كان $A = B = C$ فنقول إنّ القانون $*$ **قانون تشكيل داخلي** على A . ونكتب اختصاراً $(A, *)$.

لتكن $(A,*)$ و $(B,\bullet)$ مجموعتين مزودتين بقانوني تشكيل داخليين. وليكن التطبيق $f : A \to B$. نقول إنّ f **تشاكل** بين $(A,*)$ و $(B,\bullet)$، إذا وفقط إذا

$$\forall (x,y) \in A \times A, \quad f(x*y) = f(x) \bullet f(y)$$

وإذا كان f تقابلاً إضافةً إلى كونه تشاكلاً قلنا إنه **تشاكل تقابلي**. إنّ التابع العكسي لتشاكل تقابلي هو تشاكل أيضاً.

لتكن E مجموعة مزوّدة بقانون تشكيل داخليّ $*$.

- نقول إنّ $*$ **تجميعيّ** إذا وفقط إذا كان
$$\forall (x,y,z) \in E^3, x*(y*z) = (x*y)*z$$
- نقول إنّ العنصرين a و b من E **يتبادلان** إذا وفقط إذا كان $a*b = b*a$.
- نقول إنّ $*$ **تبديلي** إذا وفقط إذا كان $\forall (x,y) \in E^2, \quad x*y = y*x$.
- نقول إنّ العنصر e من E عنصرٌ **حيادي** بالنسبة إلى $*$ إذا وفقط إذا كان
$$\forall x \in E, \ \ x*e = e*x = x$$
وهو وحيد إن وُجِدَ.
- نقول إنّ العنصر x من E يقبل **نظيراً** (أو نظيراً من اليمين، أو نظيراً من اليسار على التوالي)، بالنسبة إلى القانون $*$ إذا وفقط إذا وُجِدَ في E عنصرٌ x' يُحقّق
$$x*x' = x'*x = e \ \ (\text{أو} \ \ x*x' = e \ \ \text{أو} \ \ x'*x = e \ \ \text{على التوالي})$$
- ليكن $*$ و $\perp$ قانوني تشكيل داخليين على E. نقول إنّ القانون $*$ **يقبل التوزيع من اليمين** (أو من اليسار) على $\perp$ إذا وفقط إذا كان
$$\forall (x,y,z) \in E^3, \quad x*(y\perp z) = (x*y)\perp(x*z)$$
$$(\text{أو} \ \ \forall (x,y,z) \in E^3, \quad (x\perp y)*z = (x*z)\perp(y*z))$$

ونقول إنّ القانون $*$ **يقبل التوزيع على** $\perp$ إذا وفقط إذا قَبِل التوزيع من اليمين ومن اليسار على $\perp$.

5-1. الزمر

الزمرة هي مجموعة مزوَّدة بقانون تشكيل داخلي تجميعي، ويقبل عنصراً حياديّاً، ويقبل فيها كل عنصر نظيراً.

- تكوّن البنى $(\mathbb{Z},+)$ و $(\mathbb{Q},+)$ و $(\mathbb{R},+)$ أمثلة تقليديّة على زمر، وكذلك $(\mathbb{Q}^*,\times)$ و $(\mathbb{R}^*,\times)$.
- هذه الزمر تبديليّة، أي إنّ قانونها تبديلي، ولكن ليست جميع الزمر كذلك؛ فزمرة التقابلات على مجموعةٍ تحوي أكثر من ثلاثة عناصر بالنسبة إلى قانون تركيب التطبيقات ليست تبديليّة.
- الزمر الجزئيّة هي مجموعة جزئيّة من زمرة، ينتمي إليها العنصر الحيادي، ومغلقة بالنسبة إلى قانون التشكيل، وينتمي إليها نظير كلِّ عنصرٍ منها.

إنّ إحدى الطرائق المتعارفة لإثبات أنّ مجموعةً، مزوّدة بقانون تشكيل داخلي معطى، هي زمرةٌ، تقضي بإثبات أنّها زمرة جزئيّة من زمرة معروفة.

5-2. الحلقات والحقول

الحلقة هي مجموعة مزوَّدة بقانوني تشكيل داخليَّين تجميعيَّن نسمِّيهما الجمع والضرب ونرمز إليهما عادة بالرمزين $+$ و $\cdot$، شرطَ أن تكون البنية $(A,+)$ زمرة تبديليّة، وأن تقبل البنية $(A,\cdot)$ عنصراً حياديّاً، ويكون الضرب توزيعيّاً على الجمع. نرمز عادة بالرمز 0 إلى حيادي الجمع وبالرمز 1 إلى حيادي الضرب ونفترض عموماً أنّ هذين العنصرين مختلفان.

- تكوّن البنى $(\mathbb{Z},+,\cdot)$ و $(\mathbb{Q},+,\cdot)$ و $(\mathbb{R},+,\cdot)$ أمثلة تقليديّة على حلقات وهي تبديليّة لأنّ الضرب تبديلي، ولكنّ هذا ليس صحيحاً عموماً.
- تبقى قواعد الحساب المتعارفة صحيحة في حلقة تبديليّة.

الحقل هو حلقة تبديليّة، لجميع عناصرها غير المعدومة نظير بالنسبة إلى قانون الضرب. وتكوّن مجموعةُ الأعداد العادية $\mathbb{Q}$، ومجموعة الأعداد الحقيقيّة $\mathbb{R}$، وكما سنرى، مجموعة الأعداد العقديّة $\mathbb{C}$، الأمثلة المعروفة على حقول.

⚠ **تحذير**. يجب التنبّه إلى أنّ الاقتضاء $xy=0 \Rightarrow (x=0)\vee(y=0)$ ليس صحيحاً في الحالة العامّة. فمثلاً في حالة حلقة التوابع من $\mathbb{R}$ إلى $\mathbb{R}$ يمكن أن يكون $fg=0$ دون أن يكون $f=0$ أو $g=0$. خذ مثلاً $f(x)=\max(0,x)$ و $g(x)=\min(x,0)$. ولكنّ الاقتضاء المشار إليه صحيح في مجموعات الأعداد المألوفة $\mathbb{N}$ أو $\mathbb{Z}$ أو $\mathbb{Q}$ أو $\mathbb{R}$ أو $\mathbb{C}$ لأنّها جميعاً أجزاء من الحقل $\mathbb{C}$، وهو صحيح في أيّ حقل.

3-5. الفضاءات الشعاعيّة

نسمّي **فضاء شعاعيّاً** على حقلٍ $\mathbb{K}$ كلَّ زمرة تبديليّة $(E,+)$ مزوّدة بقانون تشكيل خارجي $\mathbb{K}\times E\to E,(\alpha,x)\mapsto \alpha\cdot x$ يُحقّق الخواص الأربع التالية :

$$\alpha\cdot(\beta\cdot x)=(\alpha\beta)\cdot x \qquad (\alpha+\beta)\cdot x=\alpha\cdot x+\beta\cdot x$$

$$1\cdot x=x \qquad \alpha\cdot(x+y)=\alpha\cdot x+\alpha\cdot y$$

ونسمّي عناصر E أشعّة.

- هناك أمثلة متعارفة، على فضاءات شعاعيّة مثل $\mathbb{R}^2$ و $\mathbb{R}^3$ على الحقل $\mathbb{R}$ ، وبوجه عام $\mathbb{K}^n$ على الحقل $\mathbb{K}$. وكذلك فضاء التوابع المعرّفة على مجموعة A وتأخذ قيمها في حقل $\mathbb{K}$.
- نكتب عادة αx بدلاً من $\alpha\cdot x$ في حالة $\alpha\in\mathbb{K}$ و $x\in E$.
- نسمّي عبارة خطيّة لشعاعين x و y كلَّ شعاع من الشكل $\lambda x+\mu y$ مع (λ,μ) من $\mathbb{K}^2$. وعموماً، نسمّي عبارة خطّية بالأشعّة x_1 ، x_2 ، ... ، x_n كلَّ شعاع من الشكل $\lambda_1x_1+\lambda_2x_2+\cdots+\lambda_nx_n$ حيث $(\lambda_1,\lambda_2,\ldots,\lambda_n)\in\mathbb{K}^n$.
- الفضاء الشعاعي الجزئي من فضاء شعاعي E هو مجموعة جزئيّة من E ينتمي إليها 0، وتنتمي إليها كلُّ عبارة خطيّة من أشعّتها.
- إذا كان E و F فضاءَين شعاعيّين على حقل $\mathbb{K}$. نقول إنّ التطبيق $f:E\to F$ تطبيق خطّي إذا حقّق الشرط

$$\forall(x,y)\in E^2,\forall(\lambda,\mu)\in\mathbb{K}^2,\quad f(\lambda x+\mu y)=\lambda f(x)+\mu f(y)$$

ونتحدّث عن شكل خطّي في حالة $F=\mathbb{K}$.

تمرينات

التمرين 1. في مناجم ترانسلفانيا.

يعمل في مناجم ترانسلفانيا أربعة أنماطٍ من العمّال :

A البشر العقلاء.	C مصّاصو الدماء العقلاء.
B البشر المجانين.	D مصّاصو الدماء المجانين.

كلُّ ما يقوله إنسانٌ عاقلٌ صحيح، وكلُّ ما يقوله إنسانٌ مجنونٌ خطأ، وكلُّ ما يقوله مصّاص دماءٍ عاقلٌ خطأ، وكلُّ ما يقوله مصّاص دماءٍ مجنونٌ صحيح. نتعامل في الأسئلة التالية مع أزواجٍ، ونعلم أنّه في ترانسلفانيا الزواج المختلط بين إنسان ومصاص دماء محظور.

❶ السيِّد فتحي وزوجه فتحيّة جنبلباب

فتحيّة : زوجي إنسان.

فتحي : زوجي مصّاصة دماء.

فتحيّة : أحدنا مجنونٌ والآخر عاقل.

أَيكون السيّد والسيدة جنبلباب مصّاصي دماء ؟

❷ السيِّد رمزي وزوجه رمزيّة حمرالكريات

أكّدت لي السيّدة رمزيّة حمرالكريات أنّ كلَّ ما يقوله زوجها صحيح، وقال لي زوجها إنها مجنونة. ماذا تستنتج ؟

❸ السيِّد صبحي وزوجه صبحيّة عتم الليل

صبحي : نحن الاثنان مصّاصا دماء.

صبحيّة : نحن الاثنان نتمتّع بالصحّة العقليّة نفسها.

فما هما ؟

❹ السيِّد ناطر وزوجه ناطرة بنصف الطريق

ناطر : أحدنا على الأقلّ مجنون.

ناطرة : هذا خطأ.

فما هما ؟

الحل

❶ لنتبع أسلوب نقض الفرْض. لنفترض أنّ عائلة جنبلباب مكوّنة من مصّاصي دماء. عندئذ يقتضي ذلك أنّ قول فتحيّة «زوجي إنسان» خطأ، فهي إذن مصّاصة دماء عاقلة.

وكذلك يقتضي الفرْض نفسه أنّ قول فتحي «زوجي مصّاصة دماء» صحيح، فهو إذن مصّاص دماء مجنون.

ولكنّ هذه النتيجة تعني أنّ المقولة الثانية لفتحيّة «أحدنا مجنونٌ والآخر عاقل» صحيحة، وهذا يناقض كونها مصّاصة دماء عاقلة، وكلُّ ما تقوله خطأ. نستنتج أنّ الافتراض «عائلة جنبلباب مكوّنة من مصّاصي دماء» افتراض خطأ ومن ثَمّ يكون فتحي إنساناً مجنوناً وفتحيّة امرأة عاقلة.

❷ لنرمز بالرمز h إلى الزوج رمزي وبالرمز w إلى زوجه رمزيّة. ولنناقش الحالات التالية :

1. حالة $w \in A$. إذن فتحيّة إنسان فزوجها إنسان أيضاً، ولأنّ كلّ ما تقوله صحيح فإنّ زوجها إنسانٌ عاقلٌ أي $h \in A$. وهذه النتيجة تقتضي أن تكون زوجه مجنونة لأنّ كلّ ما يقوله صحيح أي إنّ $w \in B$ وهذا يناقض ما افترضناه بداية. إذن $w \notin A$.
2. حالة $w \in B$. إذن فتحيّة إنسان فزوجها إنسان أيضاً، ولأنّ كلّ ما تقوله خطأ فإنّ زوجها إنسانٌ مجنون أي $h \in B$. ولكنّ هذه النتيجة تقتضي أن تكون زوجه عاقلة لأنّ كلّ ما يقوله خطأ أي إنّ $w \in A$ وهذا يناقض ما افترضناه بداية. إذن $w \notin B$.
3. حالة $w \in C$. إذن فتحيّة مصّاصة دماء فزوجها مصّاص دماء أيضاً، ولأنّ كلّ ما تقوله خطأ فإنّ زوجها مصّاص دماء عاقل أي $h \in C$. وهذا لا يناقض كون ما قاله خطأ.
4. حالة $w \in D$. إذن فتحيّة مصّاصة دماء فزوجها مصّاص دماء أيضاً، ولأنّ كلّ ما تقوله صحيح كان زوجها مصّاص دماء مجنون أيضاً، وهذا لا يناقض كون ما قاله صحيحاً.

وهكذا نستنتج أنّ عائلة حمر الكريّات مكوّنة من مصّاصَي دماءٍ يتمتّعان بالصحّة العقليّة نفسها.

❸ لنرمز بالرمز h إلى الزوج صبحي وبالرمز w إلى زوجه صبحيّة. ولنناقش الحالات التالية:

1. حالة $h \in A$. إذن صبحي إنسان عاقل، وهذا يناقض وصفه لنفسه بأنّه مصّاص دماء، لأنّ كلّ ما يقوله يجب أن يكون صحيحاً. وعليه فإنّ $h \notin A$.

2. حالة $h \in C$. إذن صبحي مصّاص دماء عاقل، وكلُّ ما يقوله خطأ، فأحدُ الزوجين إنسانٌ، ولمّا كان من الواجب أن يكون للزوجين الطبيعة نفسها، فإنّ هذا يناقض الفرْض. إذن يجب أن يكون $h \notin C$.
3. حالة $h \in B$. إذن صبحي إنسانٌ مجنون، ولمّا كان من الواجب أن يكون للزوجين الطبيعة نفسها استنتجنا أنّ صبحيّة إنسانة، ولكن :
   - إذا كان $w \in A$ وجب أن يكون ما تقوله صبحيّة صحيحاً، فهي إذن مجنونة وهذا خُلفٌ.
   - وإذا كان $w \in B$ وجب أن يكون ما تقوله صبحيّة خطأ، فهي إذن عاقلة وهذا خُلفٌ أيضاً.

   نستنتج من هذا التناقض أنّ $h \notin B$.
4. وهكذا لا بُدّ أن يكون $h \in D$ أي إنّ صبحي مصّاص دماء مجنونٌ، ولمّا كان من الواجب أن يكون للزوجين الطبيعة نفسها، استنتجنا أنّ صبحيّة مصّاصة دماء، ولكن
   - إذا كان $w \in C$ وجب أن يكون ما تقوله صبحيّة خطأ، فهي إذن عاقلة ولا تناقضَ في ذلك.
   - وإذا كان $w \in D$ وجب أن يكون ما تقوله صبحيّة صحيحاً، فهي إذن مجنونة ولا تناقضَ في ذلك أيضاً.

وهكذا نستنتج أنّ الزوج في عائلة عتم الليل مصّاص دماءٍ مجنون والزوجة مصّاصة دماء.

❹ إنّ ما تقوله ناطرة هو تماماً نفي ما يدّعيه ناطر، فلا بُدّ أنّ يكون قول أحدهما خطأً وقول الآخر صحيحاً. ولكن أن يكون ما تقوله ناطرة صحيحاً يعني أنّ كليهما عاقلان، ولأنّها عاقلة وتقول شيئاً صحيحاً استنتجنا أنّها إنسانة عاقلة وزوجها إنسان عاقلٌ وهذا يناقض كون قول أحدهما خطأ.
نستنتج إذن أنّ ما يقوله ناطر صحيح وأنّ ما تقوله ناطرة خطأ. وهذا يؤدّي بعائلة "بنصف الطريق" إلى أحد الوضعين التاليين :

- ناطر إنسان عاقل وناطرة إنسانة مجنونة.
- ناطرمصاص دماء مجنون وناطرة مصاصة دماء عاقلة. ■

التمرين 2. على جزيرة الحكمة.

ينقسم سكّان هذه الجزيرة المئة إلى فئتين، الحكماء والمجانين. إذا علمتَ ما يلي:

- يقطن هذه الجزيرة حكيمٌ واحدٌ على الأقلّ.
- هناك على الأقل مجنونٌ واحدٌ بين كلّ اثنين من سكّان الجزيرة.

فكم حكيماً وكم مجنوناً على هذه الجزيرة ؟

الحل

في الجزيرة تسعة وتسعون مجنوناً وحكيمٌ واحدٌ لا يُحسد على حاله. لنفترض أنّ عدد الحكماء يزيد تماماً على الواحد، عندئذ يمكننا أن نختار زوجاً من الحكماء، وعندئذ لا يكون بينهما مجنونٌ وهذا يناقض المقولة الثانية. إذن يجب أن يكون عدد الحكماء أقلّ أو يساوي الواحد وهو ليس صفراً عملاً بالمقولة الأولى. إذن عدد الحكماء في الجزيرة يساوي الواحد وهي النتيجة المرجوّة. ■

التمرين 3. تأمّل القضايا الأربع التالية :

❶ $\exists x \in \mathbb{R}, \forall y \in \mathbb{R},\ x+y>0$ ❷ $\forall x \in \mathbb{R}, \exists y \in \mathbb{R},\ x+y>0$

❸ $\forall x \in \mathbb{R}, \forall y \in \mathbb{R},\ x+y>0$ ❹ $\exists x \in \mathbb{R}, \forall y \in \mathbb{R},\ y^2>x$

بيِّن أيُّ القضايا ❹, ❸, ❷, ❶ صحيح وأيّها خطأ ؟ ثُمّ أعطِ نفي كلٍّ منها.

الحل

القضيّة	قيمتها	التعليل
❶	خطأ	خذ $y=-x-1$
❷	صح	خذ $y=-x+1$
❸	خطأ	خذ $y=x=-1$
❹	صح	خذ $x=-1$

ونجد مباشرة أنّ

$\neg$❶ $\forall x \in \mathbb{R}, \exists y \in \mathbb{R},\ x+y\leq 0$ $\neg$❷ $\exists x \in \mathbb{R}, \forall y \in \mathbb{R},\ x+y\leq 0$

$\neg$❸ $\exists x \in \mathbb{R}, \exists y \in \mathbb{R},\ x+y\leq 0$ $\neg$❹ $\forall x \in \mathbb{R}, \exists y \in \mathbb{R},\ y^2\leq x$

وهي النتيجة المرجوّة. ■

التمرين 4. املأ فيما يلي الفراغات بالرمز المناسب من بين $\Rightarrow$ أو $\Leftarrow$ أو $\Leftrightarrow$.

❶ $\big(\forall x\in E, p(x)\wedge q(x)\big)\quad\cdots\cdots\quad\big(\forall x\in E, p(x)\big)\wedge\big(\forall x\in E, q(x)\big)$

❷ $\big(\exists x\in E, p(x)\wedge q(x)\big)\quad\cdots\cdots\quad\big(\exists x\in E, p(x)\big)\vee\big(\exists x\in E, q(x)\big)$

❸ $\big(\forall x\in E, p(x)\vee q(x)\big)\quad\cdots\cdots\quad\big(\forall x\in E, p(x)\big)\vee\big(\forall x\in E, q(x)\big)$

❹ $\big(\exists x\in E, p(x)\vee q(x)\big)\quad\cdots\cdots\quad\big(\exists x\in E, p(x)\big)\vee\big(\exists x\in E, q(x)\big)$

الحل

❶	❷	❸	❹
$\Leftrightarrow$	$\Rightarrow$	$\Leftarrow$	$\Leftrightarrow$

ونترك التعليل للقارئ. ■

التمرين 5. لتكن E و F و G ثلاث مجموعات غير خالية، وليكن التطبيقان $f:E\to F$ و $g:F\to G$. أثبت أنّه إذا كان التطبيق $g\circ f$ متبايناً، كان f متبايناً. وإذا كان التطبيق $g\circ f$ غامراً، كان g غامراً.

الحل

- لنفترض أنّ $g\circ f$ متباينٌ. وليكن x_1 و x_2 عنصرين من E يُحقّقان $f(x_1)=f(x_2)$ ، عندئذ يكون لدينا $g(f(x_1))=g(f(x_2))$ أو
$$g\circ f(x_1)=g\circ f(x_2)$$
ولأنّ $g\circ f$ متباينٌ نستنتج أنّ $x_1=x_2$. وهذا يُثبتُ أنّ f متباينٌ.
- لنفترض أنّ $g\circ f$ غامرٌ. وليكن y عنصراً من G ، عندئذ نستنتج من كون $g\circ f$ غامراً أنّه يوجد، في E ، عنصرٌ a يُحقّق $g\circ f(a)=y$. ومن ثَمّ يوجد، في F ، عنصرٌ $x=f(a)$ يُحقّق $y=g(x)$. وهذا يبرهن أنّ التطبيق g غامرٌ. ■

التمرين 6. لتكن E مجموعة غير خالية، وليكن $f:E\to E$ تطبيقاً يُحقّق
$$f\circ f\circ f=f$$
أثبت أنّه إذا كان f متبايناً أو غامراً، كان f تقابلاً.

الحل

- لنفترض أنّ f متباينٌ. وليكن x عنصراً من E عندئذ يكون لدينا
$$f\big(f\circ f(x)\big)=f(x)$$
ولأنّ f متباينٌ، استنتجنا أنّ $f\circ f(x)=x$. هذا محقّق أياًكان x من E ، إذن
$$f\circ f=I_E$$
ولأنّ $f\circ f$ غامرٌ، استنتجنا بناءً على نتيجة التمرين السابق أنّ f غامرٌ، ومن ثَمّ أنّ f تقابلٌ.

- لنفترض أنّ f غامرٌ. وليكن x عنصراً ما من E ، عندئذ نستنتج من كون f غامراً أنّه يوجد، في E ، عنصرٌ a يُحقِّق $f(a)=x$. ومن ثَمّ
$$f\circ f(x)=f\circ f\big(f(a)\big)=f\circ f\circ f(a)=f(a)=x$$
هذا محقّق أياًكان x من E ، إذن $f\circ f=I_E$. ولأنّ $f\circ f$ متباينٌ، استنتجنا بناءً على نتيجة التمرين السابق أنّ f متباينٌ، ومن ثَمّ أنّ f تقابلٌ. ∎

التمرين 7. لتكن E مجموعة غير خالية، وليكن $f:E\to E$ تطبيقاً يُحقّق
$$f\circ f=f$$
أثبت أنّه إذاكان f متبايناً أو غامراً، كان f هو التطبيق المطابق على E .

الحل

- لنفترض أنّ f متباينٌ. وليكن x عنصراً من E عندئذ يكون لدينا $f(f(x))=f(x)$ ، ولأنّ f متباينٌ، استنتجنا أنّ $f(x)=x$. هذا محقّق أيّاً كان x من E ، إذن $f=I_E$.

- لنفترض أنّ f غامرٌ. وليكن x عنصراً ما من E ، عندئذ نستنتج من كون f غامراً أنّه يوجد، في E ، عنصرٌ a يُحقِّق $f(a)=x$. ومن ثَمّ
$$f(x)=f(f(a))=f\circ f(a)=f(a)=x$$
وهذا محقّق أياًكان x من E ، إذن $f=I_E$. ∎

التمرين 8. لتكن E و F و G مجموعات غير خالية، ولتكن التطبيقات $f : E \to F$ و $g : F \to G$ و $h : G \to E$. أثبت أنّه إذا كان $h \circ g \circ f$ و $g \circ f \circ h$ متباينين وكان $g \circ h \circ f$ غامراً، كان كلٌّ من التطبيقات f و g و h تقابلاً.

الحل

سنستفيد من نتيجة التمرين 5.

① التطبيق $f \circ g \circ h$ متباينٌ إذن f متباينٌ، والتطبيق $g \circ h \circ f$ غامرٌ إذن f غامرٌ. وعليه يكون التطبيق f تقابلاً.

② التطبيق $(h \circ f) \circ g$ متباينٌ إذن $h \circ f$ متباينٌ، والتطبيق $g \circ (h \circ f)$ غامرٌ إذن $h \circ f$ غامرٌ. وعليه يكون التطبيق $h \circ f$ تقابلاً. ولأنّ f تقابلٌ استنتجنا أنّ h تقابلٌ أيضاً.

③ لمّا كان $g = (g \circ f \circ h) \circ (f \circ h)^{-1}$ استنتجنا أنّ g متباينٌ لأنّه تركيب تطبيقين متباينين، ولمّا كان $g = (f \circ h)^{-1} \circ (f \circ h \circ g)$ استنتجنا أنّ g غامرٌ لأنّه تركيب تطبيقين غامرين. إذن g تقابلٌ، ويتم الإثبات. ■

التمرين 9. لتكن E و F مجموعتين غير خاليتين، وليكن التطبيق $f : E \to F$.

1. أثبت أنّه أيّاً كانت المجموعتان الجزئيّتان غير الخاليتين A و B من E، فلدينا :

① $A \subset B \Rightarrow f(A) \subset f(B)$

② $f(A \cup B) = f(A) \cup f(B)$ و $f(A \cap B) \subset f(A) \cap f(B)$.

2. أثبت تكافؤ القضايا التّالية:

❶ التابع f متباين.

❷ أيّاً كانت المجموعتان الجزئيّتان غير الخاليتين A و B من E، فلدينا

$$f(A \cap B) = f(A) \cap f(B)$$

❸ أيّاً كانت المجموعة الجزئيّة غير الخالية A من E، فلدينا $f(E \backslash A) \subset F \backslash f(A)$.

الحل

1.① ليكن a' عنصراً من $f(A)$ عندئذ يوجد عنصرٌ a من A يُحقّق $f(a) = a'$، ولأنّ $A \subset B$ استنتجنا أنّ $a \in B$ ومن ثمّ $f(a) \in f(B)$ أي $a' \in f(B)$. ونكون قد أثبتنا أنّ $f(A) \subset f(B)$.

②.1 من جهة أولى لدينا $A \cap B \subset A \subset A \cup B$ و $A \cap B \subset B \subset A \cup B$ فإذا استفدنا من نتيجة السؤال السابق استنتجنا أنّ

$$f(A \cap B) \subset f(A) \cap f(B) \quad \text{و} \quad f(B) \cup f(A) \subset f(A \cup B)$$

بقي أن نثبت أنّ $f(A \cup B) \subset f(B) \cup f(A)$.

ليكن إذن y عنصراً من $f(A \cup B)$ عندئذ يوجد عنصرٌ x من $A \cup B$ يُحقّق $f(x) = y$.

- فإذا كان $x \in A$ كان $f(x) \in f(A) \subset f(B) \cup f(A)$ ، أي $y \in f(B) \cup f(A)$.
- وإذا كان $x \in B$ كان $f(x) \in f(B) \subset f(B) \cup f(A)$ ، واستنتجنا من جديد أنّ $y \in f(B) \cup f(A)$. بذلك نكون قد أثبتنا أنّ $f(A \cup B) \subset f(B) \cup f(A)$.

.2 ❶⇐❷ لتكن A و B مجموعتين جزئيّتين غير خاليتين من E ، ولنفترض أنّ f متباينٌ.

- لقد أثبتنا سابقاً أنّ الاحتواء $f(A \cap B) \subset f(A) \cap f(B)$ صحيح دون شروط.
- ليكن إذن y عنصراً من $f(A) \cap f(B)$ عندئذ يوجد عنصرٌ a من A يُحقّق $f(a) = y$ ، ويوجد عنصرٌ b من B يُحقّق $f(b) = y$ أيضاً.

لمّا كان f متبايناً استنتجنا من المساواة $f(a) = f(b)$ أنّ $a = b$ فالعنصر a ينتمي إلى B أيضاً، لأنّه يساوي b!، وهكذا نستنتج أنّه يوجد عنصرٌ a في $A \cap B$ يُحقّق $f(a) = y$ ، وعليه $y \in f(A \cap B)$. فنكون قد أثبتنا صحّة الاحتواء الآخر :

$$f(A) \cap f(B) \subset f(A \cap B) .$$

إذن الخاصّة ❷ صحيحة.

❷⇐❸ لتكن A مجموعة جزئيّة غير خالية من E .

- فإذا كانت $A = E$ كان $E \backslash A = \varnothing$ ، ومن ثَمّ كان الاحتواء $f(E \backslash A) \subset F \backslash f(A)$ محقّقاً وضوحاً.
- وإذا كان $E \backslash A \neq \varnothing$ أمكننا تطبيق الخاصّة ❷ على المجموعتين A و $E \backslash A$ ، فنجد

$$f(E \backslash A) \cap f(A) = f(A \cap (E \backslash A)) = f(\varnothing) = \varnothing$$

وهذا يعني أنّ $f(E \backslash A) \subset F \backslash f(A)$. ومنه الخاصّة ❸ .

❸⇐❶ . ليكن a و b عنصرين من E ، ولنفترض أنّ $a \neq b$. عندئذ يكون $b \in E \backslash \{a\}$ ، واستناداً إلى ❸ يكون $f(b) \in F \backslash \{f(a)\}$ أي $f(b) \neq f(a)$. والتابع f متباينٌ. ■

التمرين 10. لتكن E و F مجموعتين غير خاليتين، وليكن التطبيق $f : E \to F$.

1. أثبت أنّه أيّاً كانت المجموعتان الجزئيّتان غير الخاليتين A و B من F، فلدينا :

① $A \subset B \Rightarrow f^{-1}(A) \subset f^{-1}(B)$.

② $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$،

و $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

③ $f^{-1}(F \backslash A) = E \backslash f^{-1}(A)$،

و $f^{-1}(A \backslash B) = f^{-1}(A) \backslash f^{-1}(B)$.

2. ① أياً كانت المجموعة الجزئيّة غير الخالية A من E، فلدينا : $A \subset f^{-1}(f(A))$.

② أثبت أنّ التطبيق f متباينٌ إذا وفقط إذا

$$\forall A \subset E, \quad A \neq \varnothing \Rightarrow A = f^{-1}(f(A))$$

3. ① أياً كانت المجموعة الجزئيّة غير الخالية A من F، فلدينا : $f(f^{-1}(A)) \subset A$.

② أثبت أنّ التطبيق f غامر إذا وفقط إذا تحقّق الشّرط :

$$\forall A \subset F, \quad A \neq \varnothing \Rightarrow A = f(f^{-1}(A))$$

الحل

1.① في الحقيقة،

$$\left(x \in f^{-1}(A)\right) \Leftrightarrow \left(f(x) \in A\right) \overset{A \subset B}{\Rightarrow} \left(f(x) \in B\right) \Leftrightarrow \left(x \in f^{-1}(B)\right)$$

وهذا يبرهن صحّة الاقتضاء $A \subset B \Rightarrow f^{-1}(A) \subset f^{-1}(B)$.

1.② في الحقيقة، لدينا

$$\begin{aligned}\left(x \in f^{-1}(A \cap B)\right) &\Leftrightarrow \left(f(x) \in A \cap B\right)\\ &\Leftrightarrow \left(f(x) \in A\right) \wedge \left(f(x) \in B\right)\\ &\Leftrightarrow \left(x \in f^{-1}(A)\right) \wedge \left(x \in f^{-1}(B)\right)\\ &\Leftrightarrow \left(x \in f^{-1}(A) \cap f^{-1}(B)\right)\end{aligned}$$

إذن

$$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$$

وكذلك

$$\begin{aligned}\left(x \in f^{-1}(A \cup B)\right) &\Leftrightarrow \left(f(x) \in A \cup B\right)\\ &\Leftrightarrow \left(f(x) \in A\right) \vee \left(f(x) \in B\right)\\ &\Leftrightarrow \left(x \in f^{-1}(A)\right) \vee \left(x \in f^{-1}(B)\right)\\ &\Leftrightarrow \left(x \in f^{-1}(A) \cup f^{-1}(A)\right)\end{aligned}$$

إذن

$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$$

③.1 في الحقيقة، لدينا

$$\begin{aligned}\left(x \in f^{-1}(F\backslash A)\right) &\Leftrightarrow \left(f(x) \in F\backslash A\right) \Leftrightarrow \left(f(x) \notin A\right)\\ &\Leftrightarrow \left(x \notin f^{-1}(A)\right) \Leftrightarrow \left(x \in E\backslash f^{-1}(A)\right)\end{aligned}$$

إذن $f^{-1}(F\backslash A) = E\backslash f^{-1}(A)$.

ومن جهة ثانية

$$\begin{aligned}f^{-1}(A\backslash B) &= f^{-1}\left(A \cap (F\backslash B)\right) &&= f^{-1}(A) \cap f^{-1}(F\backslash B)\\ &= f^{-1}(A) \cap \left(E\backslash f^{-1}(B)\right) &&= f^{-1}(A)\backslash f^{-1}(B)\end{aligned}$$

①.2 لتكن A مجموعة جزئيّة غير خالية من E عندئذ

$$x \in A \Rightarrow f(x) \in f(A) \Rightarrow x \in f^{-1}(f(A))$$

وعليه فإنّ $A \subset f^{-1}(f(A))$.

②.2 **الاقتضاء الأوّل**. لنفترض أنّ f متباينٌ ولنبرهن صحّة الشرط $\left(\mathcal{I}\right)$ التالي

$$\forall A \subset E, \quad A \neq \varnothing \Rightarrow A = f^{-1}(f(A))$$

لتكن A مجموعة جزئيّة غير خالية من E . وليكن x عنصراً من $f^{-1}(f(A))$ عندئذ يكون $f(x)$ عنصراً من $f(A)$ فيوجد a في A يُحقّق $f(x) = f(a)$ ، ولكنّ f متباينٌ، إذن $x = a$ ، وعليه فإنّ $x \in A$. وهكذا نكون قد أثبتنا أنّ $f^{-1}(f(A)) \subset A$ ، وهذا يبرهن $\left(\mathcal{I}\right)$ إذا استفدنا من نتيجة السؤال ①.2 .

الاقتضاء الثاني. لنفترض صحّة الشرط $\left(\mathcal{I}\right)$ ولنبرهن أنّ f متباينٌ.

ليكن x_1 و x_2 عنصرين من E . ولنفترض أنّ $f(x_1) = f(x_2)$ ، عندئذ يكون

$$x_2 \in f^{-1}\left(f(\{x_1\}\right) \overset{(\mathcal{I})}{=} \{x_1\}$$

وهذا يعني أنّ $x_2 = x_1$ ، ومن ثَمّ يكون التابع f متبايناً.

①.3 لتكن A مجموعة جزئيّة غير خالية من F عندئذ

$$\begin{aligned}\left(y \in f(f^{-1}(A))\right) &\Rightarrow \left(\exists x \in f^{-1}(A),\ f(x) = y\right)\\ &\Rightarrow \left(\exists x \in E,\ \left(f(x) \in A\right) \wedge \left(f(x) = y\right)\right)\\ &\Rightarrow \left(y \in A\right)\end{aligned}$$

وعليه فإنّ $f(f^{-1}(A)) \subset A$.

②.3 **الاقتضاء الأوّل**. لنفترض أنّ f غامرٌ ولنبرهن صحّة الشرط $\left(\mathcal{S}\right)$ التالي

$$\forall A \subset F, \quad A \neq \varnothing \Rightarrow A = f(f^{-1}(A))$$

لتكن A مجموعة جزئيّة غير خالية من F . وليكن y عنصراً من A عندئذ يوجد عنصرٌ x من E يُحقّق $f(x) = y$ ونستنتج من كون $f(x) \in A$ أنّ $x \in f^{-1}(A)$، وعليه يكون $f(x) \in f(f^{-1}(A))$، أو $y \in f(f^{-1}(A))$. وهكذا نكون قد أثبتنا صحة الاحتواء $A \subset f(f^{-1}(A))$ ، وهذا يبرهن $\left(\mathcal{S}\right)$ إذا استفدنا من نتيجة السؤال ①.3 .

الاقتضاء الثاني. لنفترض صحّة الشرط $\left(\mathcal{S}\right)$ ولنبرهن أنّ f غامرٌ.

ليكن y عنصراً من F . لمّا كان $\{y\} = f(f^{-1}(\{y\}))$ استنتجنا أنّه يوجد x في $f^{-1}(\{y\})$ يُحقّق $f(x) = y$. وهذا يبرهن أنّ التطبيق f غامرٌ. ■

التمرين 11. يهدف التمرين إلى إثبات مبرهنة Bernstein الآتية:

إذا وُجِدَ تطبيقان متباينان $f : E \to F$ و $g : F \to E$ بين مجموعتين غير خاليتين E و F ، كان هناك تقابل بين E و F .

لتكن إذن E و F مجموعتين غير خاليتين، وليكن $f : E \to F$ و $g : F \to E$ تطبيقين متباينين، ولنعرّف $h = g \circ f$ والمجموعات

$$R = E \backslash g(F)$$

$$\mathcal{H} = \{M \subset E, R \cup h(M) \subset M\}$$

$$A = \bigcap_{M \in \mathcal{H}} M$$

1. تحقّق أنّ $E \in \mathcal{H}$ و $A \in \mathcal{H}$. ثُمّ أثبت أنّ : $\forall M \in \mathcal{H}, R \cup h(M) \in \mathcal{H}$.

2. ليكن $B = E \backslash A$ و $A' = f(A)$ و $B' = g^{-1}(B)$.

① تحقّق أنّ $R \cup h(A) = A$، وأنّ $B' = F \backslash A'$.

② ليكن التطبيقان $f' : A \to A'$ و $g' : B' \to B$ مقصورَي التطبيقين f و g بالترتيب. أثبت أنّ كلّاً من f' و g' تقابل، وأنّ التطبيق

$$\varphi : E \to F,\ x \mapsto \begin{cases} f'(x) & : x \in A \\ g'^{-1}(x) & : x \in B \end{cases}$$

تقابلٌ. ثُمّ استنتج المطلوب.

الحل

1. لمّا كان $h(E) \subset E$ و $R \subset E$ استنتجنا أنّ $E \in \mathcal{H}$. ولمّا كانت المجموعة R محتواة في جميع المجموعات M من $\mathcal{H}$ استنتجنا أنّ $R \subset A$، وكذلك لمّا كان

$$\forall M \in \mathcal{H}, \quad h(A) \subset h(M) \subset M$$

استنتجنا أنّ أنّ $h(A) \subset A$، ومن ثَمّ $R \cup h(A) \subset A$ أي $A \in \mathcal{H}$.

لتكن M مجموعة من $\mathcal{H}$. ولنعرّف $\widetilde{M} = R \cup h(M)$. عندئذ من الواضح أنّ $R \subset \widetilde{M}$. ولأنّ M تنتمي إلى $\mathcal{H}$ استنتجنا أنّ $\widetilde{M} \subset M$، ومنه $h(\widetilde{M}) \subset h(M) \subset \widetilde{M}$. وبالنتيجة $R \cup h(\widetilde{M}) \subset \widetilde{M}$، إذن $\widetilde{M} \in \mathcal{H}$. وهكذا نكون قد أثبتنا أنّ:

$$\forall M \in \mathcal{H}, \quad R \cup h(M) \in \mathcal{H}.$$

2.① لمّا كان $A \in \mathcal{H}$ استنتجنا أنّ $R \cup h(A) \subset A$، ومن جهة أخرى فإنّ $R \cup h(A) \in \mathcal{H}$ إذن $A \subset R \cup h(A)$ لأنّ A محتواة تعريفاً في جميع المجموعات M من $\mathcal{H}$. إذن $R \cup h(A) = A$.

ومن جهة ثانية، لنلاحظ أنّ

$$B' = g^{-1}(B) = g^{-1}(E\backslash A) = F\backslash g^{-1}(A)$$

ولكن

$$\begin{aligned}
\big(x \in g^{-1}(A)\big) &\Leftrightarrow \big(g(x) \in A\big) \\
&\Leftrightarrow \big(g(x) \in R \cup h(A)\big) && R \cup h(A) = A \\
&\Leftrightarrow \big(g(x) \in h\big(A\big)\big) && R = E\backslash g(F) \\
&\Leftrightarrow \big(\exists a \in A, g(x) = h(a)\big) \\
&\Leftrightarrow \big(\exists a \in A, g(x) = g(f(a))\big) && h = g \circ f \\
&\Leftrightarrow \big(\exists a \in A, x = f(a)\big) && g : E \hookrightarrow F \\
&\Leftrightarrow \big(x \in f(A)\big) \\
&\Leftrightarrow \big(x \in A'\big) && A' = f(A)
\end{aligned}$$

أي g متباين

وعليه $A' = g^{-1}(A)$ و $B' = F\backslash A'$.

②.2 في الحقيقة، نعلم أنّ التطبيق f متباينٌ، إذن التطبيق f' متباينٌ أيضاً. ولأنّ $A' = f(A) = f'(A)$ استنتجنا أنّ التطبيق f' غامرٌ. وعليه نرى أنّ التطبيق f' تقابل.

- ونجد وضوحاً أنّ التطبيق g' تطبيقٌ متباينٌ من B' إلى B. بقي أن نتوثّق أنّ g' غامرٌ. ولكن نعلم أنّ المجموعة R التي تساوي $E\backslash g(F)$ محتواة في A إذن يجب أن تحوي متمّمتُها $g(F)$ متمّمةَ A أي B. ومنه $B \subset g(F)$. فإذا كان y عنصراً من B وُجِدَ عنصرٌ x في F يُحقّق $g(x) = y$. ولأنّ $y \in B$ استنتجنا أنّ $x \in g^{-1}(B) = B'$، ومنه $g'(x) = y$. فالتطبيق g' غامرٌ. وهكذا نرى أنّ التطبيق g' تقابل أيضاً.

- من الواضح أنّ $\varphi(A) = A'$ و $\varphi(B) = B'$ ولأنّ $E = A \cup B$ استنتجنا أنّ

$$\varphi(E) = \varphi(A \cup B) = \varphi(A) \cup \varphi(B) = A' \cup B' = F$$

فالتطبيق φ غامرٌ.

ليكن x و y عنصرين من E يُحقّقان $x \neq y$. ولنناقش الحالات التالية :

- $x \in A$ و $y \in B$. عندئذ $\varphi(x) \in A'$ و $\varphi(y) \in B'$، ومن ثَمّ $\varphi(x) \neq \varphi(y)$.
- $x \in B$ و $y \in A$. عندئذ $\varphi(x) \in B'$ و $\varphi(y) \in A'$ ومن ثَمّ $\varphi(x) \neq \varphi(y)$.
- $x \in A$ و $y \in A$. هنا التابع f' متباينٌ إذن $f'(x) \neq f'(y)$ ومنه $\varphi(x) \neq \varphi(y)$.
- $x \in B$ و $y \in B$. هنا التابع g'^{-1} متباينٌ إذن $g'^{-1}(x) \neq g'^{-1}(y)$ وهذا أيضاً يثبتُ أنّ

$$\varphi(x) \neq \varphi(y).$$

إذن التطبيق φ متباينٌ. ونكون بذلك قد أوجدنا تقابلاً هو φ بين E و F وأنجزنا البرهان. ■

التمرين 12. نقول إنّ المجموعة A **قابلة للعدّ** إذا وُجِدَ تقابلٌ منها إلى مجموعة الأعداد الطبيعية $\mathbb{N}$.

1. أثبت أنّ كلَّ مجموعة جزئيّة من $\mathbb{N}$ تكون منتهيةً أو قابلة للعدّ. واستنتج أنّه إذا كانت B مجموعة قابلة للعدّ و A مجموعة جزئيّة من B، كانت A منتهية أو قابلة للعدّ.
2. أثبت أنّ التطبيق
$$f : \mathbb{N}\times\mathbb{N} \to \mathbb{N}, (n,m) \mapsto 2^n(2m+1)-1$$
تقابل، واستنتج أنّ المجموعة $\mathbb{N}\times\mathbb{N}$ قابلة للعدّ.
3. أثبت أنّ اجتماعَ جماعة منتهية أو قابلة للعدِّ من مجموعات قابلة للعدّ مجموعةٌ قابلة للعدّ.
4. استنتج ممّا سبق أنّ مجموعة الأعداد العاديّة $\mathbb{Q}$ قابلة للعدّ.
5. لتكن A مجموعة غير خالية، أثبت أنّه لا يوجد تطبيق غامر من A إلى مجموعة أجزائها. ثُمّ استنتج أنّ مجموعة أجزاء $\mathbb{N}$ غير قابلة للعدّ.

الحل

1. لتكن $\mathcal{N}$ مجموعة جزئيّة من $\mathbb{N}$. ولنفترض أنّ $\mathcal{N}$ غير منتهية. نعرّف عندئذ بالتدريج تطبيقاً φ من $\mathbb{N}$ إلى $\mathcal{N}$ كما يلي :

$$\varphi(0) = \min \mathcal{N} \quad \text{و} \quad \forall n \in \mathbb{N}, \quad \varphi(n+1) = \min\big(\mathcal{N} \cap]\varphi(n), +\infty[\big)$$

هذا التعريف صحيح لأنّ $\mathcal{N} \cap]\varphi(n), +\infty[$ مجموعة جزئيّة غير خالية من $\mathbb{N}$، وذلك بسبب افتراض أنّ $\mathcal{N}$ مجموعة غير منتهية. التطبيق φ المعرّف بهذا الأسلوب تطبيقٌ متباينٌ لأنّه في الحقيقة متزايدٌ تماماً، وهذا يقتضي أنّ $\varphi(\ell) \geq \ell$ أياًكان ℓ من $\mathbb{N}$ (لماذا ؟).

لنثبت أنّ φ غامرٌ. ليكن k عنصراً من $\mathcal{N}$. المجموعة $\{j \in \mathbb{N} : \varphi(j) \leq k\}$ غير خالية لأنّ 0 ينتمي إليها. وهي محدودة من الأعلى بالعدد k لأنّ $\varphi(j) \leq k \Rightarrow j \leq k$. ليكن إذن

$$\ell = \max\{j \in \mathbb{N} : \varphi(j) \leq k\}$$

إذا كان $\varphi(\ell) < k$ استنتجنا أنّ $k \in \mathcal{N} \cap]\varphi(\ell), +\infty[$، ونتج من ذلك أنّ $\varphi(\ell+1) \leq k$ بناءً على تعريف φ، وهذا يناقض اختيارنا للعدد ℓ. إذن $\varphi(\ell) = k$، والتطبيق φ غامرٌ. فهو تقابلٌ بين $\mathbb{N}$ و $\mathcal{N}$، والمجموعة $\mathcal{N}$ قابلة للعدّ.

وبوجه عام، لتكن A مجموعة جزئيّة من مجموعة B قابلة للعدّ. عندئذ يوجد تقابل $f : \mathbb{N} \to B$، فتكون المجموعة $\mathcal{N} = f^{-1}(A)$ مجموعة جزئيّة من $\mathbb{N}$. إذن

- إمّا أن تكون $\mathcal{N}$ منتهية وهناك تقابلٌ $\varphi : \mathbb{N}_n \to \mathcal{N}$. فيكون

$$\tilde{\varphi} : \mathbb{N}_n \to A, k \mapsto f(\varphi(n))$$

تقابلاً بين $\mathbb{N}_n$ و A، والمجموعة A منتهية.

- وإمّا أن تكون $\mathcal{N}$ قابلة للعدّ، وهناك تقابلٌ $\varphi : \mathbb{N} \to \mathcal{N}$. فيكون $f \circ \varphi$ تقابلاً بين $\mathbb{N}$ و A، والمجموعة A قابلة للعدّ.

2. لنثبت أنّ f متباينٌ. ليكن (n, m) و (n', m') عنصرين من $\mathbb{N} \times \mathbb{N}$، ولنفترض أنّ

$$f(n, m) = f(n', m')$$

عندئذ يكون لدينا $2^n(2m+1) = 2^{n'}(2m'+1)$. فإذا كان $n \neq n'$ أمكننا دون الإقلال من عموميّة الإثبات أن نفترض مثلاً أنّ $n < n'$، وعندئذ يكون

$$2m + 1 = 2^{n'-n}(2m'+1)$$

وهذا خُلفٌ إذ لا يمكن لعدد زوجي أن يساوي عدداً فرديّاً.

نستنتج أنّه يجب أن يكون $n = n'$ ومن ثَمّ $2m+1 = 2m'+1$ أو $m = m'$. ومنه $(n,m) = (n',m')$.

أمّا إثباتُ أنّ f غامرٌ، فهو نتيجة من خواص الأعداد الطبيعيّة. فإذا كان p عنصراً من $\mathbb{N}$ عرّفنا

$$m = \frac{1}{2}\left(\frac{p+1}{2^n} - 1\right) \quad \text{و} \quad n = \max\{k \in \mathbb{N} : 2^k \mid (p+1)\}$$

فيكون لدينا $f(n,m) = p$. ونكون قد أثبتنا أنّ f تقابلٌ بين $\mathbb{N}^2$ و $\mathbb{N}$، والمجموعة $\mathbb{N}^2$ قابلة للعدِّ.

3. يكفي أن نثبت الخاصّة التالية: لتكن $(A_k)_{k\in\mathbb{N}}$ جماعةً مجموعةُ أدلّتها قابلة للعدِّ، مكوّنةً من مجموعات قابلة للعدِّ. عندئذ تكون المجموعة $A = \bigcup_{k\in\mathbb{N}} A_k$ قابلة للعدِّ.

مهما تكن k من $\mathbb{N}$ يوجد تقابلٌ $\varphi_k : \mathbb{N} \to A_k$. ليكن $f : \mathbb{N}^2 \to \mathbb{N}$ التقابل الذي درسناه في الطلب السابق. نعرّف عندئذ التطبيق :

$$\psi : \bigcup_{k\in\mathbb{N}} A_k \to \mathbb{N}, \quad \psi(x) = \min\left\{f(k,n) : x = \varphi_k(n)\right\}$$

فيكون التطبيق ψ متبايناً. في الحقيقة، لنفترض أنّ $\psi(x) = \psi(y)$ ولتكن p هذه القيمة المشتركة، عندئذ يوجد (k,n) في $\mathbb{N}^2$ يُحقّق $f(k,n) = p$. وعندئذ يكون $x = \varphi_k(n)$ و $y = \varphi_k(n)$ أي $x = y$.

نستنتج إذن أنّ هناك تقابلاً من A إلى مجموعة جزئيّة هي $\psi(A)$ من $\mathbb{N}$. ولأنّ المجموعة $\psi(A)$ قابلة للعدِّ استناداً إلى نتيجة الطلب الأوّل، استنتجنا أنّ A نفسها قابلة للعدِّ.

4. لتكن n من $\mathbb{N}^*$. عندئذ تكون المجموعة

$$A_n = \left\{\tfrac{k}{n} : k \in \mathbb{N}\right\}$$

قابلة للعدِّ لأنّ هناك تقابلاً واضحاً بين A_n و $\mathbb{N}$. نستنتج إذن أنّ $\mathbb{Q}_+ = \bigcup_{n\in\mathbb{N}} A_n$ مجموعة قابلة للعدِّ. ولأنّ هناك تقابلاً واضحاً بين $\mathbb{Q}_+$ و $\mathbb{Q}_-$ استنتجنا أنّ $\mathbb{Q}_-$ أيضاً قابلة للعدِّ. وعليه تكون المجموعة $\mathbb{Q} = \mathbb{Q}_+ \cup \mathbb{Q}_-$ قابلة للعدِّ.

5. لتكن A مجموعة غير خالية، ولنفترض أنّ $f : A \to P(A)$ تطبيق غامرٌ من A إلى مجموعة أجزائها. عندئذ نعرّف المجموعة $\Omega = \{x \in A : x \notin f(x)\}$. لمّا كان f غامراً وجدنا عنصراً ω في A يحقّق $f(\omega) = \Omega$. وهنا نناقش حالتين :

- في حالة $\omega \in \Omega$ يكون لدينا $\omega \notin f(\omega)$ تبعاً لتعريف Ω، وهذا يناقض الخاصّة $f(\omega) = \Omega$.
- وفي حالة $\omega \notin \Omega$ يكون لدينا $\omega \in f(\omega)$ تبعاً لتعريف Ω، وهذا يناقض الخاصّة $f(\omega) = \Omega$.

إذن لا يمكن إيجاد تطبيق غامرٍ من A إلى $P(A)$.

نستنتج مما سبق أنّه لا يوجد تقابلٌ بين $\mathbb{N}$ ومجموعة أجزائها $P(\mathbb{N})$. فالمجموعة $P(\mathbb{N})$ غير قابلة للعدّ. ■

التمرين 13. نعرّف على المجموعة $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ العلاقة الثنائيّة

$$(x, y)\,\mathcal{R}\,(x', y') \Leftrightarrow x + y' = y + x'$$

1. أثبت أنّ $\mathcal{R}$ علاقة تكافؤ على $\mathbb{N}^2$.
2. لتكن $\mathcal{Z} = \mathbb{N}^2/\mathcal{R}$ مجموعة صفوف تكافؤ العلاقة $\mathcal{R}$. إذا كان k عنصراً من $\mathbb{N}^*$ رمزنا بالرمز $(+k)$ إلى $[(k,0)]$ أي صف تكافو العنصر $(k,0)$، وبالرمز $(-k)$ إلى $[(0,k)]$ أي صف تكافؤ العنصر $(0,k)$، وبالرمز (0) إلى $[(0,0)]$ أي صف تكافو العنصر $(0,0)$. أثبت أنّ

$$\mathcal{Z} = \{(+k) : k \in \mathbb{N}^*\} \cup \{(0)\} \cup \{(-k) : k \in \mathbb{N}^*\}$$

3. ليكن A و B صفَّي تكافؤ من $\mathcal{Z}$ أثبت أنّه يوجد صف تكافؤ وحيد نرمز إليه بالرمز $A \oplus B$ يُحقّق

$$\{(u_1 + v_1, u_2 + v_2) : (u_1, u_2) \in A, (v_1, v_2) \in B\} \subset A \oplus B$$

وبيِّن أنّه إذا كان $A = [(a_1, a_2)]$ وكان $B = [(b_1, b_2)]$ كان

$$A \oplus B = [(a_1 + b_1, a_2 + b_2)]$$

ثُمّ أثبت أنّ $(\mathcal{Z}, \oplus)$ زمرة تبديليّة.

الحل

1. لإثبات أنّ $\mathcal{R}$ علاقة تكافؤ نلاحظ ما يلي :

- لمّا كان جمع الأعداد الطبيعيّة تبديليّاً استنتجنا أنّ $x+y=y+x$ أي $(x,y)\mathcal{R}(x,y)$ أياًكان (x,y) من $\mathbb{N}^2$
وهذا يعني أنّ $\mathcal{R}$ انعكاسيّة.
- إذا كان $(x,y)\mathcal{R}(x',y')$ أي $x+y'=y+x'$ أو $x'+y=y'+x$ أي إنّ $(x',y')\mathcal{R}(x,y)$ والعلاقة $\mathcal{R}$ تناظريّة.
- إذا كان $(x,y)\mathcal{R}(x',y')$ و $(x',y')\mathcal{R}(x'',y'')$ كان
$$x'+y''=y'+x'' \quad \text{و} \quad x+y'=y+x'$$
وبجمع هاتين المساواتين طرفاً إلى طرف نجد
$$x+\cancel{y'+x'}+y''=y+\cancel{x'+y'}+x''$$
ومنه $(x,y)\mathcal{R}(x'',y'')$ أي إنّ العلاقة $\mathcal{R}$ متعديّة. وبذا نكون قد أثبتنا أنّ $\mathcal{R}$ علاقة تكافؤ.

2. ليكن $[(a,b)]$ صفّ تكافؤ العنصر (a,b) من $\mathbb{N}^2$ ولنتأمّل الحالات التالية :
- حالة $a=b$. في هذه الحالة يكون $(a,b)\mathcal{R}(0,0)$ ومن ثَمّ $[(a,b)]=(0)$.
- حالة $a>b$. في هذه الحالة يكون $(a,b)\mathcal{R}(a-b,0)$ ومن ثَمّ $[(a,b)]=(a-b)$.
- حالة $a<b$. في هذه الحالة يكون $(a,b)\mathcal{R}(0,a-b)$ ومن ثَمّ $[(a,b)]=(-(b-a))$.

إذن
$$\mathcal{Z}=\Big\{(+k):k\in\mathbb{N}^*\Big\}\cup\Big\{\{0\}\Big\}\cup\Big\{(-k):k\in\mathbb{N}^*\Big\}$$
لأنّ الاحتواء الآخر محقّق وضوحاً.

3. لنفترض أنّ $A=[(a_1,a_2)]$ و $B=[(b_1,b_2)]$. وليكن (u_1,u_2) عنصراً من صف التكافؤ A و (v_1,v_2) عنصراً من صف التكافؤ B . عندئذ
$$v_1+b_2=v_2+b_1 \quad \text{و} \quad u_1+a_2=u_2+a_1$$

ومن ثَمّ

$$u_1 + v_1 + a_2 + b_2 = u_2 + v_2 + a_1 + b_1$$

أو $(u_1 + v_1, u_2 + v_2) \in [(a_1 + b_1, a_2 + b_2)]$.

وهكذا نكون قد أثبتنا أنّ صف التكافؤ $[(a_1 + b_1, a_2 + b_2)]$ يضمّ جميع العناصر التي تُكتب بالشكل $(u_1 + v_1, u_2 + v_2)$ حيث (u_1, u_2) من A و (v_1, v_2) من B. أي

$$[(a_1, a_2)] \oplus [(b_1, b_2)] = [(a_1 + b_1, a_2 + b_2)]$$

جمع الأعداد الطبيعيّة تبديلي وتجميعي ويقبل العدد 0 عنصراً حيادياً. إذن نستنتج دون عناء أنّ البنية $(\mathcal{Z}, \oplus)$ تبديليّة وتجميعيّة وتقبل (0) عنصراً حيادياً. ثُمّ إنّ لكلّ صف تكافؤ $A = [(a_1, a_2)]$ نظيرٌ في $(\mathcal{Z}, \oplus)$ هو صفّ التكافؤ $A' = [(a_2, a_1)]$. إذن $(\mathcal{Z}, \oplus)$ زمرة تبديليّة. ■

ملاحظة. لقد استعرضنا في هذا التمرين طريقة لإنشاء زمرة الأعداد الصحيحة $(\mathbb{Z}, +)$ انطلاقاً من البنية $(\mathbb{N}, +)$.

التمرين 14. احسب بدلالة n المجاميع $S_n^{(p)} = \sum_{k=1}^{n} k^p$ في حالة $p \in \{1, 2, 3\}$.

الحل

- لحساب المجموع $S_n^{(1)} = \sum_{k=1}^{n} k$ يمكننا أن نستفيد من الطريقة التي اقترحها العالم الرياضي الألماني Gauss عندما كان في التاسعة من عمره. نكتب المجموع المطلوب مرّتين كما يلي :

$$\begin{array}{rcccccccccc}
S_n^{(1)} & = & \boxed{1} & + & \boxed{2} & + & \cdots & + & \boxed{(n-1)} & + & \boxed{n} \\
S_n^{(1)} & = & \boxed{n} & + & \boxed{(n-1)} & + & \cdots & + & \boxed{2} & + & \boxed{1} \quad + \\
\hline
2S_n^{(1)} & = & (n+1) & + & (n+1) & + & \cdots & + & (n+1) & + & (n+1)
\end{array}$$

فنستنتج أنّ $2S_n^{(1)} = n(n+1)$. ومنه $S_n^{(1)} = \dfrac{n(n+1)}{2}$.

- أمّا لحساب المجموع $S_n^{(2)} = \sum_{k=1}^{n} k^2$ فيمكننا أن نبدأ بملاحظة ما يلي:

$$(k+1)^3 - k^3 = 3k^2 + 3k + 1$$

فإذا كتبنا هذا العلاقات عندما تتحول k من 1 إلى n ثُمّ جمعناها طرفاً إلى طرف وجدنا

$$\begin{array}{ccccccccc}
\cancel{2^3} & - & 1^3 & = & 3\times 1^2 & + & 3\times 1 & + & 1\\
\cancel{3^3} & - & \cancel{2^3} & = & 3\times 2^2 & + & 3\times 2 & + & 1\\
\cancel{4^3} & - & \cancel{3^3} & = & 3\times 3^2 & + & 3\times 3 & + & 1\\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots\\
\cancel{(k+1)^3} & - & \cancel{k^3} & = & 3\times k^2 & + & 3\times k & + & 1\\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots\\
(n+1)^3 & - & \cancel{n^3} & = & 3\times n^2 & + & 3\times n & + & 1\\
\hline
(n+1)^3 & - & 1 & = & 3\times S_n^{(2)} & + & 3\times S_n^{(1)} & + & n
\end{array}$$

استنتجنا أنّ

$$\begin{aligned} 3S_n^{(2)} &= (n+1)^3 - 1 - n - \frac{3n(n+1)}{2} \\ &= \frac{n(n+1)(2n+1)}{2} \end{aligned}$$

ومنه

$$S_n^{(2)} = \frac{n(n+1)(2n+1)}{6}$$

- ولحساب المجموع $S_n^{(3)} = \sum_{k=1}^{n} k^3$ يمكننا أن نبدأ بملاحظة أنّ :

$$(k+1)^2 - (k-1)^2 = 4k$$

ومن ثَمّ

$$(k+1)^2 k^2 - k^2 (k-1)^2 = 4k^3$$

إذن بجمع العلاقات السابقة طرفاً إلى طرف عندما تتحوّل k من 1 إلى n نستنتج أنّ

$$(n+1)^2 n^2 = 4S_n^{(3)}$$

أو

$$S_n^{(3)} = \frac{n^2(n+1)^2}{4} = \left(S_n^{(1)}\right)^2$$

وهو المطلوب. ■

التمرين 15. احسب بدلالة n المجموع

$$F_n = 1\cdot 1! + 2\cdot 2! + 3\cdot 3! + \cdots + n\cdot n!$$

الحل

يكفي أن نلاحظ أنّ

$$k\cdot k! = (k+1)! - k!$$

إذن بجمع العلاقات السابقة طرفاً إلى طرف عندما تتحوّل k من 1 إلى n نستنتج أنّ

$$F_n = 1\cdot 1! + 2\cdot 2! + 3\cdot 3! + \cdots + n\cdot n! = (n+1)! - 1$$

وهو المطلوب.

التمرين 16. أثبت صحّة ما يلي

1. $$\forall n \geq 2,\quad \frac{1}{\sqrt{4n+1}} < \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2\cdot 4\cdot 6\cdots(2n)} < \frac{1}{\sqrt{3n+1}}$$
2. $$\forall n \geq 1,\quad \sum_{k=1}^{n}\sqrt{k} < \frac{4n+3}{6}\sqrt{n}$$

الحل

1. لتكن $\mathbb{P}_n$ الخاصّة

$$\frac{1}{\sqrt{4n+1}} < \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2\cdot 4\cdot 6\cdots(2n)} < \frac{1}{\sqrt{3n+1}}$$

نلاحظ أنّ

$$\mathbb{P}_2 \Leftrightarrow \frac{1}{3} < \frac{1\cdot 3}{2\cdot 4} < \frac{1}{\sqrt{7}} \Leftrightarrow (8 < 9) \wedge (63 < 64)$$

إذن $\mathbb{P}_2$ صحيحة.

لنفترض أنّ $\mathbb{P}_n$ صحيحة في حالة $n \geq 2$. عندئذ يكون لدينا

$$\frac{1}{\sqrt{4n+1}}\,\frac{2n+1}{2n+2} < \frac{1\cdot 3\cdot 5\cdots(2n-1)(2n+1)}{2\cdot 4\cdot 6\cdots(2n)(2n+2)} < \frac{1}{\sqrt{3n+1}}\,\frac{2n+1}{2n+2}$$

ولنرمز بالرمز D_1 إلى الفرق

$$D_1 = \left(\frac{1}{\sqrt{3n+4}}\right)^2 - \left(\frac{1}{\sqrt{3n+1}} \cdot \frac{2n+1}{2n+2}\right)^2$$

فنجد أنّ

$$\begin{aligned} D_1 &= \frac{1}{3n+4} - \frac{1}{3n+1}\left(\frac{2n+1}{2n+2}\right)^2 \\ &= \frac{(3n+1)(2n+2)^2 - (3n+4)(2n+1)^2}{(3n+4)(3n+1)(2n+2)^2} \\ &= \frac{n}{(3n+4)(3n+1)(2n+2)^2} > 0 \end{aligned}$$

إذن

$$n > 0 \Rightarrow \frac{1}{\sqrt{3n+1}} \cdot \frac{2n+1}{2n+2} < \frac{1}{\sqrt{3n+4}}$$

وكذلك، لنرمز بالرمز D_2 إلى الفرق

$$D_2 = \left(\frac{1}{\sqrt{4n+1}} \cdot \frac{2n+1}{2n+2}\right)^2 - \left(\frac{1}{\sqrt{4n+5}}\right)^2$$

فنجد أنّ

$$\begin{aligned} D_2 &= \frac{1}{4n+1}\left(\cdot\frac{2n+1}{2n+2}\right)^2 - \frac{1}{4n+5} \\ &= \frac{(4n+5)(2n+1)^2 - (4n+1)(2n+2)^2}{(4n+1)(4n+5)(2n+2)^2} \\ &= \frac{1}{(4n+1)(4n+5)(2n+2)^2} > 0 \end{aligned}$$

وهكذا نكون قد أثبتنا أنّ

$$\frac{1}{\sqrt{4n+5}} < \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)(2n+1)}{2 \cdot 4 \cdot 6 \cdots (2n)(2n+2)} < \frac{1}{\sqrt{3n+4}}$$

أي $\mathbb{P}_{n+1}$ صحيحة. وبذا نكون قد أثبتنا صحّة $\mathbb{P}_n$ في حالة $2 \leq n$.

2. لتكن $\mathbb{P}_n$ الخاصّة

$$\sum_{k=1}^{n}\sqrt{k} < \frac{4n+3}{6}\sqrt{n}$$

نلاحظ أنّ $\frac{7}{6} > 1 \Leftrightarrow \mathbb{P}_1$ إذن $\mathbb{P}_1$ صحيحة.

لنفترض أنّ $\mathbb{P}_n$ صحيحة في حالة $n \geq 1$. عندئذ يكون لدينا

$$\sum_{k=1}^{n+1}\sqrt{k} = \sum_{k=1}^{n}\sqrt{k} + \sqrt{n+1} < \frac{4n+3}{6}\sqrt{n} + \sqrt{n+1}$$

لنرمز إذن بالرمز D إلى الفرق الآتي:

$$D = \frac{4n+7}{6}\sqrt{n+1} - \left(\frac{4n+3}{6}\sqrt{n} + \sqrt{n+1}\right)$$

فنجد أنّ

$$\begin{aligned}
D &= \frac{4n+1}{6}\sqrt{n+1} - \frac{4n+3}{6}\sqrt{n}\\
&= \frac{4n+1}{6}(\sqrt{n+1}-\sqrt{n}) - \frac{2\sqrt{n}}{6}\\
&= \frac{4n+1}{6(\sqrt{n}+\sqrt{n+1})} - \frac{2\sqrt{n}}{6}\\
&= \frac{2n+1-2\sqrt{n(n+1)}}{6(\sqrt{n}+\sqrt{n+1})}\\
&= \frac{\left(\sqrt{n+1}-\sqrt{n}\right)^2}{6(\sqrt{n}+\sqrt{n+1})} > 0
\end{aligned}$$

إذن

$$\sum_{k=1}^{n+1}\sqrt{k} < \frac{4(n+1)+3}{6}\sqrt{n+1}$$

والقضيّة $\mathbb{P}_{n+1}$ صحيحة. وبذا نكون قد أثبتنا صحّة $\mathbb{P}_n$ في حالة $n \geq 1$. ■

التمرين 17. أوجد جميع التوابع $f:\mathbb{N}\to\mathbb{N}$ التي تحقِّق

$$\forall(n,m)\in\mathbb{N}^2,\quad f(n+m)=f(n)+f(m) \qquad \mathcal{A}$$

الحل

ليكن $f:\mathbb{N}\to\mathbb{N}$ تابعاً يُحقّق الشرط $\mathcal{A}$.

- بأخذ $n=m=0$ نستنتج أنّ $f(0)+f(0)=f(0)$، ومن ثَمّ $f(0)=0$.
- لنعرّف العدد a بالعلاقة $a=f(1)$. عندئذ نلاحظ أنّ

$$\forall n\in\mathbb{N},\quad f(n+1)=f(n)+f(1)=f(n)+a \qquad \odot$$

إذن ينتج العدد $f(n+1)$ من العدد $f(n)$ بإضافة a وهذا ما يهيِّئ لنا أن نفترض أنّ

$$\forall n\in\mathbb{N},\ f(n)=an$$

- لإثبات صحّة هذا الافتراض، نعرّف القضيّة $\mathbb{P}_n\equiv f(n)=an$. ونلاحظ أنّ القضيّتين $\mathbb{P}_0$ و $\mathbb{P}_1$ صحيحتان. وإذا كانت $\mathbb{P}_n$ صحيحة استنتجنا من $\odot$ أنّ

$$f(n+1)=f(n)+a=an+a=a(n+1)$$

فالقضيّة $\mathbb{P}_{n+1}$ صحيحة أيضاً. وبذا نكون قد أثبتنا صحّة $\mathbb{P}_n$ في حالة $n\in\mathbb{N}$.

ومن جهة أخرى كلّ تابع من النمط

$$\varphi_a:\mathbb{N}\to\mathbb{N},\varphi_a(n)=an \text{ ، حيث } a\in\mathbb{N}$$

يُحقّق الشرط $\mathcal{A}$ وضوحاً. إذن

$$\{f:\mathbb{N}\to\mathbb{N}: \text{يُحقّق } \mathcal{A}\ f\}=\{\varphi_a: a\in\mathbb{N}\} \qquad \blacksquare$$

التمرين 18. احسب بدلالة (p,n) من $\mathbb{N}^{*2}$ المقادير

$$U(n,p)=\operatorname{card}\Big(\Big\{(x_1,\dots,x_n)\in(\mathbb{N}^*)^n:\textstyle\sum_{k=1}^n x_k\le p\Big\}\Big)$$
$$\widetilde{U}(n,p)=\operatorname{card}\Big(\Big\{(x_1,\dots,x_n)\in(\mathbb{N}^*)^n:\textstyle\sum_{k=1}^n x_k= p\Big\}\Big)$$
$$T(n,p)=\operatorname{card}\Big(\Big\{(x_1,\dots,x_n)\in\mathbb{N}^n:\textstyle\sum_{k=1}^n x_k\le p\Big\}\Big)$$
$$\widetilde{T}(n,p)=\operatorname{card}\Big(\Big\{(x_1,\dots,x_n)\in\mathbb{N}^n:\textstyle\sum_{k=1}^n x_k= p\Big\}\Big)$$

الحل

▪ لنلاحظ أنّ $U(n,p)=0$ إذا كان $p<n$. لنفترض إذن أنّ $n\le p$، ولنعرّف المجموعة :

$$\mathbb{U}(n,p)=\left\{(x_1,\ldots,x_n)\in(\mathbb{N}^*)^n : \sum_{k=1}^{n}x_k\le p\right\}$$

فيكون $U(n,p)=\operatorname{card}\big(\mathbb{U}(n,p)\big)$. وكذلك لتكن $P_n^{(p)}$ مجموعة أجزاء المجموعة $\mathbb{N}_p$ التي عدد عناصر كلٍّ منها n.

لنتأمّل التطبيقين Θ و Φ المعرّفين كما يلي :

$$\Theta : \mathbb{U}(n,p)\to P_n^{(p)},(x_1,\ldots,x_n)\mapsto(x_1,x_1+x_2,\ldots,x_1+x_2+\cdots+x_n)$$

و

$$\Phi : P_n^{(p)}\to\mathbb{U}(n,p), A\mapsto(x_1(A),x_2(A),\ldots,x_n(A))$$

حيث تمثّل الأعداد $x_1(A)$ و $x_1(A)+x_2(A)$ و ... و $x_1(A)+x_2(A)+\cdots+x_n(A)$ عناصر المجموعة A بعد ترتيبها ترتيباً متزايداً تماماً. أي

$$\begin{aligned}
x_1(A)&=\min A\\
x_1(A)&=\min\big(A\backslash\{x_1(A)\}\big)-x_1(A)\\
&\vdots\\
x_{k+1}(A)&=\min\big(A\backslash\{x_1(A),\ldots,x_k(A)\}\big)-x_k(A)\\
&\vdots\\
x_n(A)&=\max A-x_{n-1}(A)
\end{aligned}$$

عندئذ نتوثّق مباشرة أنّ

$$\Phi\circ\Theta=I_{\mathbb{U}(n,p)} \quad \text{و} \quad \Theta\circ\Phi=I_{P_n^{(p)}}$$

فالتطبيق Θ تقابلٌ، ومن ثَمّ

$$U(n,p)=\operatorname{card}(\mathbb{U}(n,p))=\operatorname{card}(P_n^{(p)})=C_n^p$$

إذن

$$U(n,p)=C_n^p$$

- لنعرّف المجموعة :

$$\widetilde{\mathbb{U}}\left(n,p\right)=\left\{(x_1,\dots,x_n)\in(\mathbb{N}^*)^n\ :\sum_{k=1}^{n}x_k=p\right\}$$

عندئذ نلاحظ مباشرة أنّ

$$\widetilde{\mathbb{U}}(n,p)=\mathbb{U}(n,p)\backslash\mathbb{U}(n,p-1)$$

وعليه يكون

$$\operatorname{card}(\widetilde{\mathbb{U}}(n,p))=\operatorname{card}(\mathbb{U}(n,p))-\operatorname{card}(\mathbb{U}(n,p-1))$$

إذن

$$\widetilde{U}(n,p)=C_p^n-C_{p-1}^n=C_{p-1}^{n-1}$$

- لنعرّف المجموعة :

$$\mathbb{T}\left(n,p\right)=\left\{(x_1,\dots,x_n)\in\mathbb{N}^n\ :\sum_{k=1}^{n}x_k\leq p\right\}$$

ولنتأمّل التطبيق

$$\Psi:\mathbb{T}(n,p)\to\mathbb{U}(n,p+n),(x_1,\dots,x_n)\mapsto(1+x_1,1+x_2,\dots,1+x_n)$$

فنلاحظ بسهولة أنّه تقابل. إذن

$$\operatorname{card}(\mathbb{T}(n,p))=\operatorname{card}(\mathbb{U}(n,p+n))$$

أو

$$T(n,p)=C_{n+p}^n=\frac{(n+p)!}{n!\cdot p!}$$

- لنعرّف المجموعة :

$$\widetilde{\mathbb{T}}\left(n,p\right)=\left\{(x_1,\dots,x_n)\in\mathbb{N}^n\ :\sum_{k=1}^{n}x_k=p\right\}$$

عندئذ نلاحظ مباشرة أنّ

$$\widetilde{\mathbb{T}}(n,p)=\mathbb{T}(n,p)\backslash\mathbb{T}(n,p-1)$$

وعليه يكون

$$\operatorname{card}(\widetilde{\mathbb{T}}(n,p))=\operatorname{card}(\mathbb{T}(n,p))-\operatorname{card}(\mathbb{T}(n,p-1))$$

إذن

$$\widetilde{U}(n,p)=C_{p+n}^n-C_{p+n-1}^n=C_{p+n-1}^{n-1}$$

التمرين 19. أوجد، في الحالة العامة، عدد نقاط تقاطع أقطار مضلع محدَّب عدد رؤوسه n.

الحل

يُقابل كلُّ أربعة رؤوس من رؤوس المضلّع نقطة تقاطع قطرين من أقطاره. إذن عدد نقاط تقاطع أقطار المضلّع باستثناء رؤوسه يساوي C_n^4. وهكذا إذن رمزنا بالرمز D_n إلى عدد نقاط تقاطع أقطار مضلع محدَّب عدد رؤوسه n. كان لدينا

$$D_n = \begin{cases} 0 & : \quad n = 3 \\ 1 & : \quad n = 4 \\ C_n^4 + n & : \quad n \geq 5 \end{cases}$$

■

التمرين 20. أوجد، في الحالة العامة، عدد مناطق المستوي التي نحصل عليها برسم n مستقيماً فيه.

الحل

ليكن R_n عدد مناطق المستوي التي نحصل عليها برسم n مستقيماً فيه. فنلاحظ أنّ $R_0 = 1$ و $R_1 = 2$. يتقاطع مستقيم جديد في مستوٍ رُسِمَ فيه n مستقيماً مع هذه المستقيمات جميعاً، وهي تحدِّد عليه n نقطة مختلفة. وكلُّ قطعة من القطع المحدَّدة على هذا المستقيم، وعددها $n+1$، تقسم منطقة من مناطق المستوي إلى اثنتين. إذن، عند إضافة مستقيم جديد، يزداد عدد مناطق المستوي R_n بالمقدار $n+1$. أي

$$\forall n \in \mathbb{N}, \quad R_{n+1} = R_n + n + 1$$

ونستنتج من ذلك أنّ

$$\begin{aligned} \forall n \in \mathbb{N}, \quad R_n &= R_0 + \sum_{k=1}^{n} \left(R_k - R_{k-1} \right) \\ &= 1 + \sum_{k=1}^{n} k = 1 + \frac{n(n+1)}{2} \end{aligned}$$

وهي النتيجة المرجوّة. ■

التمرين 21. ليكن (n,r) من $\mathbb{N}^*\times\mathbb{N}$. نرمز بالرمز $f(r,n)$ إلى المتوسط الحسابي لأصغر عنصر في B عندما ترسم B مجموعة أجزاء $\mathbb{N}_n$ المؤلفة من r عنصراً. احسب $f(r,n)$ بأبسط صيغة.

الحل

في الحقيقة لدينا

$$f(r,n)=\frac{1}{\mathrm{card}(P_r^{(n)})}\sum_{B\in P_r^{(n)}}\min(B)$$

إذا كانت B مجموعة جزئيّة من $\mathbb{N}_n$ مؤلفة من r عنصراً أخذ المقدار $\min(B)$ إحدى قيم المجموعة $\mathbb{N}_{n-r+1}$. وإذا كان p عنصراً من $\mathbb{N}_{n-r+1}$ فإنّ عدد المجموعات الجزئيّة من $\mathbb{N}_n$ المؤلفة من r عنصراً والتي أصغر عناصرها هو p يساوي تماماً عدد المجموعات الجزئيّة من المجموعة $\{p+1,p+2,\ldots,n\}$ المؤلفة من $r-1$ عنصراً أي C_{n-p}^{r-1} . وهكذا نستنتج أنّ

$$f(r,n)=\frac{1}{C_n^r}\sum_{p=1}^{n-r+1}pC_{n-p}^{r-1}$$

ولكن نعلم أنّ $C_{n-p}^{r-1}=C_{n-p+1}^{r}-C_{n-p}^{r}$ و $C_{n-p}^{r}=C_{n-p+1}^{r+1}-C_{n-p}^{r+1}$ ، إذن

$$\begin{aligned}
\sum_{p=1}^{n-r+1}pC_{n-p}^{r-1} &= \sum_{p=1}^{n-r+1}pC_{n-p+1}^{r}-\sum_{p=1}^{n-r+1}pC_{n-p}^{r}\\
&=\sum_{p=0}^{n-r}(p+1)C_{n-p}^{r}-\sum_{p=0}^{n-r}pC_{n-p}^{r}\\
&=\sum_{p=0}^{n-r}C_{n-p}^{r}\\
&=\sum_{p=0}^{n-r}\left(C_{n-p+1}^{r+1}-C_{n-p}^{r+1}\right)\\
&=C_{n+1}^{r+1}
\end{aligned}$$

إذن

$$f(r,n)=\frac{C_{n+1}^{r+1}}{C_n^r}=\frac{n+1}{r+1}$$

وهي النتيجة المرجوّة. ∎

التمرين 22. أثبت صحة العلاقات التالية :

$$
\begin{aligned}
&0 \leq p \leq n, && \sum_{k=0}^{n-p} C_{p+k}^{p} = C_{n+1}^{p+1} \\
&(n,p) \in \mathbb{N}^* \times \mathbb{N}, && \sum_{k=0}^{p} (-1)^k C_n^k = (-1)^p C_{n-1}^{p} \\
&(p,q) \in \mathbb{N}^2, && \sum_{k=0}^{p} C_{p+q}^{k} C_{p+q-k}^{p-k} = 2^p C_{p+q}^{p}
\end{aligned}
$$

الحل

- لتكن $\mathbb{P}_n$ الخاصّة الآتية

$$\forall p \in \{0,1,\ldots,n\}, \sum_{k=0}^{n-p} C_{p+k}^{p} = C_{n+1}^{p+1}$$

الخاصّتان $\mathbb{P}_0$ و $\mathbb{P}_1$ صحيحتان وضوحاً. لنفترض صحّة الخاصّة $\mathbb{P}_n$. عندئذ في حالة $0 \leq p \leq n$ لدينا

$$
\begin{aligned}
\sum_{k=0}^{n+1-p} C_{p+k}^{p} &= C_{p+n+1-p}^{p} + \sum_{k=0}^{n-p} C_{p+k}^{p} \\
&= C_{n+1}^{p} + C_{n+1}^{p+1} \\
&= C_{n+2}^{p+1}
\end{aligned}
$$

والنتيجة $\sum_{k=0}^{n+1-p} C_{p+k}^{p} = C_{n+2}^{p+1}$ صحيحة أيضاً في حالة $p = n+1$. إذن لقد أثبتنا صحّة $\mathbb{P}_{n+1}$. وهكذا تكون الخاصّة $\mathbb{P}_n$ صحيحة أيّاً كانت n من $\mathbb{N}$.

- نعلم أنّ $C_n^k = C_{n-1}^{k-1} + C_{n-1}^{k}$ إذن

$$(-1)^k C_n^k = (-1)^k C_{n-1}^{k} - (-1)^{k-1} C_{n-1}^{k-1}$$

وبجمع هذه المساواة طرفاً إلى طرف عندما تتحوّل k من 0 إلى p نجد

$$\sum_{k=0}^{p} (-1)^k C_n^k = (-1)^p C_{n-1}^{p} - (-1)^{0-1} C_{n-1}^{0-1} = (-1)^p C_{n-1}^{p}$$

- لنلاحظ أنّ

$$\begin{aligned} C_{p+q}^{k} C_{p+q-k}^{p-k} &= \frac{(p+q)!}{\cancel{(p+q-k)!}\cdot k!}\cdot\frac{\cancel{(p+q-k)!}}{(p-k)!\cdot q!} \\ &= \frac{(p+q)!}{p!q!}\cdot\frac{p!}{(p-k)!\cdot k!} = C_{p+q}^{p} C_{p}^{k} \end{aligned}$$

إذن

$$\sum_{k=0}^{p} C_{p+q}^{k} C_{p+q-k}^{p-k} = C_{p+q}^{p}\sum_{k=0}^{p} C_{p}^{k} = 2^{p} C_{p+q}^{p}$$

وهي النتيجة المرجوّة.

التمرين 23. احسب، في حالة n من $\mathbb{N}$، كلّاً من المجاميع

$$\sum_{k=0}^{n} kC_n^k \quad \text{و} \quad \sum_{k=0}^{n} k^2 C_n^k \quad \text{و} \quad \sum_{k=0}^{n} \frac{C_n^k}{k+1}$$

الحل

- نعلم أنّ $\sum_{k=0}^{n} C_n^k x^k = (1+x)^n$. فإذا اشتققنا طرفي هذه المساواة بالنسبة إلى x استنتجنا أنّ

$$n(1+x)^{n-1} = \sum_{k=0}^{n} kC_n^k x^{k-1} \qquad \odot$$

وذلك في حالة $1 \leq n$. ومنه، بتعويض $x = 1$، نستنتج أنّ $\sum_{k=0}^{n} kC_n^k = n2^{n-1}$ وهي أيضاً صحيحة في حالة $n = 0$.

- نستنتج من العلاقة $\odot$ أنّ

$$\sum_{k=0}^{n} kC_n^k x^k = n(1+x)^{n-1}x = n\Big((1+x)^n - (1+x)^{n-1}\Big)$$

فإذا اشتققنا طرفي هذه المساواة بالنسبة إلى x استنتجنا، في حالة $2 \leq n$، أنّ

$$\sum_{k=0}^{n} k^2 C_n^k x^{k-1} = n\Big(n(1+x)^{n-1} - (n-1)(1+x)^{n-2}\Big)$$

وبتعويض $x=1$، نستنتج أنّ $\sum_{k=0}^{n} k^2 C_n^k = (n^2+n)2^{n-2}$ وهي أيضاً صحيحة في حالة $n=0$ و $n=1$.

- وكذلك نرى أنّ

$$\int_0^1 (1+x)^n \,\mathrm{d}\,x = \sum_{k=0}^{n} C_n^k \int_0^1 x^k \,\mathrm{d}\,x = \sum_{k=0}^{n} \frac{C_n^k}{k+1}$$

ولكن لدينا من جهة أخرى

$$\int_0^1 (1+x)^n \,\mathrm{d}\,x = \left[\frac{(1+x)^{n+1}}{n+1}\right]_0^1 = \frac{2^{n+1}-1}{n+1}$$

إذن

$$\sum_{k=0}^{n} \frac{C_n^k}{k+1} = \frac{2^{n+1}-1}{n+1}$$

وهي النتيجة المرجوّة.

التمرين 24. لتكن $n \geq 1$. احسب كلّاً من المجاميع التالية :

$$\sum_{X\in P^{(n)}} \mathrm{card}(X), \quad \sum_{(X,Y)\in P^{(n)}\times P^{(n)}} \mathrm{card}(X\cap Y), \quad \sum_{(X,Y)\in P^{(n)}\times P^{(n)}} \mathrm{card}(X\cup Y)$$

الحل

في حالة مجموعة جزئيّة X من $\mathbb{N}_n$، سنرمز بالرمز X^c إلى متمّمة X أي إلى $\mathbb{N}_n \setminus X$. ونعلم أنّ التطبيق

$$\varphi : P^{(n)} \to P^{(n)}, X \mapsto X^c$$

تقابلٌ.

- لنلاحظ إذن أنّ

$$S_1 = \sum_{X\in P^{(n)}} \mathrm{card}(X) = \sum_{X\in P^{(n)}} \mathrm{card}(X^c)$$

ومن ثَمّ

$$\begin{aligned}2S_1 &= \sum_{X\in P^{(n)}} \operatorname{card}(X) + \sum_{X\in P^{(n)}} \operatorname{card}(X^c)\\ &= \sum_{X\in P^{(n)}} (\operatorname{card}(X) + \operatorname{card}(X^c)) = \sum_{X\in P^{(n)}} n\\ &= n\operatorname{card}(P^{(n)}) = n2^n\end{aligned}$$

وهذا يثبتُ أنّ $S_1 = n2^{n-1}$، أي

$$\sum_{X\in P^{(n)}} \operatorname{card}(X) = n2^{n-1}$$

وهذا يعني أنّ التوقّع الرياضي لعدد عناصر مجموعة جزئيّة مسحوبة عشوائياً من $\mathbb{N}_n$ يساوي $\frac{n}{2}$.

- لنلاحظ أيضاً أنّ

$$\begin{aligned}S_2 &= \sum_{(X,Y)\in P^{(n)}\times P^{(n)}} \operatorname{card}(X\cap Y)\\ &= \sum_{(X,Y)\in P^{(n)}\times P^{(n)}} \operatorname{card}(X\cap Y^c)\\ &= \sum_{(X,Y)\in P^{(n)}\times P^{(n)}} \operatorname{card}(X^c\cap Y)\\ &= \sum_{(X,Y)\in P^{(n)}\times P^{(n)}} \operatorname{card}(X^c\cap Y^c)\end{aligned}$$

ومن ثَمّ

$$\begin{aligned}4S_2 &= \sum_{\substack{X\in P^{(n)}\\ Y\in P^{(n)}}} (\operatorname{card}(X\cap Y) + \operatorname{card}(X\cap Y^c) + \operatorname{card}(X^c\cap Y) + \operatorname{card}(X^c\cap Y^c))\\ &= \sum_{(X,Y)\in P^{(n)}\times P^{(n)}} n = n\operatorname{card}\left(P^{(n)}\times P^{(n)}\right) = n2^n\times 2^n\end{aligned}$$

وهذا يثبتُ أنّ $S_2 = n4^{n-1}$، أي

$$\sum_{(X,Y)\in P^{(n)}\times P^{(n)}} \operatorname{card}(X\cap Y) = n4^{n-1}$$

وهذا يعني أنّ التوقّع الرياضي لعدد عناصر تقاطع مجموعتين جزئيّتين مسحوبتين عشوائياً من $\mathbb{N}_n$ يساوي $\frac{n}{4}$.

- وأخيراً نلاحظ أنّ

$$\begin{aligned}\sum_{(X,Y)\in P^{(n)}\times P^{(n)}} \operatorname{card}(X\cup Y) &= \sum_{(X,Y)\in P^{(n)}\times P^{(n)}} (n-\operatorname{card}((X\cup Y)^c))\\ &= n4^n - \sum_{(X,Y)\in P^{(n)}\times P^{(n)}} \operatorname{card}(X^c\cap Y^c)\\ &= n4^n - S_2 = 3n4^{n-1}\end{aligned}$$

ومنه

$$\sum_{(X,Y)\in P^{(n)}\times P^{(n)}} \operatorname{card}(X\cup Y) = 3n4^{n-1}$$

وهذا يعني أنّ التوقّع الرياضي لعدد عناصر اجتماع مجموعتين جزئيّتين مسحوبتين عشوائياً من $\mathbb{N}_n$ يساوي $\dfrac{3n}{4}$. وبذا يتم إثبات المطلوب. ■

التمرين 25. ليكن $1 \leq n$. احسب ما يلي:

$$\begin{aligned}\mathcal{E}_n &= \operatorname{card}(\{(X,Y)\in P^{(n)}\times P^{(n)} : X\subset Y\}),\\ \mathcal{F}_n &= \operatorname{card}(\{(X,Y)\in P^{(n)}\times P^{(n)} : X\cap Y=\varnothing\}),\\ \overline{\mathcal{F}}_n &= \operatorname{card}(\{(X,Y)\in P^{(n)}\times P^{(n)} : X\cup Y=\mathbb{N}_n\})\\ \mathcal{G}_n^k &= \operatorname{card}(\{(X,Y)\in P^{(n)}\times P^{(n)} : \operatorname{card}(X\cap Y)=k\}),\ k\in\mathbb{N}_n\\ \overline{\mathcal{G}}_n^k &= \operatorname{card}(\{(X,Y)\in P^{(n)}\times P^{(n)} : \operatorname{card}(X\cup Y)=k\}),\ k\in\mathbb{N}_n\end{aligned}$$

الحل

- لتكن

$$\mathcal{E}_n = \operatorname{card}(\{(X,Y)\in P^{(n)}\times P^{(n)} : X\subset Y\})$$

عندئذ

$$\begin{aligned}\mathcal{E}_n &= \sum_{Y\in P^{(n)}} \operatorname{card}(\{X : X\subset Y\}) = \sum_{Y\in P^{(n)}} 2^{\operatorname{card}(Y)}\\ &= \sum_{k=0}^{n}\sum_{Y\in P_k^{(n)}} 2^{\operatorname{card}(Y)} = \sum_{k=0}^{n} 2^k \operatorname{card}(P_k^{(n)}) = \sum_{k=0}^{n} 2^k C_n^k\\ &= (1+2)^n = 3^n\end{aligned}$$

- التطبيق $(X,Y)\mapsto(X,\mathbb{N}_n\backslash Y)$ يعرّف تقابلاً بين المجموعتين
$$\left\{(X,Y)\in P^{(n)}\times P^{(n)}\,:\,X\subset Y\right\}$$
و
$$\left\{(X,Y)\in P^{(n)}\times P^{(n)}\,:\,X\cap Y=\varnothing\right\}$$
فلهما عدد العناصر نفسه، ومنه $\mathcal{F}_n=\mathcal{E}_n=3^n$.

- التطبيق $(X,Y)\mapsto(\mathbb{N}_n\backslash X,\mathbb{N}_n\backslash Y)$ يعرّف تقابلاً بين المجموعتين
$$\left\{(X,Y)\in P^{(n)}\times P^{(n)}\,:\,X\cap Y=\varnothing\right\}$$
و
$$\left\{(X,Y)\in P^{(n)}\times P^{(n)}\,:\,X\cup Y=\mathbb{N}_n\right\}$$
فلهما عدد العناصر نفسه، ومنه $\overline{\mathcal{F}}_n=\mathcal{F}_n=3^n$.

- لتكن k من $\mathbb{N}_n$ عندئذ
$$\left\{(X,Y)\in(P^{(n)})^2\,:\,\mathrm{card}(X\cap Y)=k\right\}=\bigcup_{B\in P_k^{(n)}}\left\{(X,Y)\in(P^{(n)})^2\,:\,X\cap Y=B\right\}$$
ومنه
$$\mathcal{G}_n^k=\sum_{B\in P_k^{(n)}}\mathrm{card}\Big(\left\{(X,Y)\in(P^{(n)})^2\,:\,X\cap Y=B\right\}\Big)$$
لتكن B من $P_k^{(n)}$. ولتكن $A=\mathbb{N}_n\backslash B$ عندئذ يعرّف التطبيق
$$(X,Y)\mapsto(X\cup B,Y\cup B)$$
تقابلاً بين المجموعتين
$$\left\{(X,Y)\in(P(A))^2\,:\,X\cap Y=\varnothing\right\}$$
و
$$\left\{(X,Y)\in(P^{(n)})^2\,:\,X\cap Y=B\right\}$$
فلهما عدد العناصر نفسه. أي
$$\mathrm{card}(\{(X,Y)\in(P^{(n)})^2\,:\,X\cap Y=B\})=3^{\mathrm{card}(A)}=3^{n-k}$$
إذن
$$\mathcal{G}_n^k=3^{n-k}\,\mathrm{card}(P_k^{(n)})=3^{n-k}C_n^k$$

- لتكن k من $\mathbb{N}_n$ عندئذ يعرّف التطبيق $(X,Y)\mapsto(\mathbb{N}_n\backslash X,\mathbb{N}_n\backslash Y)$ تقابلاً بين المجموعتين

$$\left\{(X,Y)\in(P^{(n)})^2 : \operatorname{card}(X\cap Y)=n-k\right\}$$

و

$$\left\{(X,Y)\in(P^{(n)})^2 : \operatorname{card}(X\cup Y)=k\right\}$$

فلهما عددُ العناصر نفسه. إذن $\overline{\mathcal{G}}_n^k=3^kC_n^k$.

التمرين 26. ليكن n من $\mathbb{N}$. أوجد عدد الثلاثيّات (x,y,z) من $\mathbb{N}^3$ التي تُحقِّق ما يلي :

$$\begin{cases} x+y+z=n\\ x\le y+z\\ y\le z+x\\ z\le x+y\end{cases}$$

الحل

لتكن Δ_n مجموعة الثلاثيّات التي تحقِّق الشرط المعطى. ولتكن المجموعة

$$D_n=\left\{(x,y)\in\mathbb{N}^2 : \left(0\le x\le\frac{n}{2}\right)\wedge\left(\frac{n}{2}-x\le y\le\frac{n}{2}\right)\right\}$$

عندئذ يعرّف التطبيق

$$\varphi : D_n\to\Delta_n,(x,y)\mapsto\left(x,y,n-x-y\right)$$

تقابلاً بين المجموعتين Δ_n و D_n .

لنناقش إذن حالتين :

- حالة $n=2m$. هنا

$$D_n=\left\{(x,y)\in\mathbb{N}^2 : \left(0\le x\le m\right)\wedge\left(m-x\le y\le m\right)\right\}$$

ومنه

$$\begin{aligned}\operatorname{card}(D_n)&=\sum_{x=0}^{m}\operatorname{card}\left(\left\{y\in\mathbb{N} : m-x\le y\le m\right\}\right)\\ &=\sum_{x=0}^{m}(x+1)=\frac{(m+1)(m+2)}{2}\end{aligned}$$

- حالة $n = 2m+1$. هنا

$$D_n = \left\{(x,y) \in \mathbb{N}^2 : \left(0 \le x \le m\right) \wedge \left(m - x < y \le m\right)\right\}$$

ومنه

$$\begin{aligned} \operatorname{card}(D_n) &= \sum_{x=0}^{m} \operatorname{card}\left(\left\{y \in \mathbb{N} : m - x < y \le m\right\}\right) \\ &= \sum_{x=0}^{m} x = \frac{m(m+1)}{2} \end{aligned}$$

وبالنتيجة

$$\operatorname{card}\left(\Delta_n\right) = \frac{1}{2}\left\lfloor \frac{n+1}{2} \right\rfloor \left(\left\lfloor \frac{n+1}{2} \right\rfloor + (-1)^n\right)$$

التمرين 27. حلّ في مجموعة الأعداد الطبيعية كلّاً من المعادلتين

- $x(x+1) = 4y(y+1)$.
- $xyz = 1 + x + y + z$.

الحل

- ليكن x و y عددين طبيعيّين يُحقّقان

$$x(x+1) = 4y(y+1)$$

عندئذ

$$\begin{aligned} (4y+2)^2 - (2x+1)^2 &= 4(4y^2 + 4y + 1) - (4x^2 + 4x + 1) \\ &= 4\left(4y(y+1) - x(x+1)\right) + 3 \\ &= 3 \end{aligned}$$

ومنه

$$(4y + 2x + 3)(4y - 2x + 1) = 3$$

إذن $4y + 2x + 3$ عددٌ طبيعي أكبر أو يساوي 3 يقسم العدد 3. ومن ثَمّ $4y + 2x + 3 = 3$ ولأنّ العددين x و y ينتميان إلى $\mathbb{N}$ نستنتج من ذلك أنّ $y = x = 0$.

▪ لتكن x و y و z أعداداً طبيعيَّة تُحقِّق $xyz = 1 + x + y + z$. يمكننا أن نفترض، دون الإقلال من عموميّة الحل أنّ $0 < x \le y \le z$.

▫ إذا كان $2 \le x$ كان

$$xyz \ge 4z > 1 + 3z \ge 1 + x + y + z$$

وهذا خُلفٌ، إذن يجب أن يكون $x = 1$. ومن ثَمّ $yz = 2 + y + z$.

▫ إذا كان $3 \le y$ كان

$$yz \ge 3z > 2z + 2 \ge 2 + y + z$$

إذن يجب أن يكون $y \in \{1,2\}$، ولكن $y = 1$ يقتضي $z = 0$ وهذا خُلفٌ. ومن ثَمّ $y = 2$. وهذا يقتضي $z = 4$.

إذن مجموعة الحلول (x,y,z) في $\mathbb{N}^3$ للمعادلة $xyz = 1 + x + y + z$ هي

$$\{(1,2,4),(1,4,2),(2,4,1),(2,1,4),(4,2,1),(4,1,2)\}$$ ■

التمرين 28. لتكن S_n مجموعة التقابلات على المجموعة $\mathbb{N}_n$.

1. احسب $\operatorname{card}(\{\sigma \in S_n : \forall i \in B, \sigma(i) = i\})$ أيّاً كان B المحتوى في $\mathbb{N}_n$.
2. لتكن j من $\mathbb{N}_n$، ولنضع $A_j = \{\sigma \in S_n : \sigma(j) = j\}$. احسب
$$\operatorname{card}\left(\bigcup_{k=1}^{n} A_k\right)$$
3. لتكن $G_n = \{\sigma \in S_n : \forall j \in \mathbb{N}_n, \sigma(j) \ne j\}$. احسب $\operatorname{card}(G_n)$.

الحل

1. في حالة $B \subset \mathbb{N}_n$ نضع $A = \mathbb{N}_n \backslash B$، ونرمز بالرمز $\mathcal{F}_B$ إلى مجموعة التباديل التي تثبت عناصر B:
$$\{\sigma \in S_n : \forall i \in B, \sigma(i) = i\}$$
وبالرمز $\mathcal{S}(A)$ إلى مجموعة التباديل على المجموعة A. عندئذ نرى أنّ التطبيق
$$\varphi : \mathcal{F}_B \to \mathcal{S}(A), \sigma \mapsto \sigma_{\|A}$$
حيث $\sigma_{\|A} : A \to A, k \mapsto \sigma(k)$، تقابلٌ. ومن ثَمّ
$$\operatorname{card}(\mathcal{F}_B) = \operatorname{card}(\mathcal{S}(A)) = (\operatorname{card}(A))! = (n - \operatorname{card}(B))!$$

2. لقد عرّفنا $A_j = \mathcal{F}_{\{j\}}$ في حالة j من $\mathbb{N}_n$. ونعلم استناداً إلى مبدأ الاحتواء والاستثناء أنّ

$$\operatorname{card}\left(\bigcup_{k=1}^{n} A_k\right) = \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in P_k^{(n)}} \operatorname{card}\left(\bigcap_{i\in B} A_i\right)\right)$$

ولكن $\bigcap_{i\in B} A_i = \mathcal{F}_B$ إذن

$$\begin{aligned}\operatorname{card}\left(\bigcup_{k=1}^{n} A_k\right) &= \sum_{k=1}^{n}(-1)^{k-1}\left(\sum_{B\in P_k^{(n)}} \operatorname{card}(\mathcal{F}_B)\right)\\ &= \sum_{k=1}^{n}(-1)^{k-1}(n-k)!\cdot \operatorname{card}(P_k^{(n)})\end{aligned}$$

وعليه نستنتج أنّ

$$\operatorname{card}\left(\bigcup_{k=1}^{n} A_k\right) = \sum_{k=1}^{n}(-1)^{k-1}(n-k)!\cdot C_n^k = n!\cdot\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k!}$$

3. المجموعة $G_n = \left\{\sigma\in S_n : \forall j\in\mathbb{N}_n, \sigma(j)\neq j\right\}$ هي متمِّمة المجموعة $\bigcup_{k=1}^{n} A_k$ ، ومن ثَمّ

$$\operatorname{card}(G_n) = n!\cdot\left(1-\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k!}\right) = n!\cdot\left(\sum_{k=0}^{n}\frac{(-1)^{k}}{k!}\right)$$

ونبرهن أنّ $\operatorname{card}(G_n) = \operatorname{round}\left(\frac{n!}{e}\right)$ والعدد e هو أساس اللوغاريتم الطبيعي. ■

حقل الأعداد العقديّة

مع حلول القرن السادس عشر صار الرياضيّون يستعملون صيغاً صوريّة من الشكل $\sqrt{-a}$ حيث a عددٌ حقيقي موجبٌ، لتمثيل حلول معادلة من الدرجة الثالثة على سبيل المثال. وبقيت هذه الأعداد «المستحيلة» في الاستعمال دون تعريف دقيق حتى نهاية القرن الثامن عشر. ولم تُعطَ معنى دقيقاً حتّى بداية القرن التاسع عشر.

1. تعريف حقل الأعداد العقديّة

1-1. **تعريف** : توجد مجموعة $\mathbb{C}$ تُكتبُ عناصرها، التي تُسمّى **أعداداً عقديّة**، بطريقة وحيدة بالشكل $a+\mathrm{i}b$ حيث a و b عددان حقيقيّان و i يُحقّق $\mathrm{i}^2=-1$. وهذه المجموعة مزوّدة بقانوني تشكيل داخليين هما الجمع $+$، والضرب $\times$ يجعلان من البنية $(\mathbb{C},+,\times)$ حقلاً نسميّه حقل الأعداد العقديّة.

تُعطى قواعد الحساب في $\mathbb{C}$ بالعلاقتين

$$\begin{aligned}(a+\mathrm{i}b)+(c+\mathrm{i}d)&=(a+c)+\mathrm{i}(b+d)\\(a+\mathrm{i}b)\times(c+\mathrm{i}d)&=ac+\mathrm{i}(ad+bc)+\mathrm{i}^2bd\\&=(ac-bd)+\mathrm{i}(ad+bc)\end{aligned}$$

عندما يكون $z=a+\mathrm{i}b$ عنصراً غير معدوم من $\mathbb{C}$، أي عندما لا يساوي العددان الصفر في آن معاً، يُعطى مقلوب z بالعلاقة :

$$\frac{1}{a+\mathrm{i}b}=\frac{a}{a^2+b^2}+\mathrm{i}\frac{-b}{a^2+b^2}$$

إثبات وجود حقل الأعداد العقديّة

نزوّد المجموعة $\mathbb{R}^2$ بقانوني الجمع $+$، والضرب $\times$ التاليين :

$$\begin{aligned}(a,b)+(c,d)&=(a+c,b+d)\\(a,b)\times(c,d)&=(ac-bd,ad+bc)\end{aligned}$$

فنحصل على البنية $\mathbb{C}=\left(\mathbb{R}^2,+,\times\right)$ التي نتيقّن أنّها تُحقّق الخواص المرجوّة.

- نتيقّن بالحساب أنّ القانونين $+$ و $\times$ تبديليّان وتجميعيّان، وأنّ الضرب توزيعي على الجمع.
- العنصر $(0,0)$ هو حيادي الجمع، والعنصر $(1,0)$ هو حيادي الضرب.
- لكل عنصر (a,b) نظير بالنسبة إلى قانون الجمع هو $(-a,-b)$.
- لكل عنصر (a,b) مختلف عن $(0,0)$ نظير بالنسبة إلى قانون الضرب، لأنّ

$$(a,b)\times\left(\frac{a}{a^2+b^2},-\frac{b}{a^2+b^2}\right)=(1,0)$$

- نطابق بين العنصر $(x,0)$ من $\mathbb{R}^2$ والعدد x من $\mathbb{R}$، مما يتيح لنا أن نكتب تجاوزاً $\mathbb{R}\subset\mathbb{C}$ وهذه المُطابقة لا تطرح أيّ مشكلة لأن

$$(x,0)+_{\mathbb{C}}(y,0)=(x+_{\mathbb{R}}y,0)$$

$$(x,0)\times_{\mathbb{C}}(y,0)=(x\times_{\mathbb{R}}y,0)$$

وعليه إجراء العمليّات على عددين حقيقيّين x و y لا يُعطي نتائج مختلفة، سواء نظرنا إليهما كعددين من $\mathbb{R}$ أو بوصفهما عنصرين من $\mathbb{C}$.

يمكن التعبير عمّا سبق بالقول إنّ التطبيق $\varphi:\mathbb{R}\to\mathbb{C},x\mapsto(x,0)$ تشاكلٌ حقلي متباين، مما يتيح المطابقة بين عنصرٍ x من $\mathbb{R}$ وصورته $\varphi(x)$ من $\mathbb{C}$.

- إذا عرّفنا $\mathrm{i}=(0,1)$، وجدنا $\mathrm{i}^2=(-1,0)=-1$، وأيّاً كان العدد الحقيقي y كان

$$(0,y)=(0,1)(y,0)=\mathrm{i}\,y$$

ومن ثَمّ، أيّاً كان (x,y) من $\mathbb{R}^2$، كان

$$(x,y)=(x,0)+(0,y)=x+\mathrm{i}\,y$$

1-2. تعريف : إذا كان z عدداً عقديّاً فيوجد عنصرٌ وحيدٌ (x,y) من $\mathbb{R}^2$ يُحقِّق

$$z=x+\mathrm{i}\,y$$

نسمّي x **الجزء الحقيقي** للعدد العقدي z ونرمز إليه بالرمز $\operatorname{Re}z$ أو $\operatorname{Re}(z)$. ونسمّي y **الجزء التخيّلي** للعدد العقدي z ونرمز إليه بالرمز $\operatorname{Im}z$ أو $\operatorname{Im}(z)$.

ونقول عن عدد عقدي من الشكل $\mathrm{i}\,y$ و $y\in\mathbb{R}$، إنّه **عددٌ تخيّلي صرف**. فيُكتَبُ كلُّ عددٍ عقدي بصيغة مجموع عددٍ حقيقي وعددٍ تخيّلي صرفٍ.

2. مُرافق عددٍ عقدي

2-1.تعريف. إذا كان $z = x + \mathrm{i}\,y$ عدداً عقديّاً حيث $(x,y) \in \mathbb{R}^2$ نسمّي **مُرافق** z العدد العقدي $\overline{z}$ المعرّف بالعلاقة $\overline{z} = x - \mathrm{i}\,y$.

ونترك للقارئ أن يثبت صحّة المبرهنتين التاليتين.

2-2.مبرهنة. إذا كان z عدداً عقديّاً تحقَّق ما يلي :

- $\mathrm{Re}(z) = \dfrac{z+\overline{z}}{2}$ و $\mathrm{Im}(z) = \dfrac{z-\overline{z}}{2\,\mathrm{i}}$.
- $\overline{(\overline{z})} = z$.
- يكون z عدداً حقيقيّاً إذا وفقط إذا كان $z = \overline{z}$.
- يكون z عدداً تخيُّليّاً صرفاً إذا وفقط إذا كان $z = -\overline{z}$.

2-3.مبرهنة. أيّاً كان العددان العقديّان z_1 و z_2 تحقَّق ما يلي :

- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.
- $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.
- وفي حالة $z_2 \neq 0$ يكون : $\overline{\left(\dfrac{z_1}{z_2}\right)} = \dfrac{\overline{z_1}}{\overline{z_2}}$.

3. طويلة عدد عقدي

3-1.تعريف. إذا كان z عدداً عقديّاً كان $z\overline{z}$ عدداً حقيقيّاً موجباً، وأسمينا العدد $\sqrt{z\overline{z}}$ **طويلة العدد العقدي** z ورمزنا إليه $|z|$، أي $|z| = \sqrt{z\overline{z}}$.

في الحقيقة، إذا كان $z = a + \mathrm{i}\,b$ كان $z\overline{z} = a^2 + b^2$ وهو ينتمي إلى $\mathbb{R}_+$، ومن ثمّ نجد أنّ $|z| = \sqrt{a^2 + b^2}$. ونستنتج من ذلك مباشرة الخواص التالية :

- $\big(|z| = 0\big) \Leftrightarrow \big(z = 0\big)$.
- $\forall z \in \mathbb{C},\quad |\overline{z}| = |z|$.
- $\forall z \in \mathbb{C},\quad \big|\mathrm{Re}\, z\big| \le |z|$ و $\forall z \in \mathbb{C},\quad \big|\mathrm{Im}\, z\big| \le |z|$.

هذا وتفيدنا العلاقة $z\overline{z}=|z|^2$ في التعبير عن مقلوب عددٍ عقدي غير معدوم كما يلي :

$$z\neq 0 \Rightarrow \frac{1}{z}=\frac{\overline{z}}{|z|^2}$$

ويكون

$$|z|=1 \Rightarrow \frac{1}{z}=\overline{z}$$

2-3. مبرهنة. أيّاً كان العددان العقديّان z_1 و z_2 تحقَّق ما يلي :

- $|z_1z_2|=|z_1||z_2|$.
- وفي حالة $z_2\neq 0$ يكون : $\left|\frac{z_1}{z_2}\right|=\frac{|z_1|}{|z_2|}$.
- $|z_1+z_2|\leq|z_1|+|z_2|$. متراجحة المثلّث
- $||z_1|-|z_2||\leq|z_1-z_2|$. متراجحة المثلّث الثانية

الإثبات

- في الحقيقة لدينا

$$|z_1z_2|^2=z_1z_2\overline{z_1z_2}=z_1\overline{z_1}\times z_2\overline{z_2}=|z_1|^2|z_2|^2$$

وهذا يثبت النتيجة المطلوبة لأنّ الأعداد $|z_1z_2|$ و $|z_1|$ و $|z_2|$ أعداد حقيقيّة موجبة.

- وهنا أيضاً لدينا

$$\left|\frac{z_1}{z_2}\right|^2=\frac{z_1}{z_2}\times\overline{\left(\frac{z_1}{z_2}\right)}=\frac{z_1}{z_2}\times\frac{\overline{z_1}}{\overline{z_2}}=\frac{z_1\overline{z_1}}{z_2\overline{z_2}}=\frac{|z_1|^2}{|z_2|^2}$$

وهذا يثبتُ المطلوب.

- لإثبات هذه المتراجحة نلاحظ أنّ

$$\begin{aligned}|z_1+z_2|^2&=(z_1+z_2)\overline{(z_1+z_2)}=(z_1+z_2)(\overline{z_1}+\overline{z_2})\\&=z_1\overline{z_1}+z_1\overline{z_2}+z_2\overline{z_1}+z_2\overline{z_2}\\&=|z_1|^2+z_1\overline{z_2}+\overline{z_1\overline{z_2}}+|z_2|^2\\&=|z_1|^2+2\,\mathrm{Re}(z_1\overline{z_2})+|z_2|^2\end{aligned}$$

ومن جهة أخرى

$$(|z_1|+|z_2|)^2=|z_1|^2+2|z_1||z_2|+|z_2|^2$$

إذن

$$(|z_1|+|z_2|)^2-|z_1+z_2|^2=2(|z_1\overline{z_2}|-\operatorname{Re}(z_1\overline{z_2}))$$

فإذا لاحظنا أنّ $\operatorname{Re}u\le\left|\operatorname{Re}u\right|\le|u|$ أيّاً كان u من $\mathbb{C}$، استنتجنا أنّ

$$(|z_1|+|z_2|)^2-|z_1+z_2|^2\ge 0$$

وهذا يُكافئ المتراجحة المطلوبة.

ملاحظة. تتحقّق المساواة $|z_1|+|z_2|=|z_1+z_2|$ إذا وفقط إذا كان $z_1\overline{z_2}\in\mathbb{R}_+$ وهذا يُكافئ الشرط $|z_2|z_1=|z_1|z_2$.

- بالاستفادة من المتراجحة السابقة يمكننا أن نكتب

$$|z_1|=|z_1-z_2+z_2|\le|z_1-z_2|+|z_2|$$

و

$$|z_2|=|z_2-z_1+z_1|\le|z_2-z_1|+|z_1|$$

ولأنّ $|z_2-z_1|=|z_1-z_2|$ استنتجنا أنّ

$$|z_1|-|z_2|\le|z_1-z_2| \quad \text{و} \quad |z_2|-|z_1|\le|z_1-z_2|$$

وهذا يُكافئ $|z_1-z_2|\ge\big||z_1|-|z_2|\big|$، وهي المتراجحة المطلوبة. ❐

4. زاوية عدد عقدي غير معدوم، الصيغة المثلّثيّة لعدد عقدي

1-4. رموز جديدة

- نرمز بالرمز $\mathbb{U}$ إلى مجموعة الأعداد العقديّة التي تساوي طويلتُها الواحد. وهي زمرة جزئيّة من الزمرة الضربيّة $(\mathbb{C}^*,\times)$. إذ نتيقّن بسهولة صحّة الخواص التالية :

$$1\in\mathbb{U} \quad \text{و} \quad \forall(z,z')\in\mathbb{U}^2,\ zz'\in\mathbb{U} \quad \text{و} \quad \forall z\in\mathbb{U},\ \frac{1}{z}=\overline{z}\in\mathbb{U}$$

- سنفترض أنّ القارئ على دراية بخواص تابعَيْ الجيب $\sin$، وجيب التمام $\cos$ المألوفة.
  - إذا كان θ عدداً من $\mathbb{R}$، رمزنا بالرمز $e^{i\theta}$ إلى العدد العقدي $\cos\theta+i\sin\theta$ وهو عددٌ عقدي طويلته تساوي 1، أي ينتمي إلى $\mathbb{U}$.

- وبالعكس، ليكن z عنصراً من $\mathbb{U}$، عندئذ $z = x + \mathrm{i}\,y$ مع $x^2 + y^2 = 1$. فيوجد عددٌ حقيقي θ يُحقّق $x = \cos\theta$ و $y = \sin\theta$. أي $z = e^{\mathrm{i}\theta}$.

في الحقيقة، نعلم أنّ تابع جيب التمام $\cos$ يأخذ جميع القيم في المجال $[-1,1]$، فيوجد عددٌ φ ينتمي إلى $[0,\pi]$، يُحقِّق $\cos\varphi = x$. وعندئذ يكون لدينا

$$\sin^2\varphi = 1 - \cos^2\varphi = 1 - x^2 = y^2$$

- فإذا كان $y = \sin\varphi$ أخذنا $\theta = \varphi$ وتمّ الإثبات.
- وإذا كان $y = -\sin\varphi$، أخذنا $\theta = -\varphi$ وتمّ الإثبات أيضاً في هذه الحالة.

- نلاحظ استناداً إلى تعريف $e^{\mathrm{i}\theta}$ أنّه في حالة $\theta = 0$ يكون $e^{\mathrm{i}\theta} = 1$ وهذا يتّفق مع دلالة الكتابة $e^0 = 1$ المعروفة لدى القارئ من دراسته للتابع الأسّي المعرّف على $\mathbb{R}$.
- لقد جرت العادة أن نكتب $e^{-\mathrm{i}\theta}$ دلالة على $e^{\mathrm{i}(-\theta)}$، في حالة $\theta \in \mathbb{R}$. ونرى مباشرة أنّ $\overline{\left(e^{\mathrm{i}\theta}\right)} = e^{-\mathrm{i}\theta}$.

بالاستفادة من الرموز السابقة يمكننا أن نستنتج مباشرة النتيجة التالية.

2-4. مبرهنة. دستورا أويلر Euler . أيّاً كان العدد θ من $\mathbb{R}$، كان

$$\sin\theta = \frac{e^{\mathrm{i}\theta} - e^{-\mathrm{i}\theta}}{2\,\mathrm{i}} \quad \text{و} \quad \cos\theta = \frac{e^{\mathrm{i}\theta} + e^{-\mathrm{i}\theta}}{2}$$

3-4. مبرهنة. أيّاً كان العددان θ و φ من $\mathbb{R}$، كان

1. $e^{\mathrm{i}\theta} \times e^{\mathrm{i}\varphi} = e^{\mathrm{i}(\theta+\varphi)}$
2. $\left(e^{\mathrm{i}\theta} = e^{\mathrm{i}\varphi}\right) \Leftrightarrow \left(\exists k \in \mathbb{Z}, \theta = \varphi + 2\pi k\right)$

الإثبات

1. ليكن θ و φ عددين حقيقيّين، عندئذ

$$\begin{aligned} e^{\mathrm{i}\theta} \times e^{\mathrm{i}\varphi} &= \left(\cos\theta + \mathrm{i}\sin\theta\right)\left(\cos\varphi + \mathrm{i}\sin\varphi\right) \\ &= \left(\cos\theta\cos\varphi - \sin\theta\sin\varphi\right) + \mathrm{i}\left(\cos\theta\sin\varphi + \sin\theta\cos\varphi\right) \\ &= \cos\left(\theta+\varphi\right) + \mathrm{i}\sin\left(\theta+\varphi\right) = e^{\mathrm{i}\left(\theta+\varphi\right)} \end{aligned}$$

2. ومن جهة أخرى، بضرب طرفي المساواة $e^{\mathrm{i}\theta} = e^{\mathrm{i}\varphi}$ بالعدد $e^{-\mathrm{i}\varphi} \neq 0$ نجد

$$\begin{aligned}\left(e^{\mathrm{i}\theta}=e^{\mathrm{i}\varphi}\right) &\Leftrightarrow \left(e^{\mathrm{i}(\theta-\varphi)}=1\right)\\ &\Leftrightarrow (\cos(\theta-\varphi)=1)\wedge(\sin(\theta-\varphi)=0)\\ &\Leftrightarrow (\exists k\in\mathbb{Z},\ \theta-\varphi=2\pi k)\end{aligned}$$

وهي النتيجة المرجوّة. ❐

ملاحظة. يمكن التعبير عمّا سبق بالقول إنّ التطبيق

$$\mathcal{E}:(\mathbb{R},+)\to(\mathbb{U},\times),\theta\mapsto e^{\mathrm{i}\theta}$$

تشاكلٌ زمري غامرٌ، نواته $2\pi\mathbb{Z}=\{2\pi k : k\in\mathbb{Z}\}$.

بالاستفادة من المبرهنة السابقة، نبرهن، بالتدريج على العدد n، أنّه مهما تكن n من $\mathbb{N}$ يكن

$$\forall\theta\in\mathbb{R},\quad \left(e^{\mathrm{i}\theta}\right)^n=e^{\mathrm{i}n\theta}$$

وهي تبقى صحيحة في حالة $n\in\mathbb{Z}$ لأنّه في حالة $n<0$ نكتب

$$\left(e^{\mathrm{i}\theta}\right)^n=\left(\frac{1}{e^{\mathrm{i}\theta}}\right)^{-n}=\left(e^{\mathrm{i}(-\theta)}\right)^{-n}=e^{\mathrm{i}(-\theta)(-n)}=e^{\mathrm{i}\theta n}$$

وتُكتب هذه النتيجة بالصيغة المُكافئة التالية.

4-4. مبرهنة. دستور دوموافر De Moivre. أيّاً كان θ من $\mathbb{R}$، وأيّاً كان n من $\mathbb{Z}$، كان

$$(\cos\theta+\mathrm{i}\sin\theta)^n=\cos n\theta+\mathrm{i}\sin n\theta$$

5-4. مثال. ليكن θ عدداً من المجال $]0,2\pi[$، لنختزل المجموع $S=\sum_{k=0}^{n}\cos k\theta$. لمّا كان

$$S=\operatorname{Re}\left(\sum_{k=0}^{n}e^{\mathrm{i}k\theta}\right)$$

بدأنا بحساب المقدار $\sum_{k=0}^{n}e^{\mathrm{i}k\theta}$ الذي يساوي مجموع أوّل $n+1$ حدّاً من متتالية هندسيّة أساسها $e^{\mathrm{i}\theta}$ وهو لا يساوي 1. إذن

$$\sum_{k=0}^{n}e^{\mathrm{i}k\theta}=\frac{1-e^{\mathrm{i}(n+1)\theta}}{1-e^{\mathrm{i}\theta}}$$

لنُعِد صياغة هذه النتيجة كما يلي :

$$\begin{aligned}\frac{1-e^{\mathrm{i}(n+1)\theta}}{1-e^{\mathrm{i}\theta}} &= \frac{e^{\mathrm{i}(n+1)\frac{\theta}{2}}}{e^{\mathrm{i}\frac{\theta}{2}}} \times \frac{e^{\mathrm{i}(n+1)\frac{\theta}{2}} - e^{-\mathrm{i}(n+1)\frac{\theta}{2}}}{e^{\mathrm{i}\frac{\theta}{2}} - e^{-\mathrm{i}\frac{\theta}{2}}} \\ &= e^{\mathrm{i}n\frac{\theta}{2}} \times \frac{2\mathrm{i}\sin\left((n+1)\frac{\theta}{2}\right)}{2\mathrm{i}\sin\frac{\theta}{2}} \\ &= e^{\mathrm{i}n\frac{\theta}{2}} \times \frac{\sin\left((n+1)\frac{\theta}{2}\right)}{\sin\frac{\theta}{2}}\end{aligned}$$

ومنه نجد العبارة المختزلة التالية للمجموع S.

$$S = \mathrm{Re}\left(\frac{1-e^{\mathrm{i}(n+1)\theta}}{1-e^{\mathrm{i}\theta}}\right) = \frac{\sin\left((n+1)\frac{\theta}{2}\right)\cos\left(n\frac{\theta}{2}\right)}{\sin\frac{\theta}{2}}$$

ليكن z عدداً عقديّاً غير معدوم. عندئذ تساوي طويلةُ العدد $\dfrac{z}{|z|}$ الواحد، فيوجد عددٌ θ من $\mathbb{R}$ يُحقّق $\dfrac{z}{|z|} = e^{\mathrm{i}\theta}$. ومن ثَمّ يكون

$$z = re^{\mathrm{i}\theta} \quad \text{حيث} \quad r = |z| > 0$$

ومنه التعريف الآتي.

4-6. تعريف. ليكن z عدداً عقديّاً **غير صفري**. عندئذ نسمّي كلَّ عدد حقيقي θ يُحقّق المساواة $z = |z|e^{\mathrm{i}\theta}$ **زاويةً** للعدد العقدي z. وإذا كانت θ_0 زاويةً ما للعدد العقدي z كان

$$\left(z = |z|e^{\mathrm{i}\theta}\right) \Leftrightarrow \left(\theta \in \left\{\theta_0 + 2\pi k : k \in \mathbb{Z}\right\}\right)$$

ونرمز عادة بالرمز $\arg(z)$ إلى مجموعة زوايا العدد العقدي z، أي

$$\arg(z) = \left\{\theta_0 + 2\pi k : k \in \mathbb{Z}\right\}$$

وعليه، في حالة z من $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$، يتحقّق التكافؤ التالي

$$\left(\theta \in \arg(z)\right) \Leftrightarrow \left(z = |z|\, e^{\mathrm{i}\theta}\right)$$

4-7. مثال. لتكن θ من $[0,2\pi[$. ولنحسب طويلة العدد العقدي $z = 1 + e^{\mathrm{i}\theta}$، ولنعيّن زاويةً له. في الحقيقة،

$$z = 1 + e^{\mathrm{i}\theta} = \left(e^{\mathrm{i}\frac{\theta}{2}} + e^{-\mathrm{i}\frac{\theta}{2}}\right)e^{\mathrm{i}\frac{\theta}{2}} = 2\cos\left(\tfrac{\theta}{2}\right)\cdot e^{\mathrm{i}\frac{\theta}{2}}$$

وهنا نناقش الحالات الآتية.

- إذا كان $\theta \in [0,\pi[$ كان $|z| = 2\cos\left(\frac{\theta}{2}\right)$ و $\frac{\theta}{2} \in \arg(z)$.
- إذا كان $\theta = \pi$ كان $z = 0$.
- إذا كان $\theta \in]\pi,2\pi]$ كان $|z| = -2\cos\left(\frac{\theta}{2}\right)$ و $\frac{\theta}{2} + \pi \in \arg(z)$.

8-4. مبرهنة. ليكن z_1 و z_2 عددين عقديَّين **غير صفريين**. نفترض أنّ $z_1 = r_1 e^{i\theta_1}$ و $z_2 = r_2 e^{i\theta_2}$. عندئذ يكون لدينا

$$z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)} \quad \text{و} \quad \frac{z_1}{z_2} = \frac{r_1}{r_2} e^{i(\theta_1-\theta_2)}$$

في حالة مجموعتين جزئيّتين غير خاليتين A و B من $\mathbb{C}$، نكتب $A+B$ و $A-B$ دلالة على ما يلي :

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

$$A - B = \{a - b : a \in A, b \in B\}$$

وهذا يتيح لنا أن نكتب النتيجة الآتية.

9-4. نتيجة. ليكن z_1 و z_2 عددين عقديَّين **غير صفريين**. عندئذ

$$\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$$

$$\arg\left(\frac{z_1}{z_2}\right) = \arg(z_1) - \arg(z_2)$$

الإثبات

لنفترض أنّ $\theta_1 \in \arg(z_1)$ و $\theta_2 \in \arg(z_2)$. عندئذ

$$\arg(z_1) = \{\theta_1 + 2\pi k : k \in \mathbb{Z}\}$$

$$\arg(z_2) = \{\theta_2 + 2\pi \ell : \ell \in \mathbb{Z}\}$$

ومن ثَمّ نستنتج مباشرة أنّ

$$\arg(z_1) + \arg(z_2) = \left\{\theta_1 + \theta_2 + 2\pi k' : k' \in \mathbb{Z}\right\}$$

$$\arg(z_1) - \arg(z_2) = \left\{\theta_1 - \theta_2 + 2\pi \ell' : \ell' \in \mathbb{Z}\right\}$$

ولمّا كانت $\theta_1 + \theta_2$ زاوية للعدد العقدي $z_1 z_2$، و $\theta_1 - \theta_2$ زاوية للعدد العقدي $\frac{z_1}{z_2}$، استنتجنا المطلوب. ❐

5. التابع الأسّي لمتحوّل عقدي

نفترض في هذه الفقرة أنّ خواص التابع الأسّي لمتحوّل حقيقي $x \mapsto e^x$ معروفة.

5-1. تعريف. ليكن $z = x + \mathrm{i}\,y$ عدداً عقديّاً، $\big((x,y) \in \mathbb{R}^2\big)$، نرمز بالرمز e^z أو $\exp(z)$ إلى العدد العقدي $e^x e^{\mathrm{i}\,y}$.

يُمدِّد التابع $z \mapsto e^z$ التابع الأسّي المألوف إلى $\mathbb{C}$، لأنّه في حالة $y = 0$ لدينا $e^{\mathrm{i}\,y} = 1$. ونجد فيما يلي بعض خواص التابع $z \mapsto e^z$.

5-2. مبرهنة

- ليكن z عدداً عقديّاً، عندئذ $|e^z| = e^{\operatorname{Re} z}$ و $\operatorname{Im} z \in \arg(e^z)$. وبوجه خاص $\forall z \in \mathbb{C},\ e^z \neq 0$.
- أيّاً كان (z,w) من $\mathbb{C}^2$ كان $e^z e^w = e^{z+w}$. وبوجه خاص $\dfrac{1}{e^z} = e^{-z}$.
- أيّاً كان ω من $\mathbb{C}^*$ يوجد z_0 في $\mathbb{C}$ يُحقّق $e^{z_0} = \omega$ وعندئذ تُعطى مجموعة حلول المعادلة $e^z = \omega$ بالصيغة $\{z_0 + 2\mathrm{i}\,\pi k : k \in \mathbb{Z}\}$.

الإثبات

- إذا كان $z = x + \mathrm{i}\,y$ حيث (x,y) من $\mathbb{R}^2$ كان $e^z = e^x \cdot e^{\mathrm{i}\,y}$ و $e^x > 0$. وهذا ما يثبت الخاصّة الأولى.
- إذا كان $z = x + \mathrm{i}\,y$ مع (x,y) من $\mathbb{R}^2$، و $w = u + \mathrm{i}\,v$ حيث (u,v) من $\mathbb{R}^2$، كان

$$e^z e^w = e^x e^{\mathrm{i}\,y} e^u e^{\mathrm{i}\,v} = e^x e^u e^{\mathrm{i}\,y} e^{\mathrm{i}\,v} = e^{x+u} e^{\mathrm{i}(y+v)} = e^{z+w}$$

وتنتج الخاصّة الثانية من كون

$$e^z e^{-z} = e^{z-z} = e^0 = 1.$$

- لمّا كان ω عدداً عقديّاً غير صفري أمكننا كتابته بالشكل $\omega = re^{\mathrm{i}\,\theta}$ مع $r > 0$. لنبحث إذن عن حلول المعادلة $e^z = \omega$.

- ليكن $z = x + \mathrm{i}\,y$ حيث (x,y) من $\mathbb{R}^2$، ولنفترض أنّ $e^z = \omega$ عندئذ يكون لدينا $r = |\omega| = \left|e^z\right| = e^x$، ومن ثَمَّ $x = \ln r$. إذن تؤول المعادلة $e^z = \omega$ إلى $e^{\mathrm{i}y} = e^{\mathrm{i}\theta}$ وهذا يقتضي أنّ $y \in \{\theta + 2\pi k : k \in \mathbb{Z}\}$، فإذا عرّفنا، في حالة k من $\mathbb{Z}$، المقدار $z_k = \ln r + \mathrm{i}\,\theta + 2\,\mathrm{i}\,\pi k$، استنتجنا مما سبق أنّ
$$z \in \{z_k : k \in \mathbb{Z}\}$$
- وبالعكس، جميع الأعداد z_k حيث $k \in \mathbb{Z}$ هي حلول للمعادلة $e^z = \omega$. ❐

3-5. ملاحظات

❶ ينتج مما سبق أنّ التابع $\exp : \mathbb{C} \to \mathbb{C}^*, z \mapsto e^z$ تابعٌ غامرٌ وهو يعرّف تشاكلاً زمريّاً من $(\mathbb{C},+)$ إلى $(\mathbb{C}^*,\times)$.

❷ ونستنتج أيضاً أنّ مجموعة حلول المعادلة $e^z = \omega$ في حالة $\omega \neq 0$ هي
$$\left\{\ln\left|\omega\right| + \mathrm{i}\,\theta : \theta \in \arg(\omega)\right\}$$
وهذا يبيِّن عدم إمكان تعريف تابع لوغاريتمي، كما في حالة الأعداد الحقيقيّة، لأنّ التابع الأسّي لمتحول عقدي ليس تقابلاً.

6. تطبيقات الأعداد العقديّة في النسب المثلّثيّة

تُعَدّ الأعداد العقديّة مفيدة جدّاً في العديد من الحسابات المتعلّقة بالنسب المثلثيّة، فما دستورَا الجمع:
$$\cos(a+b) = \cos a \cos b - \sin a \sin b$$
$$\sin(a+b) = \sin a \cos b + \cos a \sin b$$
إلاّ كتابة مُكافئة للجزأين الحقيقي والتخيّلي للمقدار $e^{\mathrm{i}a}e^{\mathrm{i}b}$.

1-6. تحويل المقدار $\cos^m\theta\sin^n\theta$ إلى عبارة خطيّة بالنسب المثلّثية لمضاعفات θ

إنّ هذا التحويل مفيد عموماً، وبوجه خاصّ عند البحث عن توابع أصليّة أو مشتقّات من مراتب عليا لصيغ من هذا النمط. لنوضّح الطريقة المُقترحة بتحويل الصيغة $\sin^6\theta$. في الحقيقة نستفيد من دستورَي أويلر فنكتب
$$\sin^6\theta = \left(\frac{e^{\mathrm{i}\theta} - e^{-\mathrm{i}\theta}}{2\,\mathrm{i}}\right)^6 = -\frac{1}{64}\left(e^{\mathrm{i}\theta} - e^{-\mathrm{i}\theta}\right)^6$$

وبنشر الطرف الثاني مستفيدين من دستور ثنائي الحدِّ نجد

$$\begin{aligned}\sin^6\theta &= \frac{-1}{64}\big(e^{6i\theta} - 6e^{4i\theta} + 15e^{2i\theta} - 20 + 15e^{-2i\theta} - 6e^{-4i\theta} + e^{-6i\theta}\big)\\ &= \frac{-1}{64}\Big((e^{6i\theta}+e^{-6i\theta}) - 6(e^{4i\theta}+e^{-4i\theta}) + 15(e^{2i\theta}+e^{-2i\theta}) - 20\Big)\\ &= \frac{-1}{32}(\cos 6\theta - 6\cos 4\theta + 15\cos 2\theta - 10)\end{aligned}$$

2-6. حساب $\cos n\theta$ و $\sin n\theta$ بدلالة $\cos\theta$ و $\sin\theta$

فمثلاً للتعبير عن $\cos 4\theta$ و $\sin 4\theta$ بدلالة $\cos\theta$ و $\sin\theta$ نبدأ بكتابة دستور دوموافر :

$$(\cos\theta + i\sin\theta)^4 = \cos 4\theta + i\sin 4\theta$$

ثُمّ بعد نشر الطرف الأيسر مستفيدين من دستور ثنائي الحدِّ، نفصل الجزأين الحقيقي والتخيلي. وهكذا نجد

$$\cos 4\theta = \cos^4\theta - 6\cos^2\theta\sin^2\theta + \sin^4\theta$$

$$\sin 4\theta = 4\cos^3\theta\sin\theta - 4\cos\theta\sin^3\theta$$

وإذا استفدنا من العلاقة $\sin^2\theta = 1 - \cos^2\theta$ وجدنا العبارة التالية للمقدار $\cos 4\theta$:

$$\cos 4\theta = 1 - 8\cos^2\theta + 8\cos^4\theta$$

ونجد بأسلوب مماثل، بعد إخراج العامل المشترك $\sin\theta$، ما يلي :

$$\sin 4\theta = 4\sin\theta\big(2\cos^3\theta - \cos\theta\big)$$

وهذا يتيح لنا أيضاً أن نوجد عبارة $\tan 4\theta$ بدلالة $\tan\theta$، إذ ننطلق من الصيغتين

$$\cos 4\theta = \cos^4\theta - 6\cos^2\theta\sin^2\theta + \sin^4\theta$$

$$\sin 4\theta = 4\cos^3\theta\sin\theta - 4\cos\theta\sin^3\theta$$

ونستنتج أنّ

$$\begin{aligned}\tan 4\theta &= \frac{4\cos^3\theta\sin\theta - 4\cos\theta\sin^3\theta}{\cos^4\theta - 6\cos^2\theta\sin^2\theta + \sin^4\theta}\\ &= \frac{4\tan\theta - 4\tan^3\theta}{1 - 6\tan^2\theta + \tan^4\theta}\end{aligned}$$

وذلك بعد قسمة البسط والمقام على $\cos^4\theta$.

7. حلُّ بعض المعادلات الجبريّة في $\mathbb{C}$

1-7. تعريف. نسمّي **جذراً تربيعيّاً** لعدد عقدي a، كلَّ عددٍ عقدي z يُحقّق $z^2 = a$.

2-7. مبرهنة. لكلِّ عددٍ عقدي غير معدوم جذران تربيعيّان وجذران تربيعيّان فقط. أحدهما نظير الآخر بالنسبة إلى الجمع.

الإثبات

ليكن a عدداً عقديّاً غير صفري. عندئذ يُكتب a بالشكل $a = re^{\mathrm{i}\theta}$ مع $r = |a| > 0$.

نعرّف عندئذ $z = \sqrt{r}\, e^{\mathrm{i}\frac{\theta}{2}}$ فنجد مباشرة أنّ $z^2 = \left(\sqrt{r}\right)^2 e^{2\mathrm{i}\frac{\theta}{2}} = re^{\mathrm{i}\theta} = a$ أي إنّ z جذرٌ تربيعي للعدد a.

وإذا كان $\omega^2 = a$ كان $\omega^2 - z^2 = 0$ أو $(\omega - z)(\omega + z) = 0$ فتكون مجموعة الجذور التربيعيّة للعدد a هي $\{z, -z\}$. ❐

3-7. أمثلة وملاحظات

❶ الجذران التربيعيّان لعدد حقيقي موجب تماماً a هما $\sqrt{a}$ و $-\sqrt{a}$.

❷ الجذران التربيعيّان لعدد حقيقي سالب تماماً a هما $\mathrm{i}\sqrt{-a}$ و $-\mathrm{i}\sqrt{-a}$.

❸ لا معنى للرمز $\sqrt{a}$ إلاّ في حالة $a \in \mathbb{R}_+$.

❹ هناك أيضاً طريقة جبريّة تفيد في حساب الجذور التربيعيّة لعدد عقدي $a = \alpha + \mathrm{i}\beta$. في حالة $\mathrm{Im}(a) = \beta \neq 0$ فالمطلوب تعيين عددٍ $z = x + \mathrm{i}y$ يُحقِّق $z^2 = a$. وهذا يُكافئ

$$x^2 - y^2 + 2\mathrm{i}xy = \alpha + \mathrm{i}\beta$$

أي

$$x^2 - y^2 = \alpha \quad \text{و} \quad 2xy = \beta$$

ونستنتج من العلاقة $|z|^2 = |a|$ أيضاً أنّ $x^2 + y^2 = \sqrt{\alpha^2 + \beta^2}$ ومنه

$$x^2 = \frac{1}{2}\left(\sqrt{\alpha^2 + \beta^2} + \alpha\right) \quad \text{و} \quad 2xy = \beta$$

وعليه

$$x = \frac{\varepsilon}{\sqrt{2}} \cdot \sqrt{\sqrt{\alpha^2 + \beta^2} + \alpha} \quad \text{و} \quad y = \frac{\varepsilon}{\sqrt{2}} \cdot \frac{\beta}{\sqrt{\sqrt{\alpha^2 + \beta^2} + \alpha}}$$

حيث $\varepsilon \in \{-1,1\}$.

والجذران التربيعيّان للعدد a في حالة $\operatorname{Im}(a) \neq 0$ هما z و $-z$ حيث

$$z = \frac{1}{\sqrt{2}}\left(\sqrt{|a| + \operatorname{Re}(a)} + \mathrm{i}\frac{\operatorname{Im}(a)}{\sqrt{|a| + \operatorname{Re}(a)}}\right)$$

فمثلاً في حالة $a = \frac{1+\mathrm{i}}{\sqrt{2}} = e^{\mathrm{i}\frac{\pi}{4}}$ نستنتج أنّ الجذر التربيعي للعدد a الذي جزؤه الحقيقي موجبٌ يساوي من جهة أولى $e^{\mathrm{i}\frac{\pi}{8}} = \cos\frac{\pi}{8} + \mathrm{i}\sin\frac{\pi}{8}$ ويساوي من جهة ثانية

$$\frac{1}{\sqrt{2}}\left(\sqrt{1 + \frac{1}{\sqrt{2}}} + \mathrm{i}\frac{\frac{1}{\sqrt{2}}}{\sqrt{1 + \frac{1}{\sqrt{2}}}}\right) = \frac{\sqrt{2+\sqrt{2}}}{2} + \mathrm{i}\frac{\sqrt{2-\sqrt{2}}}{2}$$

إذن

$$\sin\left(\frac{\pi}{8}\right) = \frac{\sqrt{2-\sqrt{2}}}{2} \quad \text{و} \quad \cos\left(\frac{\pi}{8}\right) = \frac{\sqrt{2+\sqrt{2}}}{2}$$

ومنه

$$\tan\left(\frac{\pi}{8}\right) = \sqrt{2} - 1 \; .$$

4-7. مبرهنة. لتكن a و b و c ثلاثة أعداد عقديّة، و $a \neq 0$. نتأمّل المعادلة

$$az^2 + bz + c = 0 \qquad (\mathcal{E})$$

والمميِّز $\Delta = b^2 - 4ac$.

① إذا كان $\Delta \neq 0$ ، ورمزنا بالرمز δ إلى جذرٍ تربيعي للعدد Δ ،كانت جذور المعادلة $(\mathcal{E})$ مكوّنة من الجذرين المختلفين $\frac{-b+\delta}{2a}$ و $\frac{-b-\delta}{2a}$.

② وإذا كان $\Delta = 0$ كان للمعادلة $(\mathcal{E})$ جذر وحيد مضاعف هو $-\frac{b}{2a}$.

الإثبات

لنلاحظ أنّ

$$az^2 + bz + c = a\left(\left(z + \frac{b}{2a}\right)^2 + \frac{c}{a} - \frac{b^2}{4a^2}\right) = a\left(\left(z + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right)$$

إذن

$$\begin{aligned} az^2+bz+c &= a\left(\left(z+\frac{b}{2a}\right)^2-\left(\frac{\delta}{2a}\right)^2\right)\\ &= a\left(z+\frac{b-\delta}{2a}\right)\left(z+\frac{b+\delta}{2a}\right)\end{aligned}$$

وأخيراً

$$\left(az^2+bz+c=0\right)\Leftrightarrow\left(z=\frac{-b+\delta}{2a}\right)\vee\left(z=\frac{-b-\delta}{2a}\right)$$

وهذا يثبت المطلوب. ❐

7-5. نتيجة. لتكن a و b و c ثلاثة أعداد حقيقيّة، و $a\neq 0$. نتأمّل المعادلة

$$az^2+bz+c=0 \qquad (\mathcal{E})$$

والمميِّز $\Delta=b^2-4ac$.

① إذا كان $\Delta>0$، كان للمعادلة $(\mathcal{E})$ جذران حقيقيّان مختلفان.

② وإذا كان $\Delta=0$ كان للمعادلة $(\mathcal{E})$ جذرٌ حقيقي وحيدٌ مضاعف.

③ وإذا كان $\Delta<0$ كان للمعادلة $(\mathcal{E})$ جذران عقديّان مختلفان مترافقان.

7-6. مبرهنة. لتكن a و b و c ثلاثة أعداد عقديّة، و $a\neq 0$. عندئذ يُحقِّق العددان العقديّان z_1 و z_2 العلاقتين

$$z_1z_2=\frac{c}{a} \quad \text{و} \quad z_1+z_2=-\frac{b}{a}$$

إذا وفقط إذا كانا جذري المعادلة $az^2+bz+c=0$.

الإثبات

الإثبات بسيطٌ نتركه تمريناً للقارئ. ❐

7-7. تعريف. ليكن n عدداً طبيعيّاً غير صفري. نسمّي **جذراً من المرتبة n لعدد عقدي a**، كلَّ عددٍ عقدي z يُحقّق $z^n=a$.

7-8. مبرهنة. ليكن n عدداً طبيعيّاً غير صفري. إنّ عدد الجذور من المرتبة n للواحد يساوي n وهذه الجذور هي $\{\omega_k : k\in\{0,1,\ldots,n-1\}\}$ حيث

$$\omega_k=\exp\left(\mathrm{i}\tfrac{2k\pi}{n}\right)=(\omega_1)^k$$

الإثبات

ليكن $\omega = \rho e^{\mathrm{i}\varphi}$ عدداً عقديّاً، $\rho \in \mathbb{R}_+$ و $\varphi \in \mathbb{R}$. عندئذ

$$\begin{aligned}\omega^n = 1 &\Leftrightarrow \rho^n e^{\mathrm{i}n\varphi} = 1\\ &\Leftrightarrow (\rho^n = 1) \wedge (n\varphi = 0 \bmod 2\pi)\\ &\Leftrightarrow (\rho = 1) \wedge (\exists k \in \mathbb{Z}, n\varphi = 2\pi k)\\ &\Leftrightarrow (\rho = 1) \wedge \left(\exists k \in \mathbb{Z}, \varphi = \frac{2\pi k}{n}\right)\\ &\Leftrightarrow \exists k \in \mathbb{Z}, \omega = \exp\left(\mathrm{i}\frac{2\pi k}{n}\right)\end{aligned}$$

إذن لنعرّف $\omega_k = \exp\left(\mathrm{i}\frac{2\pi k}{n}\right)$ في حالة k من $\mathbb{Z}$ فنكون قد أثبتنا أنّ

$$\omega^n = 1 \Leftrightarrow \omega \in \{\omega_k : k \in \mathbb{Z}\}$$

لنبرهن أنّ

$$\{\omega_k : k \in \mathbb{Z}\} = \{\omega_r : r \in \{0,1,\ldots,n-1\}\}$$

في الحقيقة، ليكن k من $\mathbb{Z}$. بإجراء قسمة إقليديّة للعدد k على n نستنتج وجود q و r في $\mathbb{Z}$ يُحقّقان $k = qn + r$ و $0 \leq r < n$.

وعندئذ يكون لدينا

$$\begin{aligned}\omega_k &= \exp\left(\mathrm{i}\frac{2\pi k}{n}\right) = \exp\left(\mathrm{i}\frac{2\pi(qn+r)}{n}\right)\\ &= \exp\left(\mathrm{i}2\pi q + \mathrm{i}\frac{2\pi r}{n}\right) = \exp\left(\mathrm{i}\frac{2\pi r}{n}\right) = \omega_r\end{aligned}$$

فنكون قد أثبتنا أنّ

$$\{\omega_k : k \in \mathbb{Z}\} \subset \{\omega_r : r \in \{0,1,\ldots,n-1\}\}$$

أمّا الاحتواء المُعاكس فهو مُحقّق وضوحاً. مما يُثبت المساواة المرجوّة.

بقي أن نثبتَ أنّ الأعداد $\omega_0, \omega_1, \ldots, \omega_{n-1}$ مختلفة مثنى مثنى. في الحقيقة إذا كان k و ℓ عددين من المجموعة $\{0,1,\ldots,n-1\}$ يُحقّقان $\omega_k = \omega_\ell$ أي

$$\exp\left(\mathrm{i}\frac{2\pi k}{n}\right) = \exp\left(\mathrm{i}\frac{2\pi \ell}{n}\right)$$

فيوجد q في $\mathbb{Z}$ يُحقِّق

$$\frac{2\pi k}{n}=\frac{2\pi\ell}{n}+2\pi q$$

ومن ثَمّ $k-\ell=qn$.

ولكن $|k-\ell|<n$ لأنّ k و ℓ عددين من المجموعة $\{0,1,\ldots,n-1\}$ إذن العدد q يُحقّق $|q|<1$ ومنه $q=0$، أو $k=\ell$. ❐

7-9. **مبرهنة**. ليكن n عدداً طبيعيّاً غير صفري. ولتكن $\mathbb{U}_n$ مجموعة الجذور من المرتبة n للواحد. عندئذ تكون $(\mathbb{U}_n,\times)$ زمرة جزئيّة من $(\mathbb{C}^*,\times)$. أي إنّ العدد 1 ينتمي إلى $\mathbb{U}_n$، وجداء عنصرين من $\mathbb{U}_n$ ينتمي إلى $\mathbb{U}_n$، ومقلوب عنصرٍ من $\mathbb{U}_n$ ينتمي إلى $\mathbb{U}_n$.

الإثبات

الإثبات تحقُّقٌ بسيطٌ نتركه تمريناً للقارئ. ❐

7-10. **مبرهنة**. ليكن n عدداً طبيعيّاً غير صفري. وليكن a عدداً عقديّاً غير معدوم. إذا كان z_0 جذراً من المرتبة n للعدد a، كانت مجموعة الجذور من المرتبة n للعدد a هي $\{\,z_0\omega : \omega\in\mathbb{U}_n\,\}$.

وإذا كان $a=re^{\mathrm{i}\theta}$ حيث $r=|a|>0$ كانت مجموعة الجذور من المرتبة n للعدد a هي

$$\left\{\sqrt[n]{r}\exp\left(\mathrm{i}\left(\tfrac{\theta}{n}+\tfrac{2\pi k}{n}\right)\right) : k\in\{0,1,\ldots,n-1\}\right\}.$$

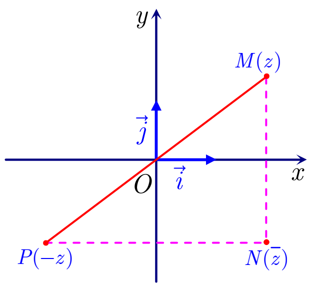
الإثبات

الإثبات تحقُّقٌ بسيطٌ نتركه تمريناً للقارئ. ❐

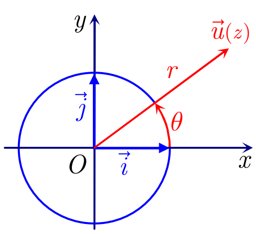
8. بعض تطبيقات الأعداد العقديّة في الهندسة المستوية

المستوي العقدي، أو مستوي Argand- Cauchy

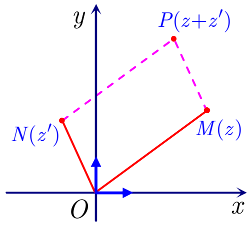
نفترض المستوي $\mathcal{P}$ منسوباً إلى مَعْلَمٍ متجانس $(O,\vec{i},\vec{j})$. نقرن بكلِّ عدد $z = x + \mathrm{i}\,y$ من $\mathbb{C}$ النقطة M التي إحداثيّاتها هي (x,y) في المَعلم $(O,\vec{i},\vec{j})$، ونقول عندئذ إنّ M هي صورة العدد العقدي z، أو إنّ z هو العدد العقدي المُمثِّل للنقطة M. ونكتب $M(z)$ أو $M\,(x,y)$ دون تمييز بين الكتابتين. ونقرن أيضاً بكلِّ عدد $z = x + \mathrm{i}\,y$ من $\mathbb{C}$ الشعاع $\vec{U} = x\vec{i} + y\vec{j}$ أي الشعاع الذي مركّباته (x,y). ونكتب $\vec{U}(z)$ أو $\vec{U}(x,y)$ دون تمييز بين الكتابتين. وهكذا نعرّف تقابلاً بين المستوي $\mathcal{P}$ وحقل الأعداد العقديّة $\mathbb{C}$، وكذلك نعرّف تقابلاً بين الفضاء الشعاعي $\mathbb{R}^2$ و $\mathbb{C}$.



- صورة العدد 0 هي نقطة المبدأ O.
- إذا كان z عدداً حقيقيّاً انتمت النقطة $M(z)$ إلى محور الفواصل Ox.
- وإذا كان z عدداً تخيّلياً صرفاً انتمت النقطة $M(z)$ إلى محور التراتيب Oy.
- للعددين z و $\bar{z}$ صورتان $M(z)$ و $N(\bar{z})$ متناظرتان بالنسبة إلى محور الفواصل.
- وللعددين z و $-z$ صورتان $M(z)$ و $P(-z)$ متناظرتان بالنسبة إلى المبدأ.



- إذا كان z عدداً عقديّاً غير صفري يمثّل شعاعاً $\vec{u}$. كان
$$\|\vec{u}\| = |z| \quad \text{و} \quad (\vec{i},\vec{u}) \in \arg(z)$$
أي إذا كان $z = re^{\mathrm{i}\,\theta}$ كان
$$\|\vec{u}\| = r \quad \text{و} \quad (\vec{i},\vec{u}) = \theta \bmod 2\pi$$
وقد رمزنا بالرمز $(\vec{i},\vec{u})$ إلى الزاوية الموجّهة للشعاعين $\vec{i}$ و $\vec{u}$ بهذا الترتيب. وإذا كانت M النقطة صورة العدد z، كان
$$OM = |z| \quad \text{و} \quad (\vec{i},\overrightarrow{OM}) \in \arg(z)$$

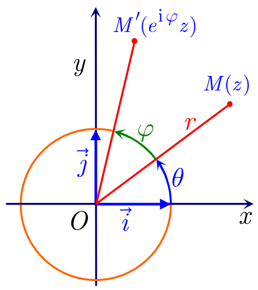


- أيّاً كان z و z' من $\mathbb{C}$ كانت صورة العدد $z+z'$ هي النقطة P المعرّفة بالعلاقة $\overrightarrow{OP}=\overrightarrow{OM}+\overrightarrow{ON}$، حيث M هي صورة z و N هي صورة z'. أي

$$\overrightarrow{OP(z+z')}=\overrightarrow{OM(z)}+\overrightarrow{ON(z')}$$

وبصيغة أخرى، إذا كان العددان z و z' من $\mathbb{C}$ يمثّلان الشعاعين $\vec{u}$ و $\vec{u}'$ على الترتيب مثّل العدد $z+z'$ الشعاع $\vec{u}+\vec{u}'$.

- فمثلاً، إذا كانت A صورة العدد العقدي z_A، وكانت B صورة العدد العقدي z_B مثّل العدد العقدي z_B-z_A الشعاع $\overrightarrow{AB}$ ومثّل العدد العقدي $\dfrac{z_B+z_A}{2}$ النقطة M منتصف القطعة المستقيمة $[AB]$.



- ليكن z عدداً من $\mathbb{C}^*$. وليكن a عدداً عقديّاً طويلته 1 أي $a\in\mathbb{U}$، إذن $a=e^{\mathrm{i}\varphi}$ حيث $\varphi\in\arg(a)$. عندئذ تكون النقطة M'، التي هي صورة العدد العقدي az، هي النقطة التي تنتج من دوران النقطة M حول O بزاوية φ بالاتجاه الموجب.

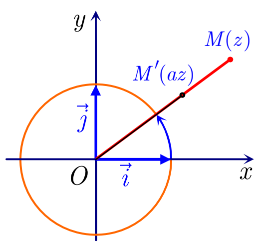
أي إذا رمزنا بالرمز $\mathcal{R}_\varphi$ إلى الدوران بزاوية قدرها φ بالاتجاه الموجب حول O، كان

$$\mathcal{R}_\varphi(M(z))=M'(az)$$

في الحقيقة، إذا كان $z=re^{\mathrm{i}\theta}$ كان $az=re^{\mathrm{i}(\theta+\varphi)}$. وعليه

$$OM=OM'=r \quad \text{و} \quad \left(\vec{i},\overrightarrow{OM'}\right)=\varphi+\left(\vec{i},\overrightarrow{OM}\right) \mod 2\pi$$

- ليكن z عدداً من $\mathbb{C}^*$. وليكن $a=k$ عدداً حقيقيّاً موجباً، عندئذ تكون النقطةُ M'، التي هي صورةُ العدد العقدي az، النقطةَ التي تنتج من M بتطبيق تحاكٍ مركزه O ونسبته k. أي إذا رمزنا بالرمز $\mathcal{H}_k$ إلى التحاكي الذي مركزه O ونسبته k، كان



$$\mathcal{H}_k(M(z))=M'(az)$$

في الحقيقة، إذا كان $z=re^{\mathrm{i}\theta}$ كان $az=kre^{\mathrm{i}\varphi}$. وعليه

$$\overrightarrow{OM'}=k\overrightarrow{OM}.$$

- وبوجه عام، ليكن z و a عددين من $\mathbb{C}^*$. عندئذ يُكتب a بالشكل $ke^{i\varphi}$ حيث k من $\mathbb{R}_+^*$ و $\varphi \in \arg(a)$، عندئذ تكون النقطة M'، التي هي صورة العدد العقدي az، هي النقطة التي تنتج من M بتطبيق تحاكٍ مركزه O ونسبته k يليه دوران بالاتجاه المباشر مركزه O وزاويته φ. أي

$$\mathcal{R}_\varphi \circ \mathcal{H}_k(M(z)) = M'(az)$$

حيث $\mathcal{R}_\varphi$ و هما التحويلان الهندسيّان المعرّفان في النقطتين السابقتين.

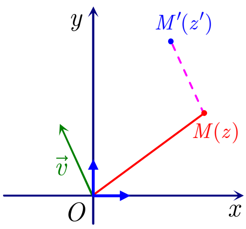
بعض التحويلات الهندسيّة الشهيرة

❶ الانسحاب

ليكن $\vec{v}$ شعاعاً في المستوي $\mathcal{P}$. نسمّي **انسحاباً** شعاعه $\vec{v}$ التحويل الهندسي

$$\mathcal{T}_{\vec{v}} : \mathcal{P} \to \mathcal{P}, M \mapsto \mathcal{T}_{\vec{v}}(M) = M'$$

و M' هي النقطة المعيّنة بالعلاقة $\overrightarrow{OM'} = \overrightarrow{OM} + \vec{v}$.



وإذا رمزنا بالرمز b إلى العدد العقدي الذي يمثِّل الشعاع $\vec{v}$، وكان z العدد العقدي المثِّل للنقطة M، كان $z+b$ هو العدد العقدي المثِّل للنقطة $M' = \mathcal{T}_{\vec{v}}(M)$.

وبالعكس، إذا كان b عدداً عقديّاً، وعرّفنا التطبيق

$$T_b : \mathbb{C} \to \mathbb{C}, z \mapsto z' = t_b(z) = z + b$$

كان التطبيق الذي يقرن بالنقطة $M(z)$ النقطة $M'(z')$ هو الانسحاب الذي شعاعه $\vec{v}(b)$.

❷ الدوران

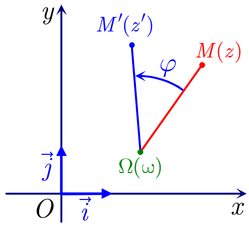
لتكن Ω نقطة في المستوي $\mathcal{P}$. نسمّي **دوراناً** مركزه B وزاويته φ التحويل الهندسي

$$\mathcal{R}_{\Omega,\varphi} : \mathcal{P} \to \mathcal{P}, M \mapsto R_{\Omega,\varphi}(M) = M'$$

و M' هي النقطة المعيّنة بالشرطين :

$$\left(\overrightarrow{\Omega M}, \overrightarrow{\Omega M'}\right) = \varphi \mod 2\pi \quad \text{و} \quad \Omega M = \Omega M'$$

لنفترض أنّ العدد العقدي ω يمثّل النقطة Ω من المستوي $\mathcal{P}$. عندئذ إذا كان z العدد العقدي الممثّل للنقطة M، وكان z' هو العدد العقدي الممثّل للنقطة $M' = \mathcal{R}_{\Omega,\varphi}(M)$. كان لدينا



$$z' - \omega = e^{i\varphi}(z - \omega)$$

أو

$$z' = e^{i\varphi}(z - \omega) + \omega$$

وبالعكس، إذا كان b عدداً عقديّاً، و φ عدداً حقيقيّاً، وعرّفنا التطبيق

$$R_{\omega,\varphi} : \mathbb{C} \to \mathbb{C}, z \mapsto z' = R_{\omega,\varphi}(z) = e^{i\varphi}(z - \omega) + \omega$$

كان التطبيق الذي يقرن بالنقطة $M(z)$ النقطة $M'(z')$ هو الدوران الذي مركزه $\Omega(\omega)$ وزاويته φ. ونلاحظ في هذه الحالة أنّ φ زاوية للعدد $\dfrac{z'-\omega}{z-\omega}$ أيّاً كان z من $\mathbb{C}\backslash\{\omega\}$.

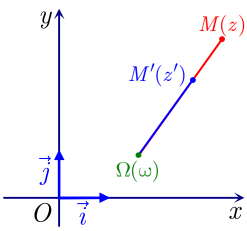
ملاحظة مهمّة. لتكن $A(a)$ و $B(b)$ و $C(c)$ ثلاث نقاط في المستوي $\mathcal{P}$ نفترض أنّ $a \neq b$ و $c \neq b$ عندئذ

$$\varphi = \left(\overrightarrow{BA}, \overrightarrow{BC}\right) \bmod 2\pi \Leftrightarrow \varphi \in \arg\left(\frac{c-b}{a-b}\right)$$

لأنّ المساواة $\theta = \left(\overrightarrow{BA}, \overrightarrow{BC}\right) \bmod 2\pi$ تُكافئ $C = \mathcal{R}_{B,\varphi}(A)$.

3 التحاكي

لتكن Ω نقطة في المستوي $\mathcal{P}$. نسمّي **تحاكياً** مركزه Ω ونسبته k من $\mathbb{R}^*$، التحويل الهندسي المعرّف كما يلي :



$$\mathcal{H}_{\Omega,k} : \mathcal{P} \to \mathcal{P}, M \mapsto \mathcal{H}_{\Omega,k}(M) = M'$$

و M' هي النقطة المعيّنة بالشرط :

$$\overrightarrow{\Omega M'} = k\overrightarrow{\Omega M}$$

لنفترض أنّ العدد العقدي ω يمثّل النقطة Ω من المستوي $\mathcal{P}$. عندئذ إذا كان z العدد العقدي الممثّل للنقطة M، وكان z' هو العدد العقدي الممثّل للنقطة $M' = \mathcal{H}_{\Omega,k}(M)$. كان لدينا $z' - \omega = k(z - \omega)$، أو $z' = k(z - \omega) + \omega$.

وبالعكس، إذا كان ω عدداً عقديّاً، و k عدداً حقيقيّاً غير معدوم، وعرّفنا التطبيق

$$H_{\omega,k} : \mathbb{C} \rightarrow \mathbb{C}, z \mapsto z' = H_{\omega,k}(z) = k(z-\omega)+\omega$$

كان التطبيق الذي يقرن بالنقطة $M(z)$ النقطة $M'(z')$ هو التحاكي الذي مركزه $\Omega(\omega)$ ونسبته k.

❹ التشابهات المباشرة

نسمّي **تشابهاً مباشراً** كلّ تحويل هندسي يقرن بالنقطة $M(z)$ النقطة $M'(z')$ المعرّفة بالعلاقة $z' = az+b$ حيث $(a,b) \in \mathbb{C}^* \times \mathbb{C}$. أي

$$S : \mathbb{C} \rightarrow \mathbb{C}, z \mapsto z' = S(z) = az+b$$

❈ إذا كان $a = 1$. كان $M \mapsto M'$ انسحاباً شعاعه $\vec{B}(b)$.

❈ إذا كان $a \neq 1$، توجد نقطة وحيدة $\Omega(\omega)$ تبقى ثابتة عند تطبيق التحويل S عليها، هي صورة العدد العقدي $\omega = \dfrac{b}{1-a}$ لأنّ هذه العدد هو الحلُّ الوحيد للمعادلة $S(z) = z$. وعندئذ نلاحظ أنّ

$$\forall z \in \mathbb{C}, \quad S(z) - \omega = a(z-\omega)$$

وهنا نناقش الحالات الآتية:

- إذا كان $|a| = 1$ أي $a = e^{\mathrm{i}\varphi}$ (حيث $\varphi \neq 0 \bmod 2\pi$) كان التحويل الهندسي $M \mapsto M'$ هو الدوران الذي مركزه Ω وزاويته φ.
- وإذا كان a عدداً حقيقيّاً (حيث $a \notin \{0,1\}$) كان التحويل الهندسي $M \mapsto M'$ هو التحاكي الذي مركزه Ω ونسبته a.
- وفي الحالة العامّة، إذا كان $a = ke^{\mathrm{i}\varphi}$ حيث $k = |a| > 0$، كان التحويل الهندسي $M \mapsto M'$ هو تركيب تحويلين، هما التحاكي الذي مركزه Ω ونسبته r، يليه الدوران الذي مركزه Ω زاويته φ.

وهنا نقول إنّ التحويل الهندسي $M \mapsto M'$ هو التشابه المباشر الذي مركزه Ω ونسبته k وزاويته φ.

التعامد والتوازي

8-1. **مبرهنة**. ليكن z_1 و z_2 عددين عقديين يمثّلان الشعاعين $\overrightarrow{u_1}$ و $\overrightarrow{u_2}$ على الترتيب.

1. يكون الشعاعان $\overrightarrow{u_1}$ و $\overrightarrow{u_2}$ مرتبطين خطيّاً، أو لهما المنحى نفسه، إذا وفقط إذا كان $\operatorname{Im}(z_1\overline{z_2}) = 0$.
2. ويكون الشعاعان $\overrightarrow{u_1}$ و $\overrightarrow{u_2}$ متعامدين، إذا وفقط إذا كان $\operatorname{Re}(z_1\overline{z_2}) = 0$.

الإثبات

1. لنفترض أنّ الشعاعين $\overrightarrow{u_1}$ و $\overrightarrow{u_2}$ مرتبطان خطيّاً، إذا كان $\overrightarrow{u_1} = \vec{0}$، كان $z_1 = 0$ ومن ثمّ $\operatorname{Im}(z_1\overline{z_2}) = 0$. وإذا كان $\overrightarrow{u_1} \neq \vec{0}$ استنتجنا وجود عددٍ حقيقي k يُحقّق $\overrightarrow{u_2} = k\overrightarrow{u_1}$، أي $z_2 = kz_1$ ومن ثَمّ $z_1\overline{z_2} = k|z_1|^2 \in \mathbb{R}$ أي $\operatorname{Im}(z_1\overline{z_2}) = 0$.

وبالعكس، إذا كان $k = z_1\overline{z_2}$ استنتجنا من الفرْض أنّ k عددٌ حقيقي، ومن ثَمّ كان لدينا $z_2 = \tilde{k}z_1$ حيث $\tilde{k} = k|z_2|^2 \in \mathbb{R}$، أو $\overrightarrow{u_2} = \tilde{k}\overrightarrow{u_1}$ إذن الشعاعان $\overrightarrow{u_1}$ و $\overrightarrow{u_2}$ مرتبطان خطيّاً.

2. لنفترض أنّ $z_1 = x_1 + \mathrm{i}\,y_1$ و $z_2 = x_2 + \mathrm{i}\,y_2$. عندئذ يُكتب الجداء السلّمي للشعاعين $\overrightarrow{u_1}$ و $\overrightarrow{u_2}$ بالشكل

$$\overrightarrow{u_1} \cdot \overrightarrow{u_2} = x_1x_2 + y_1y_2$$

ولكن

$$z_1\overline{z_2} = x_1x_2 + y_1y_2 + \mathrm{i}(y_1x_2 - x_1y_2)$$

إذن

$$\overrightarrow{u_1} \cdot \overrightarrow{u_2} = \operatorname{Re}(z_1\overline{z_2})$$

وعليه

$$\overrightarrow{u_1} \cdot \overrightarrow{u_2} = 0 \Leftrightarrow \operatorname{Re}(z_1\overline{z_2}) = 0$$

وهي النتيجة المرجوّة. ❐

2-8. تطبيق. معادلة مستقيم.

- لتكن النقطة A التي تمثّل العدد العقدي a، وليكن $\vec{\Omega}$ شعاعاً غير معدوم يمثّله العدد العقدي ω. وأخيراً ليكن $\mathcal{D}$ المستقيم المار بالنقطة A موازياً الشعاع $\vec{\Omega}$.

عندئذ تنتمي النقطة $M(z)$ إلى المستقيم $\mathcal{D}$ إذا وفقط إذا كان الشعاعان $\overrightarrow{AM}$ و $\vec{\Omega}$ مرتبطين خطّياً، وهذا يُكافئ $\mathrm{Im}((z-a)\overline{\omega}) = 0$. أو

$$(z-a)\overline{\omega} - \overline{(z-a)}\omega = 0$$

ومنه

$$\mathcal{D} = \left\{ M(z) : z\overline{\omega} - \overline{z}\omega = a\overline{\omega} - \overline{a}\omega \right\}$$

- لتكن النقطة A التي تمثّل العدد العقدي a، وليكن $\vec{\Gamma}$ شعاعاً **غير صفري** يمثّله العدد العقدي γ. وأخيراً ليكن $\mathcal{D}$ المستقيم المار بالنقطة A عمودياً على $\vec{\Gamma}$. عندئذ تنتمي النقطة $M(z)$ إلى المستقيم $\mathcal{D}$ إذا وفقط إذا كان الشعاعان $\overrightarrow{AM}$ و $\vec{\Gamma}$ متعامدين، وهذا يُكافئ $\mathrm{Re}((z-a)\overline{\gamma}) = 0$. أو

$$(z-a)\overline{\gamma} + \overline{(z-a)}\gamma = 0$$

ومنه

$$\mathcal{D} = \left\{ M(z) : z\overline{\gamma} + \overline{z}\gamma = a\overline{\gamma} + \overline{a}\gamma \right\}$$

- وبوجه عام، إذا كان (β, k) عنصراً من $\mathbb{C}^* \times \mathbb{R}$ كانت مجموعة النقاط

$$\left\{ M(z) : z\overline{\beta} + \overline{z}\beta = k \right\}$$

تمثّل المستقيم $\mathcal{D}$ المار بالنقطة A، صورة العدد العقدي $a = \dfrac{\beta k}{2|\beta|^2}$، عمودياً على الشعاع $\vec{\Gamma}(\beta)$. أو موازياً للشعاع $\vec{\Omega}(\mathrm{i}\,\beta)$.

9. تتمّات حول جذور المعادلات من الدرجة الثانية

نتأمّل في هذه التتمات معادلة من الدرجة الثانية

$$z^2 + az + b = 0 \qquad \mathcal{E}$$

نفترض أنّ z جذرٌ للمعادلة $\mathcal{E}$، ونبحث عن المعادلة التي تحقّقها طويلة z أي المقدار $|z|$.

▫ ليكن c عدداً عقديّاً يُحقّق $c^2 = b$. عندئذ

$$z^2 + c^2 = -az$$

وبجمع المقدار $2cz$ إلى طرفَي هذه المعادلة، وطرحه نجد

$$\begin{cases} z^2 + 2cz + c^2 = -(a-2c)z \\ z^2 - 2cz + c^2 = -(a+2c)z \end{cases}$$

أو

$$\begin{cases} (z+c)^2 = -(a-2c)z \\ (z-c)^2 = -(a+2c)z \end{cases}$$

وعليه

$$\begin{cases} \left|z+c\right|^2 = \left|a-2c\right|\left|z\right| \\ \left|z-c\right|^2 = \left|a+2c\right|\left|z\right| \end{cases}$$

إذن

$$\left|z+c\right|^2 + \left|z-c\right|^2 = \left(\left|a-2c\right| + \left|a+2c\right|\right)\left|z\right|$$

ولكن نعلم أنّ

$$\left|z+c\right|^2 + \left|z-c\right|^2 = 2\left|z\right|^2 + 2\left|c\right|^2$$

إذن

$$\left|z\right|^2 - \frac{\left|a-2c\right| + \left|a+2c\right|}{2}\left|z\right| + \left|b\right| = 0, \quad ➢ b = c^2 \tag{1}$$

بذا نكون قد أثبتنا الخاصّة الآتية:

9-1. مبرهنة. إذا كان z_1 و z_2 جذري معادلة من الدرجة الثانية $z^2 + az + b = 0$، وكان c جذراً تربيعيّاً للعدد b . كان $|z_1|$ و $|z_2|$ جذري المعادلة:

$$\left|z\right|^2 - \frac{\left|a-2c\right| + \left|a+2c\right|}{2}\left|z\right| + \left|b\right| = 0$$

▫ إنّ مميِّز المعادلة السابقة موجبٌ دوماً. في الحقيقة، لنضع

$$d = \frac{|a-2c|+|a+2c|}{2}$$

عندئذ

$$\begin{aligned} d^2 &= \frac{1}{4}\big(\left|a-2c\right|+\left|a+2c\right|\big)^2 \\ &= \frac{1}{4}\Big(\left|a-2c\right|^2+\left|a+2c\right|^2+2\left|a^2-4c^2\right|\Big) \\ &= \frac{1}{2}\Big(\left|a\right|^2+4\left|b\right|+\left|a^2-4b\right|\Big) \end{aligned}$$

وعلى هذا فإنّ δ مميِّز المعادلة (1) الذي يعطى بالعلاقة $\delta = d^2 - 4|b|$ يساوي

$$\delta = \frac{1}{2}\big(\left|a^2\right|+\left|a^2-4b\right|-\left|4b\right|\big) \geq 0$$

لقد وجدنا عند إثبات متراجحة المثلّث أنّ

$$\begin{aligned} \big(\left|u\right|+\left|v\right|=\left|u+v\right|\big) &\Leftrightarrow \big(u\overline{v}\in\mathbb{R}_+\big) \\ &\Leftrightarrow \big(v=0\big)\vee\left(\frac{u}{v}\in\mathbb{R}_+\right) \end{aligned}$$

وعليه يكون

$$\begin{aligned} (\delta=0) &\Leftrightarrow (a=0)\vee\left(\frac{4b}{a^2}-1\in\mathbb{R}_+\right) \\ &\Leftrightarrow (a=0)\vee\left(\frac{b}{a^2}\in\left[\tfrac{1}{4},+\infty\right[\right) \end{aligned}$$

ومنه الخاصّة الآتية:

2-9. **مبرهنة**. يكون لجذري المعادلة من الدرجة الثانية $z^2+az+b=0$ الطويلة نفسها، إذا وفقط إذا تحقَّق الشرط

$$(a=0)\vee\left(\frac{b}{a^2}\in\left[\tfrac{1}{4},+\infty\right[\right)$$

ملاحظة. يمكن الوصول إلى هذه النتيجة بطريقة أخرى. لنلاحظ أنّ

$$\begin{aligned} (u-v)\overline{(u+v)} &= |u|^2-|v|^2+u\overline{v}-\overline{u}v \\ &= |u|^2-|v|^2+2\,\mathrm{i}\,\mathrm{Im}(u\overline{v}) \end{aligned}$$

وعليه نرى أنّ $\mathrm{Re}\big((u-v)\overline{(u+v)}\big)=|u|^2-|v|^2$.

إذن $|v| = |u|$ إذا وفقط إذا تحقّق الشرط :

$$\mathrm{Re}((u-v)\overline{(u+v)}) = 0 .$$

وهذه الخاصّة تعبّر عن الخاصّة الهندسيّة البسيطة التالية :

« يكون متوازي أضلاع معيّناً إذا وفقط إذا تعامد قطراه »

وعليه إذا كان z_1 و z_2 جذري معادلة من الدرجة الثانية : $z^2 + az + b = 0$، كان الشرط اللازم والكافي لتحقُّق المساواة $|z_2| = |z_1|$ هو أن يكون $\mathrm{Re}\big((z_1 - z_2)\overline{(z_1+z_2)}\big) = 0$ أو $\mathrm{Re}((z_1 - z_2)\overline{a}) = 0$. وهذا يُكافئ كونَ

$$\mathrm{Re}\Big(\frac{z_1 - z_2}{a}\Big) = 0 \quad \text{أو} \quad a = 0$$

أو كونَ

$$\Big(\frac{z_1 - z_2}{a}\Big)^2 \in \mathbb{R}_- \quad \text{أو} \quad a = 0$$

ونجد مجدّداً الخاصّة السابقة بملاحظة أنّ

$$\Big(\frac{z_1 - z_2}{a}\Big)^2 = \frac{(z_1+z_2)^2 - 4z_1z_2}{a^2} = 1 - \frac{4b}{a^2}$$

▫ بافتراض أنّ جذري المعادلة $\mathcal{E}$ يقعان في القرص $\overline{D}(0,R)$. نستنتج أنّ $|b| \leq R^2$ لأنّ b يساوي جداء ضرب الجذرين. ونستنتج أيضاً أنّ

$$R^2 - \frac{|a-2c| + |a+2c|}{2} R + |b| \geq 0$$

لأنّه لو كان هذا المقدار سالباً لوقعت R بين $|z_1|$ و $|z_2|$ وهذا يناقض الفرْض.

وبالعكس، لنفترض أنّ

$$R^2 - \frac{|a-2c| + |a+2c|}{2} R + |b| \geq 0 \quad \text{و} \quad |b| \leq R^2$$

يمكننا دون الإخلال بعموميّة الإثبات أن نفترض أنّ $|z_1| \leq |z_2|$. عندئذ نستنتج من الشرط الثاني أنّ $R \notin \,]|z_1|,|z_2|[$.

هناك إذن حالتان:

- إذا كان $R \leq |z_1|$ استنتجنا أنّ

$$R^2 \leq |z_1|^2 \leq |z_1||z_2| = |z_1 z_2| = |b| \leq R^2$$

ومنه $R = |z_2| = |z_1|$، وينتمي الجذران z_1 و z_2 إلى $\overline{D}(0,R)$ في هذه الحالة.

- وإذا كان $|z_2| \le R$ استنتجنا أنّ z_1 و z_2 ينتميان إلى $\overline{D}(0,R)$ أيضاً في هذه الحالة.

وهكذا نكون قد أثبتنا الخاصّة الآتية:

9-3. مبرهنة. ينتمي جذرا المعادلة $z^2+az+b=0$ إلى القرص $\overline{D}(0,R)$ حيث $R>0$، إذا وفقط إذا تحقّق الشرط :

$$\left(|b| \le R^2\right) \wedge \left(R^2 - \frac{|a-2c|+|a+2c|}{2} R + |b| \ge 0\right)$$

حيث c هو جذرٌ تربيعي للعدد b. وهذا الشرط يُكافئ

$$\left(|b| \le R^2\right) \wedge \left(R^2 - \frac{1}{\sqrt{2}}\sqrt{|a|^2 + 4|b| + |a^2-4b|}\,R + |b| \ge 0\right)$$

9-4. تطبيق

نُعطى عدداً عقديّاً b، وعدداً حقيقيّاً موجباً R يُحقّق $|b| \le R^2$. لتكن $\mathcal{A}_{b,R}$ مجموعة قيم a في $\mathbb{C}$ التي تجعل جذري المعادلة $z^2+az+b=0$ يقعان في القرص $\overline{D}(0,R)$. أي

$$\mathcal{A}_{b,R} = \left\{a \in \mathbb{C} : \left\{z : z^2+az+b=0\right\} \subset \overline{D}(0,R)\right\}$$

فإذا كان c جذراً تربيعيّاً للعدد b. استنتجنا من الخاصّة السابقة أنّ

$$\begin{aligned}\mathcal{A}_{b,R} &= \left\{a \in \mathbb{C} : R^2 - \frac{|a-2c|+|a+2c|}{2} R + |b| \ge 0\right\}\\ &= \left\{a \in \mathbb{C} : |a-2c|+|a+2c| \le 2\frac{R^2+|b|}{R}\right\}\end{aligned}$$

وعليه فالمجموعة $\mathcal{A}_{b,R}$ تشمل داخل ومحيط القطع الناقص الذي محرقاه F_1 و F_2 هما صورتا النقطتين $2c$ و $-2c$، وبُعده الكبير يساوي $R+|b|/R$.

فمثلاً تقبل المعادلة $z^2+az-\frac{1}{4}=0$ جذرين ينتميان إلى القرص الواحدي $\overline{D}(0,1)$ إذا وفقط إذا انتمت a إلى داخل أو محيط القطع الناقص الذي محرقاه F_1 و F_2 هما صورتا النقطتين i و $-\mathrm{i}$، وبُعده الكبير يساوي $5/4$. أي إذا وفقط إذا كان

$$a \in \left\{x+\mathrm{i}\,y : \frac{x^2}{9} + \frac{y^2}{25} \le \frac{1}{16}\right\}$$

تمرينات

التمرين 1. ليكن z عدداً من $\mathbb{C}$. أثبت أنّ الخاصّتين التاليتين متكافئتان:

- z عددٌ حقيقي.
- $|z+\mathrm{i}|=|z-\mathrm{i}|$

الحل

في الحقيقة،

$$\begin{aligned}
\left|z+\mathrm{i}\right|-\left|z-\mathrm{i}\right| &= \frac{\left|z+\mathrm{i}\right|^2-\left|z-\mathrm{i}\right|^2}{\left|z+\mathrm{i}\right|+\left|z-\mathrm{i}\right|}\\
&= \frac{\left|z\right|^2+1-2\,\mathrm{Re}(z\,\mathrm{i})-\left|z\right|^2-1-2\,\mathrm{Re}(z\,\mathrm{i})}{\left|z+\mathrm{i}\right|+\left|z-\mathrm{i}\right|}\\
&= \frac{-4}{\left|z+\mathrm{i}\right|+\left|z-\mathrm{i}\right|}\mathrm{Re}(z\,\mathrm{i})\\
&= \frac{4}{\left|z+\mathrm{i}\right|+\left|z-\mathrm{i}\right|}\mathrm{Im}(z)
\end{aligned}$$

إذن

$$\left(\left|z+\mathrm{i}\right|-\left|z-\mathrm{i}\right|=0\right)\Leftrightarrow\left(\mathrm{Im}(z)=0\right)$$

وهو التكافؤ المنشود. ■

ملاحظة. تعني المساواة $\left|z+\mathrm{i}\right|=\left|z-\mathrm{i}\right|$ أنّ النقطة $M(z)$ تبعد عن كلٍّ من النقطتين $A(\mathrm{i})$ و $B(-\mathrm{i})$ البعدَ نفسه. فهي تقع على محور القطعة المستقيمة $[AB]$ وهو المحور الحقيقي.

التمرين 2. اكتب بالصيغة المثلّثيّة العددَ العقدي $z=\dfrac{-4}{1+\mathrm{i}\sqrt{3}}$ ، واحسب z^3 .

الحل

لنلاحظ أنّ

$$\omega=e^{\mathrm{i}\pi/3}=\cos\left(\tfrac{\pi}{3}\right)+\mathrm{i}\sin\left(\tfrac{\pi}{3}\right)=\frac{1+\mathrm{i}\sqrt{3}}{2}$$

ومنه $z=\dfrac{-2}{\omega}$ إذن

$$
\begin{aligned}
z &= -2e^{-\mathrm{i}\pi/3} = 2e^{\mathrm{i}\pi}\cdot e^{-\mathrm{i}\pi/3}\\
&= 2e^{2\mathrm{i}\pi/3} = 2\left(\cos\left(\tfrac{2\pi}{3}\right)+\mathrm{i}\sin\left(\tfrac{2\pi}{3}\right)\right)
\end{aligned}
$$

ونجد مباشرة أنّ

$$z^3 = 2^3e^{2\mathrm{i}\pi} = 8$$

التمرين 3. اكتب $\cos^7\theta$ عبارةً خطيّة بالنسب المثلّثية لمضاعفات θ.

الحل

لمّا كان $\cos\theta=\dfrac{e^{\mathrm{i}\theta}+e^{-\mathrm{i}\theta}}{2}$ استنتجنا أنّ

$$
\begin{aligned}
\cos^7\theta &= \frac{1}{2^7}\left(e^{\mathrm{i}\theta}+e^{-\mathrm{i}\theta}\right)^7\\
&= \frac{1}{2^7}\left(e^{7\mathrm{i}\theta}+7e^{5\mathrm{i}\theta}+21e^{3\mathrm{i}\theta}+35e^{\mathrm{i}\theta}+35e^{-\mathrm{i}\theta}+21e^{-3\mathrm{i}\theta}+7e^{-5\mathrm{i}\theta}+e^{-7\mathrm{i}\theta}\right)\\
&= \frac{1}{64}\left(\cos 7\theta+7\cos 5\theta+21\cos 3\theta+35\cos\theta\right)
\end{aligned}
$$

وهي النتيجة المرجوّة.

التمرين 4. اكتب $\dfrac{\sin 6\theta}{\sin\theta}$ بدلالة $\cos\theta$.

الحل

هنا نستفيد من المساواة

$$\frac{a^6-b^6}{a-b}=a^5+a^4b+a^3b^2+a^2b^3+ab^4+b^5$$

في حالة $a\neq b$. فنكتب

$$
\begin{aligned}
\frac{\sin 6\theta}{\sin\theta} &= \frac{e^{6\mathrm{i}\theta}-e^{-6\mathrm{i}\theta}}{e^{\mathrm{i}\theta}-e^{-\mathrm{i}\theta}} = e^{5\mathrm{i}\theta}+e^{3\mathrm{i}\theta}+e^{\mathrm{i}\theta}+e^{-\mathrm{i}\theta}+e^{-3\mathrm{i}\theta}+e^{-5\mathrm{i}\theta}\\
&= 2\cos 5\theta+2\cos 3\theta+2\cos\theta
\end{aligned}
$$

وهي النتيجة المرجوّة.

التمرين 5. ليكن (z_1, z_2) عنصراً من $\mathbb{C}^* \times \mathbb{C}$. أثبت أنّ الخاصّتين التاليتين متكافئتان :

- $\exists \lambda \in \mathbb{R}, \quad z_2 = \mathrm{i}\,\lambda z_1$
- $|z_1 + z_2| = |z_1 - z_2|$

الحل

في الحقيقة،

$$\begin{aligned}
\left|z_1 + z_2\right| - \left|z_1 - z_2\right| &= \frac{\left|z_1 + z_2\right|^2 - \left|z_1 - z_2\right|^2}{\left|z_1 + z_2\right| + \left|z_1 - z_2\right|}\\
&= \frac{4\,\mathrm{Re}(z_1\overline{z}_2)}{\left|z_1 + z_2\right| + \left|z_1 - z_2\right|}\\
&= \frac{4\left|z_1\right|^2}{\left|z_1 + z_2\right| + \left|z_1 - z_2\right|}\mathrm{Re}\left(\frac{z_2}{z_1}\right)
\end{aligned}$$

ومن ثَمّ $|z_1 + z_2| = |z_1 - z_2|$ يُكافئ $\mathrm{Re}(z_2/z_1) = 0$ أي يوجد عددٌ λ ينتمي إلى $\mathbb{R}$ يُحقّق $z_2 = \mathrm{i}\,\lambda z_1$. ■

ملاحظة. لقد أثبتنا الخاصّة التالية : يتساوى قطرا متوازي أضلاع إذا وفقط إذا كان مستطيلاً.

التمرين 6. ليكن (a, b) عنصراً من $\mathbb{C}^2$ يُحقّق $|a| = |b| = 1$ و $a \neq b$. أثبت أن

$$\forall z \in \mathbb{C}, \quad \frac{z + ab\overline{z} - (a+b)}{a-b} \in \mathrm{i}\,\mathbb{R}$$

الحل

نستفيد من أنّه في حالة $|c| = 1$ يكون $\overline{c} = 1/c$.

ليكن z عدداً عقديّاً. ولنعرّف $\omega = \dfrac{z + ab\overline{z} - (a+b)}{a-b}$ عندئذ

$$\begin{aligned}
\overline{\omega} &= \frac{\overline{z} + \overline{a}\overline{b}z - (\overline{a} + \overline{b})}{\overline{a} - \overline{b}} = \frac{\overline{z} + \frac{1}{ab}z - \left(\frac{1}{a} + \frac{1}{b}\right)}{\frac{1}{a} - \frac{1}{b}}\\
&= \frac{ab\overline{z} + z - (b+a)}{b-a} = -\frac{z + ab\overline{z} - (b+a)}{a-b} = -\omega
\end{aligned}$$

أي $\overline{\omega} = -\omega$. ومنه $\omega \in \mathrm{i}\,\mathbb{R}$، وهي النتيجة المرجوّة. ■

التمرين 7. ليكن $a = e^{\mathrm{i}\varphi}$ حيث $\varphi \in \mathbb{R}$. نتأمّل المعادلة: $(\mathcal{E})\quad z^2 - 2az + 1 = 0$

1. أثبت أنّ لجذري هذه المعادلة z' و z'' طويلتين إحداهما مقلوب الأخرى، وزاويتين أحداهما عكس الأخرى. ما الشرط اللازم والكافي ليكون الجذران z' و z'' حقيقيين؟ وما الشرط اللازم والكافي ليكون الجذران z' و z'' تخيليين صرفين ؟
2. احسب طويلة وزاوية كلٍّ من $z' - a$ و $z'' - a$.

الحل

1. في الحقيقة، $z'z'' = 1$ وهذا يعني أنّ $|z'||z''| = 1$ وأنّ $0 \in \arg(z') + \arg(z'')$. وهي النتيجة المطلوبة.

ونعلم من جهة أخرى أنّ $z' + z'' = 2a$. وعليه

- إذا كان $\{z', z''\} \subset \mathbb{R}$ كان $z' + z'' \in \mathbb{R}$ أي $a \in \mathbb{R}$. ولكن نعلم من جهة أخرى أنّ $|a| = 1$ إذن $a \in \{1, -1\}$. وبالعكس، إذا كان $a \in \{1, -1\}$ توثّقنا، بالحساب المباشر للجذرين z' و z'' في هذه الحالة، أنّهما حقيقيّان. وهكذا نكون قد أثبتنا أنّ

$$(\{z', z''\} \subset \mathbb{R}) \Leftrightarrow a \in \{-1, 1\}$$

- إذا كان $\{z', z''\} \subset \mathrm{i}\mathbb{R}$ كان $z' + z'' \in \mathrm{i}\mathbb{R}$ أي $a \in \mathrm{i}\mathbb{R}$. ولكن نعلم من جهة أخرى أنّ $|a| = 1$ إذن $a \in \{\mathrm{i}, -\mathrm{i}\}$. وبالعكس، إذا كان $a \in \{\mathrm{i}, -\mathrm{i}\}$ توثّقنا، بالحساب المباشر للجذرين z' و z'' في هذه الحالة، أنّهما تخيّليّان صرفان. وهكذا نكون قد أثبتنا أنّ

$$(\{z', z''\} \subset \mathrm{i}\mathbb{R}) \Leftrightarrow a \in \{-\mathrm{i}, \mathrm{i}\}$$

2. ليكن z حلّاً للمعادلة $(\mathcal{E})$ عندئذ يكون لدينا $(z-a)^2 = a^2 - 1$. ولكن

$$a^2 - 1 = 2\mathrm{i}\sin\varphi \cdot e^{\mathrm{i}\varphi} = 2\sin\varphi \cdot \exp\left(\mathrm{i}\left(\varphi + \tfrac{\pi}{2}\right)\right)$$

وهكذا نستنتج أنّ $|z' - a| = |z'' - a| = 2|\sin\varphi|$.

- في حالة $\sin\varphi \geq 0$ لدينا مثلاً

$$\frac{\varphi}{2} + \frac{\pi}{4} \in \arg(z' - a) \quad \text{و} \quad \frac{\varphi}{2} + \frac{5\pi}{4} \in \arg(z'' - a)$$

- وفي حالة $\sin\varphi < 0$ لدينا مثلاً

$$\frac{\varphi}{2} + \frac{3\pi}{4} \in \arg(z' - a) \quad \text{و} \quad \frac{\varphi}{2} + \frac{7\pi}{4} \in \arg(z'' - a)$$

وهي النتيجة المرجوّة. ■

التمرين 8. ليكن t عدداً حقيقيّاً موجباً. أثبت أنّ

$$\left(|z|=1\right)\Rightarrow\left(\left|z-t\right|\geq\frac{1+t}{2}\left|z-1\right|\right)$$

الحل

لنفترض أنّ $z=e^{\mathrm{i}\theta}$ ، ولنضع

$$\Delta=\left|z-t\right|^2-\frac{(1+t)^2}{4}\left|z-1\right|^2$$

عندئذ

$$\begin{aligned}
\Delta &=\left|\cos\theta-t+\mathrm{i}\sin\theta\right|^2-\frac{(1+t)^2}{4}\left|\cos\theta-1+\mathrm{i}\sin\theta\right|^2\\
&=(\cos\theta-t)^2+\sin^2\theta-\frac{(1+t)^2}{4}\left((\cos\theta-1)^2+\sin^2\theta\right)\\
&=1+t^2-2t\cos\theta-\frac{(1+t)^2}{4}(2-2\cos\theta)\\
&=1+t^2-2t\cos\theta-(1+2t+t^2)\sin^2\left(\tfrac{\theta}{2}\right)\\
&=\cos^2\left(\tfrac{\theta}{2}\right)((1+t)^2)-2t\left(\cos\theta+\sin^2\left(\tfrac{\theta}{2}\right)\right)\\
&=\cos^2\left(\tfrac{\theta}{2}\right)(1+t^2-2t)\\
&=(1-t)^2\cos^2\left(\tfrac{\theta}{2}\right)\geq 0
\end{aligned}$$

وهذا يثبت أنّ

$$\left|z-t\right|\geq\frac{1+t}{2}\left|z-1\right|$$

وهي النتيجة المرجوّة. ■

التمرين 9. احسب المجموع $\sum_{0\leq k\leq n/2}(-1)^k 3^k C_n^{2k}$ في حالة n من $\mathbb{N}$.

الحل

لنضع $\sum_{0\le k\le n/2}(-1)^k 3^k C_n^{2k} = S_n$. فنجد

$$\begin{aligned}
S_n &= \mathrm{Re}\left(\sum_{0\le 2k\le n}(\mathrm{i})^{2k}(\sqrt{3})^{2k}C_n^{2k} + \mathrm{i}\times\sum_{0\le 2k+1\le n}(\mathrm{i})^{2k}(\sqrt{3})^{2k+1}C_n^{2k+1}\right)\\
&= \mathrm{Re}\left(\sum_{0\le 2k\le n}(\mathrm{i}\sqrt{3})^{2k}C_n^{2k} + \sum_{0\le 2k+1\le n}(\mathrm{i}\sqrt{3})^{2k+1}C_n^{2k+1}\right)\\
&= \mathrm{Re}\left(\sum_{0\le k\le n}(\mathrm{i}\sqrt{3})^{k}C_n^{k}\right)\\
&= \mathrm{Re}\left((1+\mathrm{i}\sqrt{3})^n\right)
\end{aligned}$$

ولكن

$$1+\mathrm{i}\sqrt{3} = 2\left(\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}\right) = 2\left(\cos\left(\frac{\pi}{3}\right)+\mathrm{i}\sin\left(\frac{\pi}{3}\right)\right) = 2\cdot e^{\mathrm{i}\pi/3}$$

إذن

$$S_n = 2^n\,\mathrm{Re}\left(\left(e^{\mathrm{i}\pi/3}\right)^n\right) = 2^n\,\mathrm{Re}\left(e^{\mathrm{i}n\pi/3}\right) = 2^n\cos\left(\frac{\pi n}{3}\right)$$

وهو المطلوب. ■

التمرين 10. احسب، أيّاً كان n من $\mathbb{N}^*$، و x من $\mathbb{R}$، كلّاً من المجاميع الآتية:

$$S_n(x) = \sum_{k=1}^{n}\cos(2k-1)x$$

$$T_n(x) = 1+2\sum_{k=1}^{n}\cos 2kx$$

$$U_n(x) = \sum_{k=0}^{n}C_n^k\cos kx$$

$$V_n(x) = \sum_{k=1}^{n}C_n^k\sin kx$$

الحل

- لنلاحظ أوّلاً أنّه في حالة $x \notin \pi\mathbb{Z}$ لدينا

$$\begin{aligned}
S_n(x) &= \sum_{k=1}^{n} \cos(2k-1)x = \mathrm{Re}\left(\sum_{k=1}^{n} e^{\mathrm{i}(2k-1)x}\right)\\
&= \mathrm{Re}\left(e^{\mathrm{i}x}\sum_{k=1}^{n}(e^{2\mathrm{i}x})^{k-1}\right)\\
&= \mathrm{Re}\left(e^{\mathrm{i}x}\sum_{k=0}^{n-1}(e^{2\mathrm{i}x})^{k}\right)
\end{aligned}$$

ولكن بالاستفادة من المساواة : $\sum_{k=0}^{n-1} a^k = \dfrac{a^n-1}{a-1}$ في حالة $a \neq 1$ ، نستنتج أنّ

$$\sum_{k=0}^{n-1}(e^{2\mathrm{i}x})^k = \frac{e^{2\mathrm{i}nx}-1}{e^{2\mathrm{i}x}-1} = \frac{e^{\mathrm{i}nx}}{e^{\mathrm{i}x}} \times \frac{e^{\mathrm{i}nx}-e^{-\mathrm{i}nx}}{e^{\mathrm{i}x}-e^{-\mathrm{i}x}} = \frac{e^{\mathrm{i}nx}}{e^{\mathrm{i}x}} \times \frac{\sin nx}{\sin x}$$

ومنه

$$S_n(x) = \mathrm{Re}\left(e^{\mathrm{i}nx} \times \frac{\sin nx}{\sin x}\right) = \frac{\sin nx \cos nx}{\sin x} = \frac{\sin(2nx)}{2\sin x}$$

أمّا حالة $x \in \pi\mathbb{Z}$ فهي سهلة ونتركها للقارئ.

- لنلاحظ أنّه في حالة $x \notin \pi\mathbb{Z}$ لدينا

$$\begin{aligned}
T_n(x) &= 1 + 2\sum_{k=1}^{n} \cos 2kx = 1 + \sum_{k=1}^{n}(e^{2\mathrm{i}kx} + e^{-2\mathrm{i}kx})\\
&= \sum_{k=-n}^{n} e^{2\mathrm{i}kx} = e^{-2\mathrm{i}nx} \cdot \sum_{k=-n}^{n} e^{2\mathrm{i}(k+n)x} = e^{-2\mathrm{i}nx} \cdot \sum_{k=0}^{2n} e^{2\mathrm{i}kx}
\end{aligned}$$

ولكن

$$\begin{aligned}
\sum_{k=0}^{2n} e^{2\mathrm{i}kx} &= \sum_{k=0}^{2n}(e^{2\mathrm{i}x})^k = \frac{e^{2\mathrm{i}(2n+1)x}-1}{e^{2\mathrm{i}x}-1}\\
&= \frac{e^{\mathrm{i}(2n+1)x}}{e^{\mathrm{i}x}} \times \frac{e^{\mathrm{i}(2n+1)x} - e^{-\mathrm{i}(2n+1)x}}{e^{\mathrm{i}x}-e^{-\mathrm{i}x}}\\
&= e^{2\mathrm{i}nx} \times \frac{\sin(2n+1)x}{\sin x}
\end{aligned}$$

إذن

$$T_n(x) = 1 + 2\sum_{k=1}^{n} \cos 2kx = \frac{\sin(2n+1)x}{\sin x}$$

▫ لحساب $U_n(x) = \sum_{k=0}^{n} C_n^k \cos kx$ و $V_n(x) = \sum_{k=1}^{n} C_n^k \sin kx$ نعرّف

$$W_n(x) = U_n(x) + iV_n(x)$$

فنجد

$$\begin{aligned} W_n(x) &= \sum_{k=0}^{n} C_n^k \left(\cos kx + \mathrm{i}\sin kx\right) \\ &= \sum_{k=0}^{n} C_n^k e^{\mathrm{i}xk} = (1+e^{\mathrm{i}x})^n \end{aligned}$$

ولكن

$$1 + e^{\mathrm{i}x} = e^{\mathrm{i}x/2}\left(e^{\mathrm{i}x/2} + e^{-\mathrm{i}x/2}\right) = 2\cos\left(\frac{x}{2}\right)\cdot e^{\mathrm{i}x/2}$$

إذن

$$U_n(x) + \mathrm{i}V_n(x) = 2^n \cos^n\left(\frac{x}{2}\right)\cdot e^{\mathrm{i}nx/2}$$

ومنه

$$\sum_{k=0}^{n} C_n^k \cos kx = 2^n \cos^n\left(\frac{x}{2}\right)\cdot \cos\left(\frac{nx}{2}\right)$$

و

$$\sum_{k=1}^{n} C_n^k \sin kx = 2^n \cos^n\left(\frac{x}{2}\right)\cdot \sin\left(\frac{nx}{2}\right)$$

وهي النتيجة المرجوّة. ■

التمرين 11. احسب، أيّاً كان n من $\mathbb{N}^*$، و x من $\left[0,\frac{\pi}{2}\right[$، المجموع :

$$T_n = 1 + \sum_{k=1}^{n} \frac{\cos kx}{\cos^k x}$$

الحل

هنا نلاحظ أنّ

$$T_n = 1 + \sum_{k=1}^{n} \frac{\cos kx}{\cos^k x} = \operatorname{Re}\left(\sum_{k=0}^{n} \frac{e^{\mathrm{i}kx}}{\cos^k x} \right) = \operatorname{Re}\left(\sum_{k=0}^{n} \left(\frac{e^{\mathrm{i}x}}{\cos x} \right)^k \right)$$

ولكن

$$\begin{aligned}\sum_{k=0}^{n} \left(\frac{e^{\mathrm{i}x}}{\cos x} \right)^k &= \frac{\left(\dfrac{e^{\mathrm{i}x}}{\cos x} \right)^{n+1} - 1}{\dfrac{e^{\mathrm{i}x}}{\cos x} - 1} = \frac{e^{\mathrm{i}(n+1)x} - \cos^{n+1} x}{(e^{\mathrm{i}x} - \cos x)\cos^n x} \\ &= \frac{e^{\mathrm{i}(n+1)x} - \cos^{n+1} x}{\mathrm{i}\sin x \cdot \cos^n x} \\ &= \frac{e^{\mathrm{i}(n+1)x}}{\mathrm{i}\cos^n x \cdot \sin x} + \mathrm{i}\frac{\cos x}{\sin x}\end{aligned}$$

ومنه

$$T_n = 1 + \sum_{k=1}^{n} \frac{\cos kx}{\cos^k x} = \frac{\sin(n+1)x}{\cos^n x \cdot \sin x}$$

وهي النتيجة المرجوّة. ■

التمرين 12. اكتب بالشكل الجبري الجذور التكعيبيّة للعدد $\dfrac{1+\mathrm{i}}{\sqrt{2}}$.

الحل

نلاحظ هنا أنّ العدد $a = \dfrac{1}{\sqrt{2}}(1+\mathrm{i})$ يُكتب بالشكل الأسي بالصيغة $a = e^{i\pi/4}$. يكفي أن نعيّن جذراً تكعيبيّاً واحداً z_0 للعدد a حتّى تكون مجموعة الجذور التكعيبيّة للعدد a هي $\left\{ z_0, \mathrm{j}z_0, \mathrm{j}^2 z_0 \right\}$، وقد رمزنا بالرمز المتعارف j إلى العدد $e^{\mathrm{i}2\pi/3} = -\dfrac{1}{2} + \mathrm{i}\dfrac{\sqrt{3}}{2}$ وهو جذر تكعيبي للواحد.

في الحقيقة، نلاحظ أنّ $a^4 = -1$ ومنه $(-\overline{a})^3 = \left(\frac{-1}{a}\right)^3 = a$، فالعدد $z_0 = -\overline{a}$ هو جذرٌ تكعيبي للعدد a. وعلى هذا نرى أنّ الجذور التكعيبيّة للعدد a هي $\left\{-\overline{a}, -\mathrm{j}\,\overline{a}, -\mathrm{j}^2\,\overline{a}\right\}$. أي

$$\left\{-\frac{\sqrt{2}}{2}+\frac{\mathrm{i}\sqrt{2}}{2}, \frac{\sqrt{2}-\sqrt{6}}{4}-\mathrm{i}\frac{\sqrt{6}+\sqrt{2}}{4}, \frac{\sqrt{6}+\sqrt{2}}{4}+\mathrm{i}\frac{\sqrt{6}-\sqrt{2}}{4}\right\}$$

ولمّا كان $e^{\mathrm{i}\pi/12}$ هو الجذر التكعيبي للعدد a الذي له جزء حقيقي موجب وجزء تخيلي موجب استنتجنا أنّ

$$\cos\frac{\pi}{12} = \frac{\sqrt{6}+\sqrt{2}}{4} \text{ و } \sin\frac{\pi}{12} = \frac{\sqrt{6}-\sqrt{2}}{4} \text{ و } \tan\frac{\pi}{12} = 2-\sqrt{3}.$$

ويكتمل الحل. ■

التمرين 13. نضع $\omega_n = e^{\mathrm{i}2\pi/n}$ في حالة n من $\mathbb{N}^*$. احسب، في حالة k من المجموع $\mathbb{Z}$

$$A_n(k) = \sum_{p=0}^{n-1}\omega_n^{kp}$$

، ثمّ احسب $|G_n|^2$ عندما $G_n = \sum_{p=0}^{n-1}\omega_n^{p^2}$.

الحل

- نستفيد مُجدّداً من المساواة : $\sum_{k=0}^{n-1}a^k = \frac{a^n-1}{a-1}$ في حالة $a \neq 1$، فنلاحظ أنّه إذا كان $\omega_n^k \neq 1$ كان

$$\begin{aligned} A_n(k) &= \sum_{p=0}^{n-1}\omega_n^{kp} = \sum_{p=0}^{n-1}(\omega_n^k)^p \\ &= \frac{\omega_n^{kn}-1}{\omega_n^k-1} = \frac{e^{2\pi k\mathrm{i}}-1}{\omega_n^k-1} = 0 \end{aligned}$$

أمّا إذا كان $\omega_n^k = 1$ فعندها $A_n(k) = n$. ولكن $\omega_n^k = 1$ يُكافئ $\frac{k}{n} \in \mathbb{Z}$ أو $k \in n\mathbb{Z}$ أو $n \mid k$. إذن

$$A_n(k) = \begin{cases} n & : \quad n \mid k \\ 0 & : \quad n \nmid k \end{cases}$$

◆ ومن جهة أخرى

$$\begin{aligned}
\left|G_n\right|^2 &= \left(\sum_{p=0}^{n-1} \omega_n^{p^2}\right)\left(\sum_{q=0}^{n-1} \omega_n^{-q^2}\right) = \sum_{0\le p,q<n} \omega_n^{p^2-q^2} \\
&= \sum_{0\le p,q<n} \omega_n^{(p-q)(p+q)} \\
&= \sum_{p=0}^{n-1}\left(\sum_{p-n<r\le p} \omega_n^{r(2p-r)}\right) && : r \leftarrow p-q
\end{aligned}$$

ولكن

$$\begin{aligned}
\sum_{p-n<r\le p} \omega_n^{r(2p-r)} &= \sum_{r=0}^{p} \omega_n^{r(2p-r)} + \sum_{r=p-n+1}^{-1} \omega_n^{r(2p-r)} \\
&= \sum_{r=0}^{p} \omega_n^{r(2p-r)} + \sum_{r'=p+1}^{n-1} \omega_n^{(r'-n)(2p-r'+n)} && : r' \leftarrow r+n \\
&= \sum_{r=0}^{p} \omega_n^{r(2p-r)} + \sum_{r'=p+1}^{n-1} \omega_n^{r'(2p-r')} && : w_n^n = 1 \\
&= \sum_{r=0}^{n-1} \omega_n^{r(2p-r)} && : r \leftarrow r'
\end{aligned}$$

إذن

$$\left|G_n\right|^2 = \sum_{p=0}^{n-1}\left(\sum_{r=0}^{n-1} \omega_n^{r(2p-r)}\right)$$

وهكذا يمكننا أن نكتب

$$\begin{aligned}
\left|G_n\right|^2 &= \sum_{p=0}^{n-1}\left(\sum_{r=0}^{n-1} \omega_n^{r(2p-r)}\right) \\
&= \sum_{r=0}^{n-1}\left(\sum_{p=0}^{n-1} \omega_n^{r(2p-r)}\right) = \sum_{r=0}^{n-1} \omega_n^{-r^2}\left(\sum_{p=0}^{n-1} \omega_n^{2pr}\right)
\end{aligned}$$

وأخيراً

$$\left|G_n\right|^2 = \sum_{r=0}^{n-1} \omega_n^{-r^2} A_n(2r)$$

ولكن نعلم أنّ

$$A_n(2r) = \begin{cases} n & : \quad n \mid 2r \\ 0 & : \quad n \nmid 2r \end{cases}$$

فنناقش الحالتين التاليتين:

- إذا كان $n = 2m$ كان $(n \mid 2r) \Leftrightarrow (m \mid r)$ ولأنّ $0 \leq r < n$ استنتجنا أنّ هذا يحدث فقط في حالة $r \in \{0, m\}$. ومن ثَمّ

$$\begin{aligned} |G_n|^2 &= \sum_{r=0}^{n-1} \omega_n^{-r^2} A_n(2r) \\ &= \omega_n^{-0^2} A_n(0) + \omega_n^{-m^2} A_n(n) \\ &= n\left(1 + (-1)^m\right) \end{aligned}$$

- وإذا كان $n = 2m + 1$ كان $(n \mid 2r) \Leftrightarrow (n \mid r)$ ولأنّ $0 \leq r < n$ استنتجنا أنّ هذا يحدث فقط في حالة $r = 0$. ومن ثَمّ

$$|G_n|^2 = \sum_{r=0}^{n-1} \omega_n^{-r^2} A_n(2r) = \omega_n^{-0^2} A_n(0) = n$$

ومنه

$$|G_n|^2 = \begin{cases} n & : \quad 2 \mid n-1 \\ 2n & : \quad 4 \mid n \\ 0 & : \quad 4 \mid n-2 \end{cases}$$

وهي النتيجة المرجوّة. ■

التمرين 14. حلّ المعادلات التالية :

① $z^2 = -7 + 24\,\mathrm{i}$ ② $z^2 = -3 - 4\,\mathrm{i}$

③ $z^2 + z + 1 = 0$ ④ $z^2 - 2(2 + \mathrm{i})z + 6 + 8\,\mathrm{i} = 0$

⑤ $4(z-1)^4 + (z+1)^4 = 0$ ⑥ $\mathrm{i}\,z^2 + (4\,\mathrm{i} - 3)z + \mathrm{i} - 5 = 0$

⑦ $z^2 - z + 2 = 0$

الحل

① يؤول حَلُّ المعادلة $z^2=-7+24\,\mathrm{i}$ إلى إيجاد الجذرين التربيعيّين للعدد $-7+24\,\mathrm{i}$.
لنفترض أنّ $z=x+\mathrm{i}\,y$ عندئذ $x^2-y^2+2\,\mathrm{i}\,xy=-7+24\,\mathrm{i}$. ومنه

$$x^2-y^2=-7 \quad \text{و} \quad xy=12$$

إذن $(x,y)=(3,4)$ أو $(x,y)=(-3,-4)$. ومنه $z\in\left\{3+4\,\mathrm{i},-3-4\,\mathrm{i}\right\}$.

② يؤول حلُّ المعادلة $z^2=-3-4\,\mathrm{i}$ إلى إيجاد الجذرين التربيعيّين للعدد $-3-4\,\mathrm{i}$. لنفترض أنّ $z=x+\mathrm{i}\,y$ عندئذ $x^2-y^2+2\,\mathrm{i}\,xy=-3-4\,\mathrm{i}$. ومنه

$$x^2-y^2=-3 \quad \text{و} \quad xy=-2$$

إذن $(x,y)=(1,-2)$ أو $(x,y)=(-1,2)$. ومنه $z\in\left\{1-2\,\mathrm{i},-1+2\,\mathrm{i}\right\}$.

③ فيما يلي حَلُّ المعادلة $z^2+z+1=0$. نكتب

$$z^2+z+1=\left(z+\tfrac{1}{2}\right)^2+\tfrac{3}{4}$$

إذن

$$\left(z+\tfrac{1}{2}\right)^2=\left(\mathrm{i}\tfrac{\sqrt{3}}{2}\right)^2$$

ومنه $z+\frac{1}{2}\in\left\{\mathrm{i}\frac{\sqrt{3}}{2},-\mathrm{i}\frac{\sqrt{3}}{2}\right\}$. أو $z\in\left\{-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2},-\frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{2}\right\}$.

④ فيما يلي حَلُّ المعادلة $z^2-2\left(2+\mathrm{i}\right)z+6+8\,\mathrm{i}=0$. نكتب

$$z^2-2(2+\mathrm{i})z+(2+\mathrm{i})^2=(2+\mathrm{i})^2-6-8\,\mathrm{i}=-3-4\,\mathrm{i}$$

أو

$$\left(z-2-\mathrm{i}\right)^2=-3-4\,\mathrm{i}$$

لقد وجدنا في ② أنّ $-3-4\,\mathrm{i}=(1-2\,\mathrm{i})^2$ ، إذن

$$\begin{aligned}\left(z-2-\mathrm{i}\right)^2+3+4\,\mathrm{i}&=\left(z-2-\mathrm{i}\right)^2-\left(1-2\,\mathrm{i}\right)^2\\&=\left(z-2-\mathrm{i}-1+2\,\mathrm{i}\right)\left(z-2-\mathrm{i}+1-2\,\mathrm{i}\right)\\&=\left(z-3+\mathrm{i}\right)\left(z-1-3\,\mathrm{i}\right)\end{aligned}$$

وعليه تكون مجموعة حلول المعادلة المدروسة هي $\left\{3-\mathrm{i},1+3\,\mathrm{i}\right\}$.

⑤ فيما يلي حَلُّ المعادلة $4(z-1)^4+(z+1)^4=0$. لمّا كان 1 ليس حلاً للمعادلة المدروسة استنتجنا أنّها تُكافئ

$$\left(\frac{z+1}{z-1}\right)^4=-4=\left(\sqrt{2}\right)^4 e^{\mathrm{i}\pi}=\left(\sqrt{2}e^{\mathrm{i}\pi/4}\right)^4=(1+\mathrm{i})^4$$

ولأنّ $\left\{1,\mathrm{i},\mathrm{i}^2,\mathrm{i}^3\right\}$ هي الجذور من المرتبة الرابعة للواحد استنتجنا أنّ المعادلة المعطاة تكافئ

$$\frac{z+1}{z-1}\in\left\{1+\mathrm{i},-1+\mathrm{i},-1-\mathrm{i},1-\mathrm{i}\right\}$$

ومنه، لأنّ

$$\frac{z+1}{z-1}=\omega\Leftrightarrow z=\frac{\omega+1}{\omega-1}$$

استنتجنا أنّ $4(z-1)^4+(z+1)^4=0$ تُكافئ

$$z\in\left\{\frac{(1+\mathrm{i})+1}{(1+\mathrm{i})-1},\frac{(1-\mathrm{i})-1}{(1-\mathrm{i})+1},\frac{(1+\mathrm{i})-1}{(1+\mathrm{i})+1},\frac{(1-\mathrm{i})+1}{(1-\mathrm{i})-1}\right\}$$

وبالإصلاح نجد مجموعة الحلول الآتية

$$\left\{1-2\mathrm{i},1+2\mathrm{i},\frac{1-2\mathrm{i}}{5},\frac{1+2\mathrm{i}}{5}\right\}$$

⑥ فيما يلي حلُّ المعادلة $\mathrm{i}z^2+\left(4\mathrm{i}-3\right)z+\mathrm{i}-5=0$. لنلاحظ أنّ

$$\left(\mathrm{i}z^2+(4\mathrm{i}-3)z+\mathrm{i}-5=0\right)\Leftrightarrow\left(z^2+(4+3\mathrm{i})z+1+5\mathrm{i}=0\right)$$

ولكن

$$\begin{aligned}z^2+(4+3\mathrm{i})z+1+5\mathrm{i}&=z^2+(4+3\mathrm{i})z+\left(2+\frac{3}{2}\mathrm{i}\right)^2-\frac{3+4\mathrm{i}}{4}\\&=\left(z+2+\frac{3}{2}\mathrm{i}\right)^2-\frac{(2+\mathrm{i})^2}{4}\\&=\left(z+2+\frac{3}{2}\mathrm{i}-\frac{2+\mathrm{i}}{2}\right)\left(z+2+\frac{3}{2}\mathrm{i}+\frac{2+\mathrm{i}}{2}\right)\\&=\left(z+1+\mathrm{i}\right)\left(z+3+2\mathrm{i}\right)\end{aligned}$$

إذن مجموعة حلول المعادلة المعطاة هي $\left\{-1-\mathrm{i},-3-2\mathrm{i}\right\}$.

⑦ فيما يلي حلُّ المعادلة $z^2 - z + 2 = 0$. لنلاحظ أنّ

$$\begin{aligned} z^2 - z + 2 &= \left(z - \frac{1}{2}\right)^2 + \frac{7}{4} = \left(z - \frac{1}{2}\right)^2 - \left(\frac{\sqrt{7}}{2}\mathrm{i}\right)^2 \\ &= \left(z - \frac{1+\mathrm{i}\sqrt{7}}{2}\right)\left(z - \frac{1-\mathrm{i}\sqrt{7}}{2}\right) \end{aligned}$$

إذن حلول المعادلة $z^2 - z + 2 = 0$ هي $\left\{\frac{1+\mathrm{i}\sqrt{7}}{2}, \frac{1-\mathrm{i}\sqrt{7}}{2}\right\}$.

التمرين 15. ليكن z عدداً من $\mathbb{C}$. نفترض أنّ

$$1 + z + z^2 + \cdots + z^{n-1} - nz^n = 0$$

حيث $n \in \mathbb{N}^*$. أثبت أنّ $|z| \leq 1$.

الحل

ليكن z عدداً من $\mathbb{C}$ يُحقّق $|z| > 1$، عندئذ

$$\begin{aligned} \left|1 + z + z^2 + \cdots + z^{n-1}\right| &\leq 1 + |z| + |z|^2 + \cdots + |z|^{n-1} \\ &< n\,|z|^{n-1} < n\,|z|^n \end{aligned}$$

ومن ثَمّ يكون $1 + z + z^2 + \cdots + z^{n-1} \neq nz^n$. وهذا يثبت المطلوب.

التمرين 16. أثبت في حالة u و v المتطابقة

$$|u+v|^2 + |u-v|^2 = 2\left(|u|^2 + |v|^2\right)$$

عبّر بصياغة هندسيّة عن هذه النتيجة.

الحل

بجمع المساواتين

$$\begin{aligned} |u+v|^2 &= (u+v)(\overline{u}+\overline{v}) = |u|^2 + |v|^2 + u\overline{v} + v\overline{u} \\ |u-v|^2 &= (u-v)(\overline{u}-\overline{v}) = |u|^2 + |v|^2 - u\overline{v} - v\overline{u} \end{aligned}$$

نحصل على المتطابقة المرجوّة.

تنصّ هذه المتطابقة على أنّ مجموع مربعي القطرين في متوازي أضلاع يساوي مجموع مربّعات أضلاعه الأربعة. لهذا يُطلق على هذه المتطابقة اسم متطابقة متوازي الأضلاع.

التمرين 17. حلّ في $\mathbb{C}$ المعادلة $0 = 27(z-1)^6 + (z+1)^6$.

الحل

لمّا كان 1 ليس حلّاً للمعادلة المدروسة استنتجنا أنّها تُكافئ

$$\left(\frac{z+1}{z-1}\right)^6 = -27 = \left(\sqrt{3}\right)^6 e^{\mathrm{i}\pi} = \left(\sqrt{3}e^{\mathrm{i}\frac{\pi}{6}}\right)^6$$

ومنه فحلول المعادلة المعطاة هي التي تحقّق

$$\frac{z+1}{z-1} \in \left\{\sqrt{3}e^{\mathrm{i}\frac{\pi}{6}} \cdot e^{\mathrm{i}\frac{\pi}{3}k} : k \in \{0,1,\ldots,5\}\right\}$$

أو

$$\frac{z+1}{z-1} \in \left\{\sqrt{3}\,e^{\mathrm{i}(1+2k)\pi/6} : k \in \{0,1,\ldots,5\}\right\}$$

ومنه، لأنّ

$$\frac{z+1}{z-1} = \omega \Leftrightarrow z = \frac{\omega+1}{\omega-1}$$

استنتجنا أنّ المعادلة المعطاة تُكافئ

$$z \in \left\{\frac{\sqrt{3}e^{\mathrm{i}(1+2k)\pi/6}+1}{\sqrt{3}e^{\mathrm{i}(1+2k)\pi/6}-1} : k \in \{0,1,\ldots,5\}\right\}$$

ولكن

$$\begin{aligned}\frac{\sqrt{3}e^{\mathrm{i}\theta}+1}{\sqrt{3}e^{\mathrm{i}\theta}-1} &= \frac{\sqrt{3}\cos\theta+1+\mathrm{i}\sqrt{3}\sin\theta}{\sqrt{3}\cos\theta-1+\mathrm{i}\sqrt{3}\sin\theta}\times\frac{\sqrt{3}\cos\theta-1-\mathrm{i}\sqrt{3}\sin\theta}{\sqrt{3}\cos\theta-1-\mathrm{i}\sqrt{3}\sin\theta}\\ &= \frac{3\cos^2\theta-1+3\sin^2\theta-\mathrm{i}2\sqrt{3}\sin\theta}{(\sqrt{3}\cos\theta-1)^2+3\sin^2\theta} = \frac{1-\mathrm{i}\sqrt{3}\sin\theta}{2-\sqrt{3}\cos\theta}\end{aligned}$$

إذن مجموعة حلول المعادلة المدروسة هي

$$\left\{\frac{1-\mathrm{i}\sqrt{3}\sin((1+2k)\pi/6)}{2-\sqrt{3}\cos((1+2k)\pi/6)} : k \in \{0,1,\ldots,5\}\right\}$$

أو

$$\left\{2-\mathrm{i}\sqrt{3}, \frac{1-\mathrm{i}\sqrt{3}}{2}, \frac{2-\mathrm{i}\sqrt{3}}{7}, \frac{2+\mathrm{i}\sqrt{3}}{7}, \frac{1+\mathrm{i}\sqrt{3}}{2}, 2+\mathrm{i}\sqrt{3}\right\}$$ ■

التمرين 18. حلَّ في $\mathbb{C}$ جملة المعادلات :

$$\begin{cases} x+y+z=1 \\ xyz=1 \\ \lvert x\rvert=\lvert y\rvert=\lvert z\rvert \end{cases}$$

الحل

في الحقيقة، نستنتج من المساواة $xyz=1$ أنّ $\lvert x\rvert\lvert y\rvert\lvert z\rvert=1$ ولأنّ $\lvert x\rvert=\lvert y\rvert=\lvert z\rvert$ استنتجنا أنّ

$$\lvert x\rvert=\lvert y\rvert=\lvert z\rvert=1$$

وعليه نرى أنّ

$$xy+yz+zx=\frac{1}{z}+\frac{1}{x}+\frac{1}{y}=\overline{z}+\overline{x}+\overline{y}=\overline{(x+y+z)}=1$$

ولكن

$$\begin{aligned}(Z-x)(Z-y)(Z-z)&=Z^3-(x+y+z)Z^2+(xy+yz+zx)Z-xyz\\&=Z^3-Z^2+Z-1=(Z-1)(Z^2+1)\\&=(Z-1)(Z+\mathrm{i})(Z-\mathrm{i})\end{aligned}$$

إذن $\{x,y,z\}=\{1,\mathrm{i},-\mathrm{i}\}$. ■

التمرين 19. أوجد مجموعة الأعداد العقدية z المحقّقة للخاصة المذكورة في الحالات التالية:

- $\overline{z}=z^2$.
- للأعداد z و $\frac{1}{z}$ و $z-1$ الطويلة نفسها.
- تقع نقاط المستوي الممثّلة بالأعداد z و z^2 و z^4 على استقامة واحدة.
- المثلّث ABC حيث $A(z^2)$ و $B(z)$ و $C(z^3)$ قائم في B.

الحل

- ليكن z عدداً عقديّاً يُحقّق $\overline{z}=z^2$ عندئذ يكون $\lvert z\rvert^2=\lvert z\rvert$ ومنه إمّا أن يكون $z=0$ أو يكون $\lvert z\rvert=1$، وفي هذه الحالة $\overline{z}=z^2$ يقتضي $z^3=\lvert z\rvert^2=1$ أي
$$z\in\left\{e^{2\pi\mathrm{i}k/3}:k\in\{0,1,2\}\right\}$$

وعليه

$$z^2 = \overline{z} \Leftrightarrow z \in \left\{0, 1, \frac{-1+\mathrm{i}\sqrt{3}}{2}, \frac{-1-\mathrm{i}\sqrt{3}}{2}\right\}$$

▫ ليكن z عدداً عقديّاً يُحقّق $\left|1-z\right| = \left|\frac{1}{z}\right| = \left|z\right|$. هذا يُكافئ أنّ $\left|z\right| = 1$ و $\left|z-1\right| = 1$ أي إنّ النقطة التي تمثّل z في المستوي العقدي تنتمي إلى تقاطع الدائرتين $C(0,1)$ و $C(1,1)$ وعليه

$$z \in \left\{\frac{1+\mathrm{i}\sqrt{3}}{2}, \frac{1-\mathrm{i}\sqrt{3}}{2}\right\}$$

ومن الواضح أنّ هاتين القيمتين تُحقّقان الشرط المطلوب.

▫ تقع النقاط $A(z)$ و $B(z^2)$ و $C(z^4)$ على استقامة واحدة إذا وفقط إذا كان الشعاعان $\overrightarrow{BC}$ و $\overrightarrow{AB}$ مرتبطين خطّياً. أي إذا وفقط إذا كان

$$\mathrm{Im}((z^4 - z^2)\overline{(z^2 - z)}) = 0$$

ولكن

$$\begin{aligned}\mathrm{Im}((z^4 - z^2)\overline{(z^2 - z)}) &= \mathrm{Im}\left(z^2(z-1)(z+1)\overline{z}\cdot\overline{(z-1)}\right)\\ &= \left|z\right|^2\left|z-1\right|^2 \mathrm{Im}\left(z(z+1)\right)\end{aligned}$$

وعليه تقع النقاط A و B و C على استقامة واحدة إذا وفقط إذا كان $\mathrm{Im}\left(z(z+1)\right) = 0$. وهذا بدوره يُكافئ

$$\mathrm{Im}\left(z^2 + z + \tfrac{1}{4}\right) = 0$$

أو

$$\left(z + \tfrac{1}{2}\right)^2 \in \mathbb{R}$$

فإمّا أن يكون $z \in \mathbb{R}$ أو $\mathrm{Re}\, z = -\dfrac{1}{2}$. وبالنتيجة تقع النقاط $A(z)$ و $B(z^2)$ و $C(z^4)$ على استقامة واحدة إذا وفقط إذا انتمت النقطة $A(z)$ إلى اجتماع مستقيمين أحدهما محور الفواصل، والثاني هو المستقيم الذي معادلته $x = -\dfrac{1}{2}$.

▫ يكون المثلّث ABC في حالة $A(z^2)$ و $B(z)$ و $C(z^3)$ قائماً في النقطة B، إذا وفقط إذا تعامد الشعاعان $\overrightarrow{BA}$ و $\overrightarrow{BC}$. أي إذا وفقط إذا تحقّق الشرط

$$\mathrm{Re}((z^3-z)\overline{(z^2-z)})=0$$

ولكن

$$\begin{aligned}\mathrm{Re}((z^3-z)\overline{(z^2-z)}) &= \mathrm{Re}\Big(z(z-1)(z+1)\overline{z}\cdot\overline{(z-1)}\Big)\\ &= \left|z\right|^2\left|z-1\right|^2\mathrm{Re}(z+1)\end{aligned}$$

إذن إمّا أن يكون $z=0$ أو $z=1$ وهي حالة تافهة توافق $A=B=C$، أو أن يكون $\mathrm{Re}\,z=-1$. وعليه يكون المثلّث ABC في حالة $A(z^2)$ و $B(z)$ و $C(z^3)$ مثلّثاً قائماً في النقطة B وغير تافه إذا وفقط إذا وقعت النقطة B على المستقيم الذي معادلته $x=-1$. ■

التمرين 20. ليكن (a,b) عنصراً من $\mathbb{C}^2$. يُحقّق $a\neq b$ وليكن k من $\mathbb{R}_+^*$. أثبت أنّ مجموعة نقاط المستوي الممثلة بالعدد العقدي z المحقّق للعلاقة

$$\left|z-a\right|=k\left|z-b\right|$$

هي دائرة أو مستقيم.

الحل

▫ حالة $k=1$. في هذه الحالة يكافئ الشرط $\left|z-a\right|=\left|z-b\right|$ أنّ بُعد النقطة $M(z)$ عن $A(a)$ يساوي بُعدها عن $B(b)$. فهو يُكافئ إذن أنّ النقطة $M(z)$ تنتمي إلى محور القطعة المستقيمة $[AB]$.

وبطريقة أخرى، نعرف C منتصف القطعة المستقيمة $[AB]$ فتكون C صورة العدد العقدي $c=\frac{1}{2}(a+b)$، ونعرّف الشعاع $\vec{\Omega}=\frac{1}{2}\overrightarrow{BA}$ الذي يمثّله $\omega=\frac{1}{2}(a-b)$. فيكون لدينا $a=c+\omega$ و $b=c-\omega$. وعليه

$$\begin{aligned}\left|z-a\right|^2 &= \left|z-c-\omega\right|^2=\left|z-c\right|^2+\left|\omega\right|^2-2\,\mathrm{Re}((z-c)\overline{\omega})\\ \left|z-b\right|^2 &= \left|z-c+\omega\right|^2=\left|z-c\right|^2+\left|\omega\right|^2+2\,\mathrm{Re}((z-c)\overline{\omega})\end{aligned}$$

إذن

$$\left|z-b\right|^2-\left|z-a\right|^2=4\,\mathrm{Re}((z-c)\overline{\omega})$$

وعليه

$$\left(|z-b|=|z-a|\right) \Leftrightarrow \left(\operatorname{Re}((z-c)\overline{\omega})=0\right) \Leftrightarrow \left(\overrightarrow{CM} \perp \vec{\Omega}\right)$$

أي إنّ $|z-b|=|z-a|$ يُكافئ أن تنتمي $M(z)$ إلى المستقيم Δ المار بمنتصف القطعة المستقيمة $[AB]$ عمودياً على المستقيم (AB)، أي محور القطعة المستقيمة $[AB]$.

▫ حالة $k \neq 1$. نستفيد هنا من الخاصّة التالية

$$\forall (u,v) \in \mathbb{C}^2, \quad |u|^2 - |v|^2 = \operatorname{Re}\left((u+v)\overline{(u-v)}\right)$$

التي تنتج من كون

$$\begin{aligned}(u+v)(\overline{u}-\overline{v}) &= |u|^2 - |v|^2 + v\overline{u} - u\overline{v}\\ &= |u|^2 - |v|^2 + 2\,\mathrm{i}\,\operatorname{Im}(v\overline{u})\end{aligned}$$

فنجد

$$\begin{aligned}|z-a|^2 - k^2|z-b|^2 &= \operatorname{Re}\left((z-a+kz-kb)\overline{(z-a-kz+kb)}\right)\\ &= (1-k^2)\operatorname{Re}\left(\left(z-\frac{a+kb}{1+k}\right)\overline{\left(z-\frac{a-kb}{1-k}\right)}\right)\end{aligned}$$

فإذا عرّفنا

$$v=\frac{a-kb}{1-k} \text{ و } u=\frac{a+kb}{1+k}$$

كان لدينا

$$|z-a|^2 - k^2|z-b|^2 = (1-k^2)\operatorname{Re}\left((z-u)\overline{(z-v)}\right) \qquad ❶$$

ولكن من جهة أخرى نعلم أنّ في حالة عددين عقديين z_1 و z_2 لدينا

$$|z_1+z_2|^2 = |z_1|^2 + |z_2|^2 + 2\operatorname{Re}(z_1\overline{z}_2)$$

و

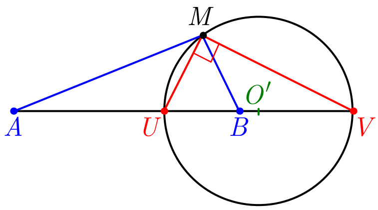
$$|z_1-z_2|^2 = |z_1|^2 + |z_2|^2 - 2\operatorname{Re}(z_1\overline{z}_2)$$

إذن

$$\operatorname{Re}(z_1\overline{z}_2) = \left|\frac{z_1+z_2}{2}\right|^2 - \left|\frac{z_1-z_2}{2}\right|^2$$

وعليه، بتطبيق هذه الخاصة بعد وضع $z_1 = z - u$ و $z_2 = z - v$ في ❶ نستنتج أنّ

$$\left|z-a\right|^2 - k^2\left|z-b\right|^2 = (1-k^2)\left(\left|z-\frac{u+v}{2}\right|^2 - \left|\frac{v-u}{2}\right|^2\right) \qquad ❷$$



لتكن $\mathfrak{C}$ مجموعة النقاط $M(z)$ صوَر الأعداد العقديّة z التي تُحقّق $\left|z-a\right| = k\left|z-b\right|$. ولنعرّف النقطة U صورة العدد العقدي u، والنقطة V صورة العدد العقدي v. وأخيراً لنعرّف النقطة O' منتصف القطعة المستقيمة $[UV]$ أي صورة العدد العقدي $\frac{1}{2}(u+v)$. بالاستفادة من هذه الرموز ومن العلاقتين ❶ و ❷ نجد ما يلي:

$$M \in \mathfrak{C} \Leftrightarrow \overrightarrow{MU}\cdot\overrightarrow{MV} = 0 \Leftrightarrow O'M = \tfrac{1}{2}UV$$

يُبيِّن التكافؤ الأخير أنّ $\mathfrak{C}$ هي الدائرة التي قطرها القطعة المستقيمة $[UV]$، وتمكن قراءة ذلك من التكافؤ الأوّل الذي يعني أنّ M تنتمي إلى مجموعة النقاط التي تُرى منها القطعة $[UV]$ ضمن زاوية قائمة، فهي إذن الدائرة التي قطرها $[UV]$. تسمّى هذه الدائرة **دائرة أبولونيوس** الموافقة للنقطتين A و B والنسبة k. ونلاحظ أنّ العلاقتين

$$v = \frac{a-kb}{1-k} \quad \text{و} \quad u = \frac{a+kb}{1+k}$$

تُكافئان

$$\overrightarrow{AV} = k\overrightarrow{BV} \text{ ،} \overrightarrow{AU} + k\overrightarrow{BU} = 0$$

فنقول إنّ U و V تقسمان القطعة $[AB]$ داخلاً وخارجاً على الترتيب بالنسبة k. ■

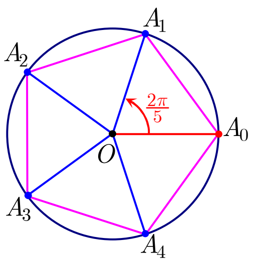
التمرين 21. إنشاء مخمّس منتظم. ليكن (A_0,A_1,A_2,A_3,A_4) مخمّساً منتظماً. نختار معلماً متجانساً $\left(O,\vec{i},\vec{j}\right)$ مبدؤه O مركز المخمّس وفيه $\vec{i}=\overrightarrow{OA_0}$.

1. أعطِ الأعداد العقديّة $(\omega_k)_{0\leq k\leq 4}$ التي تمثّل رؤوس المخمّس $(A_k)_{0\leq k\leq 4}$ بالترتيب. أثبت أنّ $\omega_k=\omega_1^k$ في حالة $0\leq k\leq 4$، وأنّ

$$1+\omega_1+\omega_1^2+\omega_1^3+\omega_1^4=0$$

2. استنتج أن $\cos\left(\frac{2\pi}{5}\right)$ أحد حلول المعادلة $4z^2+2z-1=0$، ثُمّ استنتج قيمة $\cos\left(\frac{2\pi}{5}\right)$.
3. نتأمّل النقطة B التي تمثّل العدد -1. احسب BA_1 و BA_2 بدلالة $\sqrt{5}$ ؟
4. نتأمّل النقطة $I\left(\frac{\mathrm{i}}{2}\right)$، والدائرة $\mathfrak{C}=C\left(I,\frac{1}{2}\right)$، والنقطتين J_1 و J_2 نقطتي تقاطع $\mathfrak{C}$ مع المستقيم (BI)، حيث J_1 هي الأقرب إلى B. احسب BI و BJ_1 و BJ_2.
5. **تطبيق**. استنتج مما سبق، طريقة لإنشاء مخمّس منتظم بالمسطرة والفرجار.

الحل



1. ليكن $\mathcal{R}$ الدوران حول المبدأ O بزاوية قدرها $\dfrac{2\pi}{5}$. لمّا كان المضلّع (A_0,A_1,A_2,A_3,A_4) مخمّساً منتظماً، استنتجنا أنّ $\mathcal{R}(A_k)=A_{k+1}$ وذلك أيّاً كان k من $\{0,1,\ldots,4\}$ حيث $A_5=A_0$. فإذا عرّفنا العدد $\omega_1=\exp\left(\frac{2\pi\,\mathrm{i}}{5}\right)$ استنتجنا أنّ تطبيق الدوران $\mathcal{R}$ يؤول إلى الضرب بالعدد العقدي ω_1. النقطة A_0 هي صورة العدد 1، إذن $A_1=\mathcal{R}(A_0)$ هي صورة العدد ω_1، و $A_2=\mathcal{R}(A_1)$ هي صورة العدد ω_1^2 وكذلك نجد أنّ A_3 هي صورة العدد ω_1^3 و A_4 هي صورة العدد ω_1^4.

نعلم في حالة $a\neq 1$ أنّ $1+a+a^2+a^3+a^4=\dfrac{a^5-1}{a-1}$ إذن لمّا كان $\omega_1\neq 1$ استنتجنا أنّ

$$1+\omega_1+\omega_1^2+\omega_1^3+\omega_1^4=\frac{\omega_1^5-1}{\omega_1-1}=\frac{e^{2\pi\,\mathrm{i}}-1}{\omega_1-1}=0$$

2. تُكتب المساواة السابقة بالشكل

$$\begin{aligned}0 &= 1+\omega_1+\omega_1^2+\omega_1^3+\omega_1^4 = \omega_1^2\left(\omega_1^2+\omega_1^{-2}+\omega_1+\omega_1^{-1}+1\right)\\ &= \omega_1^2\left(\left(\omega_1+\omega_1^{-1}\right)^2+\omega_1+\omega_1^{-1}-1\right)\\ &= \omega_1^2\left(\left(2\cos\left(\tfrac{2\pi}{5}\right)\right)^2+2\cos\left(\tfrac{2\pi}{5}\right)-1\right)\end{aligned}$$

وعليه

$$4\cos^2\left(\tfrac{2\pi}{5}\right)+2\cos\left(\tfrac{2\pi}{5}\right)-1=0$$

فالعدد $\cos\left(\frac{2\pi}{5}\right)$ حلٌّ للمعادلة $4z^2+2z-1=0$.

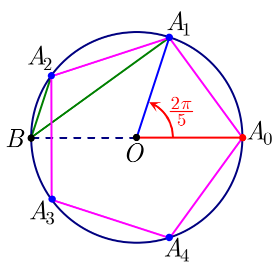
ولكن

$$\begin{aligned}4z^2+2z-1 &= 4\left(z^2+\frac{1}{2}z-\frac{1}{4}\right) = 4\left(\left(z+\frac{1}{4}\right)^2-\frac{5}{16}\right)\\ &= 4\left(z+\frac{1+\sqrt{5}}{4}\right)\left(z-\frac{\sqrt{5}-1}{4}\right)\end{aligned}$$

فللمعادلة $4z^2+2z-1=0$ جذران أحدهما موجبٌ والآخر سالبٌ، ولأنّ $\cos\left(\frac{2\pi}{5}\right)>0$ استنتجنا أنّ $\cos\left(\frac{2\pi}{5}\right)$ هو الجذر الموجب للمعادلة $4z^2+2z-1=0$ أي

$$\cos\left(\frac{2\pi}{5}\right)=\frac{\sqrt{5}-1}{4}.$$

3. يمثّل العدد $1+\omega_1$ الشعاع $\overrightarrow{BA_1}$ ولكن $1+\omega_1=1+\cos\left(\frac{2\pi}{5}\right)+\mathrm{i}\sin\left(\frac{2\pi}{5}\right)$، إذن



$$\begin{aligned}BA_1 &= \left|1+\omega_1\right| = \sqrt{\left(1+\cos\left(\tfrac{2\pi}{5}\right)\right)^2+\sin^2\left(\tfrac{2\pi}{5}\right)}\\ &= \sqrt{2+2\cos\left(\tfrac{2\pi}{5}\right)}\\ &= \sqrt{2+\frac{\sqrt{5}-1}{2}} = \sqrt{\frac{3+\sqrt{5}}{2}}\\ &= \sqrt{\frac{6+2\sqrt{5}}{4}} = \frac{1+\sqrt{5}}{2}\end{aligned}$$

وكذلك يمثّل العدد $1+\omega_1^2$ الشعاع $\overrightarrow{BA_2}$ ولكن

$$1+\omega_1^2=\omega_1\left(\omega_1+\overline{\omega}_1\right)=2\cos\left(\tfrac{2\pi}{5}\right)\cdot\omega_1$$

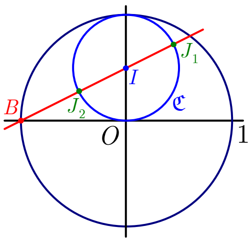
إذن

$$BA_2=\left|1+\omega_1^2\right|=2\cos\left(\tfrac{2\pi}{5}\right)=\frac{\sqrt{5}-1}{2}$$

4. يُمثّل العدد $1+\frac{1}{2}\mathrm{i}$ الشعاع $\overrightarrow{BI}$ إذن :

$$.\ BI=\left|1+\frac{\mathrm{i}}{2}\right|=\sqrt{1+\frac{1}{4}}=\frac{\sqrt{5}}{2}$$

لتكن J نقطة دارجة على المستقيم (BI) عندئذ نستنتج من الارتباط الخطّي للشعاعين $\overrightarrow{BI}$ و $\overrightarrow{IJ}$ أنّه يوجد عددٌ حقيقي t يُحقّق $\overrightarrow{IJ}=t\overrightarrow{BI}$، فإذا اشترطنا أن تنتمي J إلى الدائرة $\mathfrak{C}$ استنتجنا أنّ $IJ=\dfrac{1}{2}$، ومن ثَمّ $\left|t\right|BI=\dfrac{1}{2}$ أي $\left|t\right|=\dfrac{\sqrt{5}}{5}$، وعليه $J\in(BI)\cap\mathfrak{C}$ إذا وفقط إذا كان



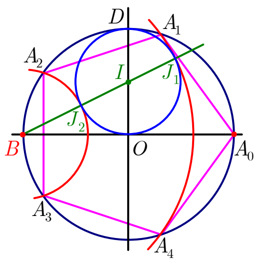
$$\overrightarrow{IJ}\in\left\{\frac{1}{\sqrt{5}}\overrightarrow{BI},-\frac{1}{\sqrt{5}}\overrightarrow{BI}\right\}$$

ولأنّ $\overrightarrow{BJ}=\overrightarrow{BI}+\overrightarrow{IJ}$ استنتجنا أنّ

$$J\in(BI)\cap\mathfrak{C}\Leftrightarrow\overrightarrow{BJ}\in\left\{\frac{\sqrt{5}+1}{\sqrt{5}}\overrightarrow{BI},\frac{\sqrt{5}-1}{\sqrt{5}}\overrightarrow{BI}\right\}$$

فإذا كانت J_1 و J_2 نقطتي تقاطع الدائرة $\mathfrak{C}$ مع المستقيم (BI)، J_2 هي أقرب إلى B، استنتجنا أنّ

$$BJ_1=\frac{\sqrt{5}+1}{\sqrt{5}}BI=\frac{\sqrt{5}+1}{2}=BA_1$$
$$BJ_2=\frac{\sqrt{5}-1}{\sqrt{5}}BI=\frac{\sqrt{5}-1}{2}=BA_2$$



5. إنشاء مخمّس منتظم بالمسطرة والفرجار.

❶ نرسم دائرة $\mathfrak{C}_1 = C\left(O,1\right)$، ونختار عليها النقطة A_0.

❷ نعيّن على $\mathfrak{C}_1$ النقطة B المقابلة قطريّاً للنقطة A_0.

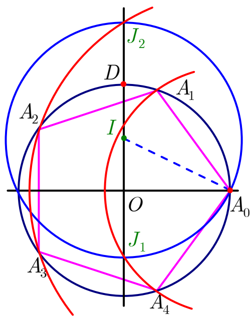
❸ يقطع محور القطعة $[A_0B]$ الدائرة $\mathfrak{C}_1$ في نقطتين إحداهما D.

❹ نرسم الدائرة $\mathfrak{C}$ التي قطرها $[OD]$، ونسمّي مركزها I.

❺ يقطع المستقيم (BI) الدائرة $\mathfrak{C}$ في نقطتين J_1 و J_2، حيث J_2 هي أقرب إلى B.

❻ نرسم الدائرة التي مركزها B وتمر بالنقطة J_1 فتقطع $\mathfrak{C}_1$ بالنقطتين A_1 و A_4.

❼ نرسم الدائرة التي مركزها B وتمر بالنقطة J_2 فتقطع $\mathfrak{C}_1$ بالنقطتين A_2 و A_3. ■



ملاحظة. هناك إنشاء آخر نترك للقارئ أن يعلّله:

❶ نرسم دائرة $\mathfrak{C}_1 = C(O,1)$، ونختار عليها النقطة A_0.

❷ يقطع المستقيم Δ العمودي على $[OA_0]$ في O، الدائرة $\mathfrak{C}_1$ في نقطتين إحداهما D.

❸ نعيِّن النقطة I منتصف القطعة $[OD]$.

❹ نرسم الدائرة $\mathfrak{C}$ التي مركزها I وتمر بالنقطة A_0.

❺ يقطع المستقيم Δ الدائرة $\mathfrak{C}$ في نقطتين J_1 و J_2، حيث J_1 داخل $\mathfrak{C}$.

❻ نرسم الدائرة التي مركزها A_0 وتمر بالنقطة J_1 فتقطع $\mathfrak{C}_1$ بالنقطتين A_1 و A_4.

❼ نرسم الدائرة التي مركزها A_0 وتمر بالنقطة J_2 فتقطع $\mathfrak{C}_1$ بالنقطتين A_2 و A_3.

التمرين 22. ليكن $\mathcal{P}$ المستوي وقد اخترنا فيه معلماً متجانساً $(O,\vec{i},\vec{j})$. ولتكن النقطتان $A(12)$ و $B(9\,\mathrm{i})$، والتطبيق f الذي يقرن بالنقطة $M(z)$ النقطة $M'(z')$ المعرّفة بالعلاقة $z' = -\dfrac{3}{4}\mathrm{i}\,z + 9\,\mathrm{i}$.

1. أثبت أنّ التطبيق f يترك نقطة ثابتة Ω. عيّن إحداثيات Ω ؟

2. ما الخواص الهندسيّة للتحويل f ؟

3. عيِّن $f(A)$ و $f(O)$. وأثبت أنّ Ω هي نقطة مشتركة للدائرتين $\mathfrak{C}_1$ و $\mathfrak{C}_2$ اللتين تقبلان على الترتيب القطعتين المستقيمتين $[OA]$ و $[OB]$ أقطاراً. وبيِّن أنّ Ω هي موقع الارتفاع النازل من O في المثلّث AOB . ثُمّ برهن أنّ $\Omega A \times \Omega B = \Omega O^2$.

4. ارسم شكلاً يضمّ النقاط A و B و Ω و $\mathfrak{C}_1$ و $\mathfrak{C}_2$.

الحل

1. نبحث عن $\Omega(\omega)$ تُحقّق $f(\Omega) = \Omega$ أي $\omega = -\frac{3}{4}\mathrm{i}\,\omega + 9\,\mathrm{i}$. ولكن

$$\begin{aligned} \omega = -\frac{3}{4}\mathrm{i}\,\omega + 9\,\mathrm{i} &\Leftrightarrow (4+3\,\mathrm{i})\omega = 36\,\mathrm{i} \\ &\Leftrightarrow \omega = \frac{36\,\mathrm{i}}{4+3\,\mathrm{i}} = \frac{108+144\,\mathrm{i}}{25} \end{aligned}$$

إذن $\Omega\left(\frac{108}{25},\frac{144}{25}\right)$ هي النقطة الثابتة وفق f .

2. لمّا كان $\omega = -\frac{3}{4}\mathrm{i}\,\omega + 9\,\mathrm{i}$ استنتجنا أنّ من العلاقة $z' = -\frac{3}{4}\mathrm{i}\,z + 9\,\mathrm{i}$ أنّ

$$z' - \omega = -\frac{3}{4}\mathrm{i}(z - \omega)$$

ومنه نستنتج أنّ f تَشَابُه مباشر مركزه Ω ونسبته $\frac{3}{4}$ وزاويته $\frac{3\pi}{2}$.

3. من الواضح أنّ $f(O) = B$ و $f(A) = O$.

- إذن صورة الشعاع $\overrightarrow{\Omega A}$ وفق f هي $\overrightarrow{\Omega O}$ ومن ثَمّ $(\overrightarrow{\Omega A},\overrightarrow{\Omega O}) = \frac{3\pi}{2} \bmod 2\pi$ أي $\overrightarrow{\Omega O}\cdot\overrightarrow{\Omega A} = 0$ إذن تُرى القطعة المستقيمة $[OA]$ ضمن زاوية قائمة من النقطة Ω، والنقطة Ω تنتمي إلى الدائرة $\mathcal{C}_1$ التي قطرها $[OA]$.
- وكذلك فإنّ صورة $\overrightarrow{\Omega O}$ وفق f هي $\overrightarrow{\Omega B}$ ومن ثَمّ $(\overrightarrow{\Omega O},\overrightarrow{\Omega B}) = \frac{3\pi}{2} \bmod 2\pi$ أي $\overrightarrow{\Omega O}\cdot\overrightarrow{\Omega B} = 0$ إذن تُرى القطعة المستقيمة $[OB]$ ضمن زاوية قائمة من النقطة Ω، والنقطة Ω تنتمي إلى الدائرة $\mathcal{C}_2$ التي قطرها $[OB]$.

- وهكذا فإنّ نقطتي تقاطع الدائرتين $\mathcal{C}_1$ و $\mathcal{C}_2$ هما $\{O,\Omega\}$.

- ونستنتج من

$$(\overrightarrow{\Omega A},\overrightarrow{\Omega O}) = \frac{3\pi}{2} \bmod 2\pi \text{ و } (\overrightarrow{\Omega O},\overrightarrow{\Omega B}) = \frac{3\pi}{2} \bmod 2\pi \text{ أنّ}$$

أنّ

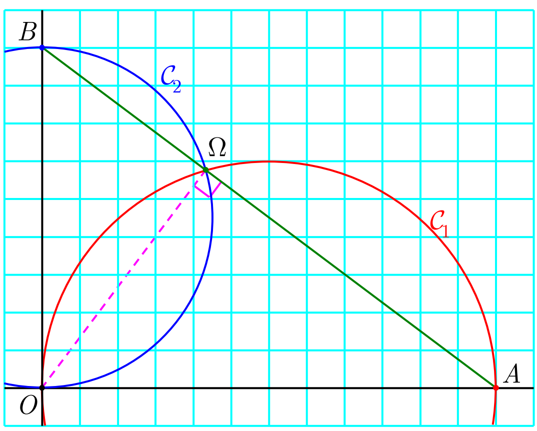
$$(\overrightarrow{\Omega A},\overrightarrow{\Omega B}) = (\overrightarrow{\Omega A},\overrightarrow{\Omega O}) + (\overrightarrow{\Omega O},\overrightarrow{\Omega B}) = \pi \bmod 2\pi$$

فالنقاط A و Ω و B تقع على استقامة واحدة. ولأنّ $\overrightarrow{\Omega O}\cdot\overrightarrow{\Omega B}=0$ استنتجنا أنّ Ω هي موقع الارتفاع النازل من O في المثلّث AOB.

- لمّا كانت صورة الشعاع $\overrightarrow{\Omega A}$ وفق f هي $\overrightarrow{\Omega O}$ استنتجنا أنّ $\frac{\Omega O}{\Omega A}=\frac{3}{4}$، ولمّا كانت صورة الشعاع $\overrightarrow{\Omega O}$ وفق f هي $\overrightarrow{\Omega B}$ استنتجنا أيضاً أنّ $\frac{\Omega B}{\Omega O}=\frac{3}{4}$. وعليه نرى أنّ

$$\Omega A \times \Omega B = \left(\frac{4}{3}\Omega O\right)\times\left(\frac{3}{4}\Omega O\right) = \Omega O^2$$

4. نجد في الشكل التالي الرسم المطلوب.



وبذا يتمّ الإثبات. ■

التمرين 23. ليكن التطبيق $f : \mathbb{C} \to \mathbb{C}, f(z) = z^4 - \sqrt{2}z^3 - 4\sqrt{2}z - 16$.

1. أوجد عددين حقيقيّين a و b ليكون

$$\forall z \in \mathbb{C}, \quad f(z) = (z^2+4)(z^2+az+b)$$

2. استنتج حلول المعادلة $f(z) = 0$ في $\mathbb{C}$، وبيّن أنّ النقاط التي تمثّل هذه الحلول في المستوي العقدي تقع على دائرة واحدة $\mathfrak{C}$ يُطلب تعيينها ؟

الحل

1. في الحقيقة، نلاحظ أنّ

$$\begin{aligned} z^4 - \sqrt{2}z^3 - 4\sqrt{2}z - 16 &= z^4 - 16 - z\sqrt{2}(z^2+4) \\ &= (z^2+4)(z^2 - z\sqrt{2} - 4) \end{aligned}$$

2. نلاحظ من جهة أخرى أنّ

$$\begin{aligned} z^2 - z\sqrt{2} - 4 &= \left(z - \frac{1}{\sqrt{2}}\right)^2 - \frac{9}{2} \\ &= (z - 2\sqrt{2})(z + \sqrt{2}) \end{aligned}$$

إذن

$$z^4 - \sqrt{2}z^3 - 4\sqrt{2}z - 16 = (z + 2\,\mathrm{i})(z - 2\,\mathrm{i})(z+\sqrt{2})(z - 2\sqrt{2})$$

ومنه

$$f(z) = 0 \Leftrightarrow z \in \left\{-\sqrt{2}, 2\sqrt{2}, 2\,\mathrm{i}, -2\,\mathrm{i}\right\}$$

لنضع $\omega = \dfrac{\sqrt{2}}{2}$ فنلاحظ أنّ

$$\left|\omega + \sqrt{2}\right| = \left|\omega - 2\sqrt{2}\right| = \left|\omega - 2\,\mathrm{i}\right| = \left|\omega + 2\,\mathrm{i}\right| = \frac{3\sqrt{2}}{2}$$

إذن تقع جذور المعادلة $f(z) = 0$ على الدائرة $\mathfrak{C} = C\left(\dfrac{1}{\sqrt{2}}, \dfrac{3}{\sqrt{2}}\right)$. ∎

التمرين 24. ليكن $\mathcal{P}$ مستوياً اخترنا فيه معلماً متجانساً $(O,\vec{i},\vec{j})$. ولنتأمّل فيه النقطتين $A(-1+2\mathrm{i})$ و $B(2-\mathrm{i})$.

1. عيِّن ومثِّل في المستوي مجموعة النقاط $\mathcal{E}_1$ المعرّفة بالعلاقة

$$\mathcal{E}_1 = \left\{M(z) : z^2-(1-2\mathrm{i})^2 = \overline{z}^2-(1+2\mathrm{i})^2\right\}$$

وتوثَّق أنّ النقطتين A و B تنتميان إلى $\mathcal{E}_1$.

2. عيِّن ومثِّل في المستوي مجموعة النقاط $\mathcal{E}_2$ المعرّفة بالعلاقة

$$\mathcal{E}_2 = \left\{M(z) : \left(z-1-\mathrm{i}\right)\left(\overline{z}-1+\mathrm{i}\right) = 5\right\}$$

وتوثَّق أنّ النقطتين A و B تنتميان إلى $\mathcal{E}_2$.

الحل

1. نلاحظ أوّلاً أنّ

$$\begin{aligned} M(z)\in\mathcal{E}_1 &\Leftrightarrow z^2-\overline{z}^2 = (1-2\mathrm{i})^2-(1+2\mathrm{i})^2 \\ &\Leftrightarrow z^2-\overline{z}^2 = -8\mathrm{i} \\ &\Leftrightarrow \mathrm{Im}(z^2) = -4 \end{aligned}$$

ومن ثَمّ
$$M(x+\mathrm{i}\,y)\in\mathcal{E}_1 \Leftrightarrow xy = -2$$

وعليه فإنّ $\mathcal{E}_1$ هو القطع الزائد الذي معادلته $xy=-2$.

2. نلاحظ من جهة ثانية أنّ

$$\begin{aligned} M(z)\in\mathcal{E}_2 &\Leftrightarrow \left(z-1-\mathrm{i}\right)\left(\overline{z}-1+\mathrm{i}\right) = 5 \\ &\Leftrightarrow \left(z-1-\mathrm{i}\right)\overline{\left(z-1-\mathrm{i}\right)} = 5 \\ &\Leftrightarrow \left|z-1-\mathrm{i}\right|^2 = 5 \\ &\Leftrightarrow z\in C\left(1+\mathrm{i},\sqrt{5}\right) \end{aligned}$$

وعليه فإنّ $\mathcal{E}_2$ هي الدائرة التي مركزها النقطة التي تمثِّلها $1+\mathrm{i}$، ونصف قطرها $\sqrt{5}$.

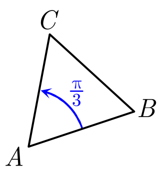
ونتحقّق مباشرة أنّ النقطتين A و B تنتميان إلى كلٍّ من $\mathcal{E}_1$ و $\mathcal{E}_2$. ∎

التمرين 25. ليكن المستوي $\mathcal{P}$ وقد اخترنا فيه معلماً متجانساً $(O,\vec{i},\vec{j})$. ولتكن فيه النقاط $A(a)$ و $B(b)$ و $C(c)$. أثبت أنّ الشرط اللازم والكافي ليكون المثلّث ABC متساوي الأضلاع هو

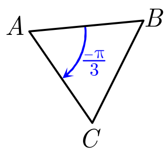
$$\left(\frac{a+b+c}{3}\right)^2 = \frac{a^2+b^2+c^2}{3}$$

الحل

لنرمز بالرمز $\mathcal{R}_M$ إلى الدوران الذي مركزه M وزاويته $\frac{\pi}{3}$، فيكون $\mathcal{R}_M^{-1}$ هو الدوران الذي مركزه M وزاويته $-\frac{\pi}{3}$.



يكون المثلّث ABC متساوي الأضلاع إذا وفقط إذا كان $\mathcal{R}_A(B)=C$ أو $\mathcal{R}_A^{-1}(B)=C$.



ولكن

$$\begin{aligned}\mathcal{R}_A(B)=C &\Leftrightarrow c-a=e^{\mathrm{i}\pi/3}(b-a)\\ &\Leftrightarrow c-e^{\mathrm{i}\pi/3}b+(e^{\mathrm{i}\pi/3}-1)a=0\end{aligned}$$

و

$$\begin{aligned}\mathcal{R}_A^{-1}(B)=C &\Leftrightarrow c-a=e^{-\mathrm{i}\pi/3}(b-a)\\ &\Leftrightarrow c-e^{-\mathrm{i}\pi/3}b+(e^{-\mathrm{i}\pi/3}-1)a=0\end{aligned}$$

ليكن $\frac{-1+\mathrm{i}\sqrt{3}}{2}=e^{\frac{2\pi}{3}\mathrm{i}}=\mathrm{j}$، الجذر التكعيبي للواحد الذي جزؤه التخيّلي موجبٌ تماماً. عندئذ يكون لدينا

$$\begin{aligned}\mathcal{R}_A(B)=C &\Leftrightarrow c+\mathrm{j}^2\,b+\mathrm{j}a=0\\ \mathcal{R}_A^{-1}(B)=C &\Leftrightarrow c+\mathrm{j}b+\mathrm{j}^2\,a=0\end{aligned}$$

وعليه يكون ABC متساوي الأضلاع إذا وفقط إذا تحقّق الشرط

$$(c+\mathrm{j}^2\,b+\mathrm{j}a)(c+\mathrm{j}b+\mathrm{j}^2\,a)=0$$

وهذا يُكافئ، بملاحظة أنّ $1+\mathrm{j}+\mathrm{j}^2=0$، ما يأتي

$$c^2+b^2+a^2-cb-ca-ba=0$$

وهذه العلاقة تُكافئ أيضاً

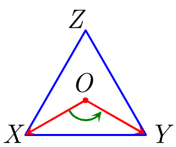
$$\begin{aligned} 3\left(c^2+b^2+a^2\right) &= c^2+b^2+a^2+2cb+2ca+2ba \\ &= \left(a+b+c\right)^2 \end{aligned}$$

أو

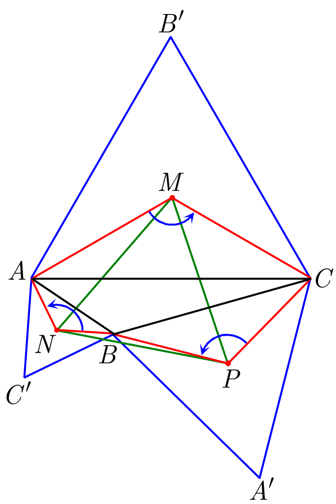
$$\frac{c^2+b^2+a^2}{3} = \left(\frac{a+b+c}{3}\right)^2$$

التمرين 26. ليكن المستوي $\mathcal{P}$، وقد اخترنا فيه معلماً متجانساً $(O,\vec{i},\vec{j})$. وليكن فيه المثلّث ABC. ننشئ على أضلاع هذا المثلّث وخارجه ثلاثة مثلّثات متساوية الأضلاع $AC'B$ و $BA'C$ و $CB'A$. أثبت أنّ مراكز المثلّثات $AC'B$ و $BA'C$ و $CB'A$ تكوّن رؤوس مثلّث متساوي الأضلاع. (تذكّر أنّ مركز مثلّث هو نقطة تقاطع متوسّطاته).

الحل



لنتأمّل بوجه عام مثلّثاً مباشراً XYZ متساوي الأضلاع، ولتكن النقطة O مركز المثلّث أي نقطة تلاقي متوسّطاته، عندئذ نعلم أنّ الدوران $\mathcal{R}_O$ الذي مركزه O وزاويته $\frac{2\pi}{3}$ ينقل X إلى Y، فيكون $\overrightarrow{OY} = \overrightarrow{O\mathcal{R}_O(X)}$، ومنه $z_Y - z_O = \mathrm{j}(z_X - z_O)$ أو $z_O = \frac{z_Y - \mathrm{j}z_X}{1-\mathrm{j}}$، وقد رمزنا بالرمز j إلى الجذر من المرتبة الثالثة للواحد $e^{2\pi\mathrm{i}/3}$.



لنأت الآن إلى مسألتنا، ولنرمز بالرموز N و P و M على الترتيب إلى مراكز المثلّثات $AC'B$ و $BA'C$ و $CB'A$، فيكون لدينا استناداً إلى ما سبق $C = \mathcal{R}_M(A)$ و $B = \mathcal{R}_P(C)$ و $A = \mathcal{R}_N(B)$. وإذا رمزنا بالرموز a و b و c و m و n و p إلى الأعداد العقديّة التي صورها A و B و C و M و N و P استنتجنا أنّ

$$m = \frac{c - \mathrm{j}a}{1-\mathrm{j}}, \quad n = \frac{a - \mathrm{j}b}{1-\mathrm{j}}, \quad p = \frac{b - \mathrm{j}c}{1-\mathrm{j}}$$

ونلاحظ مباشرة أنّ

$$m-n=\frac{c+\mathrm{j}b+\mathrm{j}^2a}{1-\mathrm{j}},\quad p-n=-\frac{a+\mathrm{j}c+\mathrm{j}^2b}{1-\mathrm{j}}$$

إذن

$$m-n=-\mathrm{j}^2\left(p-n\right)$$

فإذا كان $\mathcal{R}$ هو الدوران الذي مركزه N وزاويته $\frac{\pi}{3}$ كان $\mathcal{R}(P)=M$، وهذا يثبتُ أنّ المثلّث MNP مثلّثٌ متساوي الأضلاع.

هذا ونلاحظ أنّ

$$m+n+p=\frac{c-\mathrm{j}a+a-\mathrm{j}b+b-\mathrm{j}c}{1-\mathrm{j}}=a+b+c$$

إذن مركز المثلّث MNP هو نفسه مركز المثلّث ABC. ■

التمرين 27. ليكن المستوي $\mathcal{P}$ وقد اخترنا فيه معلماً متجانساً $(O,\vec{i},\vec{j})$. وليكن فيه المثلّث ABC. ليكن k عدداً من $\mathbb{R}_+^*$ وليكن θ عدداً من $\mathbb{R}$. إذا كانت M نقطة من $\mathcal{P}$ رمزنا بالرمز S_M إلى التشابه المباشر الذي مركزه M وزاويته θ ونسبته k. نعرّف $C_1=S_A(C)$ و $A_1=S_B(A)$ و $B_1=S_C(B)$. أثبت أنّ للمثلّثين ABC و $A_1B_1C_1$ المركز نفسه.

الحل

إذا كان m هو العدد العقدي الذي يمثّل النقطة M، كان S_M هو التطبيق الذي يقرن بالنقطة $Z(z)$ النقطة $Z'(z')$ حيث $z'=m+ke^{\mathrm{i}\theta}(z-m)$.

فإذا رمزنا بالرموز a و b و c و a_1 و b_1 و c_1 إلى الأعداد العقديّة التي صورها A و B و C و A_1 و B_1 و C_1 استنتجنا أنّ

$$\begin{aligned}a_1&=b+ke^{\mathrm{i}\theta}(a-b)\\ b_1&=c+ke^{\mathrm{i}\theta}(b-c)\\ c_1&=a+ke^{\mathrm{i}\theta}(c-a)\end{aligned}$$

ومنه

$$\frac{a_1 + b_1 + c_1}{3} = \frac{a + b + c}{3}$$

وهذا يُثبت أنّ مركز المثلّث ABC الذي يُمثّله العدد $\dfrac{a+b+c}{3}$ ينطبق على مركز المثلّث $A_1B_1C_1$ الذي يُمثّله العدد $\dfrac{a_1+b_1+c_1}{3}$.

التمرين 28. ليكن المستوي $\mathcal{P}$ وقد اخترنا فيه معلماً متجانساً $(O, \vec{i}, \vec{j})$. عيّن الطبيعة الهندسيّة لمجموعة النقاط $M(z)$ في $\mathcal{P}$ التي تُحقّق الأعداد العقديّة التي تمثّلها المساواة $\left|z + \dfrac{1}{z}\right| = 2$.

الحل

ليكن العدد العقدي غير الصفري $z = x + \mathrm{i}\, y = re^{\mathrm{i}\theta}$. عندئذ

$$\begin{aligned}
\left|z + \frac{1}{z}\right| = 2 \Leftrightarrow \left|re^{\mathrm{i}\theta} + \frac{1}{r}e^{-\mathrm{i}\theta}\right|^2 &= 4\\
\Leftrightarrow r^2 + \frac{1}{r^2} + 2\,\mathrm{Re}(e^{2\mathrm{i}\theta}) &= 4\\
\Leftrightarrow r^4 + 1 + 2r^2\cos 2\theta &= 4r^2\\
\Leftrightarrow (r^2-1)^2 - 2r^2(1-\cos 2\theta) &= 0\\
\Leftrightarrow (r^2-1)^2 - (2r\sin\theta)^2 &= 0
\end{aligned}$$

وهذا يُكافئ إذن أنّ

$$\left|z + \frac{1}{z}\right| = 2 \Leftrightarrow \left(r^2 - 1 - 2r\sin\theta\right)\left(r^2 - 1 + 2r\sin\theta\right) = 0$$

ولكن

$$\begin{aligned}
r^2 - 1 - 2r\sin\theta &= x^2 + y^2 - 2y - 1\\
&= x^2 + (y-1)^2 - 2 = \left|z - \mathrm{i}\right|^2 - 2\\
r^2 - 1 + 2r\sin\theta &= x^2 + y^2 + 2y - 1\\
&= x^2 + (y+1)^2 - 2 = \left|z + \mathrm{i}\right|^2 - 2
\end{aligned}$$

وعليه

$$\left|z+\frac{1}{z}\right|=2 \Leftrightarrow \left(\left|z-\mathrm{i}\right|^2-2\right)\left(\left|z+\mathrm{i}\right|^2-2\right)=0$$

أو

$$\left|z+\frac{1}{z}\right|=2 \Leftrightarrow \left(\left|z-\mathrm{i}\right|=\sqrt{2}\right)\vee\left(\left|z+\mathrm{i}\right|=\sqrt{2}\right)$$

إذن يتحقّق الشرط $\left|z+\frac{1}{z}\right|=2$ إذا وفقط إذا انتمت $M(z)$ إلى إحدى الدائرتين $C(\mathrm{i},\sqrt{2})$ أو $C(-\mathrm{i},\sqrt{2})$.

التمرين 29. ليكن المستوي $\mathcal{P}$ وقد اخترنا فيه معلماً متجانساً $(O,\vec{i},\vec{j})$.

I. نتأمّل في حالة (a,b) من $\mathbb{U}\times\mathbb{C}$ التطبيقين

$$f_{a,b}:\mathbb{C}\rightarrow\mathbb{C},\quad f_{a,b}(z)=az+b$$
$$g_{a,b}:\mathbb{C}\rightarrow\mathbb{C},\quad g_{a,b}(z)=a\bar{z}+b$$

ونعرّف المجموعات

$$\mathcal{N}=\left\{g_{a,b}:(a,b)\in\mathbb{U}\times\mathbb{C}\right\} \text{ و } \mathcal{D}=\left\{f_{a,b}:(a,b)\in\mathbb{U}\times\mathbb{C}\right\}$$

وأخيراً $\mathcal{I}=\mathcal{N}\cup\mathcal{D}$.

1. أثبت أنّ $(\mathcal{I},\circ)$ زمرة، وأنّ $(\mathcal{D},\circ)$ زمرة جزئيّة منها.
2. أثبت أنّ كلّ عنصر h من $\mathcal{I}$ يُحقّق الخاصّة $\mathbb{P}$ التالية :

$$\forall(u,v)\in\mathbb{C},\quad \left|h(u)-h(v)\right|=\left|u-v\right|$$

II. لتكن $\mathcal{H}$ مجموعة التطبيقات $h:\mathbb{C}\rightarrow\mathbb{C}$ التي تُحقّق الشرط $\mathbb{P}$.

1. ليكن φ تطبيقاً من $\mathcal{H}$ يُحقّق: $\varphi(0)=0$ و $\varphi(1)=1$ و $\varphi(\mathrm{i})=\mathrm{i}$. أثبت أنّ $\forall z\in\mathbb{C},\ \varphi(z)=z$.
2. وليكن ψ تطبيقاً من $\mathcal{H}$ يُحقّق: $\psi(0)=0$ و $\psi(1)=1$ و $\psi(\mathrm{i})=-\mathrm{i}$. أثبت أنّ $\forall z\in\mathbb{C},\ \psi(z)=\bar{z}$.

3. ليكن g تطبيقاً من $\mathcal{H}$ يُحقِّق الشرطين: $g(0) = 0$ و $g(1) = 1$ أثبت أنّ $g(\mathrm{i}) \in \{\mathrm{i}, -\mathrm{i}\}$. ماذا تستنتج ؟

4. ليكن h تطبيقاً من $\mathcal{H}$. نعرّف $b = h(0)$ و $a = h(1) - h(0)$. أثبت أنّ $a \in \mathbb{U}$. نعرّف إذن التطبيق

$$g : \mathbb{C} \to \mathbb{C},\ g(z) = \overline{a}(h(z) - b)$$

أثبت أنّ $g \in \mathcal{H}$، ثُمّ احسب $g(0)$ و $g(1)$.

وأخيراً برهن أنّ $\mathcal{H} = \mathcal{I}$.

5. بالعودة إلى ما أثبتناه في I . و II .، ما المبرهنة التي أثبتناها ؟

III . لتكن $A(a)$ نقطة من $\mathcal{P}$، وليكن $\vec{\Omega}(\omega)$ شعاعاً غير صفري، وأخيراً ليكن Δ المستقيم المرسوم من A موازياً $\vec{\Omega}$. نتأمّل التحويل الهندسي $\mathcal{S}$ الذي يقرن بالنقطة $M(z)$ النقطة $M'(z')$ نظيرة النقطة M بالنسبة إلى المستقيم Δ . أثبت أنّه يوجد تطبيق s من $\mathcal{N}$، يُحقّق $z' = s(z)$.

IV . أثبت أنّ كلّ تطبيق من $\mathcal{N}$ هو ناتج تركيب انسحاب وتناظر بالنسبة إلى مستقيم، وأنّ كلّ تطبيق من $\mathcal{D}$ هو ناتج تركيب انسحاب ودوران.

الحل

I.1. لنلاحظ أنّه في حالة (a,b) و (c,d) من $\mathbb{U} \times \mathbb{C}$ لدينا

$$\begin{aligned} f_{c,d} \circ f_{a,b} &= f_{ca,cb+d}, & g_{c,d} \circ f_{a,b} &= g_{c\bar{a},c\bar{b}+d},\\ f_{c,d} \circ g_{a,b} &= g_{ca,cb+d}, & g_{c,d} \circ g_{a,b} &= f_{c\bar{a},c\bar{b}+d}, \end{aligned}$$

وهذا يثبت أنّ تركيب التطبيقات $\circ$ هو قانون تشكيل داخلي على $\mathcal{I}$، وهو تجميعي كما نعلم.

- تقبل البنية $(\mathcal{I}, \circ)$ عنصراً حيادياً هو التطبيق المطابق $\mathrm{id} = f_{1,0}$.
- وبملاحظة أنّ

$$\begin{aligned} f_{\bar{a},-\bar{a}b} \circ f_{a,b} &= f_{a,b} \circ f_{\bar{a},-\bar{a}b} &= f_{1,0} = \mathrm{id}\\ g_{a,-a\bar{b}} \circ g_{a,b} &= g_{a,b} \circ g_{a,-a\bar{b}} &= f_{1,0} = \mathrm{id} \end{aligned}$$

نستنتج أنّ لكل عنصر من $\mathcal{I}$ مقلوب بالنسبة إلى القانون $\circ$. فنكون قد أثبتنا أنّ $(\mathcal{I}, \circ)$ زمرة. ونجد فيما سبق أنّ $\mathcal{D}$ مغلقة بالنسبة إلى قانون تركيب التطبيقات، وينتمي إليها العنصر الحيادي، كما ينتمي إليها نظير كلِّ عنصر من عناصرها. إذن $(\mathcal{D}, \circ)$ زمرة جزئيّة من $(\mathcal{I}, \circ)$.

I.2. لنلاحظ أنّه في حالة (a,b) من $\mathbb{U}\times\mathbb{C}$ لدينا

$$\forall(u,v)\in\mathbb{C}^2,\ \left|f_{a,b}(u)-f_{a,b}(v)\right|=\left|a(u-v)\right|=\left|a\right|\cdot\left|u-v\right|=\left|u-v\right|$$

و

$$\forall(u,v)\in\mathbb{C}^2,\ \left|g_{a,b}(u)-g_{a,b}(v)\right|=\left|a\overline{(u-v)}\right|=\left|a\right|\cdot\left|u-v\right|=\left|u-v\right|$$

إذن كلُّ عنصر h من $(\mathcal{I},\circ)$ يُحقّق الخاصّة $\mathbb{P}$.

II.1. ليكن $z\in\mathbb{C}$ ولنعرّف $\omega=\varphi(z)$. لمّا كان φ يُحقِّق الخاصّة $\mathbb{P}$ وكان

$$\varphi(0)=0 \quad \text{و} \quad \varphi(1)=1 \quad \text{و} \quad \varphi(\mathrm{i})=\mathrm{i}$$

استنتجنا أنّ

$$\left|\omega\right|=\left|z\right| \quad \text{و} \quad \left|\omega-1\right|=\left|z-1\right| \quad \text{و} \quad \left|\omega-\mathrm{i}\right|=\left|z-\mathrm{i}\right|$$

- ينتج من $\left|\omega-1\right|^2=\left|z-1\right|^2$ و $\left|\omega\right|=\left|z\right|$ أنّ $\operatorname{Re}\omega=\operatorname{Re}z$.
- وينتج من $\left|\omega-\mathrm{i}\right|^2=\left|z-\mathrm{i}\right|^2$ و $\left|\omega\right|=\left|z\right|$ أنّ $\operatorname{Re}\left(\mathrm{i}\,\omega\right)=\operatorname{Re}\left(\mathrm{i}\,z\right)$ أو $\operatorname{Im}\omega=\operatorname{Im}z$.

ومنه نستنتج أنّ $z=\omega$. فنكون قد أثبتنا أنّ $\forall z\in\mathbb{C},\ \varphi(z)=z$.

II.2. ليكن ψ تطبيقاً من $\mathcal{H}$ يُحقِّق الشروط : $\psi(0)=0$ و $\psi(1)=1$ و $\psi(\mathrm{i})=-\mathrm{i}$.
عندئذ نعرّف التطبيق $\varphi:\mathbb{C}\to\mathbb{C},\varphi(z)=\overline{\psi(z)}$. فنلاحظ أنّه يُحقِّق شروط التطبيق φ في الطلب السابق، وعليه يكون $\forall z\in\mathbb{C},\ \varphi(z)=z$، أي $\forall z\in\mathbb{C},\ \overline{\psi(z)}=z$ أو $\forall z\in\mathbb{C},\ \psi(z)=\overline{z}$.

II.3. ليكن g تطبيقاً من $\mathcal{H}$ يُحقِّق الشرطين : $g(0)=0$ و $g(1)=1$. لنضع $\xi=g(\mathrm{i})$ عندئذ

$$\left|\xi\right|=\left|g(\mathrm{i})-g(0)\right|=\left|\mathrm{i}-0\right|=1$$

و

$$\left|\xi-1\right|=\left|g(\mathrm{i})-g(1)\right|=\left|\mathrm{i}-1\right|=\sqrt{2}$$

نستنتج بتربيع طرفي المساواة $\left|\xi-1\right|=\sqrt{2}$ أنّ $\left|\xi\right|^2+1-\xi-\overline{\xi}=2$، ولكن $\left|\xi\right|=1$ إذن $\xi+\overline{\xi}=0$ ومنه $\xi^2+\left|\xi\right|^2=0$ أو $\xi^2+1=0$، وعليه نرى أنّ $g(\mathrm{i})=\xi\in\{\mathrm{i},-\mathrm{i}\}$.

- فإذا كان $g(\mathrm{i}) = \mathrm{i}$ استنتجنا، بناءً على II.1، أنّ $g = \varphi = f_{1,0}$.
- وإذا كان $g(\mathrm{i}) = -\mathrm{i}$ استنتجنا، بناءً على II.2.، أنّ $g = \psi = g_{1,0}$.

II.4. ليكن h تطبيقاً من $\mathcal{H}$. ولنعرّف $b = h(0)$ و $a = h(1) - h(0)$. عندئذ يكون لدينا

$$\left|a\right| = \left|h(1) - h(0)\right| = \left|1 - 0\right| = 1$$

ومن ثَمّ $a \in \mathbb{U}$. لنعرّف إذن التطبيق $g = f_{\overline{a},-\overline{a}b} \circ h = (f_{a,b})^{-1} \circ h$ أي

$$g : \mathbb{C} \to \mathbb{C},\ \ g(z) = \overline{a}(h(z) - b)$$

فنلاحظ أنّه في حالة (u, v) من $\mathbb{C}^2$ لدينا

$$\begin{aligned}\left|g(u) - g(v)\right| &= \left|f_{\overline{a},-\overline{a}b}(h(u)) - f_{\overline{a},-\overline{a}b}(h(v))\right| \\ &= \left|h(u) - h(v)\right| = \left|u - v\right|\end{aligned}$$

إذن $g \in \mathcal{H}$ ، ولدينا من جهة أخرى

$$\begin{aligned}g(0) &= f_{\overline{a},-\overline{a}b}\left(h(0)\right) = f_{\overline{a},-\overline{a}b}(b) = 0 \\ g(1) &= f_{\overline{a},-\overline{a}b}\left(h(1)\right) = f_{\overline{a},-\overline{a}b}(a + b) = \left|a\right|^2 = 1\end{aligned}$$

إذن استناداً إلى II.3 لدينا $g = f_{1,0}$ أو $g = g_{1,0}$ ، ومنه

$$h = f_{a,b} \circ f_{1,0} = f_{a,b} \quad \text{أو} \quad h = f_{a,b} \circ g_{1,0} = g_{a,b}$$

وهكذا نكون قد أثبتنا أنّ كلَّ عنصرٍ من $\mathcal{H}$ ينتمي إلى $\mathcal{I}$. ولقد أثبتنا الاحتواء المعاكس في I.2، إذن $\mathcal{H} = \mathcal{I}$.

II.5. لقد أثبتنا أنّ التحويلات الإيزومتريّة في المستوي، أي التي تُحقّق أنّ المسافات بين أيِّ نقطتين تساوي المسافة بين صورتيهما، هي تماماً مجموعة التحويلات $M(z) \mapsto M'(z')$ حيث $z' = h(z)$ و $h \in \mathcal{I}$.

III. لتكن $A(a)$ نقطة من $\mathcal{P}$ ، وليكن $\vec{\Omega}(\omega)$ شعاعاً غير صفري، وأخيراً ليكن Δ المستقيم المرسوم من A موازياً $\vec{\Omega}$. نتأمّل التحويل الهندسي $\mathcal{S}$ الذي يقرن بالنقطة $M(z)$ النقطة $M'(z')$ نظيرة النقطة M بالنسبة إلى المستقيم Δ .

لتكن G منتصف القطعة $[MM']$ عندئذ تكون M' نظيرة M بالنسبة إلى Δ إذا وفقط إذا كان Δ محور القطعة المستقيمة $[MM']$.

وهذا يُكافئ تحقُّق الشرطين :

- النقطة G تنتمي إلى Δ، وهذا ما نعبِّر عنه بالارتباط الخطّي للشعاعين $\overrightarrow{AG}$ و $\vec{\Omega}$.
- الشعاع $\overrightarrow{MM'}$ عمودي على $\vec{\Omega}$.

يُكتب هذان الشرطان بالشكل

$$\mathrm{Re}((z'-z)\overline{\omega}) = 0 \quad \text{و} \quad \mathrm{Im}((z_G-a)\overline{\omega}) = 0$$

وقد رمزنا بالرمز z_G إلى العدد العقدي الذي يُمثِّل النقطة G منتصف القطعة $[MM']$ أي $z_G = (z+z')/2$. وعليه يكون لدينا

$$\mathrm{Re}((z'-z)\overline{\omega}) = 0 \quad \text{و} \quad \mathrm{Im}((z+z'-2a)\overline{\omega}) = 0$$

وهذا يُكافئ الشرطين

$$\begin{aligned}\mathrm{Re}\big((z'-a)\overline{\omega}\big) &= \mathrm{Re}\big((z-a)\overline{\omega}\big)\\ \mathrm{Im}\big((z'-a)\overline{\omega}\big) &= -\mathrm{Im}\big((z-a)\overline{\omega}\big)\end{aligned}$$

أو

$$(z'-a)\overline{\omega} = \overline{\big((z-a)\overline{\omega}\big)} = (\overline{z}-\overline{a})\omega$$

وأخيراً

$$z' = \frac{\omega}{\overline{\omega}}\big(\overline{z}-\overline{a}\big)+a = \frac{\omega}{\overline{\omega}}\overline{z}+a-\frac{\omega\overline{a}}{\overline{\omega}}$$

فإذا عرّفنا $\alpha = \dfrac{\omega}{\overline{\omega}} = \dfrac{\omega^2}{|\omega|^2}$ و $\beta = a - \dfrac{\omega}{\overline{\omega}}\overline{a}$ استنتجنا أنّ $z' = g_{\alpha,\beta}(z)$. إذن يوجد في $\mathcal{N}$ تطبيق $s = g_{\alpha,\beta}$ يُحقِّق $z' = s(z)$.

IV. ليكن $g = g_{a,b}$ عنصراً من $\mathcal{N}$ عندئذ يكون $g = f_{1,b}\circ g_{a,0}$. ولمّا كان $\left|a\right| = 1$ وجدنا θ في $\mathbb{R}$ تُحقّق $a = e^{\mathrm{i}\theta}$، لنعرّف إذن $\omega = e^{\mathrm{i}\theta/2}$.

فإذا كان Δ هو المستقيم المار بالمبدأ O موازياً الشعاع $\vec{\Omega}$ الذي يمثّله العدد العقدي ω، استنتجنا استناداً إلى نتيجة السؤال السابق أنّ التناظر $M(z)\mapsto M'(z')$ بالنسبة إلى المستقيم Δ معرّف بالعلاقة

$$z \mapsto z' = \omega^2\overline{z} = a\overline{z} = g_{a,0}(z)$$

وعليه نرى أنّ $g_{a,b}$ هو ناتج تركيب تحويلين: تناظرٌ بالنسبة إلى مستقيم $g_{a,0}$ يليه الانسحاب $f_{1,b}$.

وبأسلوب مماثل، ليكن $f = f_{a,b}$ عنصراً من $\mathcal{D}$ عندئذ يكون $f = f_{1,b} \circ f_{a,0}$. وعليه نرى أنّ $f_{a,b}$ هو ناتج تركيب تحويلين : دورانٌ مركزه O هو $f_{a,0}$ يليه الانسحاب $f_{1,b}$.

الخلاصة

لقد أثبتنا أنّ التحويلات الإيزومتريّة في المستوي، أي التي تُحقّق أنّ المسافات بين أيِّ نقطتين تساوي المسافة بين صورتيهما، هي تماماً زمرة التحويلات الهندسيّة المكوّنة من تركيب انسحابات ودورانات وتناظرات بالنسبة إلى مستقيمات.

التمرين 30. ليكن المستوي $\mathcal{P}$ وقد اخترنا فيه معلماً متجانساً $(O,\vec{i},\vec{j})$. نتأمّل فيه ثلاث دوائر $\mathfrak{C}_1$ و $\mathfrak{C}_2$ و $\mathfrak{C}_3$ تقبل النقطة O مركزاً مشتركاً. نختار على الدائرة $\mathfrak{C}_k$ قوساً $\widehat{A_kB_k}$ يُقابل زاوية مركزية تساوي $\frac{\pi}{3}$، في حالة k من المجموعة $\{1,2,3\}$. لتكن M_k منتصف القطعة المستقيمة $[B_kA_{k+1}]$، مع الاصطلاح $A_4 = A_1$. أثبت أنّ المثلّث $M_1M_2M_3$ متساوي الأضلاع.

الحل

لنفترض أنّ أنصاف أقطار الدوائر $\mathfrak{C}_1$ و $\mathfrak{C}_2$ و $\mathfrak{C}_3$ تساوي R_1 و R_2 و R_3 بالترتيب. ولنفترض، في حالة k من $\{1,2,3\}$، أنّ العدد العقدي $a_k = R_k e^{\mathrm{i}\theta_k}$ يمثّل النقطة A_k . عندئذ تكون B_k صورة العدد العقدي $R_k e^{\mathrm{i}(\theta_k+\pi/3)} = -\mathrm{j}^2\, a_k$ ، وقد استعملنا الرمز j دلالة على العدد $e^{2\mathrm{i}\pi/3} = -\frac{1}{2} + \frac{\mathrm{i}\sqrt{3}}{2}$. ومنه نستنتج أنّ :

- النقطة M_1 هي صورة العدد العقدي

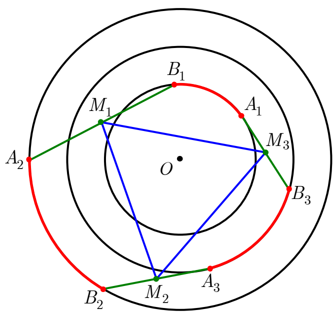
$$m_1 = \frac{1}{2}(a_2 - \mathrm{j}^2\, a_1) .$$

- النقطة M_2 هي صورة العدد العقدي

$$m_2 = \frac{1}{2}(a_3 - \mathrm{j}^2\, a_2) .$$

- النقطة M_3 هي صورة العدد العقدي

$$m_3 = \frac{1}{2}(a_1 - \mathrm{j}^2\, a_3) .$$



ومنه، بالاستفادة من كون $1+\mathrm{j}+\mathrm{j}^2=0$، نجد

$$m_2-m_1=\frac{1}{2}(a_3+\mathrm{j}a_2+\mathrm{j}^2\,a_1)$$
$$m_3-m_1=-\frac{1}{2}(a_2+\mathrm{j}a_1+\mathrm{j}^2\,a_3)$$

إذن

$$m_3-m_1=-\,\mathrm{j}^2(m_2-m_1)=e^{\mathrm{i}\pi/3}(m_2-m_1)$$

و M_3 هي صورة M_2 وفق الدوران الذي مركزه M_1 وزاويته $\frac{\pi}{3}$، وهذا يبرهن أنّ المثلّث $M_1M_2M_3$ متساوي الأضلاع. ■

البنى الجبريّة

عندما نتحدّث عن **بنية جبريّة** على مجموعة E، نقصد تزويد المجموعة E بعدد منتهٍ من قوانين التشكيل الداخلية والخارجية التي تحقّق عدداً من الخواص. وبوجه أعم، عندما نتحدّث عن بنية، نقصد بنيةً جبريّة على مجموعة، وبعض العلاقات الثنائية المتوافقة مع هذه البنية.

إنّ المفهوم الأساسي في هذا البحث هو مفهوم الإيزومورفيزم أو التشاكل التقابلي، أي التقابل المحافظ أو المتوافق مع قوانين التشكيل. فإذا كانت لدينا مجموعتان مزوّدتان ببنى جبرية ومتشاكلتان تقابلياً، فإنّ كلّ خاصة تُبرهَن في إحدى البنيتين ولا تتعلّق إلا بالبنية الجبريّة تكون صحيحة في الأخرى.

① الزمر

1. عموميّات

1-1. **تعريف**. نقول إن المجموعة G المزوّدة بقانون تشكيل داخلي $*$ هي **زمرة** إذا تحقّقت الشروط الثلاثة التالية :

❶ القانون $*$ تجميعي:

$$\forall(a,b,c)\in G^3,\ a*(b*c)=(a*b)*c$$

❷ يقبل القانون $*$ عنصراً حيادياً:

$$\exists e\in G:\forall a\in G,\ \ a*e=e*a=a$$

❸ لكلّ عنصر في G نظير في G:

$$\forall a\in G,\ \exists a'\in G: a*a'=a'*a=e$$

وإذا كان القانون $*$، إضافة إلى ما سبق، تبديلياً، أي

$$\forall(a,b)\in G^2,\ a*b=b*a$$

أسمينا $(G,*)$ **زمرة تبديلية**.

2-1. خواص وأمثلة

① في زمرة $(G,*)$ يكون العنصرُ الحياديُ وحيداً ويكون نظيرُ كلِّ عنصر وحيداً أيضاً.

② إذا كانت $(G,*)$ زمرة وكان a عنصراً من G كان التطبيقان

$$\gamma_a : G \to G : x \to a * x$$
$$\delta_a : G \to G : x \to x * a$$

تقابلين. هذا يعني أنه في زمرة منتهية $(G,*)$ يظهر كلّ عنصر من G مرّة، ومرّة واحدة فقط، في كلِّ سطر وفي كلِّ عمود من جدول القانون $*$.

③ نرمز عادة إلى قانون زمرة تبديلية G بالرمز $+$، وإلى نظير عنصر x بالرمز $-x$ وإلى العنصر الحيادي بالرمز 0 أو 0_G. وإذا كان a عنصراً من G و n عنصراً من $\mathbb{Z}$ كتبنا na دلالة على $\underbrace{a+a+\cdots+a}_{n}$ إذا كان n موجباً تماماً، ودلالة على 0 إذا كان $n=0$، وللدلالة على $(-n)(-a)$ إذا كان n سالباً تماماً.
ونتحقق بسهولة صحّةَ الخواص:

$$\forall a \in G, \forall (m,n) \in \mathbb{Z}^2, \quad ma + na = (m+n)a,$$
$$m(na) = (mn)a$$

④ نرمز عادة إلى قانون زمرة G، سواء أكانت تبديلية أو لم تكن، بالرمز $\langle\cdot\rangle$، الذي يُحذف عادة عند الكتابة، ونرمز إلى نظير عنصر x بالرمز x^{-1} ونسمّيه مقلوب x ونرمز بالرمز 1 أو 1_G إلى العنصر الحيادي.
فإذا كان a عنصراً من G، و n عدداً صحيحاً كتبنا a^n دلالة على $\underbrace{a\cdot a\cdots a}_{n}$ إذا كان n موجباً تماماً، ودلالة على 1 إذا كان $n=0$، ودلالة على $(a^{-1})^{-n}$ إذا كان n سالباً تماماً.

☞ في بقية هذا البحث سنعتمد الرمز السابق $\langle\cdot\rangle$ دلالة على قانون زمرة G، ما لم نذكر خلاف ذلك.

⑤ الأمثلة التالية: $(\mathbb{Z},+)$، $(\mathbb{Q},+)$، $(\mathbb{Q}^*,\times)$، $(\{-1,+1\},\times)$ مألوفة للقارئ.

⑥ إذا كانت E مجموعة، و Δ الفرق التناظري على E، كانت البنية $(P(E),\Delta)$ زمرة تبديلية.

⑦ إذا كانت $(G,*)$ و $(H,\perp)$ زمرتين، أمكننا أن نزوّد $G\times H$ بقانون زمرة على الوجه التالي:

$$(g_1,h_1)\top(g_2,h_2)=(g_1*g_2,h_1\perp h_2)$$

وذلك أياً كان $(g_1.h_1)$ و $(g_2.h_2)$ من $G\times H$.
نسمّي الزمرة $(G\times H,\top)$ زمرة الجداء الديكارتي للزمرتين $(G,*)$ و $(H,\perp)$.
ويمكن تعميم هذا التعريف على الجداء الديكارتي لعددٍ من الزمر.

⑧ إذا كانت E مجموعة، رمزنا بالرمز $S(E)$ إلى مجموعة التقابلات من E إلى E. إنّ $S(E)$ مزوّدةً بقانون تركيب التطبيقات $\circ$ زمرة. وإذا كانت $E=\mathbb{N}_n$، رمزنا بالرمز $(S_n,\circ)$ إلى الزمرة $(S(\mathbb{N}_n),\circ)$، وأسميناها **الزمرة المتناظرة** بعددٍ n من العناصر.

1-3. رموز جديدة

لتكن $(G,\cdot)$ زمرة، و A و B مجموعتين جزئيتين غير خاليتين من G. نكتب $A\cdot B$ للدلالة على المجموعة

$$\{ab : a\in A, b\in B\}$$

ونصطلح أن نكتب aB و Ab دلالة على $\{a\}\cdot B$ و $A\cdot\{b\}$. لاحظ أنّه إذا احتَوَتْ مجموعة A على أكثر من عنصرين كان

$$A\cdot A=\left\{ab : a\in A, b\in A\right\}\neq\left\{a^2 : a\in A\right\}$$

وإذا كانت $A\subset G$ غير خالية، رمزنا أيضاً بالرمز A^{-1} إلى المجموعة $\left\{a^{-1} : a\in A\right\}$.

2. الزمر الجزئية

2-1. تعريف. لتكن $(G,\cdot)$ زمرة، و H مجموعة جزئية من G. نقول إنّ H **زمرة جزئية** من G إذا تحقّق الشرطان:

❶ المجموعة H مغلقة بالنسبة إلى قانون G أي $\forall (x,y) \in H^2, x \cdot y \in H$.

❷ المجموعة H، مزوّدة بقانون G، بنية زمرة.

2-2. مبرهنة. لتكن $(G,\cdot)$ زمرة، و H مجموعة جزئية من G. إنّ الخواص الثلاث التالية متكافئة:

1. تكوّن المجموعة H زمرة جزئية من $(G,\cdot)$.
2. تُحقّق المجموعة H الشروط التالية :

$$(H \neq \varnothing) \text{ و } (\forall (x,y) \in H^2, x \cdot y \in H) \text{ و } (\forall x \in H, x^{-1} \in H)$$

3. تُحقّق المجموعة H الشرطين التاليين :

$$(\forall (x,y) \in H^2, x \cdot y^{-1} \in H) \quad \text{و} \quad (H \neq \varnothing)$$

الإثبات

إنّ إثبات هذه المبرهنة بسيط ومتروك تمريناً للقارئ. ❐

2-3. مثال مهم. كلّ الزمر الجزئية من $(\mathbb{Z},+)$ هي من النمط $(n\mathbb{Z},+)$، مع $n \in \mathbb{N}$.

في الحقيقة، إذا كانت H زمرة جزئية من $(\mathbb{Z},+)$ فإمّا أن تكون $H = \{0\}$ ومن ثَمّ $n = 0$ و $H = n\mathbb{Z}$. وإمّا أن تكون $H \neq \{0\}$ وعندها يوجد عنصر a ينتمي إلى $H\backslash\{0\}$. ولكن عندئذ $-a \in H$ أيضاً. ينجم عن ذلك أنّ $H \cap \mathbb{N}^* \neq \varnothing$. نعرّف إذن $n = \min(H \cap \mathbb{N}^*)$.

- لمّا كانت H مغلقة فيما يخص الجمع وأخذ النظير استنتجنا من $n \in H$ أنّ $n\mathbb{Z} \subset H$.
- من ناحية أخرى، إذا أخذنا عنصراً x من H نجد بالقسمة الإقليديّة زوجاً (q,r) من $\mathbb{Z} \times \mathbb{N}$ يُحقّق $x = qn + r$ و $0 \leq r < n$. ولكن $r = x - qn \in H \cap \mathbb{N}$، إذن يقتضي تعريف n أن يكون $r = 0$، ومن ثَمّ $x = qn \in n\mathbb{Z}$. إذن $H = n\mathbb{Z}$.

وبالعكس، من الواضح أنّ $(n\mathbb{Z},+)$ زمرة جزئية من $(\mathbb{Z},+)$.

2-4. **مبرهنة**. لتكن G زمرة ولتكن $(H_i)_{i\in I}$ جماعة من الزمر الجزئية من G. عندئذ يكون $\bigcap_{i\in I} H_i$ زمرة جزئية من G.

الإثبات

الإثباتُ تحقُّقٌ بسيط ومتروك للقارئ. □

2-5. **مبرهنة وتعريف**. لتكن $(G,\cdot)$ زمرة ولتكن X مجموعة جزئية من G. إنّ تقاطعَ جميع الزمر الجزئية من G التي تحوي X هو زمرةٌ جزئية من G، نسمّيها **الزمرة الجزئية المولَّدة** بالمجموعة X، ونرمز إليها بالرمز $\langle X\rangle$. إنّ $\langle X\rangle$ هي أصغر زمرة جزئية من G تحوي X. وإذا كانت $X\neq\varnothing$ كان

$$\langle X\rangle=\left\{x_1x_2\cdots x_n\;:\;n\in\mathbb{N}^*,\forall i\in\mathbb{N}^*,\quad x_i\in X\cup X^{-1}\right\}$$

أو بقول آخر إنّ $\langle X\rangle$ هي مجموعة كل الجداءات المنتهية من عناصر مأخوذة هي أو مقاليبها من X.

الإثبات

الجزء الأول من المبرهنة واضح باستعمال المبرهنة 2-4. أماّ لإثبات الجزء الثاني فيكفي أن نبرهن أنّ المجموعة

$$\left\{x_1x_2\cdots x_n\;:\;n\in\mathbb{N}^*,\forall i\in\mathbb{N}_n,\,x_i\in X\cup X^{-1}\right\}$$

زمرة جزئية من G تحوي X. وهذا أمر سهل نترك تفاصيله للقارئ. □

2-6. **تعريف**

- ليكن a عنصراً من زمرة $(G,\cdot)$. إذا كانت الزمرة الجزئية $\langle\{a\}\rangle$،المولَّدة بالمجموعة $\{a\}$، والتي نرمز إليها تجاوزاً بالرمز $\langle a\rangle$، هي مجموعةٌ منتهية، أسمينا عدد عناصرها **رتبة العنصر** a. وكتبنا $O(a)=\operatorname{card}(\langle a\rangle)$. أمّا إذا لم تكن المجموعة $\langle a\rangle$ منتهية فإننا نقول إنّ رتبة a لا نهائية ونكتب $O(a)=+\infty$.
- إذا وجدنا في زمرة $(G,\cdot)$ عنصراً a يحقق $G=\langle a\rangle$. قلنا إن الزمرة G **وحيدة التوليد**، أي يكفي عنصر واحد لتوليدها، وقلنا إنّ a **مولِّد** للزمرة G. لاحظ في هذه الحالة أنّ $G=\{a^n\;:\;n\in\mathbb{Z}\}$، وأنّ الزمرة G تبديليةٌ بالضرورة.

- بوجه عام، إذا كانت الزمرةُ $(G,\cdot)$ مجموعةً منتهية، فإننا نسمّيها **زمرة منتهية** ونسمّي عدد عناصرها **رتبة** هذه الزمرة.

2-7. **مثال**. الزمرة $(\mathbb{Z},+)$ وحيدة التوليد لأنّ $\mathbb{Z}=\langle 1\rangle=\langle -1\rangle$ ؛ نلاحظ في هذا المثال أنه يمكن في زمرة وحيدة التوليد أن نجد أكثر من مولّد. سنتعرض لاحقاً لأمثلة مهمّة أخرى.

2-8. **مبرهنة لاغرانج** Lagrange . لتكن $(G,\cdot)$ زمرة منتهية، ولتكن H زمرة جزئية من G . حينئذ يقسم العددُ $\mathrm{card}\,(H)$ العددَ $\mathrm{card}(G)$.

الإثبات

لنعرّف على G العلاقة الثنائية

$$\forall (x,y)\in G^2,\quad x\mathcal{R}_H y \Leftrightarrow x\cdot y^{-1}\in H$$

إنّ هذه العلاقة علاقة تكافؤ لأنّ:

- $\mathcal{R}_H$ انعكاسية لأنّ

$$(1\in H)\Rightarrow \Big(\forall x\in G,\ \ x\mathcal{R}_H x\Big)$$

- $\mathcal{R}_H$ تناظرية

$$\begin{aligned}(x\mathcal{R}_H y) &\Rightarrow x\cdot y^{-1}\in H\\ &\Rightarrow (x\cdot y^{-1})^{-1}=y\cdot x^{-1}\in H\\ &\Rightarrow (y\mathcal{R}_H x)\end{aligned}$$

- $\mathcal{R}_H$ متعدّية

$$\begin{aligned}(x\mathcal{R}_H y)\wedge(y\mathcal{R}_H z) &\Rightarrow \big(x\cdot y^{-1}\in H\big)\wedge\big(y\cdot z^{-1}\in H\big)\\ &\Rightarrow \big((x\cdot y^{-1})(y\cdot z^{-1})=y\cdot z^{-1}\in H\big)\\ &\Rightarrow (y\mathcal{R}_H z)\end{aligned}$$

لنرمز بالرمز k إلى عدد صفوف تكافؤ العلاقة السابقة أي $k=\mathrm{card}(G/\mathcal{R}_H)$. ولنختر ممثلاً من كل صفٍ من هذه الصفوف. نجد عندئذ عناصر $x_1,x_2,\ldots,x_k$ في G تحقّق $G/\mathcal{R}_H=\{[x_1],[x_2],\ldots,[x_k]\}$ ، وهي تجزئة للمجموعة G .

لننظر إلى صف تكافؤ عنصر x من G. من الواضح أنّ

$$\begin{aligned}[x] &= \left\{y \in G : y \cdot x^{-1} \in H\right\} \\ &= \left\{xh \in G : h \in H\right\} = xH\end{aligned}$$

والتطبيق $\varphi : H \to [x],\ h \mapsto xh$ تقابل بين H و $[x]$. إذن $\operatorname{card} H = \operatorname{card}[x]$. ومنه نستنتج أنّ

$$\operatorname{card}(G) = \sum_{m=1}^{k} \operatorname{card}([x_m]) = \sum_{m=1}^{k} \operatorname{card}(H) = k \cdot \operatorname{card}(H) \qquad \square$$

2-9. **ملاحظة**. لقد أثبتنا في الواقع أنّ النسبة $\dfrac{\operatorname{card}(G)}{\operatorname{card}(H)}$ تُمثِّلُ عدد صفوف تكافؤ العلاقة $\mathcal{R}_H$ الذي نرمز إليه عادة بالرمز $[G : H]$.

2-10. **ملاحظة**. لقد استعملنا في الإثبات السابق خاصّتين معروفتين ، هما أنّه في زمرة $(G,\cdot)$ لدينا $(ab)^{-1} = b^{-1}a^{-1}$ و $(a^{-1})^{-1} = a$، ونترك للقارئ مهمة إثبات هاتين الخاصتين تمريناً.

3. التشاكلات الزمرية

3-1. **تعريف**. لتكن الزمرتان $(G,\cdot)$ و $(H,*)$، وليكن f تطبيقاً من G إلى H. نقول إنّ f **تشاكلٌ زمري** إذا وفقط إذا تحقق الشرط

$$\forall (x,y) \in G \times G, \quad f(x \cdot y) = f(x) * f(y)$$

ونقول إنّه **تشاكل تقابلي زمريّ** إذا وفقط إذا كان تقابلاً وتشاكلاً زمرياً في آن معاً. وإذا كان $f : (G,\cdot) \to (H,*)$ تشاكلاً زمرياً، سمّينا **نواة** f المجموعة

$$\ker f = \{x \in G : f(x) = e_H\}$$

وسمّينا **صورة** f المجموعة

$$\operatorname{Im} f = f(G) = \{f(x) : x \in G\}$$

إنّ $\ker f$ و $\operatorname{Im} f$ زمرتان جزئيتان من G و H على التوالي. ينتج ذلك بوصفه حالةً خاصة من المبرهنة التالية:

3-2. **مبرهنة** : ليكن $f:(G,\cdot)\to(H,\cdot)$ تشاكلاً زمرياً.

- إنّ صورة الحيادي في G وفق f هي الحيادي في H أي $f(1_G)=1_H$.
- إنّ صورة نظير عنصر من G وفق f هي نظير صورة هذا العنصر
$\forall x\in G,\quad f(x^{-1})=\big(f(x)\big)^{-1}$.
- إنّ الصورة المباشرة لأي زمرة جزئية من G وفق f هي زمرة جزئية من H .
- إنّ الصورة العكسية لأي زمرة جزئية من H وفق f هي زمرة جزئية من G .

الإثبات

- تنتج الخاصّة الأولى بالاختصار على $f(1_G)$ في طرفي المساواة

$$f(1_G)=f(1_G\cdot 1_G)=f(1_G)\cdot f(1_G)$$

- ولإثبات الخاصّة الثانية، نلاحظ أنه إذا كان x عنصراً من G كان

$$f(x^{-1})\cdot f(x)=f(x^{-1}\cdot x)=f(1_G)=1_H$$

وهذا يقتضي أنّ $\big(f(x)\big)^{-1}=f(x^{-1})$.

- وإذا كانت G_1 زمرة جزئيّة من G، كان لدينا، من جهة أولى

$$1_H=f(1_G)\in f(G_1)$$

ومن جهة ثانية، مهما يكن $x=f(a)$ و $y=f(b)$ (مع (a,b) من G_1^2) يكن

$$x\cdot y^{-1}=f(a)\cdot\big(f(b)\big)^{-1}=f(a)\cdot f(b^{-1})=f(a\cdot b^{-1})\in f(G_1)$$

وهذا يُثبت أنّ $f(G_1)$ زمرة جزئيّة من G .

- وأخيراً نترك للقارئ أن يتحقق صحة الخاصّة الأخيرة بأسلوب مماثل لما سبق. ❐

3-3. **ملاحظة مهمة**. لتكن $(G,\cdot)$ زمرة، وليكن $f:G\to E$ تقابلاً بين G ومجموعة ما E . إنّ قانون التشكيل الداخلي $*$ المعرف على E بالعلاقة

$$\forall(x,y)\in E\times E,\quad x*y=f\big(f^{-1}(x)\cdot f^{-1}(y)\big)$$

يجعل من $(E,*)$ زمرة، ويكون f تشاكلاً تقابلياً زمرياً. نقول عندئذ إننا قد نقلنا بنية G إلى E .

فمثلاً يمكن للقارئ أنّ ينقل بنية الزمرة $(\mathbb{R},+)$ إلى المجال $]-1,+1[$، مُستعملاً، لتحقيق ذلك، التطبيقَ $f:\mathbb{R}\to]-1,+1[,\ x\mapsto\dfrac{x}{1+|x|}$.

4. زمرة خارج القسمة

لتكن $(G,+)$ زمرة **تبديلية**، ولتكن H زمرة جزئية من G. نعرّف على G،كما في المبرهنة 2-8. العلاقة الثنائية

$$\forall(x,y)\in G^2,\quad x\mathcal{R}_H y \Leftrightarrow x-y\in H$$

لقد وجدنا أنّ هذه العلاقة علاقة تكافؤ. لنرمز إذن بالرمز G/H إلى مجموعة صفوف التكافؤ $G/\mathcal{R}$. ولننظر إلى صف تكافؤ عنصر a من G. من الواضح أنّ

$$\begin{aligned}[a] &= \{x\in G : x-a\in H\}\\ &= \{x\in G : \exists h\in H, x=a+h\}\\ &= \{a+h\in G : h\in H\} = a+H\end{aligned}$$

وبوجه خاص $H=[0]$.

- إذا كان A و B عنصرين من G/H كانت المجموعة

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

أيضاً عنصراً من G/H. في الحقيقة سنثبت أنّه إذا كان $A=[a]$ و $B=[b]$ كان $A\dot{+}B=[a+b]$.

  - ليكن x عنصراً من $[a+b]$. يوجد عندئذ h من H يُحقّق $x=a+b+h$، ولكن $b+h\in[b]=B$ و $a\in[a]=A$ إذن $x\in A\dot{+}B$.
  - وبالعكس، إذا كان x عنصراً من $A\dot{+}B$ يوجد عندئذ $\tilde{a}$ من A و $\tilde{b}$ من B يُحقِّقان $x=\tilde{a}+\tilde{b}$. ولكن $B=[b]$ و $A=[a]$، فيوجد h_1 في H يُحقِّق $\tilde{b}=b+h_1$، و يوجد h_2 في H يُحقّق $\tilde{a}=a+h_2$، ومن ثَمّ

$$x=a+b+h_1+h_2\in a+b$$

ينتج مما سبق أنّ $\dot{+}$ هو قانون تشكيل داخلي على G/H. ونتحقق بسهولة أنّ القانون $\dot{+}$ تبديلي وتجميعي، ويقبل $[0]$ عنصراً حيادياً.

- إذا كان A عنصراً من G/H كانت المجموعة $-A = \{-a : a \in A\}$ أيضاً عنصراً من G/H . لأنه إذا كان $A = [a]$ كان $-A = [-a]$. ونتحقق بسهولة أيضاً أنّ كلّ عنصر A من G/H يقبل $-A$ نظيراً في G/H . ينتج من الدراسة السابقة أنّ $(G/H, \dot{+})$ زمرة تبديلية نسمّيها **زمرة خارج قسمة G على H** .

ونرى من ناحية أخرى أنّ الغمر القانوني $Q : G \to G/H, a \mapsto [a]$ تشاكل زمري.

سندرس فيما يلي مثالاً مهمّاً جداً من الناحية العملية. لنتأمّل الزمرة $G = (\mathbb{Z}, +)$، وزمرة جزئية منها $H = n\mathbb{Z}$ حيث $n \neq 0$. إنّ زمرة خارج القسمة $\mathbb{Z}/n\mathbb{Z}$ هي زمرة تبديلية بالنسبة إلى القانون $\dot{+}$ الذي عرّفناه سابقاً والذي سنرمز إليه $+$ تجاوزاً.

4-1.مبرهنة. إنّ الزمرة $\mathbb{Z}/n\mathbb{Z}$، $(n \neq 0)$، منتهية وعدد عناصرها n . في الحقيقة إنّ

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$$

الإثبات

يكفي أن نثبت صحّةَ الخاصتين التاليتين:

- إذا كان $0 \leq r < r' < n$ كان $[r] \neq [r']$.
- إذا كان A عنصراً من $\mathbb{Z}/n\mathbb{Z}$، فيوجد r في $\{0, \ldots, n-1\}$ يُحقّق $A = [r]$.

في الحقيقة، إذا كان $0 \leq r < r' < n$ فلا يمكن أن يكون $r' - r$ مضاعفاً للعدد n ومن ثَمّ $[r] \neq [r']$.

ومن ناحية أخرى، إذا كان A عنصراً من $\mathbb{Z}/n\mathbb{Z}$ ، فيوجد a من $\mathbb{Z}$ يُحقّق $A = [a]$. نُجري قسمة إقليدية للعدد a على n فنجد (q, r) في $\mathbb{Z} \times \mathbb{N}$ يُحقّق $a = qn + r$ و $0 \leq r < n$. ومن ثَمّ $a - r \in n\mathbb{Z} = H$ ومنه $[r] = [a] = A$. □

لاحظ أنه في $\mathbb{Z}/n\mathbb{Z}$ لدينا $[\ell] = \{\ell + kn : k \in \mathbb{Z}\}$. وفي حالة $n = 0$ فإنّ الزمرة $\mathbb{Z}/n\mathbb{Z}$ تُشاكِلُ تقابلياً $\mathbb{Z}$.

5. الزمر الوحيدة التوليد

لنذكّر بأن زمرة $(G,\cdot)$ تكون وحيدة التوليد، إذا وُجِدَ في G عنصرٌ a يحقق

$$G = \langle a \rangle = \left\{ a^k : k \in \mathbb{Z} \right\}$$

في هذه الحالة يكون التطبيق $\varphi_a : \mathbb{Z} \to G,\ k \mapsto a^k$ تشاكلاً زمرياً غامراً، نواته $\ker \varphi_a$ زمرة جزئية من $\mathbb{Z}$ فهي من النمط $n\mathbb{Z}$ مع $n \in \mathbb{N}$. لاحظ أنّه إذا كان $r \in [k]$ كان $r - k \in n\mathbb{Z} = \ker \varphi_a$ ومن ثَمّ $a^r = a^k$. ينجم عن ذلك أنّ هناك تطبيقاً

$$\tilde{\varphi}_a : \mathbb{Z}/n\mathbb{Z} \to G,\ [k] \mapsto a^k$$

ويثبتُ القارئ بسهولة أنّ التطبيق $\tilde{\varphi}_a$ تشاكل تقابلي زُمري. نستنتج من ذلك المبرهنة التالية.

5-1. مبرهنة وتعريف. لتكن $(G,\cdot)$ زمرة وحيدة التوليد وتقبل a مولّداً لها.

- إذا كانت G غير منتهية، فهي تُشاكِلُ تقابلياً الزمرة $(\mathbb{Z},+)$، وفق التشاكل $k \mapsto a^k$.
- إذا كانت G منتهية وعدد عناصرها n فهي تشاكل تقابلياً $(\mathbb{Z}/n\mathbb{Z},+)$، وفق التشاكل $[k] \mapsto a^k$. ونقول إنّ G **زمرة دوّارة** رتبتها n.

تفيدنا هذه النتيجة في إعطاء الخاصة المميّزة التالية لرتبة عنصر في زمرة.

5-2. نتيجة. ليكن a عنصراً رتبته منتهية في زمرة $(H,\cdot)$. عندئذ

$$O(a) = \min\left\{ k \in \mathbb{N}^* : a^k = 1 \right\}.$$

ذلك لأن $\langle a \rangle$ زمرة دوّارة جزئية من H، فهي تُشاكِل تقابلياً الزمرة $(\mathbb{Z}/n\mathbb{Z},+)$ حيث $n = O(a)$. □

وتبيّن الخاصّة التالية صفةً مهمّة من صفات الزمر الدّوارة.

5-3. مبرهنة : لتكن $(G,\cdot)$ زمرة دوّارة عدد عناصرها n وتقبل a مولّداً لها. عندئذ أياً كان القاسم d للعدد n، توجد زمرة جزئية وحيدة في G عدد عناصرها d. وهي الزمرة المولّدة بالعنصر $b = a^{n/d}$.

الإثبات

ليكن d قاسماً ما للعدد n، ولنضع $n = dm$. إنّ الزمرة $\langle a^m \rangle$ زمرة جزئية من G يُعطى عدد عناصرها بالعلاقة $\min\{k \in \mathbb{N}^* : mk \in n\mathbb{Z}\}$ فهو إذن d.

وبالعكس، لتكن H زمرة جزئية من G عدد عناصرها d، $n = dm$. ولنتأمّل التشاكل $\varphi_a : \mathbb{Z} \to G, k \mapsto a^k$. إنّ $\varphi_a^{-1}(H)$ زمرة جزئية من $(\mathbb{Z}, +)$ فهي من الشكل $s\mathbb{Z}$. وهذا يكافئ قولنا إنّ

$$H = \{a^{sk} : k \in \mathbb{Z}\}$$

ومن ثَمّ $H = \langle a^s \rangle$. وبناءً على النتيجة 5-2. نجد

$$d = \min\{k \in \mathbb{N}^* : a^{sk} = 1\}$$

أو إن sd هو أصغر مضاعف للعدد $n = d\,m$، أي $s = m$. إذن $H = \langle a^m \rangle$. ❐

.6 الزمر المتناظرة S_n

لنذكِّر بأنّ **الزمرة المتناظرة** S_n هي الزمرة التي عناصرها التقابلات على المجموعة $\mathbb{N}_n$ والمزودة بقانون تركيب التطبيقات. نسمّي عادة عناصر هذه الزمرة **تباديلَ**، وقد رأينا أنّ $\text{card}(S_n) = n!$. سنفترض فيما يلي أنّ $n \geq 2$ تجنباً للحالات التافهة.

إذا كان σ عنصراً من S_n كتبنا σ بالشكل

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

1-6. تعريف. لنفترض أنّ $n \geq 2$. نقول إنّ τ من S_n **مُناقلة**، إذا وُجِدَ عنصران مختلفان (a, b) من $\mathbb{N}_n^2$ يُحقِّقان

- $\tau(a) = b$.
- $\tau(b) = a$.
- $\forall k \in \mathbb{N}_n \backslash \{a, b\}, \tau(k) = k$.

نرمز في هذه الحالة إلى المناقلة τ بالرمز (a, b) أو بالرمز $\tau_{a,b}$.

لاحظ أنّ كل مناقلة τ تُحقّق $\tau \circ \tau = I$ إذ يمثِّل I التطبيق المطابق على $\mathbb{N}_n$ وهو العنصر الحيادي في S_n.

2-6. **مبرهنة**. لتكن $n \geq 2$. إنّ مجموعة المناقلات في S_n تولّد الزمرة S_n.

الإثبات

سنثبت هذه المبرهنة بالتدريج على العدد n.

- الخاصة صحيحة عندما تكون $n = 2$، لأنّ $S_2 = \{I, \tau_{1,2}\}$ و $\tau_{1,2} \circ \tau_{1,2} = I$.
- لنفترض صحة الخاصة عند $n - 1$، وليكن σ تبديلاً من S_n. نناقش حالتين :

  - إمّا أن يكون $\sigma(n) = n$، فنضع $\tilde{\sigma} : \mathbb{N}_{n-1} \to \mathbb{N}_{n-1}, k \mapsto \sigma(k)$، ويكون $\tilde{\sigma}$ عنصراً من S_{n-1}. نجد عندئذ استناداً إلى فرْض التدريج مناقلات $\tilde{\tau}_1, \tilde{\tau}_2, \ldots, \tilde{\tau}_k$ من S_{n-1} تُحقّق $\tilde{\sigma} = \tilde{\tau}_1 \circ \tilde{\tau}_2 \circ \cdots \circ \tilde{\tau}_k$.

    نعرّف عندئذ المناقلات $\tau_1, \tau_2, \ldots, \tau_k$ من S_n كما يلي:
$$\tau_i(x) = \begin{cases} n & : \quad x = n, \\ \tilde{\tau}_i(x) & : \quad x \neq n. \end{cases}$$
    ليكون $\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$. ويتم إثبات المطلوب.

  - وإمّا أن يكون $\sigma(n) = p \neq n$. فنعرّف $\overline{\sigma} = \tau_{n,p} \circ \sigma$ من S_n. إنّ التبديل $\overline{\sigma}$ يُحقّق $\overline{\sigma}(n) = n$ يمكننا إذن تطبيق الحالة السابقة عليه، فنجد مناقلات τ_1 و τ_2 و … و τ_k من S_n، تُحقّق $\overline{\sigma} = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$، ويكون من ثَمّ
$$\sigma = \tau_{n,p} \circ \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$$
    ويتم الإثبات في هذه الحالة أيضاً. ❐

3-6. توقيع تبديل

لنذكّر أنّ $P_2^{(n)}$ هي مجموعة أجزاء $\mathbb{N}_n$ المؤلّفة من عنصرين. أياً كانت المجموعة $A = \{a, b\}$ من $P_2^{(n)}$، وأيّاً كان σ من S_n، نعرّف
$$\delta(\sigma, A) = \frac{\sigma(b) - \sigma(a)}{b - a} = \frac{\sigma(a) - \sigma(b)}{a - b}$$
ونلاحظ جوْدَة هذا التعريف لأنّ قيمة العدد $\delta(\sigma, A)$ لا تتعلق إلاّ بالمجموعة A، وليس بالعنصرين a و b.

فإذا كان (σ_2,σ_1) من $S_n\times S_n$ وكانت $A=\{a,b\}$ من $P_2^{(n)}$، أمكننا أن نكتب:

$$\begin{aligned}\delta(\sigma_2\circ\sigma_1,A)&=\frac{\sigma_2(\sigma_1(b))-\sigma_2(\sigma_1(a))}{b-a}\\&=\frac{\sigma_2(\sigma_1(b))-\sigma_2(\sigma_1(a))}{\sigma_1(b)-\sigma_1(a)}\cdot\frac{\sigma_1(b)-\sigma_1(a)}{b-a}\end{aligned}$$

ومنه

$$\delta(\sigma_2\circ\sigma_1,A)=\delta(\sigma_2,\sigma_1(A))\cdot\delta(\sigma_1,A)\qquad(*)$$

لنعرّف في حالة σ من S_n المقدار

$$\Delta(\sigma)=\prod_{A\in P_2^{(n)}}\delta(\sigma,A)$$

وليكن (σ_2,σ_1) من $S_n\times S_n$، بملاحظة أنّ التطبيق $P_2^{(n)}\to P_2^{(n)},A\mapsto\sigma_1(A)$ تقابلٌ، وانطلاقاً من العلاقة $(*)$، نجد أنّ

$$\begin{aligned}\Delta(\sigma_2\circ\sigma_1)&=\prod_{A\in P_2^{(n)}}\delta(\sigma_2,\sigma_1(A))\cdot\prod_{A\in P_2^{(n)}}\delta(\sigma_1,A)\\&=\Delta(\sigma_2)\cdot\Delta(\sigma_1)\end{aligned}$$

ونستنتج من ذلك أنّ التطبيق

$$\Delta:S_n\to(\mathbb{R}^*,\cdot),\ \sigma\mapsto\Delta(\sigma)=\prod_{A\in P_2^{(n)}}\delta(\sigma,A)=\prod_{1\le i<j\le n}\frac{\sigma(j)-\sigma(i)}{j-i}$$

تشاكلٌ زمري، يحقق بوجه خاص $\Delta(I)=1$ و $\Delta(\sigma^{-1})=\dfrac{1}{\Delta(\sigma)}$.

4-6. مبرهنة. إنّ التطبيق Δ المعرّف آنفاً تشاكلٌ زمريٌّ غامر من S_n إلى $(\{-1,+1\},\cdot)$.

الإثبات

لتكن المناقلة $\tau=(1,2)$، ولنحسب $\Delta(\tau)$.

- إذا كانت A من $P_2^{(n)}$، تُحقّق $A\cap\{1,2\}=\varnothing$ كان $\delta(\tau,A)=1$.
- وإذا كانت $A=\{1,j\}$ من $P_2^{(n)}$، تُحقّق $A\cap\{1,2\}=\{1\}$ كان
$$\delta(\tau,A)=\frac{j-2}{j-1}$$
- وإذا كانت $A=\{2,j\}$ من $P_2^{(n)}$ تُحقّق $A\cap\{1,2\}=\{2\}$ كان

$$\delta(\tau, A) = \frac{j-1}{j-2}$$

▪ وأخيراً إذا كانت $A = \{1,2\}$ كان $\delta(\tau, A) = -1$. ينتج إذن أنّ $\Delta(\tau) = -1$.

لتكن المناقلة $\tau_{i,j} = (i,j)$، وليكن σ من S_n تبديلاً يحقق $\sigma(1) = i$ و $\sigma(2) = j$. عندئذ يتوثّق القارئ بسهولة من صحةِ العلاقة: $\tau_{i,j} = \sigma \circ \tau_{1,2} \circ \sigma^{-1}$. ويكون من ثَمّ

$$\Delta(\tau_{i,j}) = \Delta(\sigma) \cdot \Delta(\tau_{1,2}) \cdot \Delta(\sigma^{-1}) = -\frac{\Delta(\sigma)}{\Delta(\sigma)} = -1$$

نستنتج أنّ $\Delta(\tau) = -1$ أياً كانت المناقلة τ من S_n.

وأخيراً إذا كان σ من S_n نجد مناقلات $\tau_1, \tau_2, \ldots, \tau_k$ من S_n تُحقّق

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_k$$

وبذا يكون $\Delta(\sigma) = (-1)^k$. وهكذا نستنتج أنّ Δ يأخذ قيمه في $\{-1,+1\}$، وهو غامر لأنّ $n \geq 2$. ❐

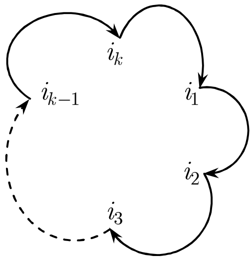
6-5. تعريف. إذا كان σ تبديلاً من S_n، أسمينا المقدار $\Delta(\sigma)$ **توقيع التبديل** σ. لقد أثبتنا أنّ $\Delta(\sigma) \mapsto \sigma$ تشاكل زمري غامر من S_n إلى $(\{-1,+1\},\cdot)$، وإذا كان σ ناتجَ تركيب k مناقلة كان $\Delta(\sigma) = (-1)^k$.

6-6. نتيجة. ينجم عمّا سبق أن $\Delta(\sigma) = -1$، إذا وفقط إذا كان σ ناتج تركيب عدد فردي من المناقلات.

6-7. تعريف. إنّ نواة التشاكل Δ، أي $\{\sigma \in S_n : \Delta(\sigma) = 1\}$ زمرة جزئية من S_n نسمّيها **الزمرة المتناوبة**، ونرمز إليها بالرمز A_n. وعليه ينتمي تبديلٌ مّا إلى الزمرة المتناوبة إذا وفقط إذا كان ناتج تركيب عدد زوجي من المناقلات.

ونظراً إلى أنّ التطبيق $\psi : A_n \to S_n \backslash A_n, \sigma \mapsto \tau_{1,2} \circ \sigma$ تَقابلٌ فإن رتبة الزمرة المتناوبة A_n تساوي $\frac{n!}{2}$.

6-8. تعريف. نقول إنّ التبديل σ من S_n **دورة** من المرتبة k، ($2 \leq k$)، إذا وفقط إذا وُجِدت عناصر $i_1, i_2, \ldots, i_k$ مختلفة مثنى مثنى وعددها k من $\mathbb{N}_n$ تُحقّق



- $\forall j \in \mathbb{N}_n \backslash \{i_1, i_2, \ldots, i_k\}, \quad \sigma(j) = j$.
- $\forall p \in \mathbb{N}_{k\text{-}1}, \quad \sigma(i_p) = i_{p+1}$.
- $\sigma(i_k) = i_1$.

نرمز عادة إلى مثل هذا التبديل بالرمز $(i_1, i_2, \ldots, i_{k-1}, i_k)$.

نلاحظ أنّ المناقلات هي دورات من المرتبة 2. ومن ناحية أخرى يمكن أن نكتب كل دورة من المرتبة k بوصفها ناتجَ تركيب $k-1$ مناقلة:

$$(i_1, i_2, \ldots, i_{k-1}, i_k) = (i_1, i_2) \circ (i_2, i_3) \circ \cdots \circ (i_{k-1}, i_k)$$

ومن ثَمّ إذا كانت σ دورة من المرتبة k كان $\Delta(\sigma) = (-1)^{k-1}$.

إذا كانت $c = (i_1, i_2, \ldots, i_{k-1}, i_k)$ دورة من المرتبة k أسمينا المجموعة $\{i_k, \ldots, i_2, i_1\}$ حامل الدورة c، ويمكننا أن نبرهن على أنّ كل تبديل σ من $S_n \backslash \{I\}$ يُكتب على أنّه ناتجُ تركيب دورات حواملها منفصلة مثنى مثنى، وهذه الكتابة وحيدة إلاّ فيما يتعلّق بالترتيب.

9-6. مثال. ليكن التبديل σ من S_{10} المعرّف كما يلي :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 5 & 2 & 3 & 4 & 1 & 6 & 10 & 7 & 8 \end{pmatrix}$$

فإذا أردنا تفريقه إلى تركيب دورات، بدأنا بتعيين الدورة التي ينتمي 1 إلى حاملها، وذلك بتعيين الصور المتتالية للعنصر 1 وفق σ، σ^2، σ^3، ... حتّى نجد أصغر عدد k_1 يُحقِّق $\sigma^{k_1}(1) = 1$ فتكون الدورة المطلوبة هي :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 5 & 2 & 3 & 4 & 1 & 6 & 10 & 7 & 8 \end{pmatrix}$$

$$C_1 = (1, \sigma(1), \sigma^2(1), \ldots, \sigma^{k_1-1}(1))$$

أي $(1, 9, 7, 6)$.

$$\sigma = \begin{pmatrix} \cancel{1} & 2 & 3 & 4 & 5 & \cancel{6} & \cancel{7} & 8 & \cancel{9} & 10 \\ \cancel{9} & 5 & 2 & 3 & 4 & \cancel{1} & \cancel{6} & 10 & \cancel{7} & 8 \end{pmatrix}$$

وأوّل عنصر من $\mathbb{N}_{10}$ لا ينتمي إلى حامل الدورة C_1 هو 2، لذلك نبحث، بالمثل عن الدورة C_2 التي ينتمي 2 إلى حاملها فنجد $C_2 = (2, 5, 4, 3)$.

$$\sigma = \begin{pmatrix} \cancel{1} & \cancel{2} & \cancel{3} & \cancel{4} & \cancel{5} & \cancel{6} & \cancel{7} & 8 & \cancel{9} & 10 \\ \cancel{9} & \cancel{5} & \cancel{2} & \cancel{3} & \cancel{4} & \cancel{1} & \cancel{6} & 10 & \cancel{7} & 8 \end{pmatrix}$$

ونتابع كما هو موضّح في الشكل لنجد الدورة $C_3 = (8, 10)$، إذ 8 هو أوّل عنصر من $\mathbb{N}_{10}$ لا ينتمي إلى اجتماع حاملَيْ الدورتين السابقتين C_1 و C_2. فنصل إلى نهاية بحثنا لأنّ اجتماع حوامل الدورات الثلاث C_1 و C_2 و C_3 يساوي $\mathbb{N}_{10}$. ويكون

$$\sigma = (1, 9, 7, 6)(2, 5, 4, 3)(8, 10)$$

وبوجه خاص $\Delta(\sigma) = -1$.

② الحلقات

1. عموميات

1-1. تعريف : لتكن $(A, +, \cdot)$ مجموعة مزوّدة بقانوني تشكيل داخليين. نقول إنّ البنية $(A, +, \cdot)$ **حلقة** إذا تحقّق الشرطان :

❶ البنية $(A, +)$ زمرة تبديلية.

❷ القانون $(\cdot)$ تجميعي، وتوزيعي على الجمع ويقبل عنصراً حيادياً نرمز إليه بالرمز 1 أي

$$\begin{aligned} \forall (a, b, c) \in A^3, \quad (a\,b)\,c &= a\,(b\,c) \\ a\,(b + c) &= ab + ac \\ (b + c)\,a &= ba + ca \\ 1 \cdot a &= a \cdot 1 = a \end{aligned}$$

وإذا كان $(\cdot)$ تبديلياً قلنا إنّ الحلقة $(A, +, \cdot)$ **تبديلية**.

2-1. أمثلة

- إنّ مجموعة الأعداد الصحيحة مزوّدة بالقوانين المألوفة $(\mathbb{Z}, +, \cdot)$ حلقة تبديلية.
- وكذلك تكون $(\mathbb{Q}, +, \cdot)$ و $(\mathbb{R}, +, \cdot)$ حلقتين تبديليتين.
- إذا كانت A حلقة، فإنّ مجموعة التطبيقات $\mathcal{F}(E, A)$ من مجموعة E غير خالية إلى A، هي حلقة بالنسبة إلى القانونين $(+, \cdot)$ المعرّفين بالعلاقتين:

$$\begin{aligned} \forall (f, g) \in (\mathcal{F}(E, A))^2, f + g \ &: E \to A : x \mapsto f(x) + g(x) \\ f \cdot g &: E \to A : x \mapsto f(x) \cdot g(x) \end{aligned}$$

وحيادي الضرب هو التطبيق الثابت $\mathbb{1} : E \to A, x \mapsto 1$.

ونرى أنّ مجموعة المتتاليات الحقيقيّة هي حلقة تبديلية لأنها حالة خاصّة مما سبق.

- إذا كانت A و B حلقتين، وإذا زوّدنا الجداء الديكارتي $A \times B$ بالقانونين

$$(a,b)+(a',b')=(a+a',b+b')$$
$$(a,b)\cdot(a',b')=(a\cdot a',b\cdot b')$$

فإنّ $(A\times B,+,\cdot)$ حلقة، تقبل $(1_A,1_B)$ عنصراً حيادياً بالنسبة إلى الضرب.

- إذا كانت E مجموعة فإنّ $(P(E),\Delta,\cap)$ حلقة تبديلية تقبل E عنصراً حيادياً بالنسبة إلى قانون الضرب.
- $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ حلقة تبديلية، حيث

$$[k]+[k']=[k+k'],\ \ [k]\cdot[k']=[k\cdot k']$$

2. الحساب في الحلقات

1-2. مبرهنة. الخواص التالية محقّقة في كلّ حلقة $(A,+,\cdot)$.

- أياً كان x من A، كان $0\cdot x=x\cdot 0=0$.
- أياً كان x و y من A، كان $x(-y)=(-x)y=-(xy)$.
- أياً كان x و y و z من A، كان

$$(x-y)z=xz-yz \quad \text{و} \quad x(y-z)=xy-xz$$

- أياً كان x و y من A، فإنّ $(x+y)^2=x^2+xy+yx+y^2$.

نترك للقارئ مهمّة إثبات الخواص السابقة، وهي بسيطة.

2-2. ملاحظة. إذا كانت $(A,+,\cdot)$ حلقة، وكان a و b عنصرين منها يُحقّقان الشرط $ab=ba$ كان $(ab)^n=a^nb^n$ وذلك مهما كان العدد $2\leq n$، ولكنّ هذه النتيجة خاطئة بوجه عام إذا كان $ab\neq ba$.

2-3. مبرهنة. لتكن $(A,+,\cdot)$ حلقة. ولنفترض أنّ (a,b) عنصر من A^2 يُحقِّق الشرط $ab = ba$. عندئذ أياً كان $0 \le n$، فلدينا

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$، دستور ثنائي الحدّ

حيث نصطلح أنّ $a^0 = 1_A$ في حلقة A . وكذلك لدينا

$$a^n - b^n = (a-b)\cdot\left(\sum_{k=0}^{n-1} a^k b^{n-k-1}\right)$$

الإثبات

يمكن إثبات هذه الخاصّة بسهولة بالتدريج على n والإثبات متروك للقارئ. ❐

3. الحلقة التامّة

1-3. تعريف. لتكن $(A,+,\cdot)$ حلقة. نقول إنّ العنصر a من A **قاسم للصفر** إذا تحقّق الشرطان

① $a \ne 0$.

② يوجد b في A يُحقّق $b \ne 0$ و $(ab = 0$ أو $ba = 0)$.

2-3. تعريف. نقول إنّ الحلقة $(A,+,\cdot)$ حلقة **تامّة** إذا تحقق الشرطان

① A حلقة تبديلية غير تافهة $(A \ne \{0\})$.

② A لا تحوي قواسم للصفر.

3-3. خاصّة مهمّة. لتكن $(A,+,\cdot)$ حلقة تامّة. عندئذ

$$\forall (a,b,c) \in A^3,\ \ (ac = bc) \wedge (c \ne 0) \Rightarrow a = b$$

ذلك لأنّ $ac = bc$ يقتضي $(a-b)c = 0$ و لمّا كان c ليس قاسماً للصفر كان $a - b = 0$ ومن ثَمّ $a = b$. تُعبِّر هذه الخاصة عن إمكان الاختصار على العناصر غير المعدومة في الحلقات التامّة.

4-3. أمثلة

- إنّ الحلقات $\mathbb{Z}$ و $\mathbb{Q}$ و $\mathbb{R}$ حلقات تامّة.
- إذا كانت E مجموعة تحقّق $\operatorname{card}(E) \geq 2$ كانت الحلقة $(P(E), \Delta, \cap)$ حلقة غير تامّة.
- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ حلقة تامّة إذا وفقط إذا كان $n = 0$ أو كان n عدداً أوّلياً.

❖ في الحقيقة إذا كانت $n = 0$ فإنّ $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ تُشاكِل تقابلياً $\mathbb{Z}$ وهي تامّة.

❖ إذا كان n عدداً أوّليّاً، وكان $[r] \cdot [s] = [0]$ في $\mathbb{Z}/n\mathbb{Z}$، فهذا يعني أنّ rs ينتمي إلى $n\mathbb{Z}$ ولمّا كان n أوّلياً و n يقسم rs، فإمّا أن يقسم n العددَ r أي $([r] = [0])$، أو أن يقسم n العددَ s أي $\big([s] = [0]\big)$، ومن ثَمّ

$$\big([r] \cdot [s] = [0]\big) \Rightarrow \big([r] = [0]\big) \vee \big([s] = [0]\big)$$

فالحلقة $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ حلقة تامّة.

❖ إذا لم يكن n عدداً أوّليّاً، فيوجد عددان a و b يحقّقان

$$n > a > 1 \text{ و } n > b > 1 \text{ و } n = b \cdot a$$

ومن ثَمّ $[a] \cdot [b] = [0]$ و $[a] \neq [0]$ و $[b] \neq [0]$. وعليه لا تكون الحلقة $\mathbb{Z}/n\mathbb{Z}$ حلقة تامّة.

4. العناصر القَلوبة في حلقة

4-1. تعريف. لتكن $(A, +, \cdot)$ حلقة، نقول إنّ عنصراً x من A، **عنصرٌ قَلوب** إذا وُجِدَ في A عنصرٌ x' يُحقّق

$$x \cdot x' = x' \cdot x = 1$$

وتكوّنُ مجموعة العناصر القَلوبة في A زمرة بالنسبة إلى قانون الضرب في A نرمز إليها بالرمز $U(A)$.

فمثلاً زمرةُ العناصر القلوبة في $\mathbb{Z}$ هي $U(\mathbb{Z}) = \{+1, -1\}$، وزمرة العناصر القلوبة في $\mathbb{Q}$ هي $U(\mathbb{Q}) = \mathbb{Q}^*$. ويتيقّن القارئ بسهولة صحةَ الخاصة التالية :

4-2. **خاصّة**. إذا كانت A و B حلقتين، كان $U(A\times B)=U(A)\times U(B)$.

4-3. **مبرهنة**. إنّ العناصر القَلوبة في $\mathbb{Z}/n\mathbb{Z}$ هي صفوف تكافؤ العناصر الأولية مع n. أي

$$U(\mathbb{Z}/n\mathbb{Z})=\left\{[x]\in\mathbb{Z}/n\mathbb{Z}:\gcd(x,n)=1\right\}$$

حيث $\gcd(x,n)$ هو **القاسم المشترك الأعظم** للعددين x و n.

الإثبات

لنفترض أنّ $\gcd(n,x)=1$، إنّ المجموعة

$$x\mathbb{Z}+n\mathbb{Z}=\left\{x\alpha+n\beta:(\alpha,\beta)\in\mathbb{Z}^2\right\}$$

زمرةٌ جزئيّة من $\mathbb{Z}$ فهي من النمط $p\mathbb{Z}$. ولأنّ $x\in p\mathbb{Z}$ و $n\in p\mathbb{Z}$، استنتجنا أنّ p قاسم مشترك للعددين x و n، ومن ثَمّ $p=1$ بمقتضى الفرْض. فنكون قد أثبتنا أنّ $x\mathbb{Z}+n\mathbb{Z}=\mathbb{Z}$. ويوجد في $\mathbb{Z}$ عددان α و β يُحقّقان الشرط $1=x\alpha+n\beta$ أو $[1]=[x]\cdot[\alpha]$ أي إنّ $[x]\in U\left(\mathbb{Z}/n\mathbb{Z}\right)$.

وبالعكس، لنفترض أنّ $[x]$ عنصرٌ من $U(\mathbb{Z}/n\mathbb{Z})$ فيوجد α في $\mathbb{Z}$ يُحقّق $[x]\cdot[\alpha]=[1]$، أي يوجد β في $\mathbb{Z}$ يُحقّق $1=x\alpha+n\beta$، فلو كان العدد p قاسماً مشتركاً لكلٍ من x و n لقسمَ العددُ p العددَ 1، ولكان من ثَمّ $p=1$، نستنتج من ذلك أنّ $\gcd(n,x)=1$. ❐

4-4. **نتيجة**. إذا كان p عدداً أوّليّاً كان $U(\mathbb{Z}/p\mathbb{Z})=(\mathbb{Z}/p\mathbb{Z})\backslash\{[0]\}$.

5. المثاليات في حلقة تبديلية

5-1. **تعريف**. لتكن $(A,+,\cdot)$ حلقة **تبديلية**. وليكن $\mathcal{I}$ جزءاً من A. نقول إنّ $\mathcal{I}$ **مثالي** في A إذا تحقّق الشرطان:

① $(\mathcal{I},+)$ زمرة جزئيّة من $(A,+)$.

② أيّاً كان x من $\mathcal{I}$ وأيّاً كان a من A انتمى ax إلى $\mathcal{I}$، أو $A\cdot\mathcal{I}\subset\mathcal{I}$.

5-2. **ملاحظة مهمّة**. إذا كان $\mathcal{I}$ مثالياً في حلقة تبديلية A، فإنّ

$$(A=\mathcal{I})\Leftrightarrow(1\in\mathcal{I})$$

لأنّه أياً كان a عنصراً من A كان $a=a\cdot1\in\mathcal{I}$.

5-3. **مثال**. إنّ جميع المثاليات في حلقة الأعداد الصحيحة $(\mathbb{Z},+,\cdot)$ هي من النمط $n\mathbb{Z}$.

5-4. **تعريف**. لتكن $(A,+,\cdot)$ حلقة تبديلية. نقول عن $\mathcal{I} \subset A$ إنّه **مثالي رئيسي** إذا وفقط إذا وُجِدَ عنصر a في A يُحقّق $\mathcal{I} = aA$ أي $\mathcal{I} = \{a\cdot b : b \in A\}$. ونقول إنّ aA هو **المثالي المولَّد** بالعنصر a.

5-5. **تعريف**. نقول إنّ الحلقة $(A,+,\cdot)$ **حلقة رئيسيّة** إذا وفقط إذا تحقّق الشرطان التاليان :

① A حلقة تامّة.

② كلُّ مثالي في A مثالي رئيسي.

فمثلاً حلقةُ الأعداد الصحيحة $(\mathbb{Z},+,\cdot)$ حلقةٌ رئيسيّة.

تُلخّص المبرهنة التالية بعض الخواص البسيطة للمثاليات في حلقة تبديليّة.

5-6. **مبرهنة**. لتكن $(A,+.\cdot)$ حلقة تبديلية. ولتكن $\mathcal{I}_1,\mathcal{I}_2,\cdots,\mathcal{I}_m$ مثاليات في A. إذن كلٌّ من

$$\mathcal{J} = \sum_{k=1}^{m}\mathcal{I}_k = \{a_1+a_2+\cdots+a_m : a_i \in \mathcal{I}_i\} \quad \text{و} \quad \mathcal{K} = \bigcap_{k=1}^{m}\mathcal{I}_k$$

مثالي في A.

الإثبات

الإثبات تحقُّقٌ مباشر من التعريف وهو متروك للقارئ. ❐

6. التشاكُلات الحَلَقية

6-1. **تعريف**. لتكن A و B حلقتين. وليكن $f : A \to B$ تطبيقاً. نقول إنّ f **تشاكلٌ حلقي** من A إلى B إذا تحقّقت الشروط التالية :

① $f(1) = 1$.

② $\forall (a,a') \in A\times A,\ \ f(a+a') = f(a)+f(a')$.

③ $\forall (a,a') \in A\times A,\ \ f(a\cdot a') = f(a)\cdot f(a')$.

6-2. **مبرهنة**. لتكن A و B حلقتين تبديليتين. وليكن $f : A \to B$ تشاكلاً حلقياً. إنّ الصورة العكسية $f^{-1}(\mathcal{I})$ لمثالي $\mathcal{I}$ في B هي مثالي في A. وبوجه خاص يكون $\ker f = f^{-1}(\{0\})$ مثالياً في A. وتتحقّق المساواة $\ker f = \{0\}$ إذا وفقط إذا كان f متبايناً.

الإثبات

الإثبات تحقُّقٌ مباشر من التعريف وهو متروك للقارئ. ❐

6-3. **مبرهنة**. إذا كان $\gcd(n,m) = 1$ شاكَلَت الحلقةُ $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ الحلقة $\mathbb{Z}/nm\mathbb{Z}$ تشاكلاً تقابليّاً.

الإثبات

سنرمز في هذا الإثبات إلى صف تكافؤ x في $\mathbb{Z}/q\mathbb{Z}$ بالرمز $[x]_q$ وذلك منعاً للالتباس.

لاحظ أنه إذا كان x_1 عنصراً من $[x]_{nm}$ كان $x - x_1 \in nm\mathbb{Z}$، ونتج من ذلك أنّ $x - x_1 \in m\mathbb{Z}$ و $x - x_1 \in n\mathbb{Z}$ ومنه $[x]_m = [x_1]_m$ و $[x]_n = [x_1]_n$. وهكذا نعرف تطبيقاً بوضع

$$\psi : (\mathbb{Z}/nm\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}), \quad [x]_{nm} \mapsto ([x]_n, [x]_m)$$

ونتحقق بسهولة أنّ ψ تشاكل حلقيّ. وإذا كان $\psi([x]_{nm}) = 0$ كان $x \in n\mathbb{Z}$ وكان $x \in m\mathbb{Z}$، أي إنّ x مضاعف لكل من العددين n و m، ولكن $\gcd(n,m) = 1$ إذن x مضاعف للعدد nm أي $[x]_{nm} = 0$. بذلك نكون قد أثبتنا أنّ $\ker \psi = \{0\}$، فالتشاكل ψ متباين. ولكن

$$\operatorname{card}(\mathbb{Z}/nm\mathbb{Z}) = \operatorname{card}(\mathbb{Z}/n\mathbb{Z}) \times \operatorname{card}(\mathbb{Z}/n\mathbb{Z}) = nm$$

فالتطبيق ψ غامر أيضاً وهو من ثَمّ تشاكل تقابليّ. ❐

نُعبِّر أحياناً عن النتيجة السابقة رمزاً بالكتابة

$$(\gcd(n,m) = 1) \Rightarrow \mathbb{Z}/nm\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

ويمكن بسهولة تعميمها على الوجه التالي :

4-6. **مبرهنة**. لتكن $m_1, m_2, \dots, m_k$ أعداداً من $\mathbb{N}^*$ تُحقِّق الشروط :

$$\forall (i,j) \in \mathbb{N}_k^2, \quad i \neq j \Rightarrow \gcd(m_j, m_i) = 1$$

نضع $M = m_1 m_2 \cdots m_k$، عندئذ تشاكل الحلقةُ $\mathbb{Z}/M\mathbb{Z}$ حلقة الجداء الديكارتي $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})$. تشاكلاً تقابليّاً.

5-6. **صياغة جديدة**. يمكننا صياغة المبرهنة السابقة على الوجه التالي:

لتكن $m_1, m_2, \dots, m_k$ أعداداً من $\mathbb{N}^*$ تُحقِّق الشروط :

$$\forall (i,j) \in \mathbb{N}_k^2, \quad i \neq j \Rightarrow \gcd(m_j, m_i) = 1$$

عندئذ أياً كان $(a_1, a_2, \dots, a_k)$ من $\mathbb{Z}^k$ **فيوجد** عدد صحيح **وحيد** b ينتمي إلى المجموعة $\{0, \dots, M-1\}$ حيث $M = m_1 m_2 \cdots m_k$ تُحقِّق

$$b = a_i \bmod m_i \text{ أياً كان } i \text{ من } \mathbb{N}_k$$

(نذكِّر أنّ الكتابة $x = y \bmod n$ تعني أنّ $x - y \in n\mathbb{Z}$). تُعرَفُ هذه الصياغة باسم **مبرهنة البواقي الصينية**.

7. العدد المميِّز لحلقة

1-7. **تعريف**. لتكن $(A, +, \cdot)$ حلقة مختلفة عن $\{0\}$ (أي $0 \neq 1$). إنّ التطبيق

$$\varphi : \mathbb{Z} \to A, \quad n \mapsto n \cdot 1$$

تشاكلٌ حَلَقي، نواته $\ker \varphi$ مثالي في $\mathbb{Z}$ فهي من النمط $n\mathbb{Z}$، مع $n \in \mathbb{N}$. نسمّي هذا العدد n **العددَ المميّز للحلقة** $(A, +, \cdot)$. وإذا كان $n \neq 0$ كان n أصغر عدد طبيعي موجب تماماً k يُحقِّق الشرط $k \cdot 1 = 0$.

2-7. أمثلة وخواص

- $\mathbb{Z}$ و $\mathbb{Q}$ و $\mathbb{R}$ حلقاتٌ أعدادها المميّز تساوي 0.
- إذا كان $n \neq 0$ كان العدد المميّز للحلقة $\mathbb{Z}/n\mathbb{Z}$ مساوياً n.

- إذا كانت A حلقة تامّة فإمّا أن يكون عددها المميّز صفراً أو عدداً أوّلياً. ذلك لأنّه إذا كان n هو العدد المميّز للحلقة A وكان $n = p \cdot q$ كان

$$(p \cdot 1)(q \cdot 1) = n \cdot 1 = 0$$

ومن ثَم، إمّا أن يكون $p \cdot 1 = 0$ أو $q \cdot 1 = 0$ و هذا يناقض تعريف n إلّا في حالة $p \in \{1, n\}$ و $q \in \{1, n\}$.

- إذا كانت A حلقة منتهية فإنّ عددها المميّز لا يساوي 0 و لكن العكس غير صحيح، إذ توجد حلقات غير منتهية وأعدادها المميّزة مختلفة عن الصفر.

8. قابلية القسمة في حلقة رئيسية

8-1. **تعريف**. لتكن A حلقة **تامّة**.

- ليكن (a, b) من A^2. نقول a **يقسم** b، ونكتب $a \mid b$، إذا وُجِدَ k في A يُحقّق $b = ka$.
- نقول إنّ العنصر p من A **غير خزول** إذا تحقق الشرطان:
  - $p \notin U(A)$،
  - $\forall (a, b) \in A^2, \;\; p = a \cdot b \Rightarrow (a \in U(A)) \vee (b \in U(A))$.

لنلاحظ من جهة أولى أنّ

$$a \mid b \Leftrightarrow bA \subset aA$$

ومن جهة ثانية، إذا كان $a \mid b$ و $b \mid a$ فهذا يكافئ وجود u في $U(A)$ يُحقّق $a = ub$. ونقول في هذه الحالة إنّ a و b **شريكان** ونكتب $a \sim b$. أي

$$a \sim b \Leftrightarrow aA = bA$$

نترك للقارئ مهمة إثبات أنّ علاقة الشراكة $\sim$ علاقة تكافؤ على A.

في حلقة الأعداد الصحيحة $\mathbb{Z}$ يكون $a \sim b$ إذا وفقط إذا كان $|b| = |a|$. أمّا العناصر غير الخزولة في $\mathbb{Z}$ فهي $\mathcal{P} \cup (-\mathcal{P})$ حيث $\mathcal{P}$ هي مجموعة الأعداد الأولية.

8-2. **تعريف**. لتكن $(A,+,\cdot)$ حلقة تامّة. ولتكن $(a_1,a_2,\ldots,a_n)$ جملة من عناصر A.

① نسمّي **قاسماً مشتركاً أعظم** للجملة $(a_1,a_2,\ldots,a_n)$ أيَّ عنصر d من A يحقّق

$$dA = a_1A + a_2A + \cdots + a_nA$$

ونرمز إليه بالرمز $\gcd(a_1,a_2,\cdots,a_n)$ وهو بوجه عام ليس وحيداً، فإذا كان d يحقق ما سبق حقّق كلُّ شريك له أيضاً ما سبق.

② نسمّي **مضاعفاً مشتركاً أصغر** للجملة $(a_1,a_2,\cdots,a_n)$ أيَّ عنصر m من A يحقّق

$$mA = \bigcap_{i=1}^{n}(a_iA)$$

ونرمز إليه بالرمز $\operatorname{lcm}(a_1,a_2,\cdots,a_n)$، وتطبّق عليه الملاحظة المتعلّقة بالوحدانيّة التي طُبّقت على $\gcd(a_1,a_2,\cdots,a_n)$.

8-3. **مبرهنة**. لتكن $(A,+,\cdot)$ حلقة رئيسيّة، ولتكن $(a_1,a_2,\cdots,a_n)$ جملة من عناصر A. يوجد عندئذ قاسم مشترك أعظم ومضاعف مشترك أصغر للجملة $(a_1,a_2,\cdots,a_n)$.

الإثبات

هذا صحيح لأنّ A حلقة رئيسية، وكلٌّ من المجموعتين

$$a_1A + a_2A + \cdots + a_nA \quad \text{و} \quad \bigcap_{i=1}^{n}(a_iA)$$

مثاليٌّ في A. □

8-4. **مبرهنة**. لتكن $(A,+,\cdot)$ حلقة رئيسيّة، ولتكن $(a_1,a_2,\cdots,a_n)$ جملة من عناصر $A\backslash\{0\}$. عندئذ يكون هناك تكافؤ بين

- $d = \gcd(a_1,a_2,\ldots,a_n)$.
- و $(\forall i \in \mathbb{N}_n, d \mid a_i) \wedge (\forall k \in A, (\forall i \in \mathbb{N}_n, k \mid a_i) \Rightarrow (k \mid d))$.

وكذلك يكون هنالك تكافؤ بين

- $m = \operatorname{lcm}(a_1,a_2,\ldots,a_n)$.
- و $(\forall i \in \mathbb{N}_n, a_i \mid m) \wedge (\forall k \in A, (\forall i \in \mathbb{N}_n, a_i \mid k) \Rightarrow (m \mid k))$.

الإثبات

الإثبات تحقُّقٌ مباشر متروك للقارئ. □

كما ذكرنا سابقاً، ليس المقداران $\gcd$ و lcm معرّفَين بطريقة وحيدة، وإنّما كلُّ عنصر ينتج من $\gcd$، أو من lcm، بضربه بعنصر قَلوب، هو أيضاً $\gcd$، أو lcm. فمثلاً العناصر القَلوبة في الحلقة $\mathbb{Z}$ هي $U(\mathbb{Z}) = \{-1, +1\}$، وإذا أردنا الوحدانيّة في تعريف المقدارين $\gcd$ و lcm في $\mathbb{Z}$ وجب أن نشترط انتماء هذين المقدارين إلى $\mathbb{N}$، وهذا ما نفعله عادة.

8-5. تعريف. لتكن $(A, +, \cdot)$ حلقة رئيسية. ولتكن $(a_1, a_2, \cdots, a_n)$ جملة من عناصر A. نقول إنّ العناصر $a_1, a_2, \ldots, a_n$ **أوليّة فيما بينها** إذا وفقط إذا كان 1 قاسماً مشتركاً أعظم لها. أي إذا كانت العناصر القَلوبة هي القواسم المشتركة الوحيدة لعناصر الجملة. ونقول إنّ العناصر $a_1, a_2, \ldots, a_n$ **أوليّة فيما بينها مثنى مثنى** إذا وفقط إذا كان 1 قاسماً مشتركاً أعظم للثنائيّة (a_i, a_j)، أيّاً كان الدليلان المختلفان i و j من $\mathbb{N}_n$.

فمثلاً الأعداد $(6, 10, 15)$ أوليّة فيما بينها في $\mathbb{Z}$، ولكنها ليست أوليّة فيما بينها مثنى مثنى.

8-6. خواص. إنّ معظم الخواص التالية بسيطة، لتكن $(A, +, \cdot)$ حلقة رئيسية.

❄ لتكن (a, b, c) من A^3، عندئذ

- $\gcd(a, b) \sim \gcd(b, a)$.
- $\gcd(a, \gcd(b, c)) \sim \gcd(\gcd(a, b), c)$.

❄ لتكن $(a_1, a_2, \cdots, a_n)$ جملة في A. وليكن $\delta = \gcd(a_1, a_2, \cdots, a_n)$. حينئذ أيّاً كان x من A كان $x\delta$ قاسماً مشتركاً أعظم للجملة $(xa_1, xa_2, \ldots, xa_n)$.

✍ في الحقيقة، تنتج هذه الخاصّة من المساواة الواضحة :

$$\begin{aligned} xa_1A + xa_2A + \cdots + xa_nA &= x(a_1A + a_2A + \cdots + a_nA) \\ &= x\delta A \end{aligned}$$

❄ لتكن $(a_1, a_2, \cdots, a_n)$ جملة ليست جميع حدودها معدومة من عناصر A. وليكن $\delta = \gcd(a_1, a_2, \cdots, a_n)$. نعرّف $(a'_1, a'_2, \cdots, a'_n)$ بالعلاقات $a_i = \delta a'_i$ حيث $i \in \mathbb{N}_n$. عندئذ تكون الأعداد $a'_1, a'_2, \cdots, a'_n$ أوليّة فيما بينها.

✍ في الحقيقة، إذا كان $\delta' = \gcd(a'_1, a'_2, \cdots, a'_n)$، كان لدينا بمقتضى المبرهنة السابقة : $\delta\delta' \sim \delta$، ومن ثَمّ يكون $\delta' \sim 1$ لأنّ $\delta \neq 0$ والحلقة A تامّة.

❄ **مبرهنة بيزو** Bézout : لتكن $(a_1, a_2, \cdots, a_n)$ جملة من عناصر A. عندئذ تكون العناصر $a_1, a_2, \ldots, a_n$ أوليّة فيما بينها إذا وفقط إذا وُجِدتْ جملة $(x_1, x_2, \cdots, x_n)$ من عناصر A، تُحقّق

$$x_1 a_1 + x_2 a_2 + \cdots + x_n a_n = 1$$

✍ تنتج هذه المبرهنة من التكافؤ الواضح الآتي

$$(a_1 A + a_2 A + \cdots + a_n A = A) \Leftrightarrow (1 \in a_1 A + a_2 A + \cdots + a_n A)$$

❄ ليكن (a, b_1, b_2) من A^3. إذا كان a و b_1 أولبين فيما بينهما، وكان a و b_2 أوليَّين فيما بينهما، فإن a و $b_1 b_2$ أوليّان فيما بينهما.

✍ في الحقيقة، نجد، بمقتضى الخاصة السابقة، عناصرَ x_1, x_2, y_1, y_2 تُحقّق

$$ax_2 + b_2 y_2 = 1 \quad \text{و} \quad ax_1 + b_1 y_1 = 1$$

وبضرب العلاقتين السابقتين طرفاً بطرف، نجد $ax + b_1 b_2 y = 1$ وقد عرّفنا

$$x = a x_1 x_2 + b_2 x_1 y_2 + b_1 y_1 x_2,$$
$$y = y_1\, y_2.$$

إذن a و $b_1 b_2$ أوليّان فيما بينهما. يمكن تعميم هذه الخاصة بالتدريج لإثبات أنّه إذا كان $(a, b_1, b_2, \ldots, b_n)$ عنصراً من A^{n+1} وكان a و b_k أولبين فيما بينهما أيّاً كان $k \in \mathbb{N}_n$، فإنّ a و $b_1 b_2 \ldots b_n$ أوليّان فيما بينهما.

❄ **مبرهنة** Gauss. لتكن (a, b, c) من A^3. نفترض أنّ العنصرين a و b أوليّان فيما بينهما و أنّ $a \mid bc$، عندئذ $a \mid c$.

✍ في الحقيقة، نجد، استناداً إلى مبرهنة بيزو، عنصرين x و y يُحقّقان $ax + by = 1$، ومن ثَمّ $acx + bcy = c$ وهذا يقتضي $a \mid c$، لأنّ a يقسم كلاً من ac و bc.

❄ ليكن (a, b_1, b_2) من A^3. إذا كان $b_1 \mid a$ و $b_2 \mid a$ وكان b_1 و b_2 أوليّين فيما بينهما، كان $b_1 b_2 \mid a$.

✍ إنّ هذه الخاصّة تطبيقٌ مباشر للخاصة السابقة.

❄ ليكن (a,b) من A^2. نضع $\gcd(a,b)=\delta$ و $\operatorname{lcm}(a,b)=\mu$. فيكون لدينا $\delta\mu \sim ab$.

✍ في الحقيقة، لنعرّف العنصرين a' و b' الأوليَّيْن فيما بينهما بالعلاقتين:

$$a=\delta a' \quad \text{و} \quad b=\delta b'$$

ولنضع $\ell = a'b'\delta$. لمّا كان $\ell = ab' = a'b$ استنتجنا أنّ $\mu \mid \ell$.

وبالعكس، نظراً إلى أنّ $\mu = x\,a = y\,b$، فإنّ $xa'\delta = yb'\delta$، ولكنّ الحلقة A تامّة و $\delta \neq 0$، إذن $xa' = yb'$. ومن ناحية أخرى، لمّا كان العنصران a' و b' أوليَّيْن فيما بينهما، وكان $a' \mid yb'$، نتج من مبرهنة غاوس السابقة أنّ $a' \mid y$ أو $y = a'\,z$.

ينجم عن ذلك أنّ $\mu = a'\,b\,z = \ell\,z$، ومن ثَمّ $\mu \mid \ell$.

بذا نكون قد أثبتنا أنّ $\mu \sim \ell$، ومنه $\delta\mu \sim \ell\delta = ab$. ❐

9. تتمات في حلقة الأعداد الصحيحة $\mathbb{Z}$

لقد وجدنا سابقاً أنّ $\mathbb{Z}$ حلقة رئيسية، إلاّ أنها في الواقع تتمتع بخاصة مهمّة لا تتمتع بها الحلقات الرئيسية بوجه عام، وهي خاصة القسمة الإقليدية التالية (لذلك نقول إنّ $\mathbb{Z}$ **حلقة إقليدية**).

> ليكن (a,b) عنصراً من $\mathbb{Z}^2$ يُحقِّق $b \neq 0$، عندئذ توجد ثنائية وحيدة (q,r) من $\mathbb{Z}^2$ تُحقّق
>
> $$a = q\,b + r \quad \text{و} \quad 0 \le r < |b|.$$
>
> نسمّي q **خارج القسمة**، ونسمّي r **باقي القسمة**.

9-1. خوارزمية إقليدس لحساب القاسم المشترك الأعظم لعددين

تعتمد هذه الخوارزمية على الملاحظة البسيطة التالية والتي نترك إثباتها تمريناً للقارئ:

﴾ أيّاً كان a من $\mathbb{Z}\backslash\{0\}$، و b و λ من $\mathbb{Z}$ كان $\gcd(a,b) = \gcd(a, b-\lambda a)$. ﴿

لنأتِ الآن إلى وصف **خوارزمية إقليدس** التي تفيد بحساب $d = \gcd(a,b)$. سنفترض فيما يلي أنّ $a > b > 0$ و ذلك دون الإخلال بعمومية المسألة لأنّ

$$\gcd(a,b) = \gcd(|a|,|b|) = \gcd(|b|,|a|)$$

نعرّف المتتالية $(R_k)_{k\geq 0}$ تدريجياً كما يلي: $R_0 = a$، $R_1 = b$، أمّا حين يكون $k \geq 1$ فإننا نعرّف R_{k+1} على الوجه الآتي: إذا كان $R_k = 0$ وضعنا $R_{k+1} = 0$، وإلّا عرّفنا R_{k+1} بأنّه باقي القسمة الإقليدية للعدد R_{k-1} على R_k.

لنفترض جدلاً أنّ

$$\forall k \in \mathbb{N}_{b+1}, \quad R_k > 0$$

ينجم عن تعريف القسمة الإقليدية أنّ

$$\forall k \in \mathbb{N}_b, \quad R_{k+1} < R_k$$

أو

$$\forall k \in \mathbb{N}_b, \quad 1 \leq R_k - R_{k+1}$$

وبجمع هذه المتراجحات طرفاً إلى طرف نجد $b \leq b - R_{b+1}$، وهذا يناقض $R_{b+1} > 0$.

نستنتج من هذا أنه يوجد p في $\mathbb{N}_b$ يُحقّق $R_{p+1} = 0$. لنعرّف إذن

$$n = \min\{p \in \mathbb{N}_b : R_{p+1} = 0\}$$

فيكون $R_n = \gcd(a,b)$.

في الحقيقة، مهما يكن k من $\mathbb{N}_n$، لدينا

$$R_{k-1} = q_k R_k + R_{k+1}$$

أو

$$R_{k+1} = R_{k-1} - q_k R_k$$

وبالاستفادة من الملاحظة البسيطة التي بدأنا بها نجد:

$$\begin{aligned}\gcd(R_k, R_{k-1}) &= \gcd(R_k, R_{k-1} - q_k R_k)\\ &= \gcd(R_k, R_{k+1}) = \gcd(R_{k+1}, R_k)\end{aligned}$$

وهذا يتيح لنا أنّ نثبتَ بالتدريج

$$\gcd(a,b) = \gcd(R_1, R_0) = \cdots = \gcd(R_{n+1}, R_n) = \gcd(0, R_n) = R_n$$

نلخّص في الجدول الآتي هذه الخوارزمية

k	1		2		$\cdots$	$n-1$		n
R_{k-1}	a	$\nearrow$	b	$\nearrow$	$\cdots$	R_{n-2}	$\nearrow$	R_{n-1}
R_k	b		R_2		$\cdots$	R_{n-1}		$R_n = d$
R_{k+1}	R_2	$\nearrow$	R_3	$\nearrow$	$\cdots$	R_n	$\nearrow$	0

وهذا مثال يهدف إلى حساب $\gcd(5313, 2047)$:

k	1	2	3	4	5	6
R_{k-1}	5313	2047	1219	828	391	46
R_k	2047	1219	828	391	46	$\boxed{23}$
R_{k+1}	1219	828	391	46	23	0

نعلم بمقتضى تعريف القاسم المشترك الأعظم أنّه يوجد عددان صحيحان x و y يُحقّقان $5313\,x + 2047\,y = 23$ ، فكيف يمكن تعيينهما؟

في الحقيقة، يمكن تعديل الخوارزميّة السابقة بحيث نحصل في نهايتها على كلٍّ من المقادير $d = \gcd(a,b)$ و x و y، حيث $ax + by = d$. تسمّى هذه الخوارزمية المعدّلة **خوارزمية إقليدس المعمّمة**.

لنأتِ إذن إلى وصف هذه الخوارزميّة :

سنفترض كما في السابق أنّ $0 < b < a$. وكما سبق نعرّف المتتالية $(R_k)_{k\geq 0}$، التي يكون آخر حدٍ غير معدوم من حدودها هو $\gcd(a,b) = d = R_n$. يمكننا في حالة k من $\mathbb{N}_n$ أن نرمز بالرمز q_k إلى خارج القسمة الإقليدية للعدد R_{k-1} على R_k :

$$R_{k-1} = q_k R_k + R_{k+1}.$$

نعرّف إذن متتاليتين جديدتين $(S_k)_{0\leq k\leq n}$ و $(T_k)_{0\leq k\leq n}$، بالعلاقات التدريجية:

$$T_0 = 1, \quad T_1 = 0, \quad T_{k+1} = T_{k-1} - q_k T_k.$$
$$S_0 = 0, \quad S_1 = 1, \quad S_{k+1} = S_{k-1} - q_k S_k.$$

فيكون لدينا

$$d = R_n = T_n a + S_n b$$

فنأخذ، مثلاً $x = T_n$ و $y = S_n$.

تنتج صحةُ هذه الخوارزميّة من الخاصة التالية، التي نترك للقارئ أن يثبتها بالتدريج على k ،

«أياً كان k من $\{0,1,\ldots,n\}$ فلدينا $R_k = T_k\, a + S_k\, b$»

ونحصل على المطلوب حين نأخذ $k = n$.

يبيّن المثال الآتي تطبيقاً عددياً لهذه الخوارزميّة المعمّمة نعيِّن فيه عددين صحيحين x و y يُحقِّقان $5313\, x + 2047\, y = 23$.

k	R_k	q_k	T_k	S_k
0	5313	–	1	0
1	2047	2	0	1
2	1219	1	1	−2
3	828	1	−1	3
4	391	2	2	−5
5	46	8	−5	13
6	23		42	−109
7	0			

ومن ثَمّ $23 = 42 \times 5313 - 109 \times 2047$.

9-1-1. **مبرهنة**. ليكن (a,b) عنصراً من $\mathbb{Z}^2$ مختلفاً عن $(0,0)$. وليكن $d = \gcd(a,b)$. لنفترض أنه لدينا زوجٌ (x_0,y_0) في $\mathbb{Z}^2$ يُحقّق $x_0a + y_0b = d$. حينئذ يكون

$$\{(x,y)\in\mathbb{Z}^2 : xa+yb=d\} = \{(x_0+\lambda b', y_0-\lambda a')\in\mathbb{Z}^2 : \lambda\in\mathbb{Z}\}$$

حيث $a = da'$ و $b = db'$.

الإثبات

لنعرّف المجموعتين

$$\mathcal{A} = \{(x,y)\in\mathbb{Z}^2 : xa+yb=d\}$$
$$\mathcal{B} = \{(x_0+\lambda b', y_0-\lambda a')\in\mathbb{Z}^2 : \lambda\in\mathbb{Z}\}$$

علينا أن نثبتَ أنّ $\mathcal{A}\subset\mathcal{B}$ لأنّ الاحتواء المعاكس واضح. لتكن إذن (x,y) من $\mathcal{A}$ نجد بالقسمة على d أنّ : $xa' + yb' = x_0a' + y_0b'$، وعليه $(x-x_0)a' = (y_0-y)b'$ فالعدد b' يقسم $(x-x_0)a'$ وهو أوّلي مع a'، إذن b' يقسم $(x-x_0)$ وذلك بمقتضى مبرهنة غاوس. نستنتج من ذلك أنّه يوجد λ في $\mathbb{Z}$ يُحقّق $x - x_0 = \lambda b'$ وبالتعويض في المساواة $(x-x_0)a' = (y_0-y)b'$ نجد أيضاً أنّ $y_0 - y = \lambda a'$. وهذا يثبت أنّ $(x,y)\in\mathcal{B}$. ويكتمل إثبات المبرهنة. □

فإذا عُدنا إلى المثال السابق استنتجنا أنّ مجموعة حلول المعادلة

$$5313\,x + 2047\,y = 23$$

في $\mathbb{Z}$، هي

$$\{(42 + 89\lambda, -109 - 231\lambda) \in \mathbb{Z}^2 : \lambda \in \mathbb{Z}\}$$

9-2. التعقيد الخوارزميّ لخوارزميّة إقليدس

تُعَدُّ دراسةُ التعقيد الخوارزمي لخوارزمية ما جزءاً لا يتجزأ من تحليل هذه الخوارزميّة، إذ تُبيِّن هذه الدراسةُ مدى جودة هذه الخوارزميّة وإمكان الاستفادة منها عمليّاً.

لا نهدف هنا إلى إجراء دراسة عامّة لموضوع تعقيد الخوارزميات، بل نريد أن نعطيَ القارئ فكرة عن هذا النوع من الدراسة بتحليل خوارزميّة إقليدس، ودراسة مدى تعقيدها الخوارزميّ، الذي يمكن أن نعتبر عدد عمليات القسمة الإقليديّة اللازمة لحساب $\gcd(a,b)$ انطلاقاً من a و b مقياساً جيداً له.

تؤدي المتتالية المعروفة باسم متتالية فيبوناتشي دوراً مهمّاً في هذه الدراسة. لنلخّص فيما يلي ما نحتاج إليه من هذه المتتالية :

9-2-1. مبرهنة وتعريف. نسمّي متتالية **فيبوناتشي** Fibonacci المتتالية $(F_n)_{n\in\mathbb{N}}$ المعرفة تدريجياً بالعلاقات

$$F_0 = 0,\ \ F_1 = 1,\ \ F_{n+1} = F_n + F_{n-1}$$

وهي تحقّق الخواص التالية:

① المتتالية $(F_n)_{n\in\mathbb{N}}$ متتالية متزايدة تماماً من الأعداد الطبيعيّة.

② إذا كانت $\omega = \dfrac{1+\sqrt{5}}{2}$ فإنّ $\forall n \geq 0,\ \ F_n = \dfrac{1}{\sqrt{5}}\left(\omega^n - \left(\dfrac{-1}{\omega}\right)^n\right)$.

③ مهما تكن (n,m) من $\mathbb{N}^2$ فلدينا الاقتضاء[1]

$$F_n \leq m \Rightarrow n \leq \log_\omega(\sqrt{5}\,m + 1)$$

الإثبات

إنّ إثبات الخاصّتين ① و ② واضح بالتدريج.

[1] نذكّر بأنّ $\log_a(b) = \ln(b)/\ln(a)$ و $\ln$ هو اللوغاريتم النيبري.

لإثبات الخاصّة ③ نلاحظ أنّ

$$\forall n \geq 0, \quad F_n \geq \frac{\omega^n - 1}{\sqrt{5}}$$

ومن ثَمّ يكون

$$\begin{aligned}(F_n \leq m) &\Rightarrow \frac{\omega^n - 1}{\sqrt{5}} \leq m \\ &\Rightarrow \omega^n \leq \sqrt{5}m + 1 \\ &\Rightarrow n \leq \log_\omega(\sqrt{5}m + 1)\end{aligned}$$

وبذا نكون قد أثبتنا الخواص المطلوبة. ❐

لتكن (a,b) من $\mathbb{N}^2$، ولنعرّف كما في خوارزميّة إقليدس المتتالية $(R_k^{a,b})_{k\geq 0}$ بالعلاقات

- $R_0^{a,b} = \max(a,b)$.
- $R_1^{a,b} = \min(a,b)$.
- و $R_{k+1}^{a,b}$ يساوي 0 في حالة $R_k^{a,b} = 0$ ويساوي باقي القسمة الإقليديّة للعدد $R_{k-1}^{a,b}$ على $R_k^{a,b}$ في حالة $R_k^{a,b} \neq 0$.

وأخيراً لتكن N من $\mathbb{N}$، ولنعرّف

$$\begin{aligned}\mathcal{D}_N &= \left\{(a,b) \in \mathbb{N}^2 : (R_N^{a,b} = 1) \wedge (R_{N+1}^{a,b} = 0) \right\} \\ \delta_N &= \min\{\min(a,b) : (a,b) \in \mathcal{D}_N\}\end{aligned}$$

تمثّل المجموعة $\mathcal{D}_N$ مجموعة الثنائيات (a,b) المؤلّفة من عددين طبيعيين أوّليين فيما بينهما، والتي يتطلّبُ تَيَقُّن كونهما أوّليين فيما بينهما، بتنفيذ خوارزميّة إقليدس، إجراءَ N وفقط N عملية قسمة إقليدية.

- لندرس حالة $F_{N+1} = a$ و $F_N = b$. يمكننا بسهولة أن نثبت بالتدريج على p من $\mathbb{N}_{N+1}$ أنّ:

$$\forall k \in \{0,1,\ldots,p\}, \quad R_k^{F_{N+1},F_N} = F_{N+1-k}$$

وبوجه خاص يكون $R_{N+1}^{F_{N+1},F_N} = F_0 = 0$ و $R_N^{F_{N+1},F_N} = F_1 = 1$، ونستنتج من ذلك أنّ $(F_{N+1}, F_N) \in \mathcal{D}_N$، وبذا يكون $\delta_N \leq F_N$.

- وبالعكس، إذا كان (a,b) من $\mathcal{D}_N$ ، عندئذ يمكننا بسهولة أن نبرهن بالتدريج على p من $\mathbb{N}_{N+1}$ أنّ:

$$\forall k \in \{0,1,\ldots,p\},\ \ R_{N+1-k}^{a,b} \geq F_k$$

وبوجه خاص يكون $R_1^{a,b} = \min(a,b) \geq F_N$ ، وهذا يقتضي أنّ $\delta_N \geq F_N$.

نستنتج من النقطتين السابقتين المساواة المهمة التالية:

$$F_N = \min\left\{\min(a,b) \in \mathbb{N}^2 : (R_N^{a,b} = 1) \wedge (R_{N+1}^{a,b} = 0)\ \right\}$$

فإذا كان a و b عددين طبيعيين موجبين تماماً، وأوليين فيما بينهما، وإذا كان تَيَقُّن كونهما أوليين فيما بينهما، بتنفيذ خوارزميّة إقليدس، يتطلّبُ إجراءَ n وفقط n عملية قسمة إقليدية، كان $(a,b) \in \mathcal{D}_n$ وهذا يقتضي أنّ $F_n \leq \min(a,b)$ ، وبناءً على المبرهنة السابقة، يكون $n \leq \log_\omega(\sqrt{5}\min(a,b)+1)$.

وبوجه عام، ليكن a و b عددين طبيعيين موجبين تماماً، وليكن $d = \gcd(a,b)$. عندئذ يكون $a = da'$ و $b = db'$ ، حيث a' و b' هما عددان أوليّان فيما بينهما، ونتحقَّق بسهولة أنّ $(R_k^{a,b})_{k\geq 0} = (dR_k^{a',b'})_{k\geq 0}$. إذن يساوي عددُ عمليات القسمة الإقليدية اللازمة لحساب $d = \gcd(a,b)$ عددَ عمليات القسمة الإقليدية اللازمة للتيقُّن أنّ a' و b' أوليّان فيما بينهما، وهذا لا يتجاوز $\log_\omega(\sqrt{5}\min(a',b')+1)$.

نكون بذلك قد أثبتنا المبرهنة التالية:

2-2-9. مبرهنة. ليكن a و b عددين طبيعيين موجبين تماماً، عندئذ لا يتجاوز عددُ عمليات القسمة الإقليدية اللازمة لحساب $d = \gcd(a,b)$ ، المقدار

$$E_{a,b} = \left\lfloor \log_\omega\left(\sqrt{5}\,\frac{\min(a,b)}{d}+1\right)\right\rfloor$$

حيث $\omega = \dfrac{1+\sqrt{5}}{2}$ ، و $\lfloor x \rfloor$ هو الجزء الصحيح للعدد x .

فمثلاً، حساب القاسم المشترك الأعظم لعددين من مرتبة 10^{100} يحتاج إلى أقلّ من 480 عملية قسمة إقليديّة. ونلاحظ أنّ الحدّ الأعلى الوارد في نص المبرهنة السابقة ليس حداً مُبالغاً فيه، فلو تأمّلنا حالة $a = 89$ و $b = 55$ لوجدنا أنّ $E_{a,b} = 10$ ويعطي تنفيذ خوارزميّة إقليدس في هذا الحالة :

k	0	1	2	3	4	5	6	7	8	9	10
$R_k^{89,55}$	89	55	34	21	13	8	5	3	2	1	0

أخيراً نترك القارئَ يبحثُ عن تعديل لخوارزمية إقليدس يُحسِّن فيه أداء هذه الخوارزمية ويجعلها تتطلب عدداً أقلّ من عمليات القسمة الإقليديّة.

9-3. الأعداد الأوليّة

نسمّي **عدداً أوليّاً** في $\mathbb{Z}$ كل عنصر من $\mathbb{N}$ غير خزول في الحلقة $\mathbb{Z}$. ونرمز عادة بالرمز $\mathcal{P}$ إلى مجموعة الأعداد الأولية. لقد اهتم الرياضيون بمجموعة الأعداد الأولية، وما تزال موضع اهتمامهم حتى عصرنا هذا. لنلخّص بعض الخواص الأساسية لهذه الأعداد.

- إذا كان $p \in \mathcal{P}$ و $n \in \mathbb{Z}$، فإمّا p يقسم n أو إنهما أوليّان فيما بينهما. لأن $\gcd(n, p)$ قاسم للعدد p.
- إذا كان $(a,b) \in \mathbb{Z}^2$ و $p \in \mathcal{P}$، فإن $p \mid ab \Rightarrow (p \mid a) \vee (p \mid b)$. وذلك استناداً إلى الملاحظة السابقة وعملاً بنتيجة مبرهنة Gauss.
- إذا كانت $q_1, q_2, \ldots, q_r$ و p أعداداً أوليّة وكان $p \mid q_1 q_2 \ldots q_r$ فيوجد k في $\mathbb{N}_r$ يُحقّق $p = q_k$.

نأتي الآن إلى ما نسمّيه **المبرهنة الأساسية في الحساب** :

9-3-1. مبرهنة. ليكن n عدداً طبيعياً يُحقّق المتراجحة $2 \leq n$. عندئذ توجد أعداد أوّليّة $p_1, p_2 \ldots, p_r$، $(1 \leq r)$، تُحقّق $n = p_1 p_2 \ldots p_r$. وهذه الكتابة وحيدة إذا لم نأخذ ترتيب عناصر الجداء بعين الاعتبار.

الإثبات

لنبدأ أولاً بإثبات الوجود، وذلك بنقض الفرْض. لنفترض وجود $m \geq 2$ لا يكتب بالشكل السابق جداءَ أعداد أوليّة. وليكن $m_0 > 2$ **أصغر** عدد طبيعي لا يكتب جداء أعداد أولية. من الواضح أنّ $m_0 \notin \mathcal{P}$ وهذا ما يبرر وجود عددين a و b يُحققان $1 < a < m_0$ و $1 < b < m_0$ و $m_0 = ab$. ولكن بناءً على تعريف m_0 لا بدّ أن نجد أعداداً أولية $p_1, p_2 \ldots, p_r$ وأعداداً أولية $q_1, q_2 \ldots, q_s$ تُحقّق

$$a = p_1 p_2 \ldots p_r \quad \text{و} \quad b = q_1 q_2 \ldots q_s$$

ومن ثَم يكون $m_0 = q_1 q_2 \ldots q_s \; p_1 p_2 \ldots p_r$، وهذا التناقض يثبت جزء الوجود في المبرهنة.

لنأتِ الآن إلى إثبات الوحدانية، ولنفترض أنّها غير صحيحة، أي إنه توجد أعداد طبيعية أكبر من 2 يمكن تفريقها بأكثر من طريقة إلى جداء أعداد أولية، وليكن n_0 **أصغر** هذه الأعداد. إذن

$$n_0 = q_1 q_2 \ldots q_s = p_1 p_2 \ldots p_r$$

لمّا كان $p_1 \mid q_1 q_2 \ldots q_s$ فلا بد أن يساوي p_1 أحد الأعداد الأولية $q_1, q_2 \ldots, q_s$، ويمكننا أن نفترض أنّ $p_1 = q_1$ بعد أن نُعيد ترقيم الأعداد $q_1, q_2 \ldots, q_s$ إذا احتاج الأمر. ولكن ينجم حينئذ أنّ

$$n_1 = q_2 \ldots q_s = p_2 \ldots p_r$$

فإمّا $n_1 = 1$ وهو يقبل القسمة على أحد الأعداد الأولية $q_2, \ldots, q_s, p_2, \ldots, p_r$ وهذا خُلفٌ، أو $2 < n_1 < n$ و العدد n_1 يقبل التفريق بأكثر من طريقة إلى جداء أعداد أولية، وهذا يناقض مُجدّداً كون n_0 أصغرياً. بهذا نكون قد أنهينا إثبات المبرهنة. □

يمكن صياغة المبرهنة السابقة على الوجه الآتي :

- يُكتب كل عدد طبيعي $n \geq 2$ بشكل وحيد $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}$، حيث $r \geq 1$، و $p_1, p_2 \ldots, p_r$ أعداد أوليّة مختلفة مثنى مثنى، و $\nu_1, \nu_2 \ldots, \nu_r$ أعداد من $\mathbb{N}^*$.
- أو يمكننا أن نقول إنّه مهما كان n من $\mathbb{N}^*$ يوجد تطبيق $\mathcal{P} \to \mathbb{N} : p \mapsto \nu_p(n)$، يُحقّق $\nu_p(n) = 0$ أياً كان العدد الأولي p الذي لا يقسم n ويكون

$$n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$$

مع الاصطلاح طبعاً أنّ $p^0 = 1$.

ومنه المبرهنة الآتية.

9-3-2. مبرهنة. أيّاً كان (a,b) من $\mathbb{N}^{*2}$، كان

$$\gcd(a,b) = \prod_{p\in\mathcal{P}} p^{\min(\nu_p(a),\nu_p(b))}$$

و

$$\operatorname{lcm}(a,b) = \prod_{p\in\mathcal{P}} p^{\max(\nu_p(a),\nu_p(b))}$$

الإثبات

الإثبات تحقُّقٌ بسيط ومتروك للقارئ. ❐

9-3-3. مبرهنة إقليدس. يوجد عدد لا نهائي من الأعداد الأوّليّة، أي $\operatorname{card}(\mathcal{P}) = +\infty$.

الإثبات

لنفترض جدلاً أنّ $\mathcal{P}$ مجموعة منتهية وأنّ $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$. عندها لا بدّ أن يقبل العددُ $P = 1 + p_1p_2\ldots p_n$ القسمة على عدد أوليّ p_k من $\mathcal{P}$. ومن ثمّ يقسم p_k كلّاً من P و $P-1$ ، فهو إذن يقسم 1، وهذا التناقض يثبت المطلوب. ❐

10. الحلقة $M_2(A)$

لتكن A حلقة تبديليّة غير تافهة $(A \neq \{0\})$، نسمّي مصفوفة من المرتبة الثانية على A ، كلّ تطبيق

$$M : \{1,2\}\times\{1,2\} \rightarrow A$$

ونصطلح أن نكتب مصفوفة من هذا النمط بالشكل $M = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ ، ونرمز بالرمز $M_2(A)$ إلى مجموعة المصفوفات من المرتبة الثانية على A .

نعرّف على A القانونين

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{bmatrix}$$

و

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix}$$

إنّ البنية $(M_2(A), +, \cdot)$ حلقة غير تبديليّة، عنصرها الحيادي هو $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$، وفيها قواسم للصفر.

لنبحث عن العناصر القَلوبة في $M_2(A)$ التي سنرمز إلى مجموعتها $GL_2(A)$. أي

$$GL_2(A) = \left\{ M \in M_2(A) : \exists M' \in M_2(A), MM' = M'M = I \right\}$$

لتكن $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$، ولنعرّف $\widetilde{M} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. عندئذ نلاحظ أنّ

$$M \cdot \widetilde{M} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix} = (ad-bc)I$$

$$\widetilde{M} \cdot M = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix} = (ad-bc)I$$

نرمز بالرمز $\det(M)$ إلى العنصر $ad-bc$.

- يمكن للقارئ أن يتحقّق صحة المساواة $\widetilde{M \cdot N} = \widetilde{N} \cdot \widetilde{M}$ ومنه

$$\begin{aligned} \det(M \cdot N)I &= (M \cdot N) \cdot (\widetilde{M \cdot N}) \\ &= M \cdot N \cdot \widetilde{N} \cdot \widetilde{M} \\ &= \det(N) M \cdot \widetilde{M} = \det(N) \cdot \det(M) I \end{aligned}$$

إذن $\forall (M, N) \in M_2(A), \ \det(MN) = \det(M)\det(N)$

- فإذا كان $M \in GL_2(A)$ فإنّ $M \cdot M' = M' \cdot M = I$ يقتضي

$$\det(M)\det(M') = \mathrm{de}(M')\det(M) = 1$$

أي إنّ $\det(M) \in U(A)$.

- وبالعكس، إذا كان $\delta = \det(M) \in U(A)$ فإنّ العنصر

$$M' = \begin{bmatrix} \delta^{-1}d & -\delta^{-1}b \\ -\delta^{-1}c & \delta^{-1}a \end{bmatrix}$$

يحقّق $M \cdot M' = M' \cdot M = I$. نستنتج أنّ

$$GL_2(A) = \{ M \in M_2(A) : \det(M) \in U(A) \}$$

تمرينات

① الزمر

التمرين 1. بيّن أنّ البنية $(\mathbb{R}^* \times \mathbb{R}, *)$، حيث $(a,b)*(\alpha,\beta) = \left(a\alpha, \dfrac{\beta}{a} + b\alpha\right)$، زمرة.

الحل

- لنلاحظ أوّلاً، في حالة (a_1,b_1) و (a_2,b_2) و (a_3,b_3) من $\mathbb{R}^* \times \mathbb{R}$ ما يلي :

$$\begin{aligned}\big((a_1,b_1)*(a_2,b_2)\big)*(a_3,b_3) &= \left(a_1a_2, \frac{b_2}{a_1} + b_1a_2\right)*(a_3,b_3)\\ &= \left(a_1a_2a_3, \frac{b_3}{a_1a_2} + \left(\frac{b_2}{a_1} + b_1a_2\right)a_3\right)\\ &= \left(a_1a_2a_3, \frac{b_3}{a_1a_2} + \frac{b_2a_3}{a_1} + b_1a_2a_3\right)\end{aligned}$$

و

$$\begin{aligned}(a_1,b_1)*\big((a_2,b_2)*(a_3,b_3)\big) &= (a_1,b_1)*\left(a_2a_3, \frac{b_3}{a_2} + b_2a_3\right)\\ &= \left(a_1a_2a_3, \frac{1}{a_1}\left(\frac{b_3}{a_2} + b_2a_3\right) + b_1a_2a_3\right)\\ &= \left(a_1a_2a_3, \frac{b_3}{a_1a_2} + \frac{b_2a_3}{a_1} + b_1a_2a_3\right)\end{aligned}$$

إذن

$$(a_1,b_1)*\big((a_2,b_2)*(a_3,b_3)\big) = \big((a_1,b_1)*(a_2,b_2)\big)*(a_3,b_3)$$

وعلى هذا فالقانون $*$ تجميعي.

- ومن جهة أخرى نلاحظ أنّه في حالة (a,b) من $\mathbb{R}^* \times \mathbb{R}$ لدينا

$$\begin{aligned}(a,b)*(1,0) &= \left(a\times 1, \frac{0}{a} + b\times 1\right) = (a,b)\\ (1,0)*(a,b) &= \left(1\times a, \frac{b}{1} + 0\times a\right) = (a,b)\end{aligned}$$

إذن العنصر $e = (1,0)$ عنصر حيادي في $(\mathbb{R}^* \times \mathbb{R}, *)$.

- وأخيراً، في حالة (a,b) من $\mathbb{R}^* \times \mathbb{R}$ لدينا

$$(a,b) * \left(\frac{1}{a}, -b\right) = \left(\frac{1}{a}, -b\right) * (a,b) = (1,0)$$

نستنتج أنّ البنية $(\mathbb{R}^* \times \mathbb{R}, *)$ زمرة، وهي غير تبديليّة، فمثلاً

$$(1,2) * (2,0) \neq (2,0) * (1,2)$$

ويكتمل الحل. ■

التمرين 2. بيّن أنّ البنية $(\mathbb{R}_+^* \times \mathbb{R}, *)$، حيث $(a,b) * (\alpha, \beta) = (a\alpha, a\beta + b)$، زمرة.

الحل

- لنلاحظ أوّلاً، في حالة (a_1,b_1) و (a_2,b_2) و (a_3,b_3) من $\mathbb{R}_+^* \times \mathbb{R}$ ما يلي :

$$\begin{aligned}\big((a_1,b_1) * (a_2,b_2)\big) * (a_3,b_3) &= (a_1a_2, a_1b_2 + b_1) * (a_3,b_3)\\ &= \big(a_1a_2a_3, a_1a_2b_3 + a_1b_2 + b_1\big)\end{aligned}$$

و

$$\begin{aligned}(a_1,b_1) * \big((a_2,b_2) * (a_3,b_3)\big) &= (a_1,b_1) * (a_2a_3, a_2b_3 + b_2)\\ &= \big(a_1a_2a_3, a_1(a_2b_3 + b_2) + b_1\big)\\ &= \big(a_1a_2a_3, a_1a_2b_3 + a_1b_2 + b_1\big)\end{aligned}$$

إذن

$$(a_1,b_1) * \big((a_2,b_2) * (a_3,b_3)\big) = \big((a_1,b_1) * (a_2,b_2)\big) * (a_3,b_3)$$

وعلى هذا فالقانون $*$ تجميعي.

- ومن جهة أخرى نلاحظ أنّه في حالة (a,b) من $\mathbb{R}_+^* \times \mathbb{R}$ لدينا

$$(a,b) * (1,0) = (a \times 1, a \times 0 + b) = (a,b)$$
$$(1,0) * (a,b) = (1 \times a, 1 \times b + 0) = (a,b)$$

إذن العنصر $e = (1,0)$ عنصر حيادي في $(\mathbb{R}_+^* \times \mathbb{R}, *)$.

- وأخيراً، في حالة (a,b) من $\mathbb{R}_+^* \times \mathbb{R}$ لدينا

$$(a,b) * \left(\frac{1}{a}, -\frac{b}{a}\right) = \left(\frac{1}{a}, -\frac{b}{a}\right) * (a,b) = (1,0)$$

نستنتج أنّ $(\mathbb{R}_+^* \times \mathbb{R}, *)$ زمرة، وهي غير تبديليّة، فمثلاً $(1,1) * (2,0) \neq (2,0) * (1,1)$. ■

التمرين 3. لتكن G مجموعة غير خالية مزوّدة بقانون تشكيل داخلي $*$، ولنفترض أنّ

- القانون $*$ تجميعي.
- $\exists e \in G, \quad \forall x \in G, \ \ x * e = x$
- $\forall x \in G, \quad \exists x' \in G, \ \ x * x' = e$

أثبت أنّ $(G, *)$ زمرة. يمكن حساب $x' * x * x' * x''$ ثمّ $x * x' * x$.

الحل

1. ليكن x عنصراً من G، إذن يوجد x' من G يُحقّق $x * x' = e$، وانطلاقاً من x' نجد x'' من G يُحقّق $x' * x'' = e$. لنحسب إذن المقدار $y = x' * x * x' * x''$ بطريقتين :

$$\begin{aligned} y &= x' * (x * (x' * x'')) \\ &= x' * (x * e) \\ &= x' * x \end{aligned}$$

وكذلك

$$\begin{aligned} y &= (x' * (x * x')) * x'' \\ &= (x' * e) * x'' \\ &= x' * x'' = e \end{aligned}$$

وعلى هذا فالعنصر x' من G الذي يُحقّق $x * x' = e$ يُحقّق أيضاً $x' * x = e$. فنكون قد أثبتنا أنّه مهما يكن x من G فيوجد عنصرٌ x' من G يُحقّق $x * x' = x' * x = e$.

2. ليكن x عنصراً من G، إذن يوجد x' من G يُحقّق $x * x' = x' * x = e$، لنحسب إذن المقدار $z = x * x' * x$ بطريقتين فنجد

$$\begin{aligned} z &= x * (x' * x) = x * e = x \\ &= (x * x') * x = e * x \end{aligned}$$

فنكون قد أثبتنا أنّ العنصر e من G يُحقّق أيضاً $e * x = x$ وذلك أيّاً كان x من G. فهو إذن عنصرٌ حيادي في G.

وهكذا نكون قد أثبتنا أنّ البنية $(G, *)$ زمرة. ■

التمرين 4. لتكن G مجموعة غير خالية مزوّدة بقانون تشكيل داخلي تجميعيّ $*$، ولنفترض أنّ التطبيقين

$$\gamma_a : G \to G, \quad x \mapsto a * x$$

و

$$\delta_a : G \to G, \quad x \mapsto x * a$$

غامران وذلك مهما تكن a من G. أثبت أنّ $(G, *)$ زمرة.

الحل

- ليكن a عنصراً من G، وهو موجود لأنّ G غير خالية، لمّا كان كلٌّ من التطبيقين γ_a و δ_a غامراً استنتجنا أنّه يوجد e و e' في G يُحقّقان $\gamma_a(e) = a$ و $\delta_a(e') = a$. أي

$$a * e = a \quad \text{و} \quad e' * a = a$$

نستنتج من ذلك أنّ

$$\forall x \in G, \quad x * a * e = x * a$$
$$\forall x \in G, \quad e' * a * x = a * x$$

أو

$$\forall x \in G, \qquad \delta_a(x) * e = \delta_a(x)$$
$$\forall x \in G, \quad e' * \gamma_a(x) = \gamma_a(x)$$

ولمّا كان التطبيقان γ_a و δ_a غامرين استنتجنا مما سبق أنّ

$$\forall y \in G, \quad y * e = y$$
$$\forall y \in G, \quad e' * y = y \qquad ①$$

وبوجه خاص نستنتج من الأولى أنّ $e' * e = e'$، ومن الثانية أنّ $e' * e = e$، فلا بُدّ أن يكون $e = e'$.

وبالعودة إلى ① نرى أنّ العنصر e يُحقّق

$$\forall y \in G, \quad y * e = e * y = y$$

فهو إذن عنصرٌ حيادي في $(G, *)$.

- ليكن a عنصراً من G، لمّا كان كلٌّ من التطبيقين γ_a و δ_a غامراً استنتجنا أنّه يوجد a' و a'' في G يُحقّقان $\gamma_a(a') = e$ و $\delta_a(a'') = e$. أي

$$a * a' = e \quad \text{و} \quad a'' * a = e$$

ولكن

$$a'' = a'' * e = a'' * (a * a') = (a'' * a) * a' = e * a' = a'$$

إذن يوجد عنصرٌ a' في G يُحقّق $a' * a = a * a' = e$. وهذا يُثبت أنّ لكلّ عنصر من G نظيراً فيها بالنسبة إلى القانون $*$، والبنية $(G,*)$ زمرة. ■

التمرين 5. لتكن G زمرة، ولتكن H_1 و H_2 زمرتين جزئيتين من G. أثبت أنّ $H_1 \cup H_2$ زمرة جزئية من G إذا وفقط إذا كان $H_1 \subset H_2$ أو $H_2 \subset H_1$.

الحل

- من الواضح أنّه في حالة $H_1 \subset H_2$ يكون $H_1 \cup H_2 = H_2$ وفي حالة $H_2 \subset H_1$ يكون $H_1 \cup H_2 = H_1$ وفي الحالتين تكون المجموعة $H_1 \cup H_2$ زمرة جزئيّة من G .
- وبالعكس، لنفترض أنّ المجموعة $H_1 \cup H_2$ زمرة جزئيّة من G، ولنفترض أنّ $H_2 \not\subset H_1$. عندئذ نجد عنصراً a_1 ينتمي إلى H_1 ولا ينتمي إلى H_2 .

ليكن x_2 عنصراً ما من H_2 . لمّا كان x_2 و a_1 عنصرين من الزمرة الجزئيّة $H_1 \cup H_2$ استنتجنا أن العنصر $x_2 a_1^{-1}$ ينتمي إلى الاجتماع $H_1 \cup H_2$. فإذا كان $x_2 a_1^{-1} \in H_2$، كان $a_1 = (x_2 a_1^{-1})^{-1} x_2 \in H_2$ وهذا خُلفٌ. إذن لا بُدّ أن يكون $x_2 a_1^{-1}$ عنصراً من H_1، ومن ثَمّ $x_2 = (x_2 a_1^{-1}) a_1 \in H_1$. لقد أثبتنا بذلك أنّ كلّ عنصرٍ من H_2 ينتمي إلى H_1، أو $H_2 \subset H_1$. وبذا يكتمل الإثبات. ■

التمرين 6. لتكن G زمرة، ولتكن H_1 و H_2 زمرتين جزئيتين من G. أوجد الشرط اللازم والكافي حتى تكون المجموعة $H_1 H_2 = \{h_1 h_2 : (h_1, h_2) \in H_1 \times H_2\}$ زمرة جزئية من G .

الحل

لنذكّر أنّه في حالة مجموعتين جزئيّتين غير خاليتين A و B من زمرة $(G,\cdot)$ فإنّ الرمز AB يدلّ على مجموعة عناصر G التي تُكتب بالشكل ab حيث $a \in A$ و $b \in B$.

سنبرهن فيما يلي تكافؤ الخاصّتين التاليتين :

❶ المجموعة H_1H_2 زمرة جزئيّة من G

❷ $H_1H_2 = H_2H_1$.

❶ ⇐ ❷ ليكن x عنصراً ما من H_1H_2 . لأنّ H_1H_2 زمرة نستنتج أنّ $x^{-1} \in H_1H_2$ ، إذن نجد h_1 في H_1 ، ونجد h_2 في H_2 ، يُحقّقان $x^{-1} = h_1h_2$. ومن ثمّ يكون

$$x = (h_1h_2)^{-1} = h_2^{-1}h_1^{-1} \in H_2H_1$$

إذن لقد أثبتنا أنّ $H_1H_2 \subset H_2H_1$.

وبالعكس، ليكن x عنصراً ما من H_2H_1 . عندئذ نجد h_1 في H_1 ، ونجد h_2 في H_2 ، يُحقّقان $x = h_2h_1$. ومن ثمّ يكون $x^{-1} = h_1^{-1}h_2^{-1}$ عنصراً من H_1H_2 ، ولكنّ هذه الأخيرة زمرة جزئيّة من G، إذن ينتج من $x^{-1} \in H_1H_2$ أنّ $x \in H_1H_2$. بذا نكون قد أثبتنا أنّ $H_2H_1 \subset H_1H_2$. أي $H_1H_2 = H_2H_1$.

❷ ⇐ ❶ لنضع $H = H_1H_2 = H_2H_1$.

- لمّا كان الحيادي 1 ينتمي إلى كلٍّ من H_1 و H_2 استنتجنا أنّ $1 \in H$.
- ليكن x عنصراً من H ، عندئذ يوجد h_1 في H_1 ، و h_2 في H_2 ، يُحقّقان $x = h_1h_2$. وعندئذ يكون $x^{-1} = h_2^{-1}h_1^{-1} \in H_2H_1 = H$. ومنه ينتمي نظير كلّ عنصرٍ من H إلى H .
- ليكن x و y عنصرين من H ، عندئذ يوجد h_1 في H_1 ، و h_2 في H_2 ، يُحقّقان $x = h_1h_2$ ، ويوجد k_1 في H_1 ، و k_2 في H_2 ، يُحقّقان $y = k_1k_2$ ، ولأنّ العنصر h_2k_1 من H_2H_1 ينتمي إلى H_1H_2 فيوجد ℓ_1 في H_1 ، و ℓ_2 في H_2 ، يُحقّقان $h_2k_1 = \ell_1\ell_2$ ، وعندئذ

$$xy = (h_1h_2)(k_1k_2) = h_1(h_2k_1)k_2 = h_1(\ell_1\ell_2)k_2 = (h_1\ell_1)(\ell_2k_2)$$

ومنه $xy \in H_1H_2 = H$ لأنّ $h_1\ell_1 \in H_1$ و $h_2\ell_2 \in H_2$. وعليه

$$\forall(x,y) \in H^2, xy \in H .$$

وبذلك نكون قد أثبتنا أنّ $H = H_1H_2$ زمرة. ■

التمرين 7. لتكن G زمرة، ولتكن H_1 و H_2 زمرتين جزئيتين منتهيتين من G. نفترض أنّ $H_1 \cap H_2 = \{1_G\}$ ، بيّن أن عددَ عناصر المجموعة

$$H_1H_2 = \{h_1h_2 : (h_1, h_2) \in H_1 \times H_2\}$$

يساوي $\operatorname{card}(H_1) \times \operatorname{card}(H_2)$.

الحل

نلاحظ أنّ $\operatorname{card}(H_1) \times \operatorname{card}(H_2) = \operatorname{card}(H_1 \times H_2)$، فهل يمكننا إيجاد تقابلٍ بين $H_1 \times H_2$ و H_1H_2 ؟ استناداً إلى تعريف H_1H_2 هناك تطبيق واضح يربط هاتين المجموعتين. لنتأمّل التطبيق

$$\varphi : H_1 \times H_2 \to H_1H_2,\ (h_1, h_2) \mapsto h_1h_2$$

من الواضح أنّ φ غامرٌ بناءً على تعريف H_1H_2 . لإثبات أنّ φ متباينٌ. نفترض أنّ (h_1, h_2) و (k_1, k_2) يُحقّقان :

$$\varphi(h_1, h_2) = \varphi(k_1, k_2)$$

عندئذ يكون لدينا $h_1h_2 = k_1k_2$، ومن ثَمّ $k_1^{-1}h_1 = k_2h_2^{-1}$، لنرمز بالرمز a إلى هذا العنصر. لمّا كان $a = k_1^{-1}h_1$، والمجموعة H_1 زمرة جزئيّة، استنتجنا أنّ $a \in H_1$، ولمّا كان $a = k_2h_2^{-1}$، والمجموعة H_2 زمرة جزئيّة، استنتجنا أنّ $a \in H_2$. وعليه ينتمي a إلى تقاطع الزمرتين الجزئيّتين H_1 و H_2 الذي لا يحوي إلّا العنصر الحيادي في G، إذن $a = 1_G$. ونستنتج من $k_1^{-1}h_1 = k_2h_2^{-1} = 1_G$ أنّ $h_1 = k_1$ و $h_2 = k_2$. وهذا يثبت أنّ φ متباين. لمّا كان φ تقابلاً استنتجنا أنّ

$$\operatorname{card}(H_1H_2) = \operatorname{card}(H_1 \times H_2) = \operatorname{card}(H_1) \times \operatorname{card}(H_2)$$ ■

التمرين 8. لتكن H_1 و H_2 زمرتين جزئيتين منتهيتين من زمرة G. نضع

$$H_1H_2 = \{h_1h_2 : (h_1, h_2) \in H_1 \times H_2\}$$

وليكن z عنصراً من H_1H_2، احسب المقدار

$$\operatorname{card}(\{(h_1, h_2) \in H_1 \times H_2 : h_1h_2 = z\})$$

واستنتج أنّ

$$\operatorname{card}(H_1H_2) = \frac{\operatorname{card}(H_1) \times \operatorname{card}(H_2)}{\operatorname{card}(H_1 \cap H_2)}$$

الحل

▫ ليكن $z = \ell_1\ell_2$ عنصراً من H_1H_2 عندئذ يعرّف التطبيق

$$\psi : H_1 \cap H_2 \to \{(h_1, h_2) \in H_1 \times H_2 : h_1h_2 = z\},\ h \mapsto (\ell_1 h, h^{-1}\ell_2)$$

تقابلاً. من الواضح أنّ ψ متباينٌ. لنثبت أنّه غامرٌ أيضاً.

ليكن (h_1, h_2) عنصراً من $H_1 \times H_2$ يُحقّق $z = h_1h_2$. عندئذ يكون لدينا

$$z = \ell_1\ell_2 = h_1h_2$$

ومن ثَمّ $\ell_2h_2^{-1} = \ell_1^{-1}h_1$. لنرمز بالرمز h إلى هذا العنصر. إنّ $h = \ell_1^{-1}h_1$ يقتضي $h \in H_1$ لأنّ H_1 زمرة جزئيّة من G، ثُمّ إنّ $h = \ell_2h_2^{-1}$ يقتضي $h \in H_2$ لأنّ H_2 زمرة جزئيّة من G . وعليه نرى أنّه يوجد h ينتمي إلى $H_1 \cap H_2$ ويُحقّق $h = \ell_2h_2^{-1} = \ell_1^{-1}h_1$ أي $\psi(h) = (h_1, h_2)$. وهكذا نكون قد أثبتنا أنّ ψ تقابلٌ ومن ثَمّ نكون قد أثبتنا أنّ

$$\forall z \in H_1H_2,\ \operatorname{card} H_1 \cap H_2 = \operatorname{card}\big(\{(h_1, h_2) \in H_1 \times H_2 : h_1h_2 = z\}\big)$$

▫ لنتأمّل كما في التمرين السابق التطبيق

$$\varphi : H_1 \times H_2 \to H_1H_2,\ (h_1, h_2) \mapsto h_1h_2$$

من الواضح أنّ φ غامرٌ بناءً على تعريف H_1H_2 . ولكنّه ليس بالضرورة متبايناً. نستنتج من كون التطبيق φ غامراً أنّ المجموعات $\left(\varphi^{-1}(\{z\})\right)_{z \in H_1H_2}$ تكوّن تجزئة للمجموعة المنتهية $H_1 \times H_2$ وعليه

$$\operatorname{card}(H_1 \times H_2) = \sum_{z \in H_1H_2} \operatorname{card}\left(\varphi^{-1}(\{z\})\right)$$

ولكن بالعودة إلى ما أثبتناه آنفاً وبملاحظة أنّ

$$\varphi^{-1}(\{z\}) = \left\{\left(h_1, h_2\right) \in H_1 \times H_2 : h_1h_2 = z\right\}$$

نستنتج أنّ

$$\forall z \in H_1H_2,\ \operatorname{card}\left(\varphi^{-1}(\{z\})\right) = \operatorname{card}(H_1 \cap H_2)$$

ومنه

$$\operatorname{card}(H_1 \times H_2) = \sum_{z \in H_1H_2} \operatorname{card}(H_1 \cap H_2) = \operatorname{card}(H_1 \cap H_2)\operatorname{card}(H_1H_2)$$

ومنه النتيجة المرجوّة. ∎

التمرين 9. لتكن $(G,\cdot)$ زمرة تُحقِّق $\forall x \in G,\ x^2 = 1$.

- بيّن أنّ $(G,\cdot)$ زمرة تبديلية.
- نفترض أنّ G منتهية. بيّن أنه يوجد عدد طبيعي n ، ومجموعة E عدد عناصرها n فتكون الزمرة $(G,\cdot)$ مشاكِلة تقابلياً للزمرة $(P(E),\Delta)$.

الحل

- ليكن x و y عنصرين من G . عندئذ يكون لدينا $x^2 = y^2 = (xy)^2 = 1$. ومنه

$$x^2y^2 = 1 = (xy)(xy)$$

ومن ثَمّ

$$x(xy)y = x(yx)y$$

وبضرب طرفي المساواة السابقة بالعنصر x من اليسار، وبالعنصر y من اليمين، نجد $xy = yx$. وهذا يثبت أنّ الزمرة $(G,\cdot)$ تبديليّة.

- لنعرف المجموعة $\mathcal{N}$ الجزئيّة من $\mathbb{N}$ والمكوّنة من أعداد عناصر المجموعات الجزئيّة من G التي تولّد الزمرة G كاملة، أي :

$$\mathcal{N} = \left\{\text{card}(H) : \left(H \subset G\right) \wedge \left(\langle H\rangle = G\right)\right\}$$

من الواضح أنّ $\mathcal{N}$ مجموعة جزئيّة من $\mathbb{N}$ ، غير خالية لأنها تضم $\text{card}(G)$ ، يمكننا إذن أن نعرّف العدد n بأنّه أصغر عناصرها. أي $n = \min \mathcal{N}$ ، ولأنّ $n \in \mathcal{N}$ نجد مجموعة E جزئيّة من G ، وتولّد G ، وتُحقِّق $n = \text{card}(E)$.

لنعرّف إذن التطبيق $\varphi : P(E) \to G, A \mapsto \prod_{a\in A} a$ ، مع الاصطلاح $\prod_{a\in\varnothing} a = 1$.

  - التطبيق φ تشاكلٌ زمري بين $\left(P(E),\Delta\right)$ و $(G,\cdot)$. لأنّ

$$\begin{aligned}\varphi(A)\varphi(\text{B}) &= \prod_{a\in A} a \prod_{a\in B} b = \left(\prod_{a\in A\setminus B} a\right)\left(\prod_{c\in A\cap B} c\right)\left(\prod_{c\in B\cap A} c\right)\left(\prod_{b\in B\setminus A} b\right)\\ &= \left(\prod_{a\in A\setminus B} a\right)\left(\prod_{b\in B\setminus A} b\right) = \prod_{a\in A\Delta B} a = \varphi(A\Delta B)\end{aligned}$$

  أيّاً كانت المجموعتان A و B من $P(E)$.

  - التطبيق φ غامرٌ لأنّ E تولّد G ولأنّ مقلوب أي عنصر من G يساويه والزمرة G تبديليّة.

- التطبيق φ متباينٌ. في الحقيقة، ليكن A عنصراً من $\ker\varphi$. إذا كان $A \neq \varnothing$ وجدنا عنصراً a_0 في A. وعندئذ نستنتج من كون $\varphi(A)=1$ أنّ $\prod_{a\in A\setminus\{a_0\}} a = a_0$، ومن ثَمّ تولِّد المجموعة $E\setminus\{a_0\}$ الزمرة G. وهذا يناقض تعريف المجموعة E، إذ هي مجموعة مولِّدة للزمرة G عدد عناصرها أصغري. وعليه $A=\varnothing$. والتطبيق φ متباينٌ.

بذلك نكون قد أوجدنا تشاكلاً زمريّاً تقابليّاً بين $(G,\cdot)$ والزمرة $\left(P(E),\Delta\right)$. وبوجه خاص نرى أنّ عدد عناصر G يساوي 2^n. ■

التمرين 10. أثبت أنّه لا يوجد تشاكل تقابلي بين الزمرتين $(\mathbb{R}^*,\cdot)$ و $(\mathbb{Q}^*,\cdot)$.

الحل

لنفترض جدلاً أنّه يوجد تشاكلٌ تقابلي زمري $\varphi:(\mathbb{R}^*,\cdot)\to(\mathbb{Q}^*,\cdot)$. نعرّف إذن العدد r من $\mathbb{Q}^*$ بالعلاقة $r=\varphi\left(\sqrt[3]{\varphi^{-1}(2)}\right)$. فنلاحظ أنّ

$$\begin{aligned}
r^3 &= \varphi\left(\sqrt[3]{\varphi^{-1}(2)}\right)\varphi\left(\sqrt[3]{\varphi^{-1}(2)}\right)\varphi\left(\sqrt[3]{\varphi^{-1}(2)}\right)\\
&= \varphi\left(\sqrt[3]{\varphi^{-1}(2)}\cdot\sqrt[3]{\varphi^{-1}(2)}\cdot\sqrt[3]{\varphi^{-1}(2)}\right) = \varphi(\varphi^{-1}(2)) = 2
\end{aligned}$$

إذن يوجد عددٌ عادي r في $\mathbb{Q}^*$ يُحقّق $r^3=2$.

لنفترض أنّ $r=\dfrac{p}{q}$ حيث (p,q) من $\mathbb{N}^{*2}$، وأنّه ليس للعددين p و q قواسم مشتركة. نستنتج من المساواة $q^3=2p^3$ أنّ العدد q^3 زوجي، ومن ثَمّ أنّ q زوجي أيضاً، وعليه يوجد q' من $\mathbb{N}^*$ يُحقّق $q=2q'$، ومنه $4q'^3=p^3$. ونستنتج مجدّداً أنّ العدد p^3 زوجي، ومن ثَمّ أنّ p زوجي أيضاً. وهذا خُلفٌ لأننا افترضنا أن ليس للعددين p و q قواسم مشتركة. نستنتج من هذا التناقض أنّه لا يوجد تشاكلٌ تقابلي زمري بين الزمرتين $(\mathbb{R}^*,\cdot)$ و $(\mathbb{Q}^*,\cdot)$. ■

التمرين 11. لتكن H زمرة جزئية من $\mathbb{Z}^2=\mathbb{Z}\times\mathbb{Z}$. بيّن أنه يوجد a و b في $\mathbb{Z}^2$ يُحقّقان $H=\left\{na+mb : (n,m)\in\mathbb{Z}^2\right\}$.

الحل

نعرّف المجموعتين

$$H_1=\left\{k\in\mathbb{Z}:(k,0)\in H\right\}=\mathrm{Pr}_1\left(H\cap(\mathbb{Z}\times\{0\})\right)$$
$$H_2=\left\{p\in\mathbb{Z}:\exists q\in\mathbb{Z},(q,p)\in H\right\}=\mathrm{Pr}_2(H)$$

إذ عرّفنا التشاكلين الزمريّين Pr_1 و Pr_2 كما يلي :

$$\mathrm{Pr}_1:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},(x_1,x_2)\mapsto x_1$$
$$\mathrm{Pr}_2:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},(x_1,x_2)\mapsto x_2$$

لمّا كان تقاطع زمرتين جزئيّتين من $\mathbb{Z}^2$ هو زمرة جزئيّة منها، ولمّا كانت صورة زمرة جزئيّة وفق تشاكل زمري هي أيضاً زمرة جزئيّة، استنتجنا أنّ كلّاً من H_1 و H_2 زمرة جزئيّة من $\mathbb{Z}$. وعليه نجد α في $\mathbb{N}$ تُحقّق $H_1=\alpha\mathbb{Z}$، ونجد β في $\mathbb{N}$ تُحقّق $H_2=\beta\mathbb{Z}$. ولأنّ $\beta\in H_2$ استنتجنا أنّه يوجد عنصرٌ γ في $\mathbb{Z}$ يُحقّق $(\gamma,\beta)\in H$.

لنعرّف إذن العنصرين $a=(\alpha,0)$ و $b=(\gamma,\beta)$ من H.

- من الواضح أنّ

$$H\supset\langle\{a,b\}\rangle=\left\{na+mb:(n,m)\in\mathbb{Z}^2\right\}.$$

- وبالعكس، ليكن $z=(x,y)$ عنصراً من H. لمّا كان $y=\mathrm{Pr}_2(z)\in H_2$ استنتجنا أنّه يوجد عددٌ m ينتمي إلى $\mathbb{Z}$ يُحقّق $y=\beta m$. وعليه نجد أنّ

$$z-mb=\left(x-\gamma m,0\right)\in H\cap\left(\mathbb{Z}\times\{0\}\right)$$

وعليه $x-\gamma m\in H_1$، إذن يوجد n ينتمي إلى $\mathbb{Z}$ يُحقّق $x-\gamma m=\alpha n$، ومن ثَمّ

$$z-mb=(x-\gamma m,0)=(\alpha n,0)=na$$

أو $z=na+mb\in\langle\{a,b\}\rangle$. إذن $H\subset\langle\{a,b\}\rangle$.

وبذا نكون قد أثبتنا أنّ $H=\langle\{a,b\}\rangle$، وهي النتيجة المرجوّة. ■

التمرين 12. لتكن $(G,\cdot)$ زمرة منتهية عدد عناصرها n. بيّن أنّ $\forall x\in G,\ x^n=1$.

الحل

ليكن x عنصراً من G. الزمرة G منتهية إذن رتبة x منتهية ولتكن m. لدينا من جهة أولى $x^m=1$، ومن جهة ثانية أنّ m يقسم n، لأنّ $m=\mathrm{card}(\langle x\rangle)$ و $\langle x\rangle$ زمرة جزئيّة من G التي عدد عناصرها n. إذن يوجد d يُحقّق $md=n$. ومنه $x^n=(x^m)^d=1$. ■

التمرين 13. لتكن $(G,\cdot)$ زمرة منتهية عدد عناصرها فردي، أثبت أنّ التطبيق φ المعرّف كما يأتي: $\varphi : G \to G, x \mapsto x^2$ تقابلٌ.

الحل

لنفترض أنّ $\text{card}(G) = 2m+1$ ، إذن استناداً إلى التمرين السابق لدينا

$$\forall x \in G,\ x^{2m+1} = 1$$

لنعرّف إذن التطبيق $\psi : G \to G, x \mapsto x^{m+1}$ ، فيكون لدينا $\varphi \circ \psi = \psi \circ \varphi = I_G$.

إذن φ تقابلٌ وتقابله العكسي هو ψ . ■

التمرين 14. لتكن $(G,\cdot)$ زمرة منتهية عدد عناصرها أوليّ p ، أثبت أنّ $(G,\cdot)$ تُشاكِل تقابلياً الزمرة $(\mathbb{Z}/p\mathbb{Z},+)$.

الحل

ليكن b عنصراً من $G\backslash\{1\}$. عندئذ تكون $\langle b\rangle$ زمرة جزئيّة غير تافهة من G، وعليه فإنّ $\text{card}(\langle b\rangle)$ قاسمٌ مختلف عن الواحد للعدد الأوّلي p . إذن يجب أن يكون

$$\text{card}(\langle b\rangle) = p = \text{card}(G)$$

ومنه $G = \langle b\rangle$. فالزمرة G زمرة وحيدة التوليد، وعدد عناصرها p . فهي إذن تُشاكل تقابليّاً الزمرة $(\mathbb{Z}/p\mathbb{Z},+)$. والتشاكل التقابلي هو $\varphi : \mathbb{Z}/p\mathbb{Z} \to G, [k] \mapsto b^k$. ■

التمرين 15. ليكن x و y عنصرين من زمرة $(G,\cdot)$. بيّن أنّ $O(xy) = O(yx)$.

الحل

في الحقيقة، نثبت بالتدريج على العدد n أنّ

$$\forall n \in \mathbb{N},\quad y(xy)^n = (yx)^n y$$

وعليه نرى أنّه في حالة n من $\mathbb{N}^*$ لدينا التكافؤ

$$\Big((xy)^n = 1\Big) \Leftrightarrow \Big((yx)^n = 1\Big)$$

وهذا يثبت أنّ للعنصرين xy و yx المرتبة نفسها، سواء كانت منتهية أم لم تكن. ■

التمرين 16. ليكن x عنصراً من زمرة $(G,\cdot)$. نفترض أنّ رتبة x منتهية وأنّ $O(x)=n$. أثبت أنه أياً كان m من $\mathbb{N}^*$، فرتبة العنصر x^m منتهية وتساوي $\dfrac{n}{\gcd\,(n,\,m)}$.

الحل

لنفترض أنّ $d=\gcd(n,m)$ ولنعرف n' و m' بالعلاقتين $n=dn'$ و $m=dm'$. نعلم أنّ رتبة عنصر a تُعطى بالعلاقة $O(a)=\operatorname{card}(\langle a\rangle)$، وهي تُحقّق :

$$\left\{k\in\mathbb{Z} : a^k=1\right\}=O(a)\mathbb{Z}.$$

فإذا كان $\lambda=O(x^m)$ كان $\lambda=\operatorname{card}(\langle x^m\rangle)$، و $\{k\in\mathbb{Z} : x^{km}=1\}=\lambda\mathbb{Z}$.

- لنلاحظ أوّلاً أنّ $(x^m)^{n'}=(x^n)^{m'}=1^{m'}=1$ إذن $\lambda\mid n'$.
- ومن جهة أخرى، لمّا كان $x^{\lambda m}=1$ استنتجنا من كون
$$\{p\in\mathbb{Z} : x^p=1\}=n\mathbb{Z}$$
أنّ $n\mid\lambda m$، أو $n'\mid\lambda m'$. ولكن $\gcd(n',m')=1$، إذن استناداً إلى خاصّة غاوس $n'\mid\lambda$.

إذن لقد أثبتنا أنّ $\lambda\mid n'$ و $\lambda\mid n'$، ولأنّ العددين λ و n' موجبان، استنتجنا أنّ $\lambda=n'$. أي

$$O(x^m)=\frac{n}{\gcd(n,m)}$$ ■

التمرين 17. ليكن x و y عنصرين من زمرة $(G,\cdot)$. نفترض أنّ رتبة كل من x و y منتهية وأنّ $O(x)=n$ و $O(y)=m$. أثبت أنه إذا كان

$$xy=yx \quad \text{و} \quad \gcd\,(n,m)=1$$

كان $O(xy)=nm$.

الحل

لنفترض أنّ $\lambda=O\big(xy\big)$.

- نلاحظ أوّلاً أنّ الشرط $xy=yx$ يقتضي $(xy)^{nm}=(x^n)^m(y^m)^n=1$ إذن $\lambda\mid nm$.

- من جهة أخرى إنّ رتبة أي عنصر من التقاطع $\langle x\rangle \cap \langle y\rangle$ تقسم كلاًّ من n و m، ولأنهما أوّليان فيما بينهما، استنتجنا أنّ رتبة ي عنصرمن $\langle x\rangle \cap \langle y\rangle$ تساوي 1 أي $\langle x\rangle \cap \langle y\rangle = \{1\}$.

ولكن نعلم أنّ $(xy)^\lambda = 1$ ومنه $x^\lambda = y^{-\lambda}$. إذن $x^\lambda \in \langle x\rangle \cap \langle y\rangle$ ومن ثمّ

$$x^\lambda = y^{-\lambda} = 1$$

نستنتج من $x^\lambda = 1$ أنّ $n \mid \lambda$، ونستنتج من $y^\lambda = 1$ أنّ $m \mid \lambda$، وأخيراً نستنتج من كون $\gcd(n,m) = 1$ ومن كون λ مُضاعفاً مشتركاً للعددين n و m أنّ $nm \mid \lambda$.

وبذلك نكون قد أثبتنا أنّ

$$(nm) \mid \lambda \quad \text{و} \quad \lambda \mid (nm)$$

أي $\lambda = nm$ لأنّ العددين λ و nm موجبان. ■

التمرين 18.

I. لتكن $(G,\cdot)$ زمرة منتهية. نفترض أن الزمرة G تحتوي على عنصرين c و b، ونفترض أن رُتب العناصر c و b و cb تساوي 2. أثبت أن G تحتوي على زمرة جزئية عدد عناصرها 4، ومن ثمّ أن 4 يقسم $\mathrm{card}(G)$.

II. لتكن $(G,\cdot)$ زمرة منتهية عدد عناصرها زوجي. نعرّف على G العلاقة الثنائية :

$$x\mathcal{R}y \Leftrightarrow x \in \left\{y, y^{-1}\right\}$$

1. أثبت أن $\mathcal{R}$ علاقة تكافؤ، ما هو صف تكافؤ العنصر الحيادي 1 ؟
2. ما هو عدد عناصر صف تكافؤ عنصر ما x من G؟
3. استنتج من كون صفوف التكافؤ تكوّن تجزئة للمجموعة G أن
$$\mathrm{card}\left(\left\{x \in G : x^2 = 1\right\}\right)$$
عددٌ زوجي.
4. أثبت أن الزمرة G تحوي عنصراً رتبته 2.

III. لتكن $(G,\cdot)$ زمرة منتهية عدد عناصرها $2p$ حيث p عدد أولي فردي.

1. نفترض أن G تحوي عنصراً وحيداً b رتبته 2.

① ليكن x عنصراً من $G\backslash\{1,b\}$. ما رتبة العنصر $x\,b\,x^{-1}$ ؟ استنتج أن جميع عناصر G تتبادل مع b.

② ليكن x عنصراً من $G\backslash\{1,b\}$. بيّن أن رتبة أحد العنصرين x أو $b\,x$ تساوي $2p$.

③ استنتج أن الزمرة $(G,\cdot)$ تُشاكل تقابلياً الزمرة $(\mathbb{Z}/2p\mathbb{Z},+)$.

2. نفترض أن G تحوي عنصرين على الأقل b و c رتبتهما 2 . نضع $a = bc$.

① بيّن أن رتبة a تساوي p . هل يمكن أن يكون $ab = ba$ ؟

② ما هي العناصر x في G التي تتبادل مع b ؟

③ نعرّف، في حالة k من $\{0,1,\ldots,p-1\}$ ، $x_k = a^k b\,a^{-k}$.بيّن أنّ رتبة أيٍّ من عناصر المجموعة $\mathcal{X} = \{x_k : 0 \le k < p\}$ تساوي 2، وأن هذه العناصر مختلفة مثنى مثنى.

④ نعرّف، أياً كان العنصر g من G، التطبيق :

$$\sigma_g : G \to G : x \mapsto gxg^{-1}$$

بيّن أن σ_g تقابل من G إلى G، وأن $\sigma_{g_1g_2} = \sigma_{g_1} \circ \sigma_{g_2}$، وأخيراً أنّ $\sigma_g(\mathcal{X}) = \mathcal{X}$.

⑤ لنرمز إذن بالرمز s_g إلى التقابل المعرّف على المجموعة $\mathcal{X}$ بالعلاقة: $s_g(x) = \sigma_g(x)$، وبالرمز $(S(\mathcal{X}),\circ)$ إلى الزمرة المتناظرة على $\mathcal{X}$. بيّن أن التطبيق

$$\Psi : G \to S(\mathcal{X}) : g \mapsto s_g$$

تشاكلٌ زمري متباين.

IV. استنتج من الدراسة السابقة أن كل زمرة $(G,\cdot)$ عدد عناصرها 6 تُشاكل تقابلياً $(\mathbb{Z}/6\mathbb{Z},+)$ أو $(S_3,\circ)$.

الحل

I. نتحقّق مباشرة أنّ المجموعة $V=\{1,b,c,bc\}$ زمرة جزئيّة من G، وعدد عناصرها يساوي 4، حيث نتيقّن أنّ العناصر 1 و b و c و bc مختلفة مثنى مثنى وأنّ $bc=cb$. إذن 4 يقسم $\text{card}(G)$.

II.1. يكفي أن نلاحظ أنّ $x\mathcal{R}y \Leftrightarrow \{x,x^{-1}\}=\{y,y^{-1}\}$ لنتيقّن مباشرة أنّ $\mathcal{R}$ علاقة تكافؤ. أمّا صفّ تكافؤ الحيادي 1 فهو $\{1\}$. أي $[1]=\{1\}$.

II.2. ليكن x عنصراً من G، من الواضح أنّ $[x]=\{x,x^{-1}\}$.

- فإذا كان $x\neq x^{-1}$، أو $x^2\neq 1$ كان $\text{card}\big([x]\big)=2$،
- وإذا كان $x=x^{-1}$، أو $x^2=1$، كان $\text{card}\big([x]\big)=1$.

II.3. لتكن $G_0=\{x\in G : x^2=1\}$، وهي مجموعة عناصر G التي صفوف تكافئها تحوي عنصراً واحداً. ولمّا كان $\forall x\in G\backslash G_0,\ [x]\subset G\backslash G_0$، استنتجنا أنّ صفوف التكافؤ تجزِّئ المجموعة $G\backslash G_0$. فتوجد عناصر $x_1,\ldots,x_m$ في $G\backslash G_0$ تجعل من $\big([x_k]\big)_{1\le k\le m}$ تجزئة للمجموعة $G\backslash G_0$، ولأنّ عدد عناصر كلِّ واحد من صفوف التكافؤ هذه يساوي 2 استنتجنا أنّ $\text{card}(G\backslash G_0)=2m$. وعليه

$$\text{card}(G_0)=\text{card}(G)-\text{card}(G\backslash G_0)=\text{card}(G)-2m$$

ولأنّ عدد عناصر G زوجي استنتجنا أنّ $\text{card}(G_0)$ زوجي أيضاً.

II.4. وجدنا أنّ عدد عناصر المجموعة $G_0=\{x\in G : x^2=1\}$ زوجي ونعلم أنّ الحيادي 1 عنصرٌ ينتمب إلى G_0، إذن $\text{card}(G_0\backslash\{1\})$ عددٌ فردي. ولكنّ المجموعة $G_0\backslash\{1\}$ هي مجموعة عناصر G التي رتبتها تساوي 2. إذن لقد أثبتنا أنّه في زمرة عدد عناصرها زوجي يوجد عددٌ فرديٌّ من العناصر التي رتبتها تساوي 2، ويوجد من ثَمّ عنصرٌ واحدٌ رتبته 2 على الأقل.

III.1. نفترض أنّ $(G,\cdot)$ زمرة منتهية عدد عناصرها $2p$ و p عددٌ أوليٌّ فردي. وأنّها تحوي عنصراً واحداً b رتبته 2.

III.1.① ليكن x عنصراً من G مختلفاً عن 1. لمّا كان $xbx^{-1}=1$ يقتضي $b=1$ استنتجنا أنّ $xbx^{-1}\neq 1$. ولكن

$$(xbx^{-1})^2=xbx^{-1}xbx^{-1}=xb^2x^{-1}=xx^{-1}=1$$

إذن رُتبة العنصر xbx^{-1} تساوي 2. ولكنّ b هو العنصر الوحيد الذي رتبته 2، إذن $xbx^{-1} = b$ أو $xb = bx$، وهذا أيضاً محقّق في حالة $x = 1$، إذن

$$\forall x \in G,\ xb = bx\ .$$

III.1.② ليكن x عنصراً من $G\backslash\{1,b\}$. إنّ رتبة العنصر x قاسمٌ للعدد $2p$ وهي لا تساوي 1 لأنّ $x \neq 1$، ولا تساوي 2 لأنّ $x \neq b$، إذن $O(x) = p$ أو $O(x) = 2p$.

فإذا كانت رتبة x تساوي p كان $O(bx) = O(b)O(x) = 2p$، لأنّ x و b يتبادلان، والعددان 2 و p أوّليّان فيما بينهما.

III.1.③ إذن، يوجد في G عنصرٌ رتبته $2p$، فهي إذن وحيدة التوليد، وتشاكل تقابليّاً $\left(\mathbb{Z}/2p\mathbb{Z},+\right)$.

III.2. نفترض أنّ $(G,\cdot)$ زمرة منتهية عدد عناصرها $2p$ و p عددٌ أولي فردي. وأنّ G تحوي عنصرين على الأقل b و c رتبتهما 2. نضع $a = bc$.

III.2.① رتبة a قاسمٌ للعدد $2p$. لنناقش إذن الحالات المختلفة :

- $O(a) = 1$. في هذه الحالة يكون $bc = 1$ ومنه $b = c^{-1} = c$ وهذا **يناقض** كون $b \neq c$.
- $O(a) = 2p$. في هذه الحالة يكون $G = \langle a\rangle$، و $G \cong (\mathbb{Z}/2p\mathbb{Z},+)$. ولكن في هذه الزمرة يوجد زمرة جزئيّة وحيدة عدد عناصرها 2 مما **يناقض** وجود عنصرين مختلفين رتبة كلٍّ منهما 2.
- $O(a) = 2$. في هذه الحالة نستفيد من السؤال I. فنستنتج أنّ 4 يقسم $\mathrm{card}(G)$ أي $2p$، وهذا تناقضٌ أيضاً.

وعليه لا بُدّ أن يكون $O(a) = p$. ثُمّ إنّ $ab \neq ba$، لأنّه لو كان $ab = ba$ لكان $O(ba) = 2p$، ومن ثَمّ يكون $G = \langle ba\rangle$، و $G \cong \left(\mathbb{Z}/2p\mathbb{Z},+\right)$. ولكن في هذه الزمرة يوجد زمرة جزئيّة وحيدة عدد عناصرها 2 مما **يناقض** وجود عنصرين مختلفين رتبة كلّ منهما 2.

III.2.② ليكن x عنصراً من $G\backslash\{1,b\}$. ولنفترض أنّ $xb = bx$. ولنناقش الحالات المختلفة بشأن رتبة العنصر x، التي لا تساوي 1 لأنّ $x \neq 1$.

- $O(x) = 2$. في هذه الحالة تكون المجموعة $\{1,b,x,bx\}$ زمرة جزئيّة من G وهذا تناقضٌ لأنّ 4 لا يقسم $2p$.

- $O(x)=p$. في هذه الحالة يكون $O(xb)=2p$ ، ومن ثَمّ $G\cong\left(\mathbb{Z}/2p\mathbb{Z},+\right)$، وهذا يناقض كون G زمرة غير تبديليّة.
- $O(x)=2p$، ومن ثَمّ $G\cong\left(\mathbb{Z}/2p\mathbb{Z},+\right)$، وهذا بدوره يناقض كون G زمرة غير تبديليّة.

إذن لقد أثبتنا أنّ

$$\forall x\in G\backslash\{1,b\},\quad xb\neq bx$$

والعناصر التي تتبادل مع b هي 1 و b فقط.

③.2. III لنعرّف إذن $x_k=a^k b\, a^{-k}$ في حالة k من $\{0,1,\ldots,p-1\}$. نلاحظ أنّ $x_k\neq 1$ لأنّ $b\neq 1$، وأنّ

$$x_k^2=a^kba^{-k}a^kba^{-k}=a^kb^2a^{-k}=a^ka^{-k}=1$$

لأنّ $b^2=1$. إذن رتبة أيٍّ من عناصر المجموعة $\mathcal{X}=\left\{x_k:0\leq k<p\right\}$ تساوي 2. وإذا كان $0\leq k<r<p$ فإن

$$\left(x_k=x_r\right)\Leftrightarrow\left(a^kba^{-k}=a^rba^{-r}\right)\Leftrightarrow\left(a^{k-r}b=ba^{k-r}\right)$$

إذن $x_r=x_k$ إذا وفقط إذا كان العنصران a^{k-r} و b يتبادلان، أي إذا وفقط إذا انتمى a^{k-r} إلى $\{1,b\}$، ولكن $\langle a\rangle\cap\langle b\rangle=\{1\}$، إذن $x_r=x_k$ إذا وفقط إذا كان $a^{k-r}=1$، ولأنّ رتبة a تساوي p فإنّ هذا يُكافئ $p\mid(k-r)$، ممّا يناقض كون $0\leq k<r<p$.

نستنتج من هذه المناقشة أنّ

$$\left(0\leq k<r<p\right)\Rightarrow x_k\neq x_r$$

لأن $\langle a\rangle\cap\mathcal{X}=\varnothing$ و $\operatorname{card}(\langle a\rangle)=\operatorname{card}(\mathcal{X})=p$ استنتجنا أنّ $\mathcal{X}=G\backslash\langle a\rangle$. وأنّ $\mathcal{X}$ هي مجموعة جميع عناصر G التي رتبتها تساوي 2.

④.2. III لنعرّف، أيّاً كان العنصر g من G، التطبيق : $\sigma_g:G\to G:x\mapsto gxg^{-1}$.

من الواضح أنّ σ_g تقابل، وأنّ تقابله العكسيّ هو $\sigma_{g^{-1}}$، وأن $\sigma_{g_1g_2}=\sigma_{g_1}\circ\sigma_{g_2}$.

ليكن g من G، وليكن x من $\mathcal{X}$، ولنتأمّل $y=\sigma_g(x)$. إنّ $x\neq 1$ إذن $y\neq 1$، وكذلك

$$y^2=gxg^{-1}gxg^{-1}=gx^2g^{-1}=gg^{-1}=1$$

إذن $O(y)=2$ ومنه $y\in\mathcal{X}$. لقد أثبتنا أنّ $\sigma_g(\mathcal{X})\subset\mathcal{X}$ ، ولأنّ $\sigma_{g^{-1}}(\mathcal{X})\subset\mathcal{X}$ استنتجنا أيضاً أنّ $\mathcal{X}\subset\sigma_g(\mathcal{X})$ ومنه $\sigma_g(\mathcal{X})=\mathcal{X}$.

III.2.⑤ لنرمز إذن بالرمز s_g إلى التقابل المعرّف على $\mathcal{X}$ بالعلاقة: $s_g(x)=\sigma_g(x)$ ، وبالرمز $(S(\mathcal{X}),\circ)$ إلى الزمرة المتناظرة على $\mathcal{X}$. ولنتأمّل التطبيق

$$\Psi: G\to S(\mathcal{X}), g\mapsto s_g$$

ليكن g_1 و g_2 عنصرين من G ، و x من $\mathcal{X}$. عندئذ

$$\begin{aligned}\Psi(g_1)\circ\Psi(g_2)(x)&=s_{g_1}(s_{g_2}(x))=g_1(g_2xg_2^{-1})g_1^{-1}\\&=g_1g_2x(g_1g_2)^{-1}=\Psi(g_1g_2)(x)\end{aligned}$$

ومنه

$$\forall(g_1,g_2)\in G^2,\quad \Psi(g_1)\circ\Psi(g_2)=\Psi(g_1g_2)$$

فالتطبيق Ψ تشاكلٌ زمري.

ومن جهة أخرى، إذا كان g عنصراً من $\ker\Psi$ كان $\Psi(g)=I$ أو

$$\forall x\in\mathcal{X},\quad gx=xg$$

إذن g يتبادل مع جميع العناصر التي رتبتها تساوي 2 ، ولكن نستنتج من III.2.② أنّ العنصر الذي يتبادل مع جميع هذه العناصر هو 1 . إذن $g=1$. ومنه $\ker\Psi=\{1\}$. والتطبيق Ψ تشاكلٌ زمري متباينٌ.

IV. لتكن G زمرة عدد عناصرها $6=2\times3$. استناداً إلى دراستنا السابقة نرى أنّ هناك حالتين :

- يوجد في G عنصرٌ وحيد رتبته 2 . وعندئذ $G\cong\left(\mathbb{Z}/6\mathbb{Z},+\right)$.
- يوجد في G عنصران على الأقلّ رتبة كلٍّ منهما 2 . وعندئذ نجد تشاكلاً زمرياً متبايناً Ψ بين G وزمرة التباديل $\left(S_3,\circ\right)$ ، لأنّ $\operatorname{card}(\mathcal{X})=3$. ولكن

$$\operatorname{card}(G)=\operatorname{card}(S_3)=6$$

إذن Ψ غامرٌ في هذه الحالة، ومنه $G\cong(S_3,\circ)$.

فهناك فقط نوعان من الزمر التي عدد عناصرها يساوي 6 هما $\left(\mathbb{Z}/6\mathbb{Z},+\right)$ و $\left(S_3,\circ\right)$. ■

التمرين 19.

I. لتكن a من $\mathbb{Z}/p\mathbb{Z}$. نرمز بالرمز T_a إلى التطبيق من $\mathbb{Z}/p\mathbb{Z}$ إلى $\mathbb{Z}/p\mathbb{Z}$ المعرّف بالعلاقة $T_a(x) = x + a$. كما نرمز بالرمز $\mathcal{T}$ إلى مجموعة التطبيقات

$$\mathcal{T} = \{T_a : a \in \mathbb{Z}/p\mathbb{Z}\}$$

أثبت أنّ

$$\forall (a,b) \in (\mathbb{Z}/p\mathbb{Z})^2, \ T_a \circ T_b = T_{a+b}$$

واستنتج أنّ البنية $(\mathcal{T},\circ)$ زمرة، وأنّ التطبيق $\varphi : (\mathbb{Z}/p\mathbb{Z},+) \to (\mathcal{T},\circ), a \mapsto T_a$ تشاكُلٌ زمريّ تقابلي.

II. لتكن $(G,\cdot)$ زمرة منتهية عدد عناصرها n. وليكن p عدداً أولياً يقسم n. نتأمّل المجموعة E المكوّنة من التطبيقات $f : \mathbb{Z}/p\mathbb{Z} \to G$ التي تُحقِّق الشرط

$$f(0)f(1)\cdots f(p-1) = 1_G$$

لاحظ أنّ ترتيب عناصر الجداء مهمٌ إذ لا نفترض الزمرة G تبديلية. كما نتأمّل المجموعة الجزئية E_0 من E المكوّنة من التطبيقات الثابتة المنتمية إلى E.

1. أثبت أنّ $E_0 \neq \varnothing$.
2. ليكن f من E. أثبت أنّ $f \circ T_1$ ينتمي إلى E، واستنتج أنّ :
$$\forall k \in \mathbb{Z}/p\mathbb{Z}, \quad f \circ T_k \in E$$
3. نعرّف، في حالة f من E، المجموعة $H_f = \{k \in \mathbb{Z}/p\mathbb{Z} : f = f \circ T_k\}$.
   ① أثبت أنّ H_f زمرة جزئية من $\mathbb{Z}/p\mathbb{Z}$.
   ② أثبت أنّ : $f \in E_0 \Leftrightarrow H_f = \mathbb{Z}/p\mathbb{Z}$.
   ③ استنتج أنّ : $f \notin E_0 \Leftrightarrow H_f = \{0\}$.
4. نعرّف على E العلاقة الثنائية $\mathcal{R}$ كما يلي :
$$f\mathcal{R}g \Leftrightarrow \exists k \in \mathbb{Z}/p\mathbb{Z} : g = f \circ T_k$$
   ① أثبت أنّ $\mathcal{R}$ علاقة تكافؤ.
   ② ليكن f من E، ولنعرّف : $\Psi_f : \mathbb{Z}/p\mathbb{Z} \to [f]_{\mathcal{R}}, k \mapsto f \circ T_k$، حيث $[f]_{\mathcal{R}}$ هو صف تكافؤ f وفق العلاقة $\mathcal{R}$. بيّن أنّ Ψ_f غامر، وأنّه يكون متبايناً إذا وفقط إذا كان f عنصراً من $E \backslash E_0$.

③ استنتج أنّه إذا كان f من E، كان :

$$\operatorname{card}([f]_{\mathcal{R}}) = \begin{cases} 1 & : \quad f \in E_0 \\ p & : \quad f \in E \backslash E_0 \end{cases}$$

④ استنتج أنه توجد تجزئة للمجموعة E على النحو

$$E = E_0 \cup \left(\bigcup_{k=1}^{m} [f_k]_{\mathcal{R}} \right)$$

مع f_1 و f_2 و ... و f_m عناصر من $E \backslash E_0$.

⑤ استنتج أنّ: $\operatorname{card}(E) = \operatorname{card}(E_0) \bmod p$.

5. لنتأمّل التطبيق

$$\Phi : E \to G^{p-1}, f \mapsto (f(0), f(1), \ldots, f(p-2))$$

أثبت أنّ Φ تقابل، واستنتج أنّ p يقسم $\operatorname{card}(E)$.

6. استفد مما سبق لتثبت أنّ p يقسم عدد عناصر المجموعة $\{x \in G : x^p = 1_G\}$. ثُم استنتج أنّ G تحوي زمرة جزئية عدد عناصرها p.

7. أثبت أنّه إذا كانت H_1 و H_2 زمرتين جزئيتين من G عدد عناصر كل منهما p، فإن $H_2 = H_1$ أو $H_1 \cap H_2 = \{1_G\}$. ثم استنتج أنّ $\lambda_p(G)$، عدد الزمر الجزئية من G التي رتبة كل منها p، يحقق العلاقة : $\lambda_p(G) = 1 \bmod p$.

8. أثبت أنّ كل زمرة عدد عناصرها 15 تكون زمرة دوّارة، أي تُشاكِل تقابليّاً الزمرة $\mathbb{Z}/15\mathbb{Z}$.

الحل

I. الخاصّة $\forall (a,b) \in \left(\mathbb{Z}/p\mathbb{Z}\right)^2,\ T_a \circ T_b = T_{a+b}$، تعبّر عن المساواة الواضحة

$$\forall (a,b,x) \in \left(\mathbb{Z}/p\mathbb{Z}\right)^3, \quad a + (b + x) = (a + b) + x$$

وعليه نرى أنّ المجموعة $\mathcal{T} = \left\{ T_a : a \in \mathbb{Z}/p\mathbb{Z} \right\}$ مغلقة بالنسبة إلى تركيب التطبيقات. وإذا لاحظنا أنّ I ينتمي إلى $\mathcal{T}$، وأنّ مقلوب العنصر T_a من $\mathcal{T}$ هو T_{-a} وهو ينتمي أيضاً إلى $\mathcal{T}$، استنتجنا أنّ $\left(\mathcal{T}, \circ\right)$ زمرة. ونتحقّق مباشرة أنّ التطبيق

$$\varphi : (\mathbb{Z}/p\mathbb{Z}, +) \to (\mathcal{T}, \circ), a \mapsto T_a$$

تشاكل زمري تقابلي.

II.1. من الواضح أنّ التطبيق الثابت $\mathbb{1} : (\mathbb{Z}/p\mathbb{Z},+) \to G, a \mapsto 1_G$ ينتمي إلى E_0 إذن $E_0 \neq \varnothing$.

II.2. ليكن f من E. عندئذ $f(0)f(1)\cdots f(p-1) = 1_G$، ومن ثَمّ

$$\begin{aligned} f(1)\cdots f(p-1)f(0) &= (f(0))^{-1}f(0)f(1)\cdots f(p-1)f(0) \\ &= (f(0))^{-1}1_G f(0) = 1_G \end{aligned}$$

إذن

$$f \circ T_1(0) f \circ T_1(1) \cdots f \circ T_1(p-1) = 1_G$$

ومنه $f \circ T_1 \in E$.

وبملاحظة أنّ $f \circ T_{k+1} = (f \circ T_k) \circ T_1$، نستنتج مباشرة وبالتدريج على k أنّه

$$\forall k \in \mathbb{Z}/p\mathbb{Z}, \quad f \circ T_k \in E$$

II.3. نعرّف، في حالة f من E، المجموعة $H_f = \{k \in \mathbb{Z}/p\mathbb{Z} : f = f \circ T_k\}$.

II.3.① من الواضح أنّ $0 \in H_f$، وإذا كان k و r من H_f استنتجنا أنّ

$$f = f \circ T_k \text{ و } f = f \circ T_r$$

ولكن ينتج من $f = f \circ T_r$ أنّ $f \circ T_{-r} = f \circ T_r \circ T_{-r}$ أو $f = f \circ T_{-r}$. وينتج من $f = f \circ T_k$ أنّ $f = f \circ T_{-r} \circ T_k = f \circ T_{k-r}$. إذن $k - r \in H_f$. وهكذا نكون قد أثبتنا أنّ H_f زمرة جزئيّة من $\mathbb{Z}/p\mathbb{Z}$. وعليه فإنّ $H_f = \mathbb{Z}/p\mathbb{Z}$ أو $H_f = \{0\}$ لأنّ p عددٌ أوّلي وليس هناك حالة أخرى.

II.3.② في الحقيقة،

$$\begin{aligned} \left(H_f = \mathbb{Z}/p\mathbb{Z}\right) &\Rightarrow \left(\forall k \in \mathbb{Z}/p\mathbb{Z},\ f = f \circ T_k\right) \\ &\Rightarrow \left(\forall k \in \mathbb{Z}/p\mathbb{Z},\ f(0) = f \circ T_k(0)\right) \\ &\Rightarrow \left(\forall k \in \mathbb{Z}/p\mathbb{Z},\ f(k) = f(0)\right) \\ &\Rightarrow \left(f \in E_0\right) \end{aligned}$$

أمّا الاقتضاء المعاكس $\left(f \in E_0\right) \Rightarrow \left(H_f = \mathbb{Z}/p\mathbb{Z}\right)$ فهو محقّق وضوحاً.

II.3.③ في الحقيقة، نستنتج مما أثبتناه سابقاً أنّ $f \notin E_0 \Leftrightarrow H_f \neq \mathbb{Z}/p\mathbb{Z}$ ولأنّ p عددٌ أوّلي نستنتج أنّ $H_f \neq \mathbb{Z}/p\mathbb{Z}$ يُكافئ $H_f = \{0\}$، ومنه $f \notin E_0 \Leftrightarrow H_f = \{0\}$.

II.4.① لنثبت أنّ العلاقة $\mathcal{R}$ علاقة تكافؤ.

- من الواضح أنّ $f = f \circ T_0$، إذن $\forall f \in E,\ f\mathcal{R}f$.
- وإذا كان $g = f \circ T_k$ كان $f = g \circ T_{-k}$، إذن

$$\forall (f,g) \in E^2,\ f\mathcal{R}g \Rightarrow g\mathcal{R}f.$$

- وإذا كان $g = f \circ T_k$ و $h = g \circ T_r$ كان $h = f \circ T_{r+k}$ إذن

$$\forall (f,g,h) \in E^2,\ \big(f\mathcal{R}g\big) \wedge \big(g\mathcal{R}h\big) \Rightarrow f\mathcal{R}h$$

وهذا يثبت أنّ $\mathcal{R}$ علاقة تكافؤ.

II.4.② ليكن f من E، ولنعرّف :

$$\Psi_f : \mathbb{Z}/p\mathbb{Z} \to [f]_{\mathcal{R}}, k \mapsto f \circ T_k$$

- ليكن g من $[f]_{\mathcal{R}}$، إذن $f\mathcal{R}g$، وعليه يوجد k في $\mathbb{Z}/p\mathbb{Z}$ يُحقّق $g = f \circ T_k$، أي $g = \Psi_f(k)$. إذن التطبيق Ψ_f غامر.
- لنلاحظ أنّ

$$\begin{aligned}\big(\Psi_f(k) = \Psi_f(\ell)\big) &\Leftrightarrow \big(f = f \circ T_{k-\ell}\big)\\ &\Leftrightarrow k - \ell \in H_f\end{aligned}$$

وعليه، استناداً إلى نتيجة II.3.، إذا كان $f \in (E \backslash E_0)$ كان $H_f = \{0\}$ وفي هذه الحالة

$$\big(\Psi_f(k) = \Psi_f(\ell)\big) \Rightarrow k = \ell$$

والتطبيق Ψ_f متباينٌ في هذه الحالة. وإذا كان $f \in E_0$ كان f ثابتاً وما كان Ψ_f متبايناً.

II.4.③ ليكن f من E، ولنناقش الحالتين التاليتين :

- إذا كان $f \in E_0$ استنتجنا أنّ $[f]_{\mathcal{R}} = \{f\}$، ومنه $\text{card}([f]_{\mathcal{R}}) = 1$.
- إذا كان $f \in E \backslash E_0$ عرّف التطبيق Ψ_f تقابلاً بين المجموعتين $\mathbb{Z}/p\mathbb{Z}$ و $[f]_{\mathcal{R}}$، ومنه $\text{card}([f]_{\mathcal{R}}) = p$.

II.4.④ لتكن $\{A_1, A_2, \ldots, A_m\}$ مجموعة صفوف تكافؤ العلاقة $\mathcal{R}$ المحتواة في $E \backslash E_0$. أي

$$A_1, A_2, \ldots, A_m = \big\{A \in E/\mathcal{R} : A \subset E \backslash E_0\big\}$$

من الواضح أنّ المجموعات $E_0, A_1, A_2, \ldots, A_m$ منفصلة مثنى مثنى وغير خالية.

ليكن f من E، إذا كان $f \notin E_0$ كان $[f]_{\mathcal{R}} \cap E_0 = \varnothing$، لأنّ صفَّ تكافؤ أيّ عنصر من E_0 يتكوّن من العنصر نفسه فقط. ومن ثَمّ $[f]_{\mathcal{R}} \subset E \backslash E_0$، إذن يوجد k من $\mathbb{N}_m$ يُحقّق

$A_k = [f]_{\mathcal{R}}$. ومنه تكوّن المجموعات $(E_0, A_1, A_2, \ldots, A_m)$ تجزئة للمجموعة E . فإذا اخترنا من كلّ صفٍّ تكافؤ A_k ممثّلاً f_k ، نكون قد وجدنا f_1 و f_2 و … و f_m من $E \backslash E_0$ ، تُحقّق

$$E = E_0 \cup \left(\bigcup_{k=1}^{m} [f_k]_{\mathcal{R}} \right)$$

II.4.⑤ وهكذا نستنتج أنّ $\operatorname{card}(E) = \operatorname{card}(E_0) + mp$ ومنه

$$\operatorname{card}(E) = \operatorname{card}(E_0) \bmod p$$

II.5. لنتأمّل التطبيق

$$\Phi : E \to G^{p-1}, f \mapsto \big(f(0), f(1), \ldots, f(p-2)\big)$$

من الواضح أنّ Φ تقابلٌ، وأنّ تقابله العكسي يُعطى بالصيغة

$$\Lambda : G^{p-1} \to E, a = \big(a_0, a_1, \ldots, a_{p-2}\big) \mapsto f_a$$

وقد عرّفنا $f_a(k) = a_k$ في حالة $0 \leq k < p-1$ و $f_a(p-1) = (a_0 a_1 \cdots a_{p-2})^{-1}$.
إذن لا بُدّ أن $\operatorname{card}(E) = \operatorname{card}(G^{p-1}) = (\operatorname{card}(G))^{p-1}$. ولأنّ $p \mid \operatorname{card}(G)$ استنتجنا أنّ $p \mid \operatorname{card}(E)$.

II.6. إنّ التطبيق

$$\Gamma : E_0 \to \{x \in G : x^p = 1_G\}, f \mapsto f(0)$$

تقابلٌ واضحٌ، إذن $\operatorname{card}(\{x \in G : x^p = 1_G\}) = \operatorname{card}(E_0)$ ، ولأنّ

$$\operatorname{card}(E_0) = \operatorname{card}(E) \bmod p = 0 \bmod p$$

استنتجنا أنّ

$$\operatorname{card}(\{x \in G : x^p = 1_G\}) = 0 \bmod p$$

ولأنّ 1_G ينتمي إلى $\{x \in G : x^p = 1_G\}$ استنتجنا أنّ

$$\operatorname{card}(\{x \in G : x^p = 1_G\}) > 0$$

وينتج من الخاصّتين السابقتين أنّ

$$\operatorname{card}(\{x \in G : x^p = 1_G\}) \geq p$$

فلا بُدّ أن يوجد عنصرٌ x يُحقّق $x \neq 1_G$ و $x^p = 1_G$ ، وعندئذ تكون $\langle x \rangle$ زمرة جزئيّة من G عدد عناصرها p .

II.7. لمّا كانت G زمرة منتهية، كان عدد الزمر الجزئيّة من G التي رتبتها تساوي p منتهياً، وليكن $\lambda_p(G)$ هذا العدد، الذي سنرمز إليه اختصاراً κ. ولنفترض أنّ هذه الزمر الجزئيّة هي H_1 و H_2 و ... و H_κ. نعرّف $\tilde{H}_\ell = H_\ell \backslash \{1_G\}$ في حالة $1 \leq \ell \leq \kappa$. وعندئذ:

- $\ell \neq r \Rightarrow \tilde{H}_\ell \cap \tilde{H}_r = \varnothing$. لأنّه إذا وُجِدَ عنصرٌ x في $\tilde{H}_\ell \cap \tilde{H}_r$ كان x عنصراً مختلفاً عن 1_G، ورتبته تقسم العدد p لأنّ $\langle x \rangle \subset H_\ell$، فلا بُدّ أن يكون $H_r = \langle x \rangle = H_\ell$، ومنه $\ell = r$.
- $\operatorname{card}(\tilde{H}_\ell) = p - 1$ وذلك أيّاً كان ℓ يُحقّق $1 \leq \ell \leq \kappa$.
- وأخيراً نرى وضوحاً أنّ $\{x \in G : x^p = 1_G\} = \{1_G\} \cup \bigcup_{\ell=1}^{\kappa} \tilde{H}_\ell$، إذن

$$\operatorname{card}(\{x \in G : x^p = 1_G\}) = 1 + \kappa(p-1) = 1 - \lambda_p(G) + p\lambda_p(G)$$

ولأنّ p يقسم $\operatorname{card}(\{x \in G : x^p = 1_G\})$، نستنتج أنّ p يقسم $\lambda_p(G) - 1$ أو

$$\lambda_p(G) = 1 \bmod p$$

II.8. لتكن G زمرة عدد عناصرها 15، عندئذ $\lambda_5(G) = 1 \bmod 5$، فإذا كان $\lambda_5(G) > 1$ كان $\lambda_5(G) \geq 6$، ونتج من ذلك أنّ

$$\operatorname{card}(\{x \in G : x^5 = 1_G\}) = 1 + \lambda_5(G)(5-1) \geq 1 + 6 \times 4 = 25$$

وهذا خُلفٌ واضحٌ. إذن لا بُدّ أن يكون $\lambda_5(G) = 1$. لتكن H الزمرة الجزئيّة الوحيدة من G التي عدد عناصرها يساوي 5. نعلم استناداً إلى دراستنا السابقة أنّ

$$H = \{x \in G : x^5 = 1_G\}.$$

إنّ رتبة أي عنصر من G قاسم للعدد 15، لنفترض جدلاً أنّه لايوجد في G عنصرٌ رتبته 15. لمّا كانت H مكوّنة من العناصر التي رتبتها 1 أو 5 استنتجنا، بناءً على الفرض الجدلي أنّ رتبة أي عنصرٍ من $G \backslash H$ تساوي 3 وعليه فإنّ

$$\{x \in G : x^3 = 1_G\} = \{1_G\} \cup (G \backslash H)$$

إذن

$$\operatorname{card}(\{x \in G : x^3 = 1_G\}) = 1 + 10 = 11$$

وهذا تناقضٌ لأنّ $3 \nmid 11$. إذن لا بدّ أن نجد في G عنصراً a رتبته 15 أي $O(a) = 15$، فالزمرة G زمرة وحيدة التوليد $G = \langle a \rangle$ عدد عناصرها 15، فهي تُشاكل تقابليّاً $\mathbb{Z}/15\mathbb{Z}$. ■

التمرين 20.

I. لتكن $(G,+)$ زمرة تبديليّة. نفترض وجود عنصر g في G رتبته $O(g)$ أكبر تماماً من 2.

نعرّف على المجموعة $\left(\mathbb{Z}/2\mathbb{Z}\right)\times G$ قانون التشكيل الداخلي $*$ التالي:

$$(\varepsilon,x)*(\varepsilon',x')=\begin{cases}(\varepsilon+\varepsilon',x+x') & : \quad \varepsilon=0\\ (\varepsilon+\varepsilon',x-x') & : \quad \varepsilon=1\end{cases}$$

1. أثبت أنّ $*$ يجعل من $\left(\mathbb{Z}/2\mathbb{Z}\right)\times G$ زمرة، نرمز إلى هذه الزمرة بالرمز $d(G)$.
2. احسب كلاً من $(0,g)*(1,0)$ و $(1,0)*(0,g)$ ماذا تستنتج؟
3. أثبت أنّ ا لمجموعتين $H=\{0\}\times G$ و $K=\left(\mathbb{Z}/2\mathbb{Z}\right)\times\{0\}$ هما زمرتان جزئيّتان من $d(G)$.
4. نفترض أنّ رتبة G منتهية وتساوي n أثبت أنّ $d(G)$ تحوي على الأقل n عنصراً رتبة كلٍّ منها 2.

II. لتكن $(G,\cdot)$ زمرة، ولتكن $\mathrm{Aut}(G)$ مجموعة التشاكلات التقابليّة الزُمريّة على G.

1. أثبت أنّ $(\mathrm{Aut}(G),\circ)$ زمرة.
2. لتكن $(H,\perp)$ زمرة، ولنفترض أنّ هناك تشاكلاً زمرياً :

$$\varphi : H\to \mathrm{Aut}(G), h\mapsto \varphi_h$$

ثُمّ لنعرّف على $H\times G$ قانون التشكيل الداخلي $*$ كما يلي:

$$(h,x)*(h',x')=(h\perp h',x\cdot\varphi_h(x'))$$

أثبت أنّ البنية $(H\times G,*)$ زمرة، نرمز إليها بالرمز $H\times_\varphi G$. وأوجد الشرط اللازم والكافي لتكون $H\times_\varphi G$ غير تبديليّة.

3. استفد مما سبق لتزوّد $\mathbb{R}^2$ بقانون $*$ يجعل منها زمرة غير تبديليّة.

الحل

I.1. لنعرّف في حالة ε من $\mathbb{Z}/2\mathbb{Z}$ التشاكل التقابلي الزمري $\varphi_\varepsilon : G\to G$ بأنّ نضع $\varphi_0(x)=x$ و $\varphi_1(x)=-x$. نتيقّن بسهولة أنّ $\varphi_\varepsilon\circ\varphi_{\varepsilon'}=\varphi_{\varepsilon+\varepsilon'}$. وعندئذ يمكن التعبير عن القانون $(*)$ بالشكل

$$(\varepsilon,x)*(\varepsilon',x')=\left(\varepsilon+\varepsilon',x+\varphi_\varepsilon(x')\right)$$

- في حالة (ε, x) و (ε', x') و (ε'', x'') من $\left(\mathbb{Z}/2\mathbb{Z}\right) \times G$ نلاحظ أنّ

$$\begin{aligned}
\big((\varepsilon, x) * (\varepsilon', x')\big) * (\varepsilon'', x'') &= \big(\varepsilon + \varepsilon', x + \varphi_\varepsilon(x')\big) * (\varepsilon'', x'') \\
&= \big(\varepsilon + \varepsilon' + \varepsilon'', x + \varphi_\varepsilon(x') + \varphi_{\varepsilon+\varepsilon'}(x'')\big) \\
&= \big(\varepsilon + \varepsilon' + \varepsilon'', x + \varphi_\varepsilon(x') + \varphi_\varepsilon \circ \varphi_{\varepsilon'}(x'')\big) \\
&= \Big(\varepsilon + \varepsilon' + \varepsilon'', x + \varphi_\varepsilon\big(x' + \varphi_{\varepsilon'}(x'')\big)\Big) \\
&= \big(\varepsilon, x\big) * \big(\varepsilon' + \varepsilon'', x' + \varphi_{\varepsilon'}(x'')\big) \\
&= \big(\varepsilon, x\big) * \big((\varepsilon', x') * (\varepsilon'', x'')\big)
\end{aligned}$$

فالقانون $(*)$ تجميعي.

- في حالة (ε, x) من $\left(\mathbb{Z}/2\mathbb{Z}\right) \times G$ نلاحظ أنّ

$$\begin{aligned}
(\varepsilon, x) * (0, 0_G) &= \big(\varepsilon + 0, x + \varphi_\varepsilon(0_G)\big) = (\varepsilon, x) \\
(0, 0_G) * (\varepsilon, x) &= \big(0 + \varepsilon, 0_G + \varphi_0(x)\big) = (\varepsilon, x)
\end{aligned}$$

إذن $(0, 0_G)$ عنصرٌ حيادي في $\left(\mathbb{Z}/2\mathbb{Z}\right) \times G$.

- في حالة x من G نلاحظ أنّ

$$\begin{aligned}
(0, x) * (0, -x) &= \big(0 + 0, x + \varphi_0(-x)\big) = (0, 0_G) \\
(1, x) * (1, x) &= \big(1 + 1, x + \varphi_1(x)\big) = (0, 0_G)
\end{aligned}$$

إذن لكلِّ عنصرٍ (ε, x) من $\left(\mathbb{Z}/2\mathbb{Z}\right) \times G$ نظير في $\left(\mathbb{Z}/2\mathbb{Z}\right) \times G$.

بذا نكون قد أثبتنا أنّ $d(G) = \left(\mathbb{Z}/2\mathbb{Z} \times G, *\right)$ زمرة.

I.2. في حالة x من G نلاحظ أنّ

$$\begin{aligned}
(1, 0) * (0, x) &= \big(1 + 0, 0 + \varphi_1(x)\big) = (1, -x) \\
(0, x) * (1, 0) &= \big(0 + 1, x + \varphi_0(0)\big) = (1, x)
\end{aligned}$$

وهكذا نرى أنّه يكفي أن يوجد في $G\backslash\{0\}$ عنصرٌ رتبته لا تساوي 2 حتى تكون $d(G)$ غير تبديليّة. وهذا محقَّقٌ إذ افترضنا أنّ $O(g) > 2$.

I.3. إنّ التحقُّقَ من كون $H = \{0\} \times G$ و $K = \left(\mathbb{Z}/2\mathbb{Z}\right) \times \{0\}$ زمرتين جزئيّتين من $d(G)$ أمرٌ بسيط ومباشرٌ نتركه للقارئ.

I.4. ليكن γ من G, نلاحظ أنّ $(1, \gamma) \neq (0, 0_G)$ و $(1, \gamma) * (1, \gamma) = (0, 0_G)$. إذن أيّاً كان γ من G كانت رتبة العنصر $(1, \gamma)$ مساوية 2. إذن يوجد n عنصراً على الأقلّ رتبته 2 في $d(G)$.

.1.II إنّ تحقُّقَ أنّ $(\mathrm{Aut}(G),\circ)$ زمرة أمرٌ بسيط ومباشرٌ نتركه للقارئ.

.2.II

- في حالة (h,x) و (h',x') و (h'',x'') من $H\times G$ نلاحظ أنّ

$$\begin{aligned}\big((h,x)*(h',x')\big)*(h'',x'') &= \big(h\perp h', x\cdot\varphi_h(x')\big)*(h'',x'')\\ &= \big((h\perp h')\perp h'', \big(x\cdot\varphi_h(x')\big)\cdot\varphi_{h\perp h'}(x'')\big)\\ &= \big(h\perp h'\perp h'', x\cdot\varphi_h(x')\cdot\varphi_h\circ\varphi_{h'}(x'')\big)\\ &= \big(h\perp(h'\perp h''), x\cdot\varphi_h(x'\cdot\varphi_{h'}(x''))\big)\\ &= \big(h,x\big)*\big(h'\perp h'', x'\cdot\varphi_{h'}(x'')\big)\\ &= (h,x)*\big((h',x')*(h'',x'')\big)\end{aligned}$$

فالقانون $(*)$ تجميعي.

- في حالة (h,x) من $H\times G$ نلاحظ أنّ

$$\begin{aligned}(h,x)*(e_H,1_G) &= \big(h\perp e_H, x\cdot\varphi_h(1_G)\big)=(h,x)\\ (e_H,1_G)*(h,x) &= \big(e_H\perp h, 1_G\cdot\varphi_{e_H}(x)\big)=(h,x)\end{aligned}$$

إذن $(e_H,1_G)$ عنصرٌ حيادي في $H\times G$.

- في حالة (h,x) من $H\times G$ نلاحظ أنّ

$$\begin{aligned}(h,x)*(h^{-1},\varphi_{h^{-1}}(x^{-1})) &= \big(h\perp h^{-1}, x\cdot\varphi_h(\varphi_{h^{-1}}(x^{-1}))\big)=(e_H,1_G)\\ (h^{-1},\varphi_{h^{-1}}(x^{-1}))*(h,x) &= \big(h^{-1}\perp h, \varphi_{h^{-1}}(x^{-1})\cdot\varphi_{h^{-1}}(x)\big)=(e_H,1_G)\end{aligned}$$

إذن لكلّ عنصرٍ (h,x) من $H\times G$ نظير في $H\times G$.

بذا نكون قد أثبتنا أنّ $H\times_\varphi G$ زمرة بالنسبة إلى القانون $(*)$.

متى تكون الزمرة $H\times_\varphi G$ تبديليّة ؟ في الحقيقة، لدينا

$$\begin{aligned}(h,x)*(h',x') &= \big(h\perp h', x\cdot\varphi_h(x')\big)\\ (h',x')*(h,x) &= \big(h'\perp h, x'\cdot\varphi_{h'}(x)\big)\end{aligned}$$

فإذا افترضنا أنّ الزمرة $G \times_\varphi H$ زمرة تبديليّة استنتجنا أنّ

$$\forall (h,h') \in H^2, \forall (x,x') \in G^2, \qquad \begin{aligned} h \perp h' &= h' \perp h \\ x \cdot \varphi_h(x') &= x' \cdot \varphi_{h'}(x) \end{aligned}$$

- ينتج من ذلك أنّ $(H,\perp)$ زمرة تبديليّة.
- وإذا اخترنا $x' = 1_G$ في المساواة الثانية استنتجنا :

$$\forall h' \in H, \forall x \in G, \ \ \varphi_{h'}(x) = x$$

أو $\varphi_{h'} = I_G$ في حالة h' من H، أو $\operatorname{Im}\varphi = \{I_G\}$.

- وبالعودة إلى المساواة الثانية نجد $x \cdot x' = x' \cdot x$ ، $\forall (x,x') \in G^2,$ فالزمرة $(G,\cdot)$ زمرة تبديليّة أيضاً.

وهكذا نكون قد أثبتنا أنّ كون $G \times_\varphi H$ زمرة تبديليّة، يقتضي أنّ G و H تبديليّتان و φ هو التشاكل الزمري التافه من $(H,\perp)$ إلى $(\operatorname{Aut}(G),\circ)$ الذي يقرن بكلّ h من H التطبيق المطابق I_G على G.

وبالعكس، إذا كانت الزمرتان G و H تبديليّتين وكان φ التشاكل الزمري التافه من $(H,\perp)$ إلى $(\operatorname{Aut}(G),\circ)$ الذي يقرن بكلّ h من H التطبيق المطابق I_G على G. كانت الزمرة $G \times_\varphi H$ هي زمرة الجداء الديكارتي $H \times G$ لزمرتين تبديليّتين فهي تبديليّة.

II.3. في حالة h من $\mathbb{R}$ نعرّف التقابل $\varphi_h : \mathbb{R} \to \mathbb{R}, \varphi_h(x) = e^h x$ ، ونلاحظ ببساطة أنّ

$$\varphi : \mathbb{R} \to \operatorname{Aut}(\mathbb{R}), h \mapsto \varphi_h$$

تشاكلٌ زمري، لأنّ $\varphi_{h+h'} = \varphi_h \circ \varphi_{h'}$. ولمّا كان φ ليس تافهاً استنتجنا أنّ $\mathbb{R} \times_\varphi \mathbb{R}$ زمرة غير تبديليّة. يكفي إذن أن نلاحظ أنّ $\mathbb{R} \times_\varphi \mathbb{R} = (\mathbb{R}^2, *)$ مع

$$(x,y) * (x',y') = (x+x', y+e^x y')$$

وهو المطلوب. ∎

التمرين 21. لنتأمّل التشاكل الزمري $f : G \to G'$.

1. نعرّف على الزمرة G العلاقة الاثنانيّة:

$$\forall (x,y) \in G^2,\ x\mathcal{R}y \Leftrightarrow f(x) = f(y)$$

① بيّن أنّ $\mathcal{R}$ علاقة تكافؤ.

② نرمز بالرمز H إلى نواة التشاكل f أي $H = \ker f$. أثبت أنّه مهما تكن (x,y) من G^2 فلدينا :

$$(x\mathcal{R}y) \Leftrightarrow (xy^{-1} \in H) \Leftrightarrow (x^{-1}y \in H)$$

③ ليكن a من G، ولنرمز بالرمز $[a]$ إلى صف تَكافُئِهِ بالنسبة إلى العلاقة $\mathcal{R}$.

أثبت أنّ : $[a] = aH = Ha$.

سنرمز فيما يلي بالرمز G/H للدلالة على مجموعة صفوف التكافؤ الموافقة للعلاقة $\mathcal{R}$.

2. ليكن A و B عنصرين من G/H، أثبت أنّ المجموعتين التاليتين هما عنصران من G/H أيضاً:

$$A^{-1} = \{a^{-1} : a \in A\} \quad \text{و} \quad A \cdot B = \{ab : a \in A, b \in B\}$$

3. أثبت أننا بذلك نعرّف على G/H قانون تشكيل داخلي $(\cdot)$ يجعل منها زمرة.

4. ليكن A عنصراً من G/H، أثبت أنّ المجموعة $f(A)$ تتكوّن من عنصر واحد ينتمي إلى $\operatorname{Im} f$ نرمز إليه بالرمز $\tilde{f}(A)$، أي : $f(A) = \{\tilde{f}(A)\}$.

5. برهن أنّ التطبيق : $\tilde{f} : G/H \to \operatorname{Im} f,\ A \mapsto \tilde{f}(A)$ تشاكلٌ زمري تقابلي.

الحل

1.① إنّ تيقُّن أنّ $\mathcal{R}$ علاقة تكافؤ أمرٌ بسيطٌ ومباشر نترك تفاصيله للقارئ.

1.② ليكن x و y عنصرين من G، عندئذ

$$\begin{aligned}
x\mathcal{R}y &\Leftrightarrow f(x) = f(y)\\
&\Leftrightarrow f(x)(f(y))^{-1} = 1\\
&\Leftrightarrow f(x)f(y^{-1}) = 1\\
&\Leftrightarrow f(xy^{-1}) = 1\\
&\Leftrightarrow xy^{-1} \in \ker f = H
\end{aligned}$$

وكذلك

$$\begin{aligned} x\mathcal{R}y &\Leftrightarrow f(x) = f(y) \\ &\Leftrightarrow (f(x))^{-1} f(y) = 1 \\ &\Leftrightarrow f(x^{-1}) f(y) = 1 \\ &\Leftrightarrow f(x^{-1}y) = 1 \\ &\Leftrightarrow x^{-1}y \in \ker f = H \end{aligned}$$

③.1 ليكن a من G. نلاحظ أوّلاً أنّ

$$y \in [a] \Leftrightarrow y\mathcal{R}a \Leftrightarrow ya^{-1} \in H \Leftrightarrow y \in Ha$$

إذن $[a] = Ha$. ونلاحظ ثانياً أنّ

$$y \in [a] \Leftrightarrow a\mathcal{R}y \Leftrightarrow a^{-1}y \in H \Leftrightarrow y \in aH$$

إذن $[a] = aH$. فنكون قد أثبتنا أنّ

$$[a] = aH = Ha$$

.2 ليكن A و B من G/H. إذن يوجد عنصران a_0 و b_0 في G يُحقّقان $A = [a_0]$ و $B = [b_0]$. لنثبت أنّ $A \cdot B = [a_0 b_0]$ و $A^{-1} = [a_0^{-1}]$.

- ليكن x من $A \cdot B$، إذن يوجد (a,b) من $A \times B$ يُحقّق $x = ab$. ولمّا كان $a_0^{-1}a \in H$ استنتجنا أنّ

$$a_0^{-1}x \in Hb = [b] = [b_0] = b_0H$$

ومنه $x \in a_0b_0H$ أو $x \in [a_0b_0]$.

- وبالعكس، ليكن x من $[a_0b_0]$. عندئذ نجد h من H تُحقّق $x = a_0b_0h$. ولأنّ $a_0 \in A$ و $b_0h \in B$ استنتجنا أنّ $x \in A \cdot B$. فنكون بذلك قد أثبتنا أنّ $A \cdot B = [a_0b_0]$.

- وأخيراً نلاحظ أنّ

$$\begin{aligned} (x \in A^{-1}) &\Leftrightarrow (x^{-1} \in [a_0]) \Leftrightarrow (x^{-1}\mathcal{R}a_0) \\ &\Leftrightarrow (a_0x \in H) \Leftrightarrow x \in a_0^{-1}H \Leftrightarrow x \in [a_0^{-1}] \end{aligned}$$

ومنه $A^{-1} = [a_0^{-1}]$.

3. نلاحظ أنّه أياًكان a و b و c من G، كان

$$\begin{aligned}\big([a]\cdot[b]\big)\cdot[c] &= [ab]\cdot[c] = \big[(ab)c\big]\\ &= \big[a(bc)\big] = [a]\cdot[bc] = [a]\cdot\big([b]\cdot[c]\big)\end{aligned}$$

فالبنية $(G/H,\cdot)$ تجميعيّة.

وأياًكان a من G، كان

$$[1_G]\cdot[a] = [1_G\,\mathrm{a}] = [a] \quad \text{و} \quad [a]\cdot[1_G] = [a1_G] = [a]$$

ومنه $[1_G]$ عنصرٌ حيادي في $(G/H,\cdot)$.

وأخيراً، إذا كان A من G/H، كان A^{-1} نظير A في $(G/H,\cdot)$. لأنّه إذا كان $A=[a]$ كان

$$\begin{aligned}A\cdot A^{-1} &= [a]\cdot[a^{-1}] = [aa^{-1}] = [1_G]\\ A^{-1}\cdot A &= [a^{-1}]\cdot[a] = [a^{-1}a] = [1_G]\end{aligned}$$

بذلك نكون قد أثبتنا أنّ $(G/H,\cdot)$ زمرة.

4. ليكن A من G/H، يوجد a من G يُحقّق $A=[a]$. وعندئذ

$$(x\in A) \Rightarrow \big(x\mathcal{R}a\big) \Rightarrow \big(f(x)=f(a)\big)$$

ومنه $f(A)=\{f(a)\}$. إذن $\tilde f(A)=f(a)$ و a هو أي عنصر من A.

5. نكون إذن قد عرّفنا التطبيق

$$\tilde f : G/H \to \operatorname{Im} f,\ \ A\mapsto \tilde f(A)$$

وهو يُحقّق

$$\forall (a,b)\in G^2,\quad \tilde f\big([a]\big)\tilde f\big([b]\big) = f(a)f(b) = f(ab) = \tilde f\big([ab]\big)$$

فهو إذن تشاكلٌ زمريّ.

- إنّ $\tilde f$ غامرٌ، لأنّه إذا كان y من $\operatorname{Im} f$ وُجِد x من G يُحقّق $y=f(x)=\tilde f([x])$.
- ثُمّ إنّ $\tilde f$ متباينٌ، لأنّه إذا كان $A=[a]$ عنصراً من $\ker\tilde f$ كان $\tilde f(A)=1_G$ ومن ثَمّ

$$f(a)=1_G=f(1_G)$$

أي $a\mathcal{R}1_G$ ومنه $[a]=[1_G]$. إذن لقد أثبتنا أنّ $\ker\tilde f=\{[1_G]\}$. والتشاكل $\tilde f$ متباينٌ.

إذن يوجد تشاكلٌ زمري تقابلي بين $G/\ker f$ و $\operatorname{Im} f$. ■

التمرين 22.

I. لتكن $\mathcal{B}$ مجموعة الأعداد العاديّة التي تُكتب بالشكل $\dfrac{k}{2^n}$ حيث $(k,n)\in\mathbb{Z}\times\mathbb{N}$:

$$\mathcal{B}=\left\{\frac{k}{2^n}:(k,n)\in\mathbb{Z}\times\mathbb{N}\right\}$$

1. أثبت أنّ $\mathcal{B}$ زمرة جزئيّة من $(\mathbb{Q},+)$.

2. لنفترض أنّ $x_1,x_2,\ldots,x_m$ هي عناصر من $\mathcal{B}$، ولتكن H هي الزمرة الجزئيّة من $\mathcal{B}$ التي تولِّدها المجموعة $X=\{x_1,x_2,\ldots,x_m\}$، أي $H=\langle X\rangle$.

① أثبت أنّ

$$H=\{\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_mx_m:(\alpha_1,\ldots,\alpha_m)\in\mathbb{Z}^m\}$$

② أثبت أنّه يوجد عدد N في $\mathbb{N}$ يجعل $2^NH=\left\{2^Nh:h\in H\right\}$ زمرة جزئيّة من $\mathbb{Z}$.

③ استنتج أنّه يوجد r في $\mathbb{N}$، يُحقّق $H=\left\langle\dfrac{r}{2^N}\right\rangle$، واستنتج أنّ $H\neq\mathcal{B}$.

④ هل يمكن توليد الزمرة $(\mathcal{B},+)$ بعدد منته من العناصر؟

II. لتكن $G=\mathbb{Q}^*\times\mathbb{Q}$ ولنزوّد G بقانون التشكيل الداخلي $(\odot)$ المعرّف كما يلي :

$$(a_1,b_1)\odot(a_2,b_2)=(a_1a_2,b_1+a_1b_2)$$

1. أثبت أنّ $(G,\odot)$ زمرة.

2. لنتأمّل المجموعة $\mathcal{A}=\left\{\left(2^m,\dfrac{k}{2^n}\right):(k,n,m)\in\mathbb{Z}^3\right\}$.

① أثبت أنّ $\mathcal{A}$ زمرة جزئيّة من $(G,\odot)$.

② لنتأمّل العنصرين $\alpha=(1,1)$ و $\beta=(2,0)$ من $\mathcal{A}$. احسب في الزمرة $(G,\odot)$ كلاًّ من α^p و β^p وذلك بدلالة p من $\mathbb{Z}$. [نذكّر هنا أنّ x^p في $(G,\odot)$ هو ناتج تشكيل x مع نفسه p مرّة إذا كانت $p>0$، وهو يساوي نظير x^{-p} في حالة $p<0$ ويساوي الحيادي في حالة $p=0$].

③ لتكن (k,n,m) من $\mathbb{Z}^3$، احسب المقدار $\beta^{-n}\odot\alpha^k\odot\beta^{n+m}$، واستنتج أنّ $\mathcal{A}$ هي الزمرة الجزئية من $(G,\odot)$ المولَّدة بالعنصرين α و β؛ أي $\mathcal{A}=\langle\{\alpha,\beta\}\rangle$.

3. لنتأمّل المجموعة $\mathcal{C} = \{1\} \times \mathcal{B}$، و $\mathcal{B}$ هي المجموعة المعرّفة في I. أثبت أنّ $\mathcal{C}$ زمرة جزئيّة من $\mathcal{A}$. وأثبت أنّ هناك تشاكلاً تقابلياً بين الزمرتين $(\mathcal{C},\odot)$ و $(\mathcal{B},+)$.

4. هل يمكن توليد الزمرة الجزئيّة $\mathcal{C}$ بعدد منته من العناصر؟

الحل

I.1. نترك تيقُّن كون المجموعة $\mathcal{B} = \left\{k2^{-n} : (k,n) \in \mathbb{Z} \times \mathbb{N}\right\}$ زمرة جزئيّة من $(\mathbb{Q},+)$ تمريناً للقارئ نظراً إلى سهولته.

I.2. لتكن $x_1, x_2, \ldots, x_m$ هي عناصر من $\mathcal{B}$. ولنعرّف

$$\begin{aligned} H &= \left\langle \left\{ x_1, x_2, \ldots, x_m \right\} \right\rangle \\ K &= \left\{ \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_m x_m : (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}^m \right\} \end{aligned}$$

I.2.① من الواضح أنّ K زمرة جزئيّة من $(\mathcal{B},+)$، تضمّ العناصر $x_1, x_2, \ldots, x_m$، إذن $H \subset K$. ثُمّ إنّه من الواضح أنّ كلّ زمرة تحوي المجموعة $\{x_1, \ldots, x_m\}$ لا بُدَّ أن تحوي جميع العناصر $(\alpha_k x_k)_{k\in\mathbb{N}_m}$ حيث $(\alpha_1, \ldots, \alpha_m)$ من $\mathbb{Z}^m$ فهي إذن تحوي جميع العبارات من الشكل $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_m x_m$ في حالة $(\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}^m$، أي جميع عناصر K . فلا بُدّ أن يكون $K \subset H$. بذا نكون قد أثبتنا أنّ $H = K$.

I.2.② نعلم أنّه في حالة p من $\mathbb{N}_m$ يُكتب العدد x_p بالشكل $k_p / 2^{n_p}$ حيث (k_p, n_p) من $\mathbb{Z} \times \mathbb{N}$. فإذا عرّفنا $N = \max\{n_p : p \in \mathbb{N}_m\}$، كان

$$\forall p \in \mathbb{N}_m, \quad 2^N x_p = 2^{N-n_p} k_p \in \mathbb{Z}$$

ولأنّ

$$H = \left\{ \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_m x_m : (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}^m \right\}$$

استنتجنا أنّ

$$2^N H = \left\{ \alpha_1 z_1 + \alpha_2 z_2 + \cdots + \alpha_m z_m : (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}^m \right\}$$

وقد رمزنا بالرمز z_p إلى العدد $2^{N-n_p} k_p$ من $\mathbb{Z}$. فنرى مباشرة أنّ $2^N H$ زمرة جزئيّة من $\mathbb{Z}$.

I.2.③ لمّا كانت $2^N H$ زمرة جزئيّة من $\mathbb{Z}$ استنتجنا أنّه يوجد عدد طبيعي r من $\mathbb{N}$، يُحقّق $2^N H = r\mathbb{Z}$. وعليه فإنّ

$$H = \left\{ \frac{rk}{2^N} : k \in \mathbb{Z} \right\} = \left\langle \frac{r}{2^N} \right\rangle$$

ونرى أنّ العنصر $\frac{1}{2^{N+1}}$ من $\mathcal{B}$ لا ينتمي إلى H. إذن $\mathcal{B} \neq H$.

I.2.④ لقد أثبتنا إذن أنّه لا يمكن توليد الزمرة $\mathcal{B}$ بعدد منته من العناصر.

II.1. لتكن $G = \mathbb{Q}^* \times \mathbb{Q}$ مزوّدة بقانون التشكيل الداخلي $\odot$ المعرّف كما يلي :

$$(a_1, b_1) \odot (a_2, b_2) = (a_1 a_2, b_1 + a_1 b_2)$$

- نلاحظ أنّه في حالة (a_1, b_1) و (a_2, b_2) و (a_3, b_3) من G لدينا

$$\begin{aligned}\big((a_1, b_1) \odot (a_2, b_2)\big) \odot (a_3, b_3) &= (a_1 a_2, b_1 + a_1 b_2) \odot (a_3, b_3)\\ &= (a_1 a_2 a_3, b_1 + a_1 b_2 + a_1 a_2 b_3)\end{aligned}$$

وكذلك

$$\begin{aligned}(a_1, b_1) \odot \big((a_2, b_2) \odot (a_3, b_3)\big) &= (a_1, b_1) \odot (a_2 a_3, b_2 + a_2 b_3)\\ &= (a_1 a_2 a_3, b_1 + a_1(b_2 + a_2 b_3))\\ &= (a_1 a_2 a_3, b_1 + a_1 b_2 + a_1 a_2 b_3)\end{aligned}$$

إذن

$$\big((a_1, b_1) \odot (a_2, b_2)\big) \odot (a_3, b_3) = (a_1, b_1) \odot \big((a_2, b_2) \odot (a_3, b_3)\big)$$

والبنية $(G, \odot)$ تجميعيّة.

- ونلاحظ أنّه في حالة (a_1, b_1) من G لدينا

$$(a_1, b_1) \odot (1, 0) = (1, 0) \odot (a_1, b_1) = (a_1, b_1)$$

إذن $(1, 0)$ عنصرٌ حيادي في $(G, \odot)$.

- وأخيراً في حالة (a_1, b_1) من G لدينا

$$(a_1, b_1) \odot \left(\frac{1}{a_1}, -\frac{b_1}{a_1} \right) = \left(\frac{1}{a_1}, -\frac{b_1}{a_1} \right) \odot (a_1, b_1) = (1, 0)$$

إذن لكل عنصرٍ (a_1, b_1) من G نظيرٌ $\left(\frac{1}{a_1}, -\frac{b_1}{a_1} \right)$ من G بالنسبة إلى القانون $\odot$. والبنية $(G, \odot)$ زمرة.

II.2.① من الواضح أنّ الحيادي $\left(1,0\right)=1_G$ ينتمي إلى

$$\mathcal{A}=\left\{\left(2^m,k2^{-n}\right):(k,n,m)\in\mathbb{Z}^3\right\}$$

ونظير العنصر $\left(2^m,k2^{-n}\right)$ من $\mathcal{A}$ هو العنصر $\left(2^{-m},-k2^{-n-m}\right)$ وهو ينتمي إلى $\mathcal{A}$.
وأخيراً نلاحظ أنّ

$$\begin{aligned}\left(2^m,k2^{-n}\right)\odot\left(2^{m'},k'2^{-n'}\right)&=\left(2^{m+m'},k2^{-n}+2^mk'2^{-n'}\right)\\&=\left(2^{m+m'},\frac{k2^{n'}+k'2^{m+n}}{2^{n+n'}}\right)\in\mathcal{A}\end{aligned}$$

إذن $\mathcal{A}$ زمرة جزئيّة من $(G,\odot)$.

II.2.② لنتأمّل العنصرين $\alpha=(1,1)$ و $\beta=(2,0)$ من $\mathcal{A}$. نبرهن بالتدريج أنّ :

$$\forall p\in\mathbb{Z},\quad \alpha^p=(1,p),\beta^p=(2^p,0)$$

II.2.③ لتكن (k,n,m) من $\mathbb{Z}^3$، عندئذ

$$\begin{aligned}\beta^{-n}\odot\alpha^k\odot\beta^{n+m}&=\left(\frac{1}{2^n},0\right)\odot\left(1,k\right)\odot\left(2^{n+m},0\right)\\&=\left(\frac{1}{2^n},\frac{k}{2^n}\right)\odot\left(2^{n+m},0\right)\\&=\left(2^m,\frac{k}{2^n}\right)\end{aligned}$$

ومنه نستنتج أنّ $\mathcal{A}\subset\langle\{\alpha,\beta\}\rangle$، أمّا الاحتواء المعاكس $\langle\{\alpha,\beta\}\rangle\subset\mathcal{A}$ فهو واضح لأنّ $\alpha\in\mathcal{A}$ و $\beta\in\mathcal{A}$. إذن $\mathcal{A}=\langle\{\alpha,\beta\}\rangle$.

II.3. نضع

$$\mathcal{C}=\{1\}\times\mathcal{B}=\left\{(1,k2^{-n}):(k,n)\in\mathbb{Z}\times\mathbb{N}\right\}$$

من الواضح أنّ $\mathcal{C}$ مجموعة جزئيّة من $\mathcal{A}$، وهي غير خالية لأنّ الحيادي $(1,0)$ ينتمي إليها، ونظير كلِّ عنصر $\left(1,k2^{-n}\right)$ منها هو العنصر $\left(1,-k2^{-n}\right)$ الذي ينتمي إليها، ثُمَّ إنّ

$$\left(1,\frac{k}{2^n}\right)\odot\left(1,\frac{k'}{2^{n'}}\right)=\left(1,\frac{k2^{n'}+k'2^n}{2^{n+n'}}\right)\in\mathcal{C}$$

وهذا يثبت أنّ $\mathcal{C}$ زمرة جزئيّة من $\mathcal{A}$.

ومن الواضح أنّ $\varphi:(\mathcal{B},+)\to(\mathcal{C},\odot),b\mapsto(1,b)$ تشاكلٌ تقابلي زمري.

II.4. لمّا كان $(\mathcal{C},\odot)\cong(\mathcal{B},+)$ وكنّا قد أثبتنا أنّه لا يمكن توليد الزمرة $(\mathcal{B},+)$ بعددٍ منته من العناصر استنتجنا أنّه لا يمكن توليد الزمرة $(\mathcal{C},\odot)$ بعدد منته من العناصر.

إذن، توجد زمرة من النمط المنتهي $\mathcal{A}$ أي يمكن توليدها بعدد منته من العناصر، بل بعنصرين اثنين تحديداً، وتحوي زمرة جزئيّة $\mathcal{C}$ لا يمكن توليدها بعددٍ منته من العناصر. ■

التمرين 23. نذكّر أنّ A_4 هي الزمرة المتناوبة على المجموعة $\mathbb{N}_4=\{1,2,3,4\}$.

1. اكتب قائمة بعناصر الزمرة A_4 واذكر رتبة كلِّ عنصر من هذه العناصر.
2. برهن أنّ A_4 لا تحوي زمرة جزئيّة عدد عناصرها يساوي 6.

الحل

1. تضم الزمرة المتناوبة A_4 اثني عشر عنصراً، وفيما يلي قائمة بهذه العناصر.

x			$O(x)$	x			$O(x)$
c_1	$=$	$(1,2,3)$	3	c_3	$=$	$(1,3,4)$	3
c_1^{-1}	$=$	$(1,3,2)$	3	c_3^{-1}	$=$	$(1,4,3)$	3
c_2	$=$	$(1,2,4)$	3	c_4	$=$	$(2,3,4)$	3
c_2^{-1}	$=$	$(1,4,2)$	3	c_4^{-1}	$=$	$(2,4,3)$	3
t_1	$=$	$(1,2)(3,4)$	2	t_3	$=$	$(1,4)(2,3)$	2
t_2	$=$	$(1,3)(2,4)$	2	I			1

2. لنفترض أنّ V زمرة جزئيّة من A_4 عدد عناصرها 6. نلاحظ أنّ تقاطع زمرتين جزئيّتين من V مختلفتين ورتبتهما تساوي 3 لا يحوي إلّا الحيادي. فإذا رمزنا بالرمز λ إلى عدد الزمر الجزئيّة التي رتبتها 3 من V كان $1+2\lambda\le 6$ ومنه $\lambda\in\{0,1,2\}$.

ولكن

- في حالة $\lambda=0$، تكون رتب جميع عناصر $V\backslash\{I\}$ تساوي 2 وهذا مستحيل لأنّ في A_4 لا يوجد إلا ثلاثة عناصر رتبتها تساوي 2.
- في حالة $\lambda=2$، توجد في V زمرتان جزئيّتان H_1 و H_2 مختلفتان، عدد عناصر كلٍّ منهما يساوي 3. وعندئذ يكون $H_1H_2\subset V$ وهذا تناقضٌ لأنّه عندئذ $\operatorname{card}(H_1H_2)=3^2=9$.
- في حالة $\lambda=1$، إذن توجد في V زمرة جزئيّة وحيدة H عدد عناصرها 3، وعليه فإنّ رُتب العناصر الثلاثة من $V\backslash H$ تساوي 2 أي $\{I,t_1,t_2,t_3\}\subset V$، ولكن نتيقّن

بسهولة وبالحساب المباشر أنّ $\{I, t_1, t_2, t_3\}$ زمرة جزئيّة من V. وهذا خُلفٌ لأنّ $6 \nmid 4$.

فلا يوجد في A_4 زمرة جزئيّة عدد عناصرها 6. ■

التمرين 24. بيّن أنه إذا كانت $n \geq 2$. فإنّ مناقلات المجموعة

$$\mathcal{A} = \{(1, j) : j \in \{2, 3, \ldots, n\}\}$$

تولّد الزمرة المتناظرة S_n.

الحل

لنلاحظ أنّه في حالة $j \neq i$ لدينا $(i, j) = (1, i)(1, j)(1, i)$. إذن تولِّد عناصر المجموعة $\mathcal{A}$ جميع المناقلات، ونعلم أنّ المُناقلات تولِّد الزمرة المتناظرة S_n. إذن $S_n = \langle \mathcal{A} \rangle$. ■

التمرين 25. بيّن أنه إذا كانت $n \geq 2$. فإنّ المناقلات

$$\mathcal{B} = \{(j, j+1) : j \in \{1, \ldots, n-1\}\}$$

تولّد الزمرة المتناظرة S_n.

الحل

لنرمز بالرمز τ_k إلى المناقلة $(1, k)$ في حالة $k \geq 2$. ولنثبت بالتدريج على العدد k بين 2 و n أنّ $\tau_k \in \langle \mathcal{B} \rangle$.

- في الحقيقة، لدينا استناداً إلى الفرض $\tau_2 = (1, 2) \in \mathcal{B}$.
- لنفترض أنّ $\tau_k \in \langle \mathcal{B} \rangle$ في حالة $2 \leq k < n$. عندئذ نلاحظ أنّ

$$\tau_{k+1} = \tau_k \circ (k, k+1) \circ \tau_k$$

إذن $\tau_{k+1} \in \langle \mathcal{B} \rangle$.

وبملاحظة أنّه في حالة $j \neq i$ لدينا $(i, j) = \tau_i \circ \tau_j \circ \tau_i$، نستنتج أنّ جميع المناقلات (i, j) تنتمي إلى الزمرة $\langle \mathcal{B} \rangle$. ولكنّ المُناقلات تولِّد كامل الزمرة S_n، إذن $S_n = \langle \mathcal{B} \rangle$. ■

التمرين 26. بيّن أنه إذا كانت $n \geq 2$. فإنّ الدورة c_n المعرّفة بالصيغة $(1, 2, \ldots, n)$، والمناقلة τ المعطاة بالصيغة $(1, 2)$ تولّدان الزمرة المتناظرة S_n.

الحل

لتكن $\mathcal{C} = \{c_n, \tau\}$، ولنرمز بالرمز τ_k إلى المناقلة $(k, k+1)$ في حالة $1 \le k < n$. ولنثبت بالتدريج على العدد k بين 1 و $n-1$ أنّ $\tau_k \in \langle \mathcal{C} \rangle$.

- في الحقيقة، لدينا $\tau_1 = (1,2) = \tau \in \mathcal{C}$.
- لنفترض أنّ $\tau_k \in \langle \mathcal{C} \rangle$ في حالة $1 \le k < n-1$. عندئذ نلاحظ أنّ
$$\tau_{k+1} = c_n \circ \tau_k \circ c_n^{-1}$$
ومن ثَمّ $\tau_{k+1} \in \langle \mathcal{C} \rangle$.

إذن مجموعة المناقلات $\mathcal{B} = \{(k, k+1) : 1 \le k < n\}$ محتواة في $\langle \mathcal{C} \rangle$، ولكن كنّا قد أثبتنا في التمرين السابق أنّ $S_n = \langle \mathcal{B} \rangle$، إذن $S_n = \langle \mathcal{C} \rangle$. وهي النتيجة المطلوبة. ■

التمرين 27. لتكن $(G, \cdot)$ زمرة منتهية عدد عناصرها n، أثبت أنه يوجد تشاكل تقابلي بين G وبين زمرة جزئية من الزمرة المتناظرة S_n.

الحل

إذا كان g عنصراً من G رمزنا بالرمز σ_g إلى التطبيق $\sigma_g : G \to G, x \mapsto gx$. من الواضح أنّ σ_g تقابلٌ، تقابله العكسي هو $\sigma_{g^{-1}}$. ليكن $\varphi : \mathbb{N}_n \to G$ تقابلاً ما. ولنعرّف التطبيق
$$\Psi : G \to S_n, g \mapsto \varphi^{-1} \circ \sigma_g \circ \varphi$$

- التطبيق Ψ معرّف تعريفاً جيّداً لأنّ $\varphi^{-1} \circ \sigma_g \circ \varphi$ تبديلٌ على $\mathbb{N}_n$ أيّاً كان g من G.
- في حالة g و g' من G لدينا
$$\begin{aligned}\Psi(g) \circ \Psi(g') &= \varphi^{-1} \circ \sigma_g \circ \varphi \circ \varphi^{-1} \circ \sigma_{g'} \circ \varphi = \varphi^{-1} \circ \sigma_g \circ \sigma_{g'} \circ \varphi \\ &= \varphi^{-1} \circ \sigma_{gg'} \circ \varphi = \Psi(gg')\end{aligned}$$
إذن Ψ تشاكلٌ زمري.
- وإذا كان $g \in \ker \Psi$، كان $\Psi(g) = I$ أي
$$\forall k \in \mathbb{N}_n,\ \varphi^{-1}(\sigma_g(\varphi(k))) = k$$
فإذا اخترنا $k = \varphi^{-1}(1_G)$ استنتجنا أنّ $g = 1_G$. ومنه $\ker \Psi = \{1_G\}$. والتشاكل الزمري Ψ متباينٌ، فهو يعرّف تشاكلاً تقابلياً زمريّاً بين G والزمرة الجزئيّة $\Psi(G)$ من S_n. وهي النتيجة المرجوّة، التي تُعرف باسم مبرهنة Cayley. ■

② الحلقات والحقول

التمرين 28. لتكن المجموعة $A = \{a + b\sqrt{2} : (a,b) \in \mathbb{Z} \times \mathbb{Z}\}$، مزودة بجمع وضرب الأعداد الحقيقية.

1. بيّن أنّ A حلقة تامّة.
2. إذا كان $x = a + b\sqrt{2}$ من A عرّفنا $\overline{x} = a - b\sqrt{2}$ و $R(x) = \dfrac{x + \overline{x}}{2}$ و $I(x) = \dfrac{x - \overline{x}}{2\sqrt{2}}$ وأخيراً $N(x) = x\,\overline{x}$. أثبت أن الأعداد $R(x)$ و $I(x)$ و $N(x)$ أعداد صحيحة أياً كان x من A، وأنّ

$$\forall (x,y) \in A^2, \;\; \overline{x\,y} = \overline{x}\,\overline{y}, \;\; N(x\,y) = N(x)\,N(y)$$

3. أثبت أنّ $U(A) = \{x \in A : N(x) \in \{-1,+1\}\}$.
4. لنضع $\omega = 1 + \sqrt{2}$. أثبت أنّ

$$\forall \varepsilon \in \{-1,+1\}, \forall n \in \mathbb{Z}, \quad \varepsilon\omega^n \in U(A)$$

5. لتكن H الزمرة الجزئية من $U(A)$ المولّدة بالعنصرين -1 و ω. نعرّف، أياً كان x من $U(A)$، المقدار

$$T(x) = \min\{|R(ux)| + |I(ux)| : u \in H\}$$

وليكن u_0 من H عنصراً يُحقّق

$$T(x) = |R(u_0x)| + |I(u_0x)|$$

   - i. علل وجود u_0، وبيّن أنّ $T(x) \geq 1$.
   - ii. نفترض أنّ $u_0x = \lambda + \mu\sqrt{2}$، نعرّف $\beta = |\mu|$ و $\alpha = |\lambda|$. أثبت بحساب $\omega\,u_0x$ و $\dfrac{u_0x}{\omega}$ أنّ

$$\alpha + \beta \leq |\alpha - 2\beta| + |\alpha - \beta|$$

     وأثبت من ناحية أخرى أنّ $\alpha^2 - 2\beta^2 \in \{-1,+1\}$، مستنتجاً أنّ الشرط $\beta \neq 0$ يقتضي $\beta \leq \alpha \leq 2\beta$ ويناقض ما سبق.
   - iii. استنتج أنّ $u_0x \in \{-1,+1\}$، ومن ثَمّ $x \in H$. وأخيراً عيّن $U(A)$.

الحل

1. إنّ تيقُّن أنّ $A = \mathbb{Z}\left[\sqrt{2}\right] = \mathbb{Z} + \sqrt{2}\,\mathbb{Z}$ حلقة تامّة أمرٌ بسيط نترك تفاصيله تمريناً للقارئ. والغرض من هذا التمرين تعيين العناصر القَلوبة في A أي $U(A)$.

2. ليكن $x = a + b\sqrt{2}$ عنصراً من A، أي $(a,b) \in \mathbb{Z}^2$، عندئذ
$$N(x) = a^2 - 2b^2 \text{ و } I(x) = b \text{ و } R(x) = a$$
فالأعداد $R(x)$ و $I(x)$ و $N(x)$ تنتمي جميعاً إلى $\mathbb{Z}$.

وإذا كان $x = a + b\sqrt{2}$ و $y = a' + b'\sqrt{2}$ عنصرين من A كان
$$\overline{x} = a - b\sqrt{2}, \quad \overline{y} = a' - b'\sqrt{2}$$
$$xy = aa' + 2bb' + (ba' + ab')\sqrt{2}$$
$$\overline{x}\,\overline{y} = aa' + 2bb' - (ba' + ab')\sqrt{2}$$
ومنه $\overline{xy} = \overline{x}\,\overline{y}$. وأخيراً، في حالة x و y من A نرى أنّ
$$N(x) = xy\overline{xy} = xy\overline{x}\,\overline{y} = x\overline{x}y\overline{y} = N(x)N(y)$$

3. لنفترض أنّ x عنصرٌ من $U(A)$، إذن يوجد y في A يُحقّق $xy = 1$، ومن ثَمّ يكون
$$N(x)N(y) = 1$$
أي إنّ $N(x)$ ينتمي إلى المجموعة $U(\mathbb{Z}) = \{-1, +1\}$.

وبالعكس، إذا كان $x = a + b\sqrt{2}$ عنصراً من A يُحقّق $N(x) \in \{-1, +1\}$، عرّفنا العنصر
$$y = N(x)\overline{x} = N(x)a - N(x)b\sqrt{2}$$
فيكون $xy = N(x)x\overline{x} = (N(x))^2 = 1$. فالعنصر x قلوبٌ ومقلوبه y في هذه الحالة، وبذلك نكون قد أثبتنا أنّ $x \in U(A)$. ومنه المساواة
$$U(A) = \left\{x \in A : N(x) \in \{-1, +1\}\right\}$$

4. نضع $\omega = 1 + \sqrt{2}$. فيكون $N(\omega) = 1 - 2 = -1$، إذن $\omega \in U(A)$. ونرى مباشرة أنّ $-1 \in U(A)$. ولأنّ مجموعة العناصر القلوبة $U(A)$ مزوّدة بقانون الضرب في الحلقة A زمرة، استنتجنا أنّ $U(A)$ تحوي الزمرة الجزئيّة H المولَّدة بالمجموعة $\{-1, \omega\}$، ومنه
$$\forall \varepsilon \in \{-1, +1\}, \forall n \in \mathbb{Z}, \quad \varepsilon\omega^n \in U(A)$$

5. ليكن x من $U(A)$، ولنعرّف المقدار
$$T(x) = \min\left\{\left|R(ux)\right| + \left|I(ux)\right| : u \in H\right\}$$

.$i.5$ لأنّ $\left\{|R(ux)|+|I(ux)| : u\in H\right\}$ مجموعة جزئيّة غير خالية من $\mathbb{N}$ ، قَبِلَت هذه المجموعة أصغر عنصرٍ، إذن يوجد في H عنصرٌ u_0 يُحقّق

$$T(x)=|R(u_0x)| + |I(u_0x)|$$

فإذا كان $T(x)=0$ كان $R(u_0x)=I(u_0x)=0$ أو $u_0x=0$ وهذا خُلفٌ لأنّ $0\notin U(A)$. إذن $T(x)\geq 1$.

.$ii.5$ يُكتب u_0x بالشكل $\lambda+\mu\sqrt{2}$. لنعرّف إذن $\beta=\left|\mu\right|$ و $\alpha=\left|\lambda\right|$ ، ولنلاحظ أنّ

$$\omega u_0x=(2\mu+\lambda)+(\lambda+\mu)\sqrt{2}$$
$$\frac{u_0x}{\omega}=(2\mu-\lambda)+(\lambda-\mu)\sqrt{2}$$

- فإذا كان $\lambda\mu\geq 0$ استنتجنا من كون $u_0\omega^{-1}\in H$ أنّ

$$T(x)\leq\left|R\left(\frac{u_0}{\omega}x\right)\right|+\left|I\left(\frac{u_0}{\omega}x\right)\right|=\left|2\mu-\lambda\right|+\left|\lambda-\mu\right|$$

أو

$$\alpha+\beta\leq\left|\alpha-2\beta\right|+\left|\alpha-\beta\right|$$

- وإذا كان $\lambda\mu<0$ استنتجنا من كون $\omega u_0\in H$ أنّ

$$T(x)\leq\left|R\left(\omega u_0x\right)\right|+\left|I\left(\omega u_0x\right)\right|=\left|2\mu+\lambda\right|+\left|\lambda+\mu\right|$$

أو

$$\alpha+\beta\leq\left|\alpha-2\beta\right|+\left|\alpha-\beta\right|$$

إذن تتحقّق في جميع الأحوال المتراجحة

$$\alpha+\beta\leq\left|\alpha-2\beta\right|+\left|\alpha-\beta\right| \tag{1}$$

ولمّا كان u_0 و x عنصرين من $U(A)$ كان $u_0x\in U(A)$ ومن ثَمّ $N(u_0x)\in\{-1,1\}$ أي

$$\alpha^2-2\beta^2\in\{-1,1\} \tag{2}$$

لنفترض جدلاً أنّ $\beta\neq 0$ ، فيكون $\beta\geq 1$ لأنّ $\mu\in\mathbb{Z}$. وعندئذ نستنتج من (2) أنّ

$$\beta^2\leq\beta^2+\beta^2-1=2\beta^2-1\leq\alpha^2\leq 2\beta^2+1\leq 3\beta^2<4\beta^2$$

وعليه $4\beta^2 > \alpha^2 \geq \beta^2$، ولأنّ α و β عددان موجبان، استنتجنا أنّ $\beta \leq \alpha < 2\beta$.
وعندئذ يكون

$$\left|\alpha - 2\beta\right| + \left|\alpha - \beta\right| = 2\beta - \alpha + \alpha - \beta = \beta$$

فإذا عُدنا إلى (1) استنتجنا أنّ $\alpha + \beta \leq \beta$ وهذا يقتضي أنّ $\alpha = 0$ ممّا يناقض (2)، لأنّ β عددٌ طبيعي.

iii.5. إذن لا بُدّ أن يكون $\beta = 0$، من ثَمّ $\alpha = 1$. أي إنّ $u_0 x \in \{-1,1\}$ وهذا يقتضي أن يكون $x \in \{-u_0^{-1}, u_0^{-1}\} \subset H$.

وهكذا نكون قد أثبتنا صحة الاحتواء $U(A) \subset H$، وبرهنّا من ثَمّ أنّ

$$U(A) = \langle\{-1,\omega\}\rangle = \left\{\varepsilon\left(1+\sqrt{2}\right)^n : \varepsilon \in \{-1,1\}, n \in \mathbb{Z}\right\}$$

وهي النتيجة المرجوّة. ■

التمرين 29. نقول عن حلقة تامّة $(A,+,\cdot)$ إنها **إقليدية** إذا وُجِدَ تطبيق φ_A من $A\backslash\{0\}$ إلى $\mathbb{N}$ يحقق الشرطين التاليين :

- $(b \neq 0) \wedge (a \mid b) \Rightarrow \varphi_A(a) \leq \varphi_A(b)$
- $\forall (a,b) \in A \times (A\backslash\{0\}), \exists (q,r) \in A^2, \ \begin{cases} a = qb + r \\ (r = 0) \vee (\varphi_A(r) < \varphi_A(b)) \end{cases}$

1. تحقق أنّ $\mathbb{Z}$ حلقة إقليدية.
2. أوجد خاصة مميّزة للعناصر القلوبة في حلقة إقليدية A بدلالة التابع φ_A الموافق.
3. بيّن أنّ كلَّ حلقة إقليدية حلقةٌ رئيسية.
4. لتكن $G = \{x + \mathrm{i}y \in \mathbb{C} : (x,y) \in \mathbb{Z} \times \mathbb{Z}\}$. بيّن أنّ G، مزودةً بالجمع والضرب العقديين، هي حلقة إقليديّة.

مساعدة : يمكن أن نضع $\varphi_G(x + iy) = x^2 + y^2$.

الحل

1. إنّ حلقة الأعداد الصحيحة $\mathbb{Z}$ حلقة إقليدية. إذ يكفي أن نعرّف

$$\varphi_{\mathbb{Z}} : \mathbb{Z}\backslash\{0\} \to \mathbb{N}, \ \ \varphi_{\mathbb{Z}}(a) = |a|$$

فنتيقّن مباشرة أنّ $\varphi_{\mathbb{Z}}$ يُحقّق الخاصة المطلوبة.

2. ليكن u عنصراً من $U(A)$، عندئذ، مهما كان العنصر b من $A\backslash\{0\}$ كان $b \mid u$ ومن ثَمّ

$$\forall b \in A\backslash\{0\}, \quad \varphi_A(u) \le \varphi_A(b)$$

فإذا عرّفنا $\alpha = \min\left\{\varphi_A(b) : b \in A\backslash\{0\}\right\}$ استنتجنا استناداً إلى ما سبق أنّ

$$\forall u \in U(A), \quad \varphi_A(u) \le \alpha$$

ولكن، استناداً إلى تعريف α، من الواضح أنّ $\forall u \in U(A), \quad \varphi_A(u) \ge \alpha$. إذن

$$\forall u \in U(A), \quad \varphi_A(u) = \alpha$$

وبالعكس، ليكن b عنصراً من $A\backslash\{0\}$، يُحقّق $\varphi_A(b) = \alpha$. نُجري قسمة إقليديّة للعنصر 1_A على b فنجد (q,r) في A^2 يُحقّق

$$1_A = qb + r، \text{ حيث } r = 0 \text{ أو } \varphi_A(r) < \varphi_A(b) = \alpha$$

ولكنّ المتراجحة $\varphi_A(r) < \alpha$ مستحيلة استناداً إلى تعريف α، إذن لا بُدّ أن يكون $r = 0$، ومن ثَمّ $qb = 1_A$، وهذا يعني أنّ b عنصرٌ قَلوب أي $b \in U(A)$.

إذن لقد أثبتنا أنّ $U(A) = \varphi_A^{-1}(\{\alpha\})$، والعدد α معطى بالعلاقة

$$\alpha = \min\left\{\varphi_A(b) : b \in A\backslash\{0\}\right\}$$

3. لتكن A حلقة إقليديّة. وليكن $\mathcal{I}$ مثالياً في A . لمّا كانت المجموعة $\varphi_A(\mathcal{I}\backslash\{0\})$ مجموعة جزئيّة غير خالية من $\mathbb{N}$، كان فيها أصغر عنصر. لنعرّف إذن $\beta = \min \varphi_A(\mathcal{I}\backslash\{0\})$. وليكن b عنصراً من $\mathcal{I}\backslash\{0\}$ يُحقّق $\varphi_A(b) = \beta$.

- لمّا كان b عنصراً من $\mathcal{I}$ استنتجنا أنّ $bA \subset \mathcal{I}$.
- وبالعكس، ليكن x عنصراً من $\mathcal{I}$، بإجراء قسمة إقليديّة للعنصر x على b نستنتج وجود عنصرٍ (q,r) في A^2 يُحقّق $x = bq + r$، ولكنّ العنصر r ينتمي إلى $\mathcal{I}$ لأنّ $r = x - bq$، فإذا كان $r \ne 0$ كان $\varphi_A(r) < \varphi_A(b) = \beta$، وهذا يناقض تعريف β . إذن يجب أن يكون $r = 0$ أي $x = bq \in bA$. فنكون قد أثبتنا أنّ $\mathcal{I} \subset bA$.

أي $\mathcal{I} = bA$. فكلُّ مثالي في A مثالي رئيسي، فالحلقة A حلقة رئيسيّة.

4. لتكن

$$G = \mathbb{Z}[\mathrm{i}] = \left\{x + \mathrm{i}\,y \in \mathbb{C} : (x,y) \in \mathbb{Z} \times \mathbb{Z}\right\}$$

من الواضح أنّ $(G,+,\cdot)$ حلقة تبديليّة لأنّها حلقة جزئيّة من الحقل $\mathbb{C}$.

لنعرّف التطبيق

$$\varphi_G : G\backslash\{0\} \to \mathbb{N},\ \ \varphi_G(x+\mathrm{i}\,y) = x^2+y^2 = |x+\mathrm{i}\,y|^2$$

ولنلاحظ ما يأتي:

- إذا كان z عنصراً من $G\backslash\{0\}$، وكان $v \mid z$ استنتجنا أنّه يوجد w في G يُحقّق $z = vw$، وعندئذ يكون $|z|^2 = |v|^2\,|w|^2$ أي $\varphi_G(v) \mid \varphi_G(z)$، ولأنّ $\varphi_G(z) \neq 0$ استنتجنا من ذلك أنّ $\varphi_G(v) \le \varphi_G(z)$.
- ليكن a من G و b من $G\backslash\{0\}$. ولنتأمّل العدد العقدي $z = \dfrac{a}{b} = x+\mathrm{i}\,y$. ولنعرّف

$$n = \left\lfloor y+\tfrac{1}{2}\right\rfloor \ \text{ و } \ m = \left\lfloor x+\tfrac{1}{2}\right\rfloor$$

وأخيراً لنضع $x' = x-m$ و $y' = y-n$. فيكون m أقرب عددٍ صحيح إلى x ويكون n أقرب عددٍ صحيح إلى y. نعرّف إذن $q = m+\mathrm{i}\,n$ وهو عنصرٌ من G، و $z' = x'+\mathrm{i}\,y'$ من $\mathbb{C}$. فيكون لدينا $a = bq+r$ مع $r = z'b$. العدد r ينتمي إلى G لأنّه يساوي $a-qb$، ثُمّ إنّ

$$\begin{aligned}
|r|^2 = |z'|^2\,|b|^2 &\le (x'^2+y'^2)\varphi_G(b)\\
&\le \left(\frac{1}{4}+\frac{1}{4}\right)\varphi_G(b)\\
&= \frac{1}{2}\varphi_G(b) < \varphi_G(b)
\end{aligned}$$

فإذا كان $r \neq 0$ كان $\varphi_G(r) < \varphi_G(b)$.

وهكذا نكون قد أثبتنا أنّ الحلقة $G = \mathbb{Z}[\mathrm{i}]$ حلقة إقليديّة. فهي حلقة رئيسيّة، وعناصرها القلوبة هي

$$U\left(\mathbb{Z}[\mathrm{i}]\right) = \left\{1,\mathrm{i},-1,-\mathrm{i}\right\}$$

وبذا نُنجز إثبات المطلوب. ■

التمرين 30. لتكن E مجموعة غير خالية ومنتهية، ولتكن $\mathbb{A} = (P(E), \Delta, \cap)$. إذا كان $\mathcal{I}$ مثالياً في $\mathbb{A}$ أسمينا $h(\mathcal{I})$ العددَ

$$h(\mathcal{I}) = \max\{\operatorname{card}(B) : B \in \mathcal{I}\}$$

1. ليكن $\mathcal{I}$ مثالياً في $\mathbb{A}$.
   - i. بيّن أنه يوجد عنصر وحيد B_0 من $\mathcal{I}$ يُحقّق $h(\mathcal{I}) = \operatorname{card}(B_0)$.
   - ii. أثبت أنّ $\mathcal{I} = B_0 \cdot \mathbb{A}$ ومن ثمّ $\mathcal{I} = \{C \in \mathbb{A} : C \subset B_0\}$ ، ما هو عدد عناصر $\mathcal{I}$؟ هل $\mathbb{A}$ حلقة رئيسية ؟ وما هو عدد مثاليات الحلقة $\mathbb{A}$ ؟
2. بيّن أنّ $\mathbb{A}$ تشاكِل تقابلياً الحلقة $\left((\mathbb{Z}/2\mathbb{Z})^p, +, \cdot\right)$ مع $p = \operatorname{card}(E)$.

الحل

$1.i$. استناداً إلى تعريف $h(\mathcal{I})$ توجد مجموعة B_0 تنتمي إلى $\mathcal{I}$ تُحقّق $h(\mathcal{I}) = \operatorname{card}(B_0)$.

- ليكن B عنصراً ما من $\mathcal{I}$ ، نستنتج من كون

$$B \cup B_0 = B \,\Delta\, B_0 \,\Delta\, (B \cap B_0)$$

أنّ $B \cup B_0$ ينتمي إلى $\mathcal{I}$ ، وبناءً على تعريف B_0 ، نستنتج أنّ

$$\operatorname{card}(B \cup B_0) \leq \operatorname{card}(B_0)$$

ولكن $B_0 \subset B \cup B_0$ إذن لا بُدّ أن يكون $B \cup B_0 = B_0$ ، أي $B \subset B_0$.

- فإذا كان B_1 عنصراً من $\mathcal{I}$ يُحقّق $\operatorname{card}(B_1) = h(\mathcal{I})$ استنتجنا مما سبق أنّ $B_1 \subset B_0$ ، فلا بُدّ أن يكون $B_1 = B_0$ لأنّ لهاتين المجموعتين عدد العناصر $h(\mathcal{I})$ نفسه. فالمجموعة B_0 من $\mathcal{I}$ التي تُحقّق المساواة $h(\mathcal{I}) = \operatorname{card}(B_0)$ وحيدة.

$1.ii$. لقد أثبتنا أنّ $\forall B \in \mathcal{I},\ B \subset B_0$. ومن ثَمّ إذا كان B عنصراً ما من $\mathcal{I}$ ، كان $B = B_0 \cap B$ ومن ثَمّ $B \in B_0 \cdot \mathbb{A}$ أي $\mathcal{I} \subset B_0 \cdot \mathbb{A}$ ، ومنه $\mathcal{I} = B_0 \cdot \mathbb{A}$ لأنّ الاحتواء المُعاكس مُحقّق وضوحاً نظراً إلى انتماء B_0 إلى $\mathcal{I}$.

- إذا كانت C مجموعة جزئيّة من B_0 ، كان $\mathcal{I} = B_0 \cdot \mathbb{A} \ni C = B_0 \cap C$. وبالعكس، كلّ عنصر B من $\mathcal{I}$ يُحقِّق $B \subset B_0$. إذن لقد أثبتنا أنّ

$$\mathcal{I} = B_0 \cdot \mathbb{A} = \left\{C \in \mathbb{A} : C \subset B_0\right\} = P(B_0)$$

- وعليه،

$$\operatorname{card}(\mathcal{I}) = \operatorname{card}(P(B_0)) = 2^{\operatorname{card}(B_0)} = 2^{h(\mathcal{I})}$$

- صحيح أنّ كلّ مثالي من $\mathbb{A}$ مثالي رئيسي، إلّا أنّ الحلقة $\mathbb{A}$ ليست رئيسيّة لأنّها ليست حلقة تامّة.

- التطبيق $B_0 \mapsto B_0 \cdot A$ يعرّف تقابلاً من $\mathbb{A}$ إلى مجموعة مثاليّات الحلقة $\mathbb{A}$. إذن عدد المثاليّات في $\mathbb{A}$ يساوي $\operatorname{card}(\mathbb{A}) = 2^{\operatorname{card}(E)} = 2^p$.

2. لنعرّف في حالة مجموعة جزئيّة B من E التابع للمميِّز للمجموعة B كما يلي :

$$\mathbb{1}_B : A \to \mathbb{Z}/2\mathbb{Z},\ \mathbb{1}_B(x) = \begin{cases} 1 & : \quad x \in B \\ 0 & : \quad x \notin B \end{cases}$$

لمّا كان $p = \operatorname{card}(E)$ استنتجنا أنّه يوجد تقابل $\varphi : \mathbb{N}_p \to E$. عندئذ نعرّف التطبيق

$$\Phi : \mathbb{A} \to (\mathbb{Z}/2\mathbb{Z})^p,\ \Phi(B) = \left(\mathbb{1}_B \circ \varphi(1), \mathbb{1}_B \circ \varphi(2), \ldots, \mathbb{1}_B \circ \varphi(p)\right)$$

وبملاحظة أنّ

$$\forall (A,B) \in P(E),\quad \begin{aligned} \mathbb{1}_{A\Delta B} &= \mathbb{1}_A + \mathbb{1}_B \\ \mathbb{1}_{A\cap B} &= \mathbb{1}_A \cdot \mathbb{1}_B \end{aligned}$$

نرى مباشرة أنّ Φ تشاكل حلقي تقابلي. ■

التمرين 31. الحلقة البوليانيّة.

نقول إنّ حلقة $(\mathbb{A}, +, \cdot)$ حلقة بوليانيّة إذا كان : $\forall x \in \mathbb{A}, x^2 = x$.

1. بيّن أنه إذا كانت E مجموعة غير خالية، كانت $(P(E), \Delta, \cap)$ حلقة بوليانيّة.
2. لتكن $\mathbb{A}$ حلقة بوليانية. أثبت أنّ $\forall x \in \mathbb{A}, x + x = 0$، واستنتج أنّ $\mathbb{A}$ تبديليّة.
3. لتكن $\mathbb{A}$ حلقة بوليانية منتهية يزيد عدد عناصرها تماماً عن 2 . أثبت أنها ليست تامّة. يمكنك حساب $x\,y\,(x+y)$.
4. بيّن أن العلاقة الثنائية $\leq$ المعرّفة علىحلقة بوليانية $\mathbb{A}$ بالعلاقة

$$(x \leq y) \Leftrightarrow (x \cdot y = x)$$

هي علاقة ترتيب، و أنّ $\forall x \in \mathbb{A}, 0 \leq x \leq 1$.

5. نعرّف على حلقة بوليانية $\mathbb{A}$ قانون التشكيل الداخلي $\vee$ بالعلاقة :
$$x \vee y = x + y + xy$$
بيّن أنّ القانون $\vee$ تجميعيّ وتبديليّ ويقبل عنصراً حيادياً، وأن كلاً من $(\vee)$ و $(\cdot)$ يقبل التوزيع على الآخر.

6. لتكن $\mathbb{A}$ حلقة بوليانية منتهية.

i. بيّن أنّ أي مثاليّ $\mathcal{I}$ في $\mathbb{A}$ يكون مغلقاً بالنسبة إلى القانون $(\vee)$.

ii. ليكن $\mathcal{I}$ مثالياً في $\mathbb{A}$، و لنعرّف $x_{\mathcal{I}} = \bigvee_{x\in\mathcal{I}} x$ من $\mathcal{I}$. أثبت أنّ
$$\mathcal{I} = x_{\mathcal{I}}\mathbb{A} = \{y \in \mathbb{A} : y \leq x_{\mathcal{I}}\}$$
وأنّ $x_{\mathcal{I}}$ هو العنصر الوحيد في $\mathcal{I}$ الذي يحقق ما سبق.

iii. ليكن $\mathcal{I}$ مثالياً في $\mathbb{A}$ يُحقّق $\mathcal{I} \neq \{0\}$ أثبت أنّ
$$2 = \min\{\text{card}(x\mathbb{A}) : x \in \mathcal{I}\backslash\{0\}\}$$
واستنتج أنه يوجد في $\mathcal{I}$ عنصر x_1 يُحقّق $\text{card}(x_1\mathbb{A}) = 2$.

iv. نفترض أنّ $2 \leq \text{card}(\mathbb{A})$، ونعرّف $E = \{x \in \mathbb{A} : \text{card}(x\mathbb{A}) = 2\}$.
بيّن أنّ

❶ $E \neq \varnothing,$

❷ $\forall(x,y) \in E^2, x \neq y \Rightarrow xy = 0,$

❸ $\sum_{x\in E} x = 1.$

v. نعرّف التطبيق :
$$\varphi : P(E) \to \mathbb{A},\ Z \mapsto \sum_{x\in Z} x \quad \text{مع الاصطلاح} \quad \sum_{x\in\varnothing} x = 0$$
أثبت أنّ φ تشاكلٌ حَلَقي تقابلي بين $(P(E), \Delta, \cap)$ و $\mathbb{A}$. ماذا عن عدد عناصر $\mathbb{A}$؟

الحل

1. في الحقيقة إنّ الحلقة $(P(E), \Delta, \cap)$ حلقة بوليانيّة، لأنّ
$$\forall B \in P(E), \quad B \cap B = B.$$

2. لتكن $\mathbb{A}$ حلقة بوليانيّة، وليكن x من $\mathbb{A}$. نستنتج من كون $(1+x)^2 = 1+x$ و $x^2 = x$ أنّ

$$1 + x = 1 + x + x + x^2 = 1 + x + x + x$$

ومنه $x + x = 0$.

ليكن (x, y) من $\mathbb{A}^2$. عندئذ نستنتج من $(x+y)^2 = x+y$ و $x^2 = x$ و $y^2 = y$ أنّ

$$x + y = (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$$

ومنه $xy + yx = 0$. إذن

$$xy = xy + 0 = xy + \underbrace{yx + yx} = \overbrace{xy + yx} + yx = 0 + yx = yx$$

فنكون قد أثبتنا أنّ $xy = yx \quad \forall (x,y) \in \mathbb{A},$ ، أي إنّ الحلقة $\mathbb{A}$ تبديليّة.

3. لتكن $\mathbb{A}$ حلقة بوليانية منتهية يزيد عدد عناصرها تماماً عن 2 . إذن يوجد في $\mathbb{A}\backslash\{0\}$ عنصران مختلفان نرمز إليهما بالرمزين x و y على سبيل المثال. عندئذ يكون لدينا

$$xy(x+y) = x^2y + xy^2 = xy + yx = 0$$

ومع ذلك $x \neq 0$ و $y \neq 0$ و $x + y \neq 0$. فالحلقة $\mathbb{A}$ ليست تامّة في هذه الحالة.

4. لتكن $\mathbb{A}$ حلقة بوليانية. ولنعرّف العلاقة الثنائية $\leq$ بالعلاقة $(xy = x) \Leftrightarrow (x \leq y)$.

- ليكن x من $\mathbb{A}$. عندئذ $xx = x^2 = x$ ، ومنه $x \leq x$. فالعلاقة $\leq$ انعكاسيّة.
- ليكن x و y من $\mathbb{A}$. ولنفترض أنّ $x \leq y$ و $y \leq x$. عندئذ

$$\left.\begin{array}{l}(x \leq y) \Leftrightarrow (xy = x)\\ (y \leq x) \Leftrightarrow (yx = y)\end{array}\right\} \Rightarrow (x = y)$$

فالعلاقة $\leq$ تخالفيّة.

- ليكن x و y و z من $\mathbb{A}$. ولنفترض أنّ $x \leq y$ و $y \leq z$.

$$\left.\begin{array}{l}(x \leq y) \Leftrightarrow (xy = x)\\ (y \leq z) \Leftrightarrow (yz = y)\end{array}\right\} \Rightarrow (xz = xyz = xyz = xy = x)$$
$$\Leftrightarrow (x \leq z)$$

فالعلاقة $\leq$ متعدّية. إذن $(\mathbb{A}, \leq)$ علاقة ترتيب.

وأخيراً، في حالة x من $\mathbb{A}$ ، يكون $0x = 0$ و $1x = x$ ، إذن $0 \leq x \leq 1$.

5. لتكن $\mathbb{A}$ حلقة بوليانية. ولنعرّف قانون التشكيل الداخلي $\vee$ بالعلاقة :

$$x \vee y = x + y + xy .$$

▫ ليكن x و y و z من $\mathbb{A}$. عندئذ

$$\begin{aligned}(x \vee y) \vee z &= (x + y + xy) \vee z \\ &= x + y + xy + z + (x + y + xy)z \\ &= x + y + z + xy + yz + zx + xyz \\ &= x + (y + z + yz) + x(y + z + yz) \\ &= x + y \vee z + x(y \vee z) \\ &= x \vee (y \vee z)\end{aligned}$$

وهذا يثبت أنّ $\vee$ قانون تجميعي.

▫ ليكن x و y من $\mathbb{A}$. عندئذ

$$x \vee y = x + y + xy = y + x + yx = y \vee x$$

وهذا يثبت أنّ $\vee$ قانون تبديلي.

▫ وكذلك، من الواضح أنّ $\forall x \in \mathbb{A},\ x \vee 0 = x + 0 + 0x = x$.

إذن 0 عنصر حيادي بالنسبة إلى القانون $\vee$.

▫ ليكن x و y و z من $\mathbb{A}$. عندئذ

$$\begin{aligned}(x \vee y)(x \vee z) &= (x + y + xy)(x + z + xz) \\ &= x^2 + xz + x^2z + xy + yz + xyz + x^2y + xyz + x^2yz \\ &= x + \cancel{xz} + \cancel{xz} + \cancel{xy} + yz + xyz + \cancel{xy} + \cancel{xyz} + \cancel{xyz} \\ &= x + yz + xy \\ &= x \vee (yz)\end{aligned}$$

و

$$\begin{aligned}(xy) \vee (xz) &= xy + xz + x^2yz \\ &= xy + xz + xyz \\ &= x(y + z + yz) \\ &= x(y \vee z)\end{aligned}$$

إذن كلٌّ من $(\vee)$ و $(\cdot)$ يقبل التوزيع على الآخر.

6. لتكن $\mathbb{A}$ حلقة بوليانية منتهية.

$i.6$. ليكن $\mathcal{I}$ مثالياً في $\mathbb{A}$، ولنتأمّل عنصرين x و y من $\mathcal{I}$. عندئذ ينتمي كلٌّ من $x+y$ و xy إلى $\mathcal{I}$، ومن ثَمّ ينتمي العنصر $x+y+xy$ أيضاً إلى $\mathcal{I}$. أي

$$\forall(x,y)\in\mathcal{I}^2,\quad x\vee y\in\mathcal{I}.$$

$ii.6$. لنتأمّل إذن مثالياً $\mathcal{I}$ في $\mathbb{A}$، ولنعرّف $x_{\mathcal{I}}=\bigvee\limits_{x\in\mathcal{I}}x$ من $\mathcal{I}$.

- نستنتج من النتيجة $i.6$ أنّ $x_{\mathcal{I}}\in\mathcal{I}$ وعليه فإنّ $x_{\mathcal{I}}\mathbb{A}\subset\mathcal{I}$.
- وبالعكس، إذا كان y عنصراً من $\mathcal{I}$، عرّفنا $z=\bigvee\limits_{x\in\mathcal{I}\setminus\{y\}}x$. فيكون $x_{\mathcal{I}}=y\vee z$، ومن ثَمّ

$$\begin{aligned}x_{\mathcal{I}}\cdot y&=y(y\vee z)=y(y+z+yz)\\&=y^2+yz+y^2z=y+yz+yz=y\end{aligned}$$

إذن $y\in x_{\mathcal{I}}\mathbb{A}$، فنكون قد أثبتنا أنّ $\mathcal{I}\subset x_{\mathcal{I}}\mathbb{A}$.

ومنه $\mathcal{I}=x_{\mathcal{I}}\mathbb{A}$.

- وإذا كان y عنصراً من $\mathbb{A}$ يُحقّق $y\le x_{\mathcal{I}}$، كان $y=x_{\mathcal{I}}y\in x_{\mathcal{I}}\mathbb{A}$.
- وبالعكس، إذا كان $y=x_{\mathcal{I}}z$ و z من $\mathbb{A}$، كان $x_{\mathcal{I}}y=(x_{\mathcal{I}})^2z=x_{\mathcal{I}}z=y$ أي $y\le x_{\mathcal{I}}$.

إذن لقد أثبتنا أنّ

$$\mathcal{I}=x_{\mathcal{I}}A=\{y\in\mathbb{A}:y\le x_{\mathcal{I}}\}$$

- لنفترض أنّه يوجد عنصر $\tilde{x}$ في $\mathcal{I}$ يُحقّق $\mathcal{I}=\tilde{x}\mathbb{A}$ نستنتج من المساواة $x_{\mathcal{I}}\mathbb{A}=\tilde{x}\mathbb{A}$، بعد ملاحظة أنّ $1\in\mathbb{A}$، أنّه يوجد عنصران a و a' في $\mathbb{A}$ يُحقّقان $x_{\mathcal{I}}=\tilde{x}a$، و $\tilde{x}\le x_{\mathcal{I}}$.

نستنتج من $x_{\mathcal{I}}=\tilde{x}a$ أنّ

$$\tilde{x}x_{\mathcal{I}}=(\tilde{x})^2a=\tilde{x}a=x_{\mathcal{I}}$$

ومن ثَمّ $x_{\mathcal{I}}\le\tilde{x}$. ومنه $x_{\mathcal{I}}=\tilde{x}$. فالعنصر $x_{\mathcal{I}}$ هو العنصر الوحيد في $\mathcal{I}$ الذي يُحقّق

$$\mathcal{I}=x_{\mathcal{I}}\mathbb{A}=\left\{y\in\mathbb{A}:y\le x_{\mathcal{I}}\right\}$$

.6iii ليكن $\mathcal{I}$ مثالياً في $\mathbb{A}$ يُحقّق $\mathcal{I} \neq \{0\}$. مهما يكن x من $\mathcal{I}\setminus\{0\}$، يكن $\{0,x\} \subset x\mathbb{A}$ ومن ثمّ $\operatorname{card}(x\mathbb{A}) \geq 2$. إذن مجموعة الأعداد الطبيعيّة الآتية

$$\{\operatorname{card}(x\mathbb{A}) : x \in \mathcal{I}\setminus\{0\}\}$$

محدودة من الأدنى بالعدد 2، فإذا عرّفنا $\alpha = \min\{\operatorname{card}(x\mathbb{A}) : x \in \mathcal{I}\setminus\{0\}\}$ كان $\alpha \geq 2$.

ليكن x_0 عنصراً من $\mathcal{I}\setminus\{0\}$ يُحقِّق $\alpha = \operatorname{card}(x_0\mathbb{A})$، ولنفترض أنّ $x_0\mathbb{A} \neq \{0,x_0\}$. إذن يوجد عنصرٌ x_1 ينتمي إلى $x_0\mathbb{A}\setminus\{0,x_0\}$.

لمّا كان $x_0\mathbb{A} = \{y \in \mathbb{A} : y \leq x_0\}$ استنتجنا أنّ $x_1 \leq x_0$ ومن ثَمّ $x_1\mathbb{A} \subset x_0\mathbb{A}$. ولأنّ $x_0 \in \mathcal{I}$ كان $x_0\mathbb{A} \subset \mathcal{I}$ إذن $x_1 \in \mathcal{I}\setminus\{0\}$، وبناءً على تعريف α، نستنتج أنّ $\alpha \leq \operatorname{card}(x_1\mathbb{A})$، أو $\operatorname{card}(x_0\mathbb{A}) \leq \operatorname{card}(x_1\mathbb{A})$، فإذا تذكّرنا أنّ $x_1\mathbb{A} \subset x_0\mathbb{A}$ استنتجنا أنّ $x_1\mathbb{A} = x_0\mathbb{A}$. ولكنّ هذا يقتضي أن يكون $x_1 = x_0$ مما يناقض كون x_1 ينتمي إلى $x_0\mathbb{A}\setminus\{0,x_0\}$. إذن يجب أن يكون $x_0\mathbb{A} = \{0,x_0\}$ ومن ثَمّ $\alpha = 2$، فيوجد عنصرٌ x_0 من $\mathcal{I}$ يُحقِّق $\operatorname{card}(x_0\mathbb{A}) = 2$.

.6iv لنفترض أنّ $\operatorname{card}(\mathbb{A}) \geq 2$ تجنّباً للحالة التافهة. ولنعرّف المجموعة

$$E = \{x \in \mathbb{A} : \operatorname{card}(x\mathbb{A}) = 2\}$$

- إنّ $\mathbb{A}$ نفسها مثالي غير تافه في $\mathbb{A}$، إذن، استناداً إلى نتيجة السؤال السابق، يوجد x في $\mathbb{A}$ يُحقّق $\operatorname{card}(x\mathbb{A}) = 2$ وهذا يُثبت أنّ $E \neq \varnothing$.
- إذا كان x عنصراً من E كان $x \neq 0$ وضوحاً.
- ليكن x و y عنصرين من E، ولنفترض أنّ $x \neq y$ عندئذ يكون

$$xy \in x\mathbb{A} \cap y\mathbb{A} = \{0,x\} \cap \{0,y\} = \{0\}$$

أي $xy = 0$.

- ليكن $z = \sum_{x\in E} x$، ولنفترض أنّ $z \neq 1$. عندئذ يكون $z + 1 \neq 0$، فنعرّف في $\mathbb{A}$ المثالي غير التافه $\mathcal{I} = (1+z)\mathbb{A}$. لمّا كان $\mathcal{I}$ مثاليّاً مختلفاً عن $\{0\}$ استنتجنا بناءً على نتيجة السؤال .6iii أنّه يوجد في $\mathcal{I}$ عنصرٌ t يُحقِّق $\operatorname{card}(t\mathbb{A}) = 2$، ومن ثَمّ $t \in E$.

ولكن $\mathcal{I}=(1+z)\mathbb{A}$ إذن $t\le 1+z$ أو $t=t(1+z)=t+tz$ أي $tz=0$، فإذا وضعنا $z'=\sum_{x\in E\setminus\{t\}} x$ كان لدينا $t(t+z')=0$ وهذا يُكافئ $t^2+tz'=0$ أو $t=0$ بعد الاستفادة من الخاصّة التي أثبتناها سابقاً لنستنتج أنّ $tz'=0$. ولكنّ النتيجة $t=0$ تُناقض المساواة $\mathrm{card}(t\mathbb{A})=2$، وهذا التناقض يبرهن على خطأ الافتراض $z\neq 1$، إذن يجب أن يكون $z=1$، أو $\sum\limits_{x\in E} x=1$.

v.6. لنفترض أنّ $\mathrm{card}(\mathbb{A})\ge 2$ تجنّباً للحالة التافهة. ولنعرّف المجموعة E كما في السؤال السابق، والتطبيق:

$$\varphi : P(E)\to \mathbb{A},\ Z\mapsto \sum_{x\in Z} x$$

مع الاصطلاح $\sum\limits_{x\in\varnothing} x=0$.

- أيّاً كان Z_1 و Z_2 من $P(E)$ كان

$$\begin{aligned}
\varphi(Z_1\Delta Z_2) &= \sum_{x\in Z_1\Delta Z_2} x = \sum_{x\in Z_1\setminus Z_2} x + \sum_{x\in Z_2\setminus Z_1} x\\
&= \sum_{x\in Z_1\setminus Z_2} x + \sum_{x\in Z_1\cap Z_2} x + \sum_{x\in Z_1\cap Z_2} x + \sum_{x\in Z_2\setminus Z_1} x\\
&= \sum_{x\in Z_1} x + \sum_{x\in Z_2} x = \varphi(Z_1)+\varphi(Z_2)
\end{aligned}$$

و

$$\begin{aligned}
\varphi(Z_1)\varphi(Z_2) &= \Big(\sum_{x\in Z_1} x\Big)\Big(\sum_{y\in Z_2} y\Big) = \sum_{(x,y)\in Z_1\times Z_2} xy\\
&= \sum_{\substack{(x,y)\in Z_1\times Z_2\\ x=y}} x^2 + \cancel{\sum_{\substack{(x,y)\in Z_1\times Z_2\\ x\neq y}} xy}\\
&= \sum_{x\in Z_1\cap Z_2} x = \varphi(Z_1\cap Z_2)
\end{aligned}$$

إذ استفدنا من الخاصّة ❷.

- وكذلك فإنّ

$$\varphi(1_{P(E)})=\varphi(E)=\sum_{x\in E} x = 1$$

وذلك بناءً على الخاصّة ❸.

وهكذا نكون قد أثبتنا أنّ φ تشاكلٌ حلقي.

- ليكن Z عنصراً من $\ker\varphi$ ، أي $\varphi(Z)=0$. فإذا افترضنا جدلاً أنّ $Z\neq\varnothing$ وجدنا عنصراً z_0 ينتمي إلى Z . وينتج من كون $\varphi(Z)=0$ أنّ $z_0=\sum_{x\in Z\setminus\{z_0\}} x$ ، وعليه

$$z_0=(z_0)^2=z_0\cdot\sum_{x\in Z\setminus\{z_0\}} x=\sum_{x\in Z\setminus\{z_0\}} z_0x\overset{❷}{=}0$$

وهذا يناقض كون z_0 عنصراً من E . إذن يجب أن يكون $\ker\varphi=\{\varnothing\}$ ، والتشاكل φ متباينٌ.

- ليكن y عنصراً من $\mathbb{A}$ ، ولنعرّف المجموعة $Y=\{x\in E: xy\neq 0\}$. في الحقيقة، في حالة x من E لدينا $xy\in x\mathbb{A}$ أي $xy\in\{0,x\}$ ، ومن ثَمّ

$$Y=\{x\in E: xy=x\}=\{x\in E: x\leq y\}=E\cap y\mathbb{A}$$

ومن ثَمّ

$$\begin{aligned}\varphi(Y)&=\sum_{x\in Y}x=\sum_{x\in Y}xy\\&=\sum_{x\in Y}xy+\sum_{x\in E\setminus Y}xy\\&=\sum_{x\in E}xy=\left(\sum_{x\in E}x\right)y=y\end{aligned}$$

والتطبيق φ غامرٌ. إذن φ تشاكلٌ حَلَقي تقابلي بين $\big(P(E),\Delta,\cap\big)$ و $\mathbb{A}$.

وعليه فإنّ $\operatorname{card}(\mathbb{A})$ يساوي 2^p إذا رمزنا بالرمز p إلى $\operatorname{card}(E)$. ■

التمرين 32. لنزوّد المجموعة $\mathbb{K}=(\mathbb{Z}/5\mathbb{Z})\times(\mathbb{Z}/5\mathbb{Z})$ بالقانونين

$$\begin{bmatrix}a\\b\end{bmatrix}*\begin{bmatrix}a'\\b'\end{bmatrix}=\begin{bmatrix}aa'+2bb'\\ab'+a'b\end{bmatrix},\quad\begin{bmatrix}a\\b\end{bmatrix}+\begin{bmatrix}a'\\b'\end{bmatrix}=\begin{bmatrix}a+a'\\b+b'\end{bmatrix}$$

بيّن أنّ $(\mathbb{K},+,\cdot)$ حقل تبديلي، ما عدد عناصره ؟ هل للمعادلة $x^2=2$ حلول في $\mathbb{Z}/5\mathbb{Z}$ ؟ وهل للمعادلة $x^2=(2,0)$ حلول في $\mathbb{K}$؟

الحل

- من الواضح أنّ $(\mathbb{K},+)$ زمرة تبديليّة حياديها $(0,0)$.
- لنثبت أنّ $(\mathbb{K},\cdot)$ تجميعيّة وتبديليّة وتقبل عنصراً حياديّاً.
  - في حالة (a,b) و (a',b') و (a'',b'') من $\mathbb{K}$، نضع

$$M_1 = \left(\begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} a' \\ b' \end{bmatrix}\right) * \begin{bmatrix} a'' \\ b'' \end{bmatrix} \quad \text{و} \quad M_2 = \begin{bmatrix} a \\ b \end{bmatrix} * \left(\begin{bmatrix} a' \\ b' \end{bmatrix} * \begin{bmatrix} a'' \\ b'' \end{bmatrix}\right)$$

فيكون

$$\begin{aligned} M_1 &= \begin{bmatrix} aa' + 2bb' \\ ab' + ba' \end{bmatrix} * \begin{bmatrix} a'' \\ b'' \end{bmatrix} \\ &= \begin{bmatrix} aa'a'' + 2bb'a'' + 2ab'b'' + 2ba'b'' \\ aa'b'' + 2bb'b'' + ab'a'' + ba'a'' \end{bmatrix} \end{aligned}$$

و

$$\begin{aligned} M_2 &= \begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} a'a'' + 2b'b'' \\ a'b'' + b'a'' \end{bmatrix} \\ &= \begin{bmatrix} aa'a'' + 2ab'b'' + 2ba'b'' + 2bb'a'' \\ aa'b'' + ab'a'' + ba'a'' + 2bb'b'' \end{bmatrix} \end{aligned}$$

إذن $M_1 = M_2$ والقانون $(\cdot)$ تجميعي.

  - في حالة (a,b) و (a',b') من $\mathbb{K}$، نلاحظ مباشرة أنّ

$$\begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} a' \\ b' \end{bmatrix} * \begin{bmatrix} a \\ b \end{bmatrix}$$

فالقانون $(\cdot)$ تبديلي.

  - في حالة (a,b) من $\mathbb{K}$، نلاحظ مباشرة أنّ

$$\begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$$

فالقانون $(\cdot)$ يقبل العنصر $(1,0)$ عنصراً حياديّاً.

- لنثبت أنّ $(\cdot)$ توزيعي على $(+)$. في حالة (a,b) و (a',b') و (a'',b'') من $\mathbb{K}$، نلاحظ أنّ

$$\begin{bmatrix} a \\ b \end{bmatrix} * \left(\begin{bmatrix} a' \\ b' \end{bmatrix} + \begin{bmatrix} a'' \\ b'' \end{bmatrix} \right) = \begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} a' + a'' \\ b' + b'' \end{bmatrix}$$
$$= \begin{bmatrix} aa' + aa'' + 2bb' + 2bb'' \\ ab' + ab'' + ba' + ba'' \end{bmatrix}$$
$$= \begin{bmatrix} aa' + 2bb' \\ ab' + ba' \end{bmatrix} * \begin{bmatrix} aa'' + 2bb'' \\ ab'' + ba'' \end{bmatrix}$$
$$= \begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} a' \\ b' \end{bmatrix} + \begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} a'' \\ b'' \end{bmatrix}$$

وهكذا نكون قد أثبتنا أنّ $(\mathbb{K},+,\cdot)$ حلقة تبديليّة.

بقي أنّ نثبتَ أنّ كلَّ عنصرٍ من $\mathbb{K}^* = \mathbb{K}\backslash\{0\}$ قَلوبٌ. ليكن (a,b) عنصراً من $\mathbb{K}^*$. ولنثبت أنّ $a^2 - 2b^2 \neq 0$.

في الحقيقة، إذا افترضنا أنّ $a^2 - 2b^2 = 0$ لاحظنا ما يأتي:

- في حالة $b = 0$ يكون $a^2 = 0$ في الحقل $\mathbb{Z}/5\mathbb{Z}$، وهذا يقتضي $a = 0$، ويناقض انتماء العنصر (a,b) إلى $\mathbb{K}^*$، أي $(a,b) \neq (0,0)$.
- وفي حالة $b \neq 0$ استنتجنا أنّ b قَلوب في $\mathbb{Z}/5\mathbb{Z}$، ومن ثَمّ نتج من $a^2 - 2b^2 = 0$ أنّ العنصر $x = b^{-1}a$ من $\mathbb{Z}/5\mathbb{Z}$ يُحقّق $x^2 - 2 = 0$ أو $x^2 = 2$ وهذا يناقض الخاصّة التالية :

$$\forall x \in \mathbb{Z}/5\mathbb{Z}, \quad x^2 \in \{0,1,4\}$$

- إذن لقد أثبتنا أنّ

$$\forall (a,b) \in \mathbb{K}^*, \quad a^2 - 2b^2 \neq 0$$

لنعرّف إذن في حالة (a,b) من $\mathbb{K}^*$ العنصر

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = \begin{bmatrix} (a^2 - 2b^2)^{-1}a \\ -(a^2 - 2b^2)^{-1}b \end{bmatrix}$$

عندئذ نتيقّن مباشرة أنّ $(a,b) * (a',b') = (1,0)$، والعنصر (a,b) قلوب في الحلقة $(\mathbb{K},+,\cdot)$ ومقلوبه هو (a',b'). وهكذا نكون قد أثبتنا أنّ الحقل $(\mathbb{K},+,\cdot)$ حقلٌ تبديلي عدد عناصره 25.

ولقد رأينا أنّ المعادلة $x^2 = 2$ لا تقبل حلّاً في $\mathbb{Z}/5\mathbb{Z}$. ولكن نلاحظ مباشرة أنّ

$$\begin{bmatrix}0\\1\end{bmatrix} * \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}2\\0\end{bmatrix} \quad \text{و} \quad \begin{bmatrix}0\\4\end{bmatrix} * \begin{bmatrix}0\\4\end{bmatrix} = \begin{bmatrix}2\\0\end{bmatrix}$$

فللمعادلة $x^2 = (2,0)$ حلّان في الحقل $(\mathbb{K},+,\cdot)$، الذي يحوي الحقل $\mathbb{Z}/5\mathbb{Z}$ حقلاً جزئيّاً.

التمرين 33. لتكن A حلقة تبديلية غير $\{0\}$. نفترض أنّ المثاليات الوحيدة في A هي $\{0\}$ و A . أثبت أنّ A حقل.

الحل

ليكن a عنصراً من $A\backslash\{0\}$. عندئذ يكون المثالي الرئيسي aA مثالياً مختلفاً عن $\{0\}$ فلا بُدَّ أن يساوي A . أي $aA = A$ ومنه $1_A \in aA$ أي يوجد a' في A يُحقِّق $aa' = 1_A$ وهذا ما يُثبت أنّ العنصر a قَلوب. لقد أثبتنا إذن أنّ كلَّ عنصرٍ من $A\backslash\{0\}$ قلوبٌ وهذا يبرهن أنّ A حقل.

③ حلقة الأعداد الصحيحة

التمرين 34. لتكن a و b و c أعداداً صحيحة. أثبت أنّ

$$\gcd(a,b)=1 \Rightarrow \gcd(a,bc)=\gcd(a,c)$$

الحل

لنضع $d=\gcd(a,c)$ و $d'=\gcd(a,bc)$. لما كان d يقسم a و c استنتجنا أنّه قاسم مشترك a و bc إذن $d\mid d'$.

وبالعكس، نستنتج من كون $\gcd(a,b)=1$ أنّ كلّ قاسم للعدد a يكون أوّليّاً مع b، إذن d' يقسم bc وهو أوّلي مع b فلا بُدّ أن يقسم c، وذلك بناءً على توطئة Gauss . وعليه يكون d' قاسماً مشتركاً للعددين a و c، أي $d'\mid d$. بذا نكون قد أثبتنا أنّ $d\mid d'$ و $d'\mid d$ أي $d=d'$ لأنّ d و d' موجبان. ■

التمرين 35. ليكن a و b عددين صحيحين. ولنضع

$$m=\operatorname{lcm}(a,b) \quad \text{و} \quad d=\gcd(a,b)$$

احسب المقدار $\gcd(a+b,m)$.

تطبيق. عيّن a و b إذا علمتَ أنّ $a+b=144$ و $\operatorname{lcm}(a,b)=420$.

الحل

إذا عرّفنا a' و b' بالعلاقتين : $a=da'$ و $b=db'$، كان العددان a' و b' أوليّين فيما بينهما، وينتج من ذلك أنّ كلّاً من a' و b' أوّلي مع $a'+b'$، وهذا بدوره يقتضي أنّ $a'b'$ أوّلي مع $a'+b'$ أي

$$\gcd\left(a'+b',a'b'\right)=1 \qquad (*)$$

ومن ثَمّ يكون لدينا $\gcd\left(da'+db',da'b'\right)=d$، أو

$$\gcd\left(a+b,m\right)=d$$

لأنّ $da'b'=\operatorname{lcm}(a,b)=m$. فنكون قد أثبتنا الخاصّة التالية :

$$\gcd\left(a+b,\operatorname{lcm}(a,b)\right)=\gcd(a,b)$$

ملاحظة. يمكن إثبات $(*)$ بملاحظة أنّ $xa'+yb'=1$ يقتضي

$$(x^2a'+y^2b')(a'+b')-(x-y)^2a'b'=1$$

تطبيق. إذا كان $s=a+b$ و $m=\operatorname{lcm}(a,b)$ كان $d=\gcd(s,m)$، وكان

$$ab=dm=\varepsilon\gcd(s,m)m,\quad \varepsilon\in\{-1,1\}$$

وعليه يكون a و b جذري إحدى المعادلتين

$$X^2-sX-\gcd(s,m)m=0 \quad \text{أو} \quad X^2-sX+\gcd(s,m)m=0$$

وفي الحالة الخاصّة المدروسة تقبل $X^2-144X+12\times 420=0$، الجذرين $\{a,b\}=\{60,84\}$. في حين لا تقبل المعادلة الثانية $X^2-144X-12\times 420=0$ جذوراً صحيحة.

لا حظ أنّه في حالة $s=3$ و $m=18$ لا نجد حلولاً للمعادلة الأولى، ونجد الحلول جذوراً للمعادلة الثانية. وبذا يتم حلّ التمرين. ■

التمرين 36. ليكن d و m عددين من $\mathbb{N}^*$. ما الشرط اللازم والكافي على d و m حتّى نجد عددين طبيعيّين a و b يُحقّقان: $d=\gcd(a,b)$ و $m=\operatorname{lcm}(a,b)$ ؟

تطبيق. حلّ المسألة في حالة $m=600$ و $d=50$.

الحل

- من الواضح أنّ الشرط $d\mid m$ شرطٌ لازمٌ.
- وبالعكس، لنفترض أنّ $d\mid m$. عندئذ نعرّف $a=d$ و $b=m$ فيتحقّق وضوحاً الشرطان:

$$d=\gcd(a,b) \text{ و } m=\operatorname{lcm}(a,b)$$

إذن الشرط اللازم والكافي على d و m لنجد عددين طبيعيَّين a و b يُحقّقان $d=\gcd(a,b)$ و $m=\operatorname{lcm}(a,b)$ هو $d\mid m$.

في الحقيقة، لنفترض أنّ $m=dm'$، وليكن (a,b) حلّاً للمسألة، عندئذ يكون العددان a' و b' المعرّفين بالعلاقتين: $a=da'$ و $b=db'$، أوليّين فيما بينهما، ويكون $a'b'=m'$.

وبالعكس، إذا كان $\gcd(a',b')=1$ و $a'b'=m'$. وعرّفنا $a=da'$ و $b=db'$، كان

$$d=\gcd(a,b) \quad \text{و} \quad m=\operatorname{lcm}(a,b)$$

إذن تُعطى الحلول بالعلاقة

$$\{a,b\} \in \{\{da',db'\} : a'b' = m', \quad \gcd(a',b') = 1\}$$

وفي الحالة الخاصّة $m = 600$ و $d = 50$ لدينا $m' = 12$، ومن ثَمّ

$$\{\{a',b'\} : a'b' = m', \quad \gcd(a',b') = 1\} = \{\{1,12\},\{3,4\}\}$$

فمجموعة الحلول هي

$$\{a,b\} \in \{\{50,600\},\{150,200\}\}$$

وهو المطلوب.

التمرين 37. أوجد جميع الثنائيّات (x,y) من $\mathbb{Z}^2$ التي تُحقّق :

$$\operatorname{lcm}(x,y) + 11\gcd(x,y) = 203$$

الحل

لنفترض أنّ (x,y) حلٌّ للمعادلة المعطاة، نعرّف $d = \gcd(x,y)$. عندئذ يمكن أن نكتب $|x| = dx'$ و $|y| = dy'$ والعددان x' و y' أوّليّان فيما بينهما. فتأخذ المعادلة المعطاة الصيغة $d(x'y' + 11) = 203$. وعليه فالعدد d يقسم $203 = 7 \times 29$، ولأنّ $x'y' + 11 \geq 11$ نستنتج أنّ $d \leq \frac{203}{11}$، فلا بُدّ أن يكون $d = 1$ أو $d = 7$.

- في حالة $d = 7$ يكون لدينا $x'y' = 18$ ومن ثَمّ $\{x',y'\} \in \{\{1,18\},\{2,9\}\}$، وهذا يُعطي الحلول $\{x,y\}$ المعرّفة بالعلاقة :
$$\{|x|,|y|\} \in \{\{7,126\},\{14,63\}\}.$$
- وفي حالة $d = 1$ لدينا $x'y' = 192$ ومن ثَمّ $\{x',y'\} \in \{\{1,192\},\{3,64\}\}$، وهذا يُعطي الحلول $\{x,y\}$ المعرّفة بالعلاقة :
$$\{|x|,|y|\} \in \{\{1,192\},\{3,64\}\}.$$

إذن $\operatorname{lcm}(x,y) + 11\gcd(x,y) = 203$ إذا وفقط إذا كان

$$\{|x|,|y|\} \in \{\{1,192\},\{3,64\},\{7,126\},\{14,63\}\}$$

وهي النتيجة المطلوبة.

التمرين 38. أوجد جميع الثنائيّات (x,y) من $\mathbb{Z}^2$ التي تُحقّق :

$$\begin{cases} x^2+y^2 = 85113 \\ \operatorname{lcm}(x,y) = 1764 \end{cases}$$

الحل

لنفترض أنّ (x,y) حلٌ للجملة المعطاة، ولنضع $d=\gcd(x,y)$. نعرّف عندئذ العددين x' و y' بالعلاقتين $|x|=dx'$ و $|y|=dy'$، فيكون x' و y' أوّليّان فيما بينهما. وعلى هذا تُكتب الجملة بالصيغة المُكافئة

$$\begin{cases} d^2(x'^2+y'^2) = 3^2 7^2 193 \\ dx'y' = 2^2 3^2 7^2 \end{cases}$$

- نلاحظ أوّلاً أنّ العدد الأولي $d \nmid 193$ وإلاّ كان $(193)^2$ قاسماً للعدد $d^2(x'^2+y'^2)$ وهذا خُلفٌ. إذن $\gcd(193,d^2)=1$ وينتج من المساواة الأولى أنّ $193 \mid (x'^2+y'^2)$.
- لمّا كان $\gcd(x',y')=1$ كان $\gcd(x',y'^2)=1$ و $\gcd(y',x'^2)=1$ ومن ثَمّ
$$\gcd(x',y'^2+x'^2)=1 \quad \text{و} \quad \gcd(y',x'^2+y'^2)=1$$
وهذا يقتضي أنّ $\gcd(x'y',y'^2+x'^2)=1$.
- ليكن k عنصراً من $\{3,7\}$. عندئذ إذا افترضنا أنّ $k \nmid d$ استنتجنا من المعادلة الثانية، لأنّ k أوّلي، أنّ $k \mid x'y'$. وهذا يقتضي أنّ $k \nmid (x'^2+y'^2)$ لأنّ
$$\gcd(x'y',y'^2+x'^2)=1$$
ولكن بالعودة إلى المعادلة الأولى نجد أنّ k يقسم $d^2(x'^2+y'^2)$ وهو أوّلي مع $x'^2+y'^2$، إذن $k \mid d^2$، فهو يقسم d وهذا خُلفٌ واضحٌ. نستنتج إذن أنّ $3 \mid d$ و $7 \mid d$. فيوجد عددٌ δ يُحقّق $d=21\delta$.
- وبالعودة إلى المعادلة الأولى نستنتج أنّ $\delta^2(x'^2+y'^2)=193$ ولأنّ $193 \mid (x'^2+y'^2)$ نجد بالضرورة أنّ $\delta=1$، (إذن $d=21$) و $x'^2+y'^2=193$.

وتأخذ الجملة الصيغة التالية :

$$\begin{cases} x'^2 + y'^2 = 193 \\ x'y' = 2^2 \times 3 \times 7 = 84 \end{cases}$$

فإذا جمعنا إلى الأولى ضعفي الثانية، وتذكّرنا أنّ x' و y' موجبان، استنتجنا أنّ هذه الجملة تُكافئ

$$\begin{cases} x' + y' = 19 \\ x'y' = 84 \end{cases}$$

أي $\{x', y'\} = \{7, 12\}$.

- وأخيراً نستنتج أنّ

$$\{x, y\} \in \Big\{\{147, 252\}, \{-147, 252\}, \{147, -252\}, \{-147, -252\}\Big\}$$

أمّا تَيَقُّن كون جميع هذه القيم حلولاً فهو تحقُّق مباشر نتركه للقارئ. ■

التمرين 39. أوجد جميع الثنائيّات (x, y) من $\mathbb{Z}^2$ التي تُحقّق :

$$\begin{cases} \operatorname{lcm}(x, y) = 210 \gcd(x, y) \\ y - x = \gcd(x, y) \end{cases}$$

الحل

لنفترض أنّ (x, y) حلٌ للجملة المعطاة مختلفٌ عن $(0, 0)$. ولنضع $d = \gcd(x, y)$. نعرّف عندئذ العددين x' و y' بالعلاقات : $|x| = dx'$ و $|y| = dy'$، فيكون x' و y' أوّليّان فيما بينهما. وعلى هذا تُكتب الجملة بالصيغة المُكافئة

$$\begin{cases} x'y' = 210 \\ \alpha y' - \beta x' = 1 \end{cases}$$

وقد عرّفنا $\alpha = \operatorname{sgn}(y)$ و $\beta = \operatorname{sgn}(x)$. وهنا نناقش الحالات المختلفة التالية :

- إذا افترضنا أنّ $\alpha\beta < 0$ كان $y' + x' = \alpha$ بناءً على المعادلة الثانية، وهذا تناقضٌ لأنّ x' و y' ينتميان إلى $\mathbb{N}^*$. فلا بُدّ أن يكون $\alpha\beta > 0$.
- في حالة $\alpha = \beta = 1$ تُكتب الجملة بالصيغة المُكافئة

$$\begin{cases} x'^2 + x' = 210 \\ y' = x' + 1 \end{cases}$$

وهذا يقتضي $(x',y')=(14,15)$. أي $(x,y)\in\left\{(14k,15k):k\in\mathbb{N}^*\right\}$.

- وفي حالة $\alpha=\beta=-1$ تُكتب الجملة بالصيغة المُكافئة

$$\begin{cases} y'^2+y'=210 \\ x'=y'+1 \end{cases}$$

وهذا يقتضي $(x',y')=(15,14)$. أي $(x,y)\in\left\{(-15k,-14k):k\in\mathbb{N}^*\right\}$.

وهكذا نكون قد أثبتنا أنّ كلّ حلٍّ للمسألة ينتمي إلى المجموعة

$$\mathcal{S}=\left\{(-15k,-14k):k\in\mathbb{N}^*\right\}\cup\left\{(0,0)\right\}\cup\left\{(14k,15k):k\in\mathbb{N}^*\right\}$$

ونتيقّن بسهولة مباشرة أنّ كلّ عنصرٍ من $\mathcal{S}$ هو حلٌّ للجملة المدروسة. فيتم الإثبات. ■

التمرين 40. أثبت صحة التكافؤ

$$\gcd(n^3+n,2n+1)=1\Leftrightarrow n-2\notin 5\mathbb{Z}$$

الحل

بملاحظة أنّ $\gcd(2n+1,m)=\gcd(2n+1,2m)$ يمكننا أن نكتب

$$\begin{aligned}\gcd\left(n^3+n,2n+1\right)&=\gcd\left(2n^3+2n,2n+1\right)\\&=\gcd\left(2n^3+2n-n^2(2n+1),2n+1\right)\\&=\gcd\left(-n^2+2n,2n+1\right)=\gcd\left(-2n^2+4n,2n+1\right)\\&=\gcd\left(-2n^2+4n+n(2n+1),2n+1\right)\\&=\gcd\left(5n,2n+1\right)=\gcd\left(5n-2(2n+1),2n+1\right)\\&=\gcd\left(n-2,2n+1\right)=\gcd\left(n-2,2n+1-2(n-2)\right)\\&=\gcd\left(n-2,5\right)\end{aligned}$$

إذن

$$\gcd(n^3+n,2n+1)=\gcd(n-2,5)$$

ولأنّ العدد 5 عددٌ أوّلي استنتجنا أنّ

$$\gcd(n^3+n,2n+1)=1\Leftrightarrow 5\nmid(n-2)\Leftrightarrow n\neq 2\bmod 5$$

وهي النتيجة المرجوّة. ■

التمرين 41. أثبت أنّ

$$\forall n \in \mathbb{Z},\quad \gcd(15n^2+8n+6, 30n^2+21n+13)=1$$

الحل

سنستفيد من الخاصّة المهمّة التالية :

$$\forall (a,b,\lambda)\in\mathbb{Z}^3,\quad \gcd(a,b)=\gcd(a-\lambda b, b)$$

ليكن n من $\mathbb{Z}$، ولنضع $d=\gcd(15n^2+8n+6, 30n^2+21n+13)$، عندئذ

$$\begin{aligned} d &= \gcd\left(15n^2+8n+6, 30n^2+21n+13-2(15n^2+8n+6)\right)\\ &= \gcd\left(15n^2+8n+6, 5n+1\right)\\ &= \gcd\left(15n^2+8n+6-3n(5n+1), 5n+1\right)\\ &= \gcd\left(5n+6, 5n+1\right)=\gcd\left(5n+6-(5n+1), 5n+1\right)\\ &= \gcd\left(5, 5n+1\right)=\gcd\left(5, 5n+1-5n\right)=\gcd(5,1)=1\end{aligned}$$

وهي النتيجة المرجوّة. ■

التمرين 42. نعرّف العددين الطبيعيين a_n و b_n، أياً كان n من $\mathbb{N}$ بالعلاقة

$$a_n+\sqrt{2}\,b_n=(1+\sqrt{2})^n$$

أثبت أنّ $\gcd(a_n, b_n)=1$.

الحل

في الحقيقة، نعلم أنّ

$$\begin{aligned}\left(1+\sqrt{2}\right)^n &= \sum_{k=0}^{n} C_n^k\left(\sqrt{2}\right)^k\\ &= \sum_{0\le 2k\le n} C_n^{2k}\left(\sqrt{2}\right)^{2k}+\sqrt{2}\sum_{0\le 2k+1\le n} C_n^{2k+1}\left(\sqrt{2}\right)^{2k}\\ &= \sum_{0\le 2k\le n} C_n^{2k}2^k+\sqrt{2}\sum_{0\le 2k+1\le n} C_n^{2k+1}2^k\end{aligned}$$

إذن

$$b_n=\sum_{0\le 2k+1\le n} C_n^{2k+1}2^k \quad \text{و} \quad a_n=\sum_{0\le 2k\le n} C_n^{2k}2^k$$

نستنتج إذن أنّه لدينا أيضاً $a_n-\sqrt{2}\,b_n=(1-\sqrt{2})^n$.

وعليه

$$a_n^2 - 2b_n^2 = \left((1-\sqrt{2})(1+\sqrt{2})\right)^n = (-1)^n$$

ومن ثَمّ يوجد عددان $x = (-1)^n a_n$ و $y = -2(-1)^n b_n$ يُحقّقان $xa_n + yb_n = 1$ ، وهذا يثبتُ، استناداً إلى مبرهنة Bézout ، أنّ a_n و b_n أوّليان فيما بينهما. وهي النتيجة المطلوبة. ■

التمرين 43. لتكن (a,b,c) من $\mathbb{N}^{*3}$ مع $a \geq 2$. نعرّف العددين

$$\operatorname{lcm}(b,c) = m \quad \text{و} \quad \gcd(b,c) = d$$

أثبت أنّ $\gcd(a^b - 1, a^c - 1) = a^d - 1$ ، ثُمّ أثبت أنّ $(a^b - 1)(a^c - 1)$ يقسم $(a^d - 1)(a^m - 1)$.

الحل

يمكننا دون الإخلال بعموميّة الحلّ أن نفترض أنّ $b \geq c$ و $a > 1$. نعرّف المتتالية $(R_n)_{n\in\mathbb{N}}$ كما يلي: $R_0 = b$ و $R_1 = c$ ، وإذا كان $R_n = 0$ كان $R_{n+1} = 0$ ، أمّا في حالة $R_n \neq 0$ ، فنعرّف R_{n+1} بأنّه باقي قسمة R_{n-1} على R_n . فإذا عرّفنا

$$N = \min\left\{k \in \mathbb{N} : R_{k+1} = 0\right\}$$

كان $d = R_N$.

لنفترض أنّ $1 \leq k \leq N$ ، عندئذ يكون لدينا $R_{k-1} = Q_k R_k + R_{k+1}$ ومن ثَمّ

$$\begin{aligned} a^{R_{k-1}} - 1 &= a^{Q_k R_k + R_{k+1}} - 1 = a^{Q_k R_k} a^{R_{k+1}} - 1 \\ &= (a^{Q_k R_k} - 1)a^{R_{k+1}} + a^{R_{k+1}} - 1 \\ &= (a^{R_k} - 1)S_k + a^{R_{k+1}} - 1 \end{aligned}$$

وقد عرّفنا

$$S_k = a^{R_{k+1}}\left(\frac{a^{Q_k R_k} - 1}{a^{R_k} - 1}\right) = a^{R_{k+1}} \sum_{p=0}^{Q_k - 1} a^{pR_k}$$

وهو عدد طبيعي.

نستنتج مما سبق أنّه في حالة $1 \le k \le N$، لدينا

$$\gcd(a^{R_{k-1}}-1, a^{R_k}-1) = \gcd(a^{R_k}-1, a^{R_{k+1}}-1)$$

فالمقادير $\left(\gcd(a^{R_{k-1}}-1, a^{R_k}-1)\right)_{1\le k\le N+1}$ متساوية. نستنتج إذن أنّ

$$\begin{aligned}\gcd(a^b-1, a^c-1) &= \gcd(a^{R_0}-1, a^{R_1}-1)\\ &= \gcd(a^{R_N}-1, a^{R_{N+1}}-1) = a^d-1\end{aligned}$$

ومن جهة أخرى، لمّا كان $b \mid m$ و $c \mid m$ استنتجنا أنّ

$$(a^b-1) \mid (a^m-1) \quad \text{و} \quad (a^c-1) \mid (a^m-1)$$

إذن

$$\operatorname{lcm}(a^c-1, a^b-1) \mid (a^m-1)$$

وعليه يقسم $\gcd(a^c-1, a^b-1)\operatorname{lcm}(a^c-1, a^b-1)$ العددَ $(a^d-1)(a^m-1)$.
فإذا تذكّرنا أنّ $\gcd(a^c-1, a^b-1)\operatorname{lcm}(a^c-1, a^b-1) = (a^c-1)(a^b-1)$ استنتجنا أنّ

$$(a^c-1)(a^b-1) \mid (a^d-1)(a^m-1)$$

وهو المطلوب. ■

التمرين 44. أثبت أنه، أياً كان n من $\mathbb{N}$، يقسم العددُ 7 كلّاً من

$$2^{2^{2n}}-2 \quad \text{و} \quad 2^{2^{2n+1}}-4 \quad \text{و} \quad 4^{2^{2n}}+2^{2^{2n}}+1$$

الحل

- لنضع $a_n = 2^{2^{2n}}-2$، فنلاحظ أنّ

$$\begin{aligned}a_{n+1} &= 2^{4\times 2^{2n}}-2 = (2^{2^{2n}})^4-2 = (a_n+2)^4-2\\ &= a_n^4+8a_n^3+24a_n^2+32a_n+14\\ &= Q_na_n+14 : \qquad ☞\ Q_n = a_n^3+8a_n^2+24a_n+32\end{aligned}$$

لتكن $\mathbb{P}_n$ القضيّة $7 \mid a_n$، نلاحظ أنّ $\mathbb{P}_0$ صحيحة وضوحاً. ونستنتج من المساواة $a_{n+1} = Q_na_n+14$ أنّ $\mathbb{P}_n \Rightarrow \mathbb{P}_{n+1}$. إذن لقد أثبتنا بالتدريج على n أنّ $\mathbb{P}_n$ صحيحة أيّاً كانت n من $\mathbb{N}$.

أي

$$\forall n \in \mathbb{N}, \quad 7 \mid (2^{2^{2n}} - 2)$$

▫ لنضع أيضاً $b_n = 2^{2^{2n+1}} - 4$ ، فنلاحظ أنّ

$$\begin{aligned} b_n &= 2^{2\times 2^{2n}} - 4 = (2^{2^{2n}})^2 - 4 \\ &= (a_n + 2)^2 - 4 = a_n(a_n + 4) \end{aligned}$$

ولمّا كان $7 \mid a_n$ استنتجنا من المساواة السابقة أنّ $7 \mid b_n$ ، أي $\forall n \in \mathbb{N}, \quad 7 \mid (2^{2^{2n+1}} - 4)$.

▫ لنضع أخيراً $c_n = 4^{2^{2n}} + 2^{2^{2n}} + 1$ ، فنلاحظ أنّ

$$\begin{aligned} c_n &= 2^{2^{2n+1}} + 2^{2^{2n}} + 1 \\ &= b_n + 4 + a_n + 2 + 1 \\ &= b_n + a_n + 7 \end{aligned}$$

ولمّا كان $7 \mid a_n$ و $7 \mid b_n$ ، استنتجنا من المساواة السابقة أنّ $7 \mid c_n$ ، أي

$$\forall n \in \mathbb{N}, \quad 7 \mid (4^{2^{2n}} + 2^{2^{2n}} + 1)$$

■

التمرين 45. أثبت أنّه، أيّاً كان n من $\mathbb{N}$ ، لا يقسم العددُ 121 المقدارَ $n^2 + 3n + 5$.

الحل

لنفترض أنّه يوجد n في $\mathbb{Z}$ يُحقّق $11 \mid (n^2 + 3n + 5)$. عندئذ هذا يُكافئ

$$n^2 + 3n + 5 = 0 \bmod 11$$

ولأنّ $3 = -8 \bmod 11$ و $5 = 16 \bmod 11$ استنتجنا أنّ المعادلة السابقة تُكافئ

$$n^2 - 8n + 16 = 0 \bmod 11$$

ولكن $n^2 - 8n + 16 = (n-4)^2$ ، فهي إذن تُكافئ

$$(n-4)^2 = 0 \bmod 11$$

ولأنّ $\mathbb{Z}/11\mathbb{Z}$ حقل استنتجنا أنّ $n - 4 = 0 \bmod 11$ أو $n = 4 \bmod 11$. وهكذا نجد

$$11 \mid (n^2 + 3n + 5) \Leftrightarrow \exists k \in \mathbb{Z}, \;\; n = 4 + 11k$$

لنفترض أنّ 121 يقسم n^2+3n+5، عندئذ 11 يقسم n^2+3n+5، فيوجد k في $\mathbb{Z}$ يُحقّق المساواة $n=4+11k$، ولكن في هذه الحالة لدينا

$$\begin{aligned} n^2+3n+5 &= 16+88k+121k^2+12+33k+5 \\ &= 33+121k(k+1) \end{aligned}$$

إذن لا بُدّ أن يقسم العددُ 121 العددَ 33 وهذا خُلفٌ. إذن

$$\forall n \in \mathbb{Z}, \quad 121 \nmid (n^2+3n+5)$$

وهو المطلوب إثباته.

التمرين 46. ليكن العددان $a=58\,483$ و $b=60\,809$.

1. احسب $d=\gcd(a,b)$.
2. عيّن عددين (s,t) من $\mathbb{N}^2$ يُحقّقان $s\,b-t\,a=d$.

الحل

نطبّق خوارزميّة إقليدس المعمّمة، ونبيّن النتائج في الجدول التالي :

k	R_k	Q_k	S_k	T_k
0	60 809	–	1	0
1	58 483	1	0	1
2	2 326	25	1	−1
3	333	6	−25	26
4	328	1	151	−157
5	5	65	−176	183
6	3	1	11 591	−12 052
7	2	1	−11 767	12 235
8	1		23 358	−24 287

وعليه فإنّ

$$\gcd(60809, 58483)=1$$

وإذا وضعنا $s=23358$ و $t=24287$ كان $sb-ta=1$. وهي النتيجة المرجوّة.

التمرين 47. أوجد أصغر عدد طبيعي n من $\mathbb{N}^*$، بحيث يوجد (a,b,c) في $\mathbb{N}^{*3}$ تُحقّق الشروط $n = 2a^2$ و $n = 3b^3$ و $n = 5c^5$.

الحل

بالاستفادة من المبرهة الأساسيّة في الحساب، نكتب $n = 2^\alpha 3^\beta 5^\gamma \prod_{p\in\mathcal{P}^*} p^{\nu_p}$ حيث عرّفنا $\mathcal{P}^* = \mathcal{P}\backslash\{2,3,5\}$.

- يُكافئ وجود a من $\mathbb{N}^*$ يُحقّق $n = 2a^2$ أنّ $\alpha = 1 \bmod 2$ و $\beta = 0 \bmod 2$ و $\gamma = 0 \bmod 2$ و $\nu_p = 0 \bmod 2$ عندما p من $\mathcal{P}^*$.
- يُكافئ وجود b من $\mathbb{N}^*$ يُحقّق $n = 3b^3$ أنّ $\alpha = 0 \bmod 3$ و $\beta = 1 \bmod 3$ و $\gamma = 0 \bmod 3$ و $\nu_p = 0 \bmod 3$ في حالة p من $\mathcal{P}^*$.
- يُكافئ وجود c من $\mathbb{N}^*$ يُحقّق $n = 5b^5$ أنّ $\alpha = 0 \bmod 5$ و $\beta = 0 \bmod 5$ و $\gamma = 1 \bmod 5$ و $\nu_p = 0 \bmod 5$ في حالة p من $\mathcal{P}^*$.

إذن تتحقَّق الشروط الثلاثة إذا وفقط إذا كان

$$\begin{array}{lll} \alpha = 1 \bmod 2 & \alpha = 0 \bmod 3 & \alpha = 0 \bmod 5 \\ \beta = 0 \bmod 2 & \beta = 1 \bmod 3 & \beta = 0 \bmod 5 \\ \gamma = 0 \bmod 2 & \gamma = 0 \bmod 3 & \gamma = 1 \bmod 5 \\ \forall p \in \mathcal{P}^*, & \nu_p = 0 \bmod 30 & \end{array}$$

الشروط على α تعني أنّ α مضاعف فردي للعدد 15 أي إنّ $\alpha = 15 + 30\alpha'$.
الشروط على β تعني أنّ β مضاعف للعدد 10 يساوي 1 بالقياس 3 أي $\beta = 10 + 30\beta'$.
الشروط على γ تعني أنّ γ مضاعف للعدد 6 يساوي 1 بالقياس 5 أي $\gamma = 6 + 30\gamma'$.
وهكذا نستنتج أنّ n يُحقّق الشرط المطلوب إذا وفقط إذا كان $n = 2^{15}3^{10}5^6 K^{30}$ و K عددٌ من $\mathbb{N}^*$ أوّلي مع 30. إذن أصغر عدد n من $\mathbb{N}^*$ يُحقّق المطلوب هو

$$n = 2^{15}3^{10}5^6 = 30\ 233\ 088\ 000\ 000$$

وهي النتيجة المطلوبة.

التمرين 48. لتكن a و b و c أعداداً صحيحة. ولنتأمّل في $\mathbb{Z}^2$ المعادلة

$$ax + by = c \qquad \mathcal{E}$$

1. أعطِ شرطاً لازماً وكافياً كي تقبل هذه المعادلة حلولاً.
2. ليكن $d = \gcd(a,b)$، وليكن (x_0, y_0) زوجاً يُحقّق $ax_0 + by_0 = d$. أوجد جميع حلول المعادلة $\mathcal{E}$ بدلالة a و b و c و d و x_0 و y_0.
3. حلّ في $\mathbb{Z}^2$ المعادلة :

$$252x - 396y = 648$$

الحل

1. في الحقيقة، ليكن $d = \gcd(a,b)$ عندئذ

$$\begin{aligned}\exists(x,y) \in \mathbb{Z}^2, c = ax + by \quad &\Leftrightarrow c \in (a\mathbb{Z} + b\mathbb{Z})\\ &\Leftrightarrow c \in d\mathbb{Z}\\ &\Leftrightarrow d \mid c\end{aligned}$$

فالشرط اللازم والكافي كي تقبل المعادلة $ax + by = c$ حلولاً هو أن يكون c مُضاعفاً للعدد $\gcd(a,b)$.

2. لنفترض أنّ $d \mid c$، ولنرمز بالرمز $\mathcal{S}$ إلى مجموعة الثنائيّات (x,y) التي تُحقّق المعادلة $ax + by = c$. سنفترض أنّ $(a,b) \neq (0,0)$ وإلاّ كان $c = 0$ و $\mathcal{S} = \mathbb{Z}^2$. نعرّف عندئذ الأعداد a' و b' و c' بالعلاقات $a = da'$ و $b = db'$ و $c = dc'$، وعندئذ يكون لدينا $a'x_0 + b'y_0 = 1$. إذا كان $(x,y) \in \mathcal{S}$ كان $a'x + b'y = c'$ ونتج من ذلك أنّ

$$a'x + b'y = c'(a'x_0 + b'y_0)$$

وهذا يُكافئ

$$a'(x - c'x_0) = b'(c'y_0 - y)$$

إذن a' يقسم $b'(c'y_0 - y)$ وهو أوّلي مع b'، فلا بُدّ أن يقسم a' المقدار $(c'y_0 - y)$. وعليه يوجد k في $\mathbb{Z}$ يُحقّق $c'y_0 - y = ka'$ أو $y = c'y_0 - ka'$. وهذا يقتضي أن يكون أيضاً $x = c'x_0 + kb'$. أي إنّ

$$(x,y) \in \left\{\left(\frac{cx_0 + kb}{d}, \frac{cy_0 - ka}{d}\right), \quad k \in \mathbb{Z}\right\}$$

وبالعكس، نتيقَّن مباشرة أنّ كلَّ عنصر من المجموعة السابقة يُحقِّق المعادلة $\mathcal{E}$. إذن نلخِّص النتيجة السابقة كما يأتي:

لتكن a و b و c أعداداً صحيحة. ولنرمز بالرمز $\mathcal{S}$ إلى مجموعة الثنائيّات (x,y) التي تُحقِّق $ax+by=c$. عندئذ :

- في حالة $c \nmid \gcd(a,b)$ يكون $\mathcal{S}=\varnothing$.
- في حالة $(a,b,c)=(0,0,0)$ يكون $\mathcal{S}=\mathbb{Z}^2$.
- في حالة $(a,b)\neq(0,0)$ و $\gcd(a,b)\mid c$ يكون

$$\mathcal{S}=\left\{\left(\frac{cx_0+kb}{d},\frac{cy_0-ka}{d}\right):k\in\mathbb{Z}\right\}$$

حيث (x_0,y_0) زوج يُحقِّق $ax_0+by_0=d$.

3. لحلِّ المعادلة $252x-396y=648$ في $\mathbb{Z}^2$ ، نلاحظ بالقسمة على العدد 36 أنّها تُكافئ المعادلة $7x-11y=18$ ، وهذه الأخيرة تقبل الحلّ الخاصّ $(x,y)=(1,-1)$ ، إذن تُكافئ المعادلةُ المدروسة المعادلة $7(x-1)=11(y+1)$ ، فيوجد k في $\mathbb{Z}$ يُحقّق

$$x=1+11k \quad \text{و} \quad y=-1+7k$$

ومجموعة الحلول هي

$$\mathcal{S}=\left\{(1+11k,-1+7k):k\in\mathbb{Z}\right\}.$$ ■

التمرين 49. حلّ في مجموعة الأعداد الصحيحة كلاً من المعادلات التالية :

❶ $95x+71y=46$

❷ $20x-53y=3$

❸ $12x+15y+20z=7$

الحل

❶ في الحقيقة، نلاحظ أنّ $3\times95-4\times71=1$ وعلى هذا يكون

$$\begin{aligned}\left(95x+71y=46\right)&\Leftrightarrow\left(95x+71y=46(3\times95-4\times71)\right)\\&\Leftrightarrow\left(95(x-46\times3)+71(y+4\times46)=0\right)\end{aligned}$$

ولأنّ $\gcd(95,71)=1$ نستنتج من المعادلة الأخيرة أنّه يوجد k في $\mathbb{Z}$ يُحقّق

$$\begin{aligned} x &= 46\times 3 - 71k & &= 138-142-71(k-2) & &= -4-71n \\ y &= -4\times 46+95k & &= 190-184+95(k-2) & &= 6+95n \end{aligned}$$

إذن

$$\big(95x+71y=46\big) \Leftrightarrow \Big((x,y)\in\big\{(-4+71k,6-95k) : k\in\mathbb{Z}\big\}\Big)$$

❷ نلاحظ أنّ $8\times 20-3\times 53=1$ وعلى هذا يكون

$$\begin{aligned} \big(20x-53y=3\big) &\Leftrightarrow \big(20x-53y=3(8\times 20-3\times 53)\big) \\ &\Leftrightarrow \big(20(x-24)=53(y-9)\big) \end{aligned}$$

ولأنّ $\gcd(20,53)=1$ نستنتج من المعادلة الأخيرة أنّه يوجد k في $\mathbb{Z}$ يُحقّق

$$\begin{aligned} x &= 24+53k \\ y &= 9+20k \end{aligned}$$

إذن

$$\big(20x-53y=3\big) \Leftrightarrow \Big((x,y)\in\big\{(24+53k,9+20k) : k\in\mathbb{Z}\big\}\Big)$$

❸ نلاحظ أنّ $12+15-20=7$ وعلى هذا يكون

$$\big(12x+15y+20z=7\big) \Leftrightarrow \big(12(x-1)+15(y-1)+20(z+1)=0\big)$$

ولمّا كان

$$\gcd(12,15)=3 \text{ و } \gcd(12,20)=4 \text{ و } \gcd(15,20)=5$$

استنتجنا من المعادلة الأخيرة أنّ 5 يقسم $x-1$ و 4 يقسم $y-1$ و 3 يقسم $z+1$، فيوجد u و v و w من $\mathbb{Z}$ تُحقّق

$$x=1+5u \quad \text{و} \quad y=1+4v \quad \text{و} \quad z=-1+3w$$

والأعداد u و v و w ليست مستقلّة لأنّ العلاقة

$$12(x-1)+15(y-1)+20(z+1)=0$$

تُكافئ

$$u+v+w=0.$$

وعليه يكون

$$(x,y,z)\in\Big\{(1+5u,1+4v,-1-3u-3v) : (u,v)\in\mathbb{Z}^2\Big\}$$

وبالعكس، نتحقّق مباشرة أنّ كلّ عنصر من المجموعة

$$\mathcal{S}=\left\{(1+5u,1+4v,-1-3u-3v):(u,v)\in\mathbb{Z}^2\right\}$$

حلٌّ للمعادلة $12x+15y+20z=7$، فهي إذن مجموعة الحلول المطلوبة.

التمرين 50. ليكن a و b عددين طبيعيين موجبين تماماً وأوليين فيما بينهما.

1. استفد من مبرهنة بيزو لتثبت الخاصّة التالية:
$$\forall n\in\mathbb{Z},\quad \exists!(x_n,y_n)\in\{0,1,\ldots,b-1\}\times\mathbb{Z},\qquad x_na+y_nb=n$$
2. لتكن المجموعة $\mathcal{E}=\left\{xa+yb:(x,y)\in\mathbb{N}^2\right\}$ أثبت صحة التكافؤ
$$n\in\mathcal{E}\Leftrightarrow y_n\geq 0$$
3. أثبت كذلك صحة التكافؤ
$$n\in(\mathbb{Z}\backslash\mathcal{E})\Leftrightarrow(ab-a-b-n)\in\mathcal{E}$$
4. أثبت أنّ $[(a-1)(b-1),+\infty[\cap\mathbb{N}\subset\mathcal{E}$.
5. أثبت أن التطبيق $\varphi:[0,ab-a-b]\cap\mathcal{E}\to[0,ab-a-b]\backslash\mathcal{E}$ المعرّف بالعلاقة: $\varphi(n)=ab-a-b-n$ تقابلٌ.
واستنتج عدد عناصر المجموعة $[0,ab-a-b]\cap\mathcal{E}$.

الحل

1. لمّا كان $\gcd(a,b)=1$ استنتجنا أنه يوجد (α,β) في $\mathbb{Z}^2$ يُحقّق $\alpha a+\beta b=1$.
ليكن n من $\mathbb{Z}$، عندئذ يكون $\alpha na+n\beta b=n$، ليكن q_n و x_n على الترتيب خارج وباقي القسمة الإقليديّة للعدد αn على b، أي $\alpha n=q_nb+x_n$، حيث x_n تنتمي إلى $\{0,1,\ldots,b-1\}$. وعندئذ يكون لدينا
$$x_na+\left(n\beta+q_na\right)b=n$$
أو $x_na+y_nb=n$ بعد أن عرّفنا $y_n=n\beta+q_na$.

لنفترض جدلاً أنّ $x'_na+y'_nb=n$ حيث $x'_n\in\left\{0,1,\ldots,b-1\right\}$. عندئذ يكون لدينا
$$(x_n-x'_n)a=(y'_n-y_n)b$$

إذن b يقسم الجداء $(x_n - x'_n)a$ وهو أوّلي مع a، فهو يقسم $(x_n - x'_n)$ ولكن، استناداً إلى تعريف x_n و x'_n نرى أنّ $\left|x_n - x'_n\right| < b$، إذن يجب أن يكون $x_n = x'_n$. وهذا يقتضي أن يكون $y_n = y'_n$. وهكذا نكون قد أثبتنا ما يلي :

$$\forall n \in \mathbb{Z},\ \exists!(x_n, y_n) \in \{0,1,\ldots,b-1\} \times \mathbb{Z}, \quad x_n a + y_n b = n$$

2. لتكن المجموعة $\mathcal{E} = \left\{xa + yb : (x,y) \in \mathbb{N}^2\right\}$.

- من الواضح أنّ الشرط $y_n \geq 0$ يقتضي $n \in \mathcal{E}$.
- ليكن n من $\mathcal{E}$. إذن يوجد (x,y) من $\mathbb{N}^2$ يُحقّق $n = xa + yb$. عندئذ يكون

$$(x_n - x)a = (y - y_n)b$$

إذن b يقسم جداء الضرب $(x_n - x)a$ وهو أوّلي مع a، فهو يقسم $(x_n - x)$ فيوجد k من $\mathbb{Z}$ يُحقّق $x = x_n + kb$. وهذا يقتضي أن يكون $y = y_n - ka$.

نستنتج من كون $x = x_n + kb \geq 0$ أنّ $kb \geq -x_n > -b$ أي $k > -1$، ولأنّ k عددٌ صحيح استنتجنا أنّ $k \geq 0$. ونستنتج من كون $y = y_n - ka \geq 0$ أنّ $y_n \geq ka \geq 0$.

وهكذا نكون قد أثبتنا أنّ

$$n \in \mathcal{E} \Leftrightarrow y_n \geq 0$$

3. نعرّف في حالة n من $\mathbb{Z}$ العدد $\hat{n} = ab - a - b - n$. وعندئذ نستنتج من أنّ $n = x_n a + y_n b$

$$\begin{aligned}\hat{n} &= ab - a - b - x_n a - y_n b\\ &= (b - 1 - x_n)a + (-1 - y_n)b\end{aligned}$$

ولأنّ $b - 1 - x_n \in \{0,1,\ldots,b-1\}$ استنتجنا أنّ

$$y_{\hat{n}} = -1 - y_n \quad \text{و} \quad x_{\hat{n}} = b - 1 - x_n$$

وذلك الأنّ الزوج (x_n, y_n) معيّن بأسلوب وحيد انطلاقاً من n. وإذا استفدنا من التكافؤ الذي أثبتناه في 2. أمكننا أن نكتب

$$\left(n \in \mathbb{Z} \backslash \mathcal{E}\right) \Leftrightarrow \left(y_n < 0\right) \Leftrightarrow \left(y_{\hat{n}} \geq 0\right) \Leftrightarrow \left(\hat{n} \in \mathcal{E}\right)$$

وهو التكافؤ المطلوب.

وينتج منه بأخذ نفي الطرفين أنّ

$$\left(n \in \mathcal{E}\right) \Leftrightarrow \left(\hat{n} \notin \mathcal{E}\right)$$

4. ليكن n عدداً طبيعيّاً يُحقّق $n \geq (a-1)(b-q)$ عندئذ يكون

$$\hat{n} = ab - a - b - n \leq -1$$

إذن $\hat{n} \notin \mathcal{E}$ وهذا يقتضي أنّ $n \in \mathcal{E}$. إذن لقد أثبتنا أنّ

$$\left[(a-1)(b-1), +\infty\right[\cap \mathbb{N} \subset \mathcal{E}$$

5. من الواضح أنّ

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}, n \mapsto \hat{n} = ab - a - b - n$$

تقابلٌ.

ولقد أثبتنا أنّ $\varphi(\mathcal{E}) = \mathbb{Z} \backslash \mathcal{E}$ ثُمّ إنّه من الواضح أنّ

$$\varphi\left([0, ab - a - b]\right) = [0, ab - a - b]$$

إذن

$$\varphi\left([0, ab - a - b] \cap \mathcal{E}\right) = [0, ab - a - b] \cap \left(\mathbb{Z} \backslash \mathcal{E}\right) = [0, ab - a - b] \backslash \mathcal{E}$$

وعلى هذا يكون التطبيق

$$[0, ab - a - b] \cap \mathcal{E} \rightarrow [0, ab - a - b] \backslash \mathcal{E}, n \mapsto \hat{n}$$

تقابلاً. إذن

$$\begin{aligned} 2 \operatorname{card}\left([0, ab - a - b] \cap \mathcal{E}\right) &= \operatorname{card}\left([0, ab - a - b] \cap \mathcal{E}\right) \\ &\quad + \operatorname{card}\left([0, ab - a - b] \backslash \mathcal{E}\right) \\ &= \operatorname{card}\left([0, ab - a - b]\right) \\ &= ab - a - b + 1 = (a-1)(b-1) \end{aligned}$$

ومنه

$$\operatorname{card}\left([0, ab - a - b] \cap \mathcal{E}\right) = \frac{(a-1)(b-1)}{2}$$

أو

$$\operatorname{card}\left(\left\{n < (a-1)(b-1) : \exists (x, y) \in \mathbb{N}^2, n = ax + by\right\}\right) = \frac{(a-1)(b-1)}{2}$$

وهو المطلوب. ■

التمرين 51. عيّن أُسّ العدد 2 في تفريق $1000!$ إلى جداء أعداد أوّليّة. وبكم صفراً تنتهي الكتابة العشريّة لهذه العدد.

الحل

لنعرّف في حالة عدد طبيعي n أكبر أو يساوي 2، وعدد أوّلي p، وعدد طبيعي α، المجموعة

$$A(n,p,\alpha)=\left\{k\in\mathbb{N}_n : p^\alpha \mid k\right\}=\left\{p^\alpha\ell\in\mathbb{N}_n : 1\leq\ell\leq\frac{n}{p^\alpha}\right\}$$

فيكون $\operatorname{card}A(n,p,\alpha)=\left\lfloor np^{-\alpha}\right\rfloor$ أي الجزء الصحيح للعدد $np^{-\alpha}$. كما يكون

$$\begin{aligned}B(n,p,\alpha)&=\left\{k\in\mathbb{N}_n : (p^\alpha\mid k)\wedge(p^{\alpha+1}\nmid k)\right\}\\&=A(n,p,\alpha)\backslash A(n,p,\alpha+1)\end{aligned}$$

إذن

$$\operatorname{card}B(n,p,\alpha)=\left\lfloor\frac{n}{p^\alpha}\right\rfloor-\left\lfloor\frac{n}{p^{\alpha+1}}\right\rfloor.$$

المجموعات $\left(B(n,p,\alpha)\right)_{\alpha\in\mathbb{N}^*}$ منفصلة مثنى مثنى، واجتماعها يساوي $\mathbb{N}_n$ وتصبح خالية بدءاً من حدٍّ معيّن، إذن

$$n!=\prod_{\alpha\geq1}\Big(\prod_{k\in B(n,p,\alpha)}k\Big)$$

ولكن p^α هو قوّة العدد p في التفريق إلى جداء أعداد أوّلية لأي عنصر من $B(n,p,\alpha)$. إذن بافتراض أنّ تفريق العدد $n!$ إلى جداء أعداد أوّليّة، يُعطى بالصيغة $n!=\prod_{p\leq n,p\in\mathcal{P}}p^{\nu_p(n)}$ نجد أنّ

$$\begin{aligned}\nu_p(n)&=\sum_{\alpha\geq1}\alpha\operatorname{card}B(n,p,\alpha)\\&=\sum_{\alpha\geq1}\alpha\left\lfloor\frac{n}{p^\alpha}\right\rfloor-\sum_{\alpha\geq1}\alpha\left\lfloor\frac{n}{p^{\alpha+1}}\right\rfloor\\&=\sum_{\alpha\geq1}\alpha\left\lfloor\frac{n}{p^\alpha}\right\rfloor-\sum_{\alpha\geq1}(\alpha-1)\left\lfloor\frac{n}{p^\alpha}\right\rfloor=\sum_{\alpha\geq1}\left\lfloor\frac{n}{p^\alpha}\right\rfloor\end{aligned}$$

وأخيراً، نستنتج أنّ

$$\nu_p(n) = \sum_{\alpha\geq 1}\left\lfloor \frac{n}{p^\alpha}\right\rfloor \quad \text{حيث} \quad n! = \prod_{p\leq n, p\in\mathcal{P}} p^{\nu_p(n)}$$

فمثلاً، أسّ العدد 2 في التفريق إلى جداء أعداد أوّلية للعدد $1000!$ يساوي

$$\begin{aligned}\nu_2(1000) &= \sum_{k=1}^{9}\left\lfloor\frac{1000}{2^k}\right\rfloor \\ &= 500+250+125+62+31+15+7+3+1 \\ &= 994\end{aligned}$$

وأسّ العدد 5 في التفريق إلى جداء أعداد أوّلية للعدد $1000!$ يساوي

$$\nu_5(1000) = \left\lfloor\frac{1000}{5}\right\rfloor + \left\lfloor\frac{1000}{25}\right\rfloor + \left\lfloor\frac{1000}{125}\right\rfloor + \left\lfloor\frac{1000}{625}\right\rfloor = 249$$

وعليه فإنّ أكبر قوّة للعدد 10 تقسم $1000!$ تساوي 10^{249}، والعدد $1000!$ ينتهي بتسعة وأربعين ومئتي صفر. ■

التمرين 52. أثبت أنّه أيّاًكان ℓ من $\mathbb{N}^*$ فيوجد في $\mathbb{N}$ مجال طوله ℓ لا يحوي أعداداً أوّليّة.

الحل

هذا أمرٌ بسيطٌ، إذ يكفي أن نلاحظ أنّ جميع الأعداد في المجموعة

$$I_\ell = \left\{(\ell+1)! + k : 2\leq k\leq \ell+1\right\}$$

ليست أوّليّة. ■

التمرين 53. أوجد العدد n من الشكل 3^p5^q إذا علمتَ أنّ جداء ضرب قواسمه الموجبة يساوي 45^{105}.

الحل

في الحقيقة، إنّ مجموعة القواسم الموجبة للعدد $n = 3^p5^q$ هي

$$\mathcal{D} = \left\{3^k5^\ell : 0\leq k\leq p, 0\leq \ell\leq q\right\}$$

وجداء ضرب هذه القواسم يساوي

$$\begin{aligned}\Delta &= \prod_{\substack{0\le k\le p\\ 0\le \ell\le q}} 3^k5^\ell = \prod_{k=0}^{p}\left(\prod_{\ell=0}^{q}\left(3^k5^\ell\right)\right)\\ &= \prod_{k=0}^{p} 3^{k(q+1)}5^{\frac{q(q+1)}{2}} = 3^{\frac{p(p+1)(q+1)}{2}}5^{\frac{q(q+1)(p+1)}{2}}\end{aligned}$$

فإذا افترضنا أنّ $\Delta = 45^{42} = 3^{84}5^{42}$ استنتجنا أنّ

$$3^{\frac{p(p+1)(q+1)}{2}}5^{\frac{q(q+1)(p+1)}{2}} = 3^{84}5^{42}$$

ومنه

$$p(q+1)(p+1) = 168 \quad \text{و} \quad q(q+1)(p+1) = 84$$

وعليه

$$q(q+1)(2q+1) = 84 \quad \text{و} \quad p = 2q \; .$$

ولكن تُكافئ المعادلةُ

$$q(q+1)(2q+1) = 84$$

المعادلةَ الآتية

$$(q-3)(2q^2+9q+28) = 0$$

إذن $q = 3$ ومن ثَمّ $p = 6$ ، والعدد المطلوب هو

$$n = 3^6 5^3 = 91125 \; .$$ ■

التمرين 54. ليكن p عدداً أوّليّاً.

1. أثبت أنّ $p \mid C_p^k$ في حالة $0 < k < p$.
2. ليكن (a,b) من $\mathbb{Z}^2$ أثبت أنّ $p \mid \left((a+b)^p - a^p - b^p\right)$.
3. أثبت أنّه، أيّاً كانت m من $\mathbb{Z}$ كان $p \mid \left(m^p - m\right)$.
4. استنتج أنّه أيّاً كانت m من $\mathbb{Z}$ كان

$$p \nmid m \Rightarrow p \mid \left(m^{p-1}-1\right) \qquad (\text{Fermat})$$

الحل

1. في حالة $0 < k < p$. يُكتب C_p^k بالصيغة

$$C_p^k = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

والعدد p أوّلي مع مقام هذا الكسر ويقسم بسطه، فهو يقسم C_p^k، أي $p \mid C_p^k$.

2. ليكن (a,b) من $\mathbb{Z}^2$ عندئذ يكون

$$(a+b)^p - a^p - b^p = \sum_{k=1}^{p-1} C_p^k a^k b^{p-k}$$

ولأنّ p يقسم جميع الأعداد $C_p^1, C_p^2, \ldots, C_p^{p-1}$ استنتجنا أنّ p يقسم العدد $(a+b)^p - a^p - b^p$.

3. في حالة $p = 2$ لدينا $m^2 - m = m(m-1)$ وهويقبل وضوحاً القسمة على 2 .
لنفترض فيما يأتي أنّ $p > 2$. فيكون p عدداً فرديّاً ومن ثَمّ

$$\forall m \in \mathbb{Z}, \quad (-m)^p - (-m) = -(m^p - m)$$

إذن يكفي أن نثبتَ المطلوب في حالة $m \in \mathbb{N}$.

لتكن $\mathbb{P}_m$ القضيّة $p \mid (m^p - m)$ في حالة m من $\mathbb{N}$. إنّ صحّة $\mathbb{P}_0$ واضحة. لنفترض صحّة $\mathbb{P}_m$. فيكون لدينا $p \mid (m^p - m)$ واستناداً إلى ما سبق

$$p \mid \Big((m+1)^p - m^p - 1^p\Big)$$

إذن

$$p \mid \Big((m+1)^p - m^p - 1^p + (m^p - m)\Big)$$

أو

$$p \mid \Big((m+1)^p - (m+1)\Big)$$

فالقضيّة $\mathbb{P}_{m+1}$ صحيحة. فنكون قد أثبتنا الخاصّة المطلوبة بالتدريج على m .

4. ليكن m من $\mathbb{Z}$ يُحقّق $p \nmid m$. لمّا كان العدد p أوّليّاً استنتجنا أنّ $\gcd(p,m) = 1$ ، وعندئذ نستنتج استناداً إلى توطئة غاوس أنّ $p \mid m(m^{p-1} - 1)$ يقتضي $p \mid (m^{p-1} - 1)$.

أو

$$\forall m \in \mathbb{Z}, \quad (p \nmid m) \Rightarrow (m^{p-1} = 1 \bmod p)$$

وتُعرف هذه الخاصّة باسم، مبرهنة Fermat الصغرى. ■

التمرين 55. ليكن n عدداً طبيعيّاً أكبر أو يساوي 2. أثبت أنّ

$$(\text{عددٌ أوّليّ } 2^n - 1) \Leftarrow (\text{عددٌ أوّليّ } n)$$

هل العكس صحيح ؟

الحل

في الحقيقة، ليكن p عدداً أوّليّاً ما يقسم n، وهو موجود لأنّ $2 \leq n$. عندئذ يوجد m في $\mathbb{N}^*$ يُحقّق $n = pm$ ومن ثَمّ

$$2^n - 1 = 2^{mp} - 1 = (2^p - 1)\sum_{k=0}^{m-1} 2^{kp}$$

فإذا افترضنا أنّ $2^n - 1$ عددٌ أوّلي استنتجنا من المساواة السابقة، ومن كون $2^p - 1$ قاسماً أكبر تماماً من 1 للعدد الأوّلي $2^n - 1$، أنّ $2^n - 1 = 2^p - 1$ أي إنّ $n = p$ ومن ثَمّ أنّ n عددٌ أوّلي. بالطبع، العكس غير صحيح لأنّ $2^{11} - 1 = 23 \times 89$. ■

التمرين 56. ليكن m عدداً من $\mathbb{N}^*$. أثبت أنّ

$$(m = 2^n \text{ يُحقّق } \mathbb{N} \text{ في } n \text{ يوجد}) \Leftarrow (\text{عددٌ أوّليّ } 2^m + 1)$$

هل العكس صحيح برأيك ؟

الحل

في الحقيقة، ليكن $n = \max\{k \in \mathbb{N} : 2^k \mid m\}$ عندئذ يكون $m = 2^n q$ و q عددٌ فردي من $\mathbb{N}^*$. وعندها

$$2^m + 1 = 2^{2^n q} + 1 = (2^{2^n} + 1) \cdot \sum_{k=0}^{q-1} 2^{2^n k}(-1)^{q-1-k}$$

فإذا افترضنا أنّ $2^m + 1$ عددٌ أوّلي استنتجنا من المساواة السابقة، ومن كون $2^{2^n} + 1$ قاسماً أكبر تماماً من 1 للعدد الأوّلي $2^m + 1$، أنّ $2^m + 1 = 2^{2^n} + 1$ أي إنّ $m = 2^n$.

العكس غير صحيح لأنّ $2^{2^5} + 1 = 641 \times 6700417$. ■

التمرين 57. نعرّف في حالة n من $\mathbb{N}$ العدد $F_n = 2^{2^n}+1$.

1. أثبت في حالة $m > n$ أنّ $F_n \mid (F_m - 2)$.
2. أثبت في حالة $m \neq n$ أنّ $\gcd(F_n, F_m) = 1$.
3. استنتج من ذلك أنّه يوجد عددٌ لا نهائي من الأعداد الأوّليّة.
4. أثبت أنّ F_5 يقبل القسمة على 641 .

الحل

1. لنذكّر أنّ $(a-1) \mid (a^k - 1)$. فإذا وضعنا $a = 2^{2^{n+1}}$ و $k = 2^{m-n-1}$ بافتراض $m > n$ استنتجنا أنّ

$$(2^{2^{n+1}} - 1) \mid ((2^{2^{n+1}})^{2^{m-n-1}} - 1)$$

ولكن

$$2^{2^{n+1}} - 1 = (2^{2^n}+1)(2^{2^n}-1) = (2^{2^n}-1)F_n$$

أي $(2^{2^{n+1}}-1) \mid F_n$ ، إذن F_n يقسم $2^{2^m}-1$ أو $F_n \mid (F_m - 2)$.

2. لنفترض أنّ $m \neq n$ يمكننا دون الإخلال بعموميّة الحل أن نفترض أنّ $n < m$. ليكن d قاسماً مشتركاً للعددين F_n و F_m . عندئذ يكون d فرديّاً لأنّ F_m فردي. نستنتج من نتيجة السؤال الأوّل أنّ d يقسم كلّاً من F_m و $F_m - 2$ فهو إذن يقسم 2. وعليه يكون d عدداً فرديّاً يقسم 2 فهو إذن عنصرٌ من $\{-1,1\}$. ومنه $\gcd(F_n, F_m) = 1$.

3. لنعرّف في حالة n من F_n العدد الأوّلي p_n بأنّه أصغر عددٍ أوّلي يقسم F_n أي

$$p_n = \min\{p \in \mathcal{P} : p \mid F_n\}$$

عندئذ يكون التطبيق $\mathcal{I} : \mathbb{N} \to \mathcal{P}, \mathcal{I}(n) = p_n$ متبايناً.

لأنّه إذا كان $\mathcal{I}(n) = \mathcal{I}(m)$ استنتجنا أنّ $p = \mathcal{I}(n) = \mathcal{I}(m)$ قاسمٌ مشترك للعددين F_n و F_m وهذا يقتضي بناءً على ما سبق أنّ $n = m$. إذ في حالة $n \neq m$ يكون $\gcd(F_n, F_m) = 1$.

وينتج من كون التطبيق $\mathcal{I}$ متبايناً أنّ مجموعة الأعداد الأولية $\mathcal{P}$ غير منتهية.

4. نلاحظ أنّ $641 = 1 + 5 \times 2^7 = 5^4 + 2^4$ ومنه

$$5^4 = -2^4 \bmod 641 \quad \text{و} \quad 5 \times 2^7 = -1 \bmod 641$$

وعليه يكون لدينا

$$5^4 \times 2^{28} = (5 \times 2^7)^4 = (-1)^4 \bmod 641 = 1 \bmod 641$$

وبالاستفادة من العلاقة $5^4 = -2^4 \bmod 641$ نستنتج أنّ

$$5^4 \times 2^{28} = -2^4 \times 2^{28} = 1 \bmod 641$$

أي $2^{32} + 1 = 0 \bmod 641$، وهي النتيجة المرجوّة. ■

التمرين 58. ليكن n عدداً من $\mathbb{N}^*$. وليكن $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ تحليل n إلى جداء عوامل أوّليّة.

1. احسب $d(n)$ عدد القواسم الموجبة للعدد n.
2. احسب $\mathcal{S}(n)$ مجموع القواسم الموجبة للعدد n.
3. أثبت أنّ

$$\forall (n,m) \in \mathbb{N}^{*2}, \gcd(n,m) = 1 \Rightarrow \mathcal{S}(nm) = \mathcal{S}(n)\mathcal{S}(m)$$

الحل

1. في الحقيقة، إنّ مجموعة القواسم الموجبة للعدد n هي

$$\mathcal{D}(n) = \left\{ p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \,:\, \forall k \in \mathbb{N}_r, 0 \le \beta_k \le \alpha_k \right\}$$

ومن ثَمّ

$$d(n) = \operatorname{card}(\mathcal{D}(n)) = \prod_{k=1}^{r} (1 + \alpha_k)$$

2. يُعطى مجموع قواسم n بالعلاقة

$$\begin{aligned} \mathcal{S}(n) &= \sum_{d \in \mathcal{D}(n)} d = \sum_{0 \le \beta_k \le \alpha_k} p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \\ &= \prod_{k=1}^{r} \left(\sum_{\beta_k = 0}^{\alpha_k} p_k^{\beta_k} \right) = \prod_{k=1}^{r} \frac{p_k^{\alpha_k + 1} - 1}{p_k - 1} \end{aligned}$$

3. هذه النتيجة واضحة استناداً إلى العلاقة السابقة. ■

التمرين 59. نتأمّل متتالية أعداد Fibonacci . $(F_n)_{n\in\mathbb{N}}$ المعرّفة تدريجيّاً كما يلي :

$$F_0=0, F_1=1, \quad \forall n\in\mathbb{N}, \quad F_{n+2}=F_{n+1}+F_n$$

1. أثبت أنّه $\forall n\in\mathbb{N}, \gcd(F_n,F_{n+1})=1$.
2. أثبت أنّه في حالة (n,p) من $\mathbb{N}^{*2}$ لدينا

$$F_{n+p-1}=F_{n-1}F_{p-1}+F_nF_p$$

3. أثبت أنّه في حالة n من $\mathbb{N}$ و q من $\mathbb{N}^*$ و r من $\mathbb{N}$ لدينا

$$\gcd(F_{qn+r},F_n)=\gcd(F_{(q-1)n+r},F_n)$$

ومن ثَمّ أنّ $\gcd(F_{qn+r},F_n)=\gcd(F_n,F_r)$.

4. أثبت أنّه في حالة n و m من $\mathbb{N}^*$ لدينا $\gcd(F_n,F_m)=F_{\gcd(n,m)}$.

الحل

1. في الحقيقة، نلاحظ في حالة n من $\mathbb{N}$ أنّ

$$\gcd(F_{n+2},F_{n+1})=\gcd(F_{n+1},F_{n+2}-F_{n+1})=\gcd(F_{n+1},F_n)$$

فالمتتالية $\big(\gcd(F_{n+1},F_n)\big)_{n\in\mathbb{N}}$ ثابتة، ولأنّ $\gcd(F_1,F_0)=1$ نستنتج أنّ

$$\forall n\in\mathbb{N}, \gcd(F_n,F_{n+1})=1$$

2. لنعرّف القضيّة $\mathbb{P}_n$ كما يلي :

$$\mathbb{P}_n : \forall p\in\mathbb{N}^*, \quad F_{n+p-1}=F_{n-1}F_{p-1}+F_nF_p$$

- القضيّة $\mathbb{P}_1$ صحيحة وضوحاً، وكذلك تكون القضيّة $\mathbb{P}_2$، بناءً على تعريف متتالية فيبوناتشي.
- لنثبت أنّ $\mathbb{P}_n\wedge\mathbb{P}_{n+1}\Rightarrow\mathbb{P}_{n+2}$ وذلك أياً كان n من $\mathbb{N}^*$. في الحقيقة بافتراض صحّة $\mathbb{P}_n$ و $\mathbb{P}_{n+1}$ نستنتج أنّه، في حالة p من $\mathbb{N}^*$، يكون

$$\begin{aligned} F_{n+p-1}&=F_{n-1}F_{p-1}+F_nF_p\\ F_{n+p}&=F_nF_{p-1}+F_{n+1}F_p \end{aligned}$$

وبالجمع طرفاً إلى طرف نجد

$$F_{n+p+1}=F_{n+1}F_{p-1}+F_{n+2}F_p$$

ومنه

$$\forall p \in \mathbb{N}^*, \quad F_{(n+2)+p-1} = F_{(n+2)-1}F_{p-1} + F_{n+2}F_p$$

فالقضيّة $\mathbb{P}_{n+2}$ صحيحة أيضاً.

وهكذا نكون قد أثبتنا صحّة القضيّة $\mathbb{P}_n$ أيّاً كانت قيمة n من $\mathbb{N}^*$. مما يثبت المطلوب.

3. في حالة n من $\mathbb{N}^*$ و q من $\mathbb{N}^*$ و r من $\mathbb{N}$ لدينا

$$F_{nq+r} = F_{n+n(q-1)+r} = F_{n(q-1)+r}F_{n-1} + F_{n(q-1)+r+1}F_n$$

إذن

$$\begin{aligned}\gcd(F_{nq+r}, F_n) &= \gcd(F_{nq+r} - F_{n(q-1)+r+1}F_n, F_n)\\ &= \gcd(F_{n(q-1)+r}F_{n-1}, F_n)\end{aligned}$$

فإذا استفدنا من كون $\gcd(F_n, F_{n-1}) = 1$ استنتجنا أنّ

$$\gcd(F_{qn+r}, F_n) = \gcd(F_{(q-1)n+r}, F_n)$$

وهي وضوحاً صحيحة في حالة $n = 0$.

تفيدنا الخاصّة السابقة في إثبات أنّ $\gcd(F_{qn+r}, F_n) = \gcd(F_r, F_n)$ $\forall q \in \mathbb{N},$ وذلك بالتدريج على العدد q.

5. لتكن n و m من $\mathbb{N}^*$، ولنضع $d = \gcd(n, m)$. تنصُّ خوارزميّة إقليدس لحساب القاسم المشترك الأعظم، أنّه إذا عرّفنا المتتالية $(R_k)_{k\geq 0}$ بوضع $R_0 = n$ و $R_1 = m$، ثُمّ عرّفنا R_{k+1} بأنّه باقي قسمة R_{k-1} على R_k في حالة $R_k \neq 0$، وبأنّه يساوي 0 في حالة $R_k = 0$.

وإذا عرّفنا أيضاً

$$N = \min\{k \in \mathbb{N} : R_{k+1} = 0\}$$

كان $d = R_N$. لنرمز بالرمز Q_k إلى خارج قسمة R_{k-1} على R_k في حالة $0 < k \leq N$.

عندئذ يكون لدينا، في حالة $1 \leq k \leq N$ ما يلي

$$\begin{aligned}\gcd(F_{R_{k-1}}, F_{R_k}) &= \gcd(F_{Q_kR_k+R_{k+1}}, F_{R_k})\\ &= \gcd(F_{R_{k+1}}, F_{R_k}) = \gcd(F_{R_k}, F_{R_{k+1}})\end{aligned}$$

أي إنّ المتتالية $\left(\gcd(F_{R_{k-1}}, F_{R_k})\right)_{1\leq k\leq N+1}$ ثابتة، ومن ثَمّ

$$\gcd(F_{R_0}, F_{R_1}) = \gcd(F_{R_N}, F_0)$$

وهذا يُكافئ $\gcd(F_n, F_m) = F_d$، وهي النتيجة المرجوّة. ∎

التمرين 60. احسب $a \bmod b$ في الحالات التالية

a	$(1945)^8$	5^{10}	$(1999)^{12}$	$(2001)^{2001}$	7^{355}	7^{355}	$(17)^{88}$
b	7	11	11	26	10	100	1001

الحل

- في حالة $c = 1945$ نلاحظ أنّ $c \equiv -1 \bmod 7$، إذن

$$a \equiv (1945)^8 \equiv c^8 \equiv (-1)^8 \equiv 1 \bmod 7$$

- إذا كان p عدداً أوّلياً، كانت رتبة زمرة العناصر القلوبة في الحقل $\mathbb{Z}/p\mathbb{Z}$ تساوي $p-1$، إذن أيّاً كان x من $\mathbb{Z}$ تحقّق الاقتضاء : $p \nmid x \Rightarrow x^{p-1} \equiv 1 \bmod p$، وهذا نصُّ مبرهنة Fermat. إذن بملاحظة أنّ $5 \nmid 11$ نستنتج أنّ $5^{10} \equiv 1 \bmod 11$.

- في حالة $c = 1999$ نلاحظ أنّ $c \equiv -3 \bmod 11$. وإذا استفدنا من مبرهنة Fermat التي أشرنا إليها سابقاً استنتجنا أنّ $c^{10} \equiv 1 \bmod 11$، إذن

$$a \equiv (1999)^{12} = c^{10}c^2 \equiv (-3)^2 \equiv 9 \bmod 11$$

- في حالة $c = 2001$ نلاحظ أنّ $c \equiv -1 \bmod 26$. إذن

$$a \equiv (2001)^{2001} \equiv c^{2001} \equiv (-1)^{2001} \equiv -1 \bmod 26$$

- لحساب $7^{355} \bmod 10$ نبدأ بملاحظة أنّ $7^2 = 49 \equiv -1 \bmod 10$. إذن

$$7^{355} = 7 \times (7^2)^{177} \equiv 7 \times (-1)^{177} \equiv -7 \equiv 3 \bmod 10$$

- لحساب $7^{355} \bmod 100$ نبدأ بملاحظة أنّ $7^4 = (50-1)^2 \equiv 1 \bmod 100$. إذن

$$7^{355} = 7^3 \times (7^4)^{88} \equiv 7^3 \equiv 43 \bmod 100$$

- لحساب $(17)^{88} \bmod 1001$ نلاحظ أوّلاً أنّ $88 = 64 + 16 + 8$.

$$\begin{aligned}
(17)^2 &\equiv 289 \bmod 1001\\
(17)^4 &\equiv 289 \times 289 \equiv 438 \bmod 1001\\
(17)^8 &\equiv 438 \times 438 \equiv -348 \bmod 1001\\
(17)^{16} &\equiv 348 \times 348 \equiv -17 \bmod 1001
\end{aligned}$$

وأخيراً

$$\begin{aligned}(17)^{32} &\equiv 17\times 17 \equiv 289 \bmod 1001\\ (17)^{64} &\equiv 289\times 289 \equiv 438 \bmod 1001\end{aligned}$$

إذن

$$\begin{aligned}(17)^{88} &= (17)^{64}\times(17)^{16}\times(17)^{8}\\ &\equiv 438\times 17\times 348 \equiv 620 \bmod 1001\end{aligned}$$

وهي النتيجة المطلوبة.

التمرين 61. عيّن قيم x من مجموعة الأعداد الصحيحة، التي هي، في حال وجودها، حلولٌ للمعادلات، أو لجمل المعادلات، المعطاة في كل من الحالات التالية :

❶ $91x = 84 \bmod 143$ ❷ $91x = 84 \bmod 147$

❸ $\begin{cases} x = 2 \bmod 12\\ x = 3 \bmod 13\\ x = 5 \bmod 7\end{cases}$ ❹ $\begin{cases} 3x = 2 \bmod 5\\ 5x = 2 \bmod 12\\ 17x = 8 \bmod 19\end{cases}$

الحل

❶ ليس للمعادلة $91x = 84 \bmod 143$ حلول. إذ لو كان x حلاً لهذه المعادلة وجدنا عدداً صحيحاً k يُحقّق $84 = 91x + 143k = 13(7+11k)$، وكان من ثَمّ $13 \mid 84$ وهذا خُلفٌ.

❷ لحلّ المعادلة $91x = 84 \bmod 147$. نلاحظ أنّها تُكافئ $13x = 12 \bmod 21$، وهذه بدورها تُكافئ $8x = 9 \bmod 21$، ولأنّ $8^2 \equiv 1 \bmod 21$، نرى أنّ المعادلة المعطاة تُكافئ $x \equiv 72 \equiv 9 \bmod 21$. إذن مجموعة حلول المعادلة $91x = 84 \bmod 147$ هي $\{9+21k : k\in\mathbb{Z}\}$.

❸ لنذكّر أنّه إذا كان $\gcd(a,b)=1$ أمكننا إيجاد عددين α و β يُحقّقان $\alpha a + \beta b = 1$ وعندئذ تعطى حلول جملة المعادلتين :

$$\begin{cases} x = & m \bmod a\\ x = & n \bmod b\end{cases}$$

بالعلاقة $x = \big(n\alpha a + m\beta b\big) \bmod ab$. لنتأمّل إذن الجملة

$$\mathcal{E} : \begin{cases} x & = 2 \mod 12 \\ x & = 3 \mod 13 \\ x & = 5 \mod 7 \end{cases}$$

لمّا كان $1 = 12 - 13$ استنتجنا أنّ

$$\begin{cases} x = 2 \bmod 12 \\ x = 3 \bmod 13 \end{cases} \Leftrightarrow x = \big(2 \times 13 - 3 \times 12\big) \bmod 156 = -10 \bmod 156$$

فالجملة $\mathcal{E}$ تُكافئ

$$\begin{cases} x = & 5 \mod 7 \\ x = & -10 \mod 156 \end{cases}$$

ولأنّ $1 = 3 \times 156 - 7 \times 67$ استنتجنا أنّ

$$x = \big(-67 \times 7 \times 10 - 3 \times 156 \times 5\big) \bmod 1092 = 614 \bmod 1092$$

إذن مجموعة حلول المعادلة $\mathcal{E}$ هي $\{614 + 1092k : k \in \mathbb{Z}\}$.

❹ لنتأمّل الجملة

$$\mathcal{E} : \begin{cases} 3x & = 2 \mod 5 \\ 5x & = 2 \mod 12 \\ 17x & = 8 \mod 19 \end{cases}$$

بملاحظة أنّ $2 \times 3 \equiv 1 \bmod 5$ و $5 \times 5 \equiv 1 \bmod 12$ و $9 \times 17 \equiv 1 \bmod 19$ نستنتج أنّ $\mathcal{E}$ تُكافئ

$$\mathcal{E}' : \begin{cases} x & = -1 \mod 5 \\ x & = -2 \mod 12 \\ x & = -4 \mod 19 \end{cases}$$

لمّا كان $1 = 2 \times 12 - 5 \times 5$ استنتجنا أنّ

$$\begin{cases} x = & -1 & \mod & 5 \\ x = & -2 & \mod & 12 \end{cases} \Leftrightarrow x = \big(-50 + 24\big) \bmod 60 = 34 \bmod 60$$

والجملة $\mathcal{E}'$ تُكافئ الجملة

$$\begin{cases} x = & 34 \mod 60 \\ x = & -4 \mod 19 \end{cases}$$

ولأنّ $19\times 19 - 6\times 60 = 1$ استنتجنا أنّ

$$x = \left(34\times 361 + 4\times 360\right)\bmod 1140 = 34 \bmod 1140$$

إذن مجموعة حلول المعادلة $\mathcal{E}$ هي $\left\{34 + 1140k : k\in\mathbb{Z}\right\}$. ■

التمرين 62. في حالة n من $\mathbb{N}^*$، و a من $\mathbb{Z}$ نكتب $r_n(a)$ دلالة على باقي قسمة a على n. ونعرّف

$$D_n = \{k\in\{0,\ldots,n-1\} : \gcd(k,n) = 1\}$$

و $\varphi(n) = \operatorname{card}\left(D_n\right)$.

1. احسب كلاً من $\varphi\left(p^\alpha\right)$ في حالة p أوّلي و α من $\mathbb{N}$.
2. لنفترض أنّ n و m عددان طبيعيّان أكبر من 2، وأوّليّان فيما بينهما. أثبت أنّ التطبيق : $\Lambda : D_{nm}\to D_n\times D_m, k\mapsto \left(r_n(k), r_m(k)\right)$ تقابلٌ. ما هي الخاصّة التي تستنتجها بشأن التابع φ المعروف باسم تابع Euler؟
3. استنتج أنّه مهما تكن n من $\mathbb{N}^*$ يكن

$$\varphi(n) = n\prod_{p\in\mathcal{P}, p|n}\left(1-\frac{1}{p}\right).$$

الحل

1. ▫ في حالة $\alpha = 0$ يكون $D_1 = \{0\}$ ومن ثَمّ $\varphi(0) = 1$.
   - ▫ وفي حالة $\alpha = 1$ لدينا $D_p = \{1,2,\ldots,p-1\}$ ومن ثَمّ $\varphi(p) = p-1$.
   - ▫ وبوجه عام، لدينا

$$D_{p^\alpha} = \mathbb{N}_{p^\alpha}\setminus\{kp : 1\le k\le p^{\alpha-1}\}$$

إذن

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right).$$

2. لنفترض أنّ n و m عددان طبيعيّان أكبر من 2، وأوّليّان فيما بينهما. ولنتأمّل التطبيق

$$\Lambda : D_{nm}\to D_n\times D_m, k\mapsto \left(r_n(k), r_m(k)\right)$$

- لنلاحظ أنّ هذا التطبيق معرّف تعريفاً جيّداً، لأنّه إذا كان k من D_{nm} استنتجنا من كون $\gcd(k,nm)=1$ أنّ $\gcd(k,n)=1$ و $\gcd(k,m)=1$. ومن ثَمّ $\gcd(r_n(k),n)=1$ و $\gcd(r_m(k),m)=1$. فالعنصر $\left(r_n(k),r_m(k)\right)$ ينتمي فعلاً إلى $D_n\times D_m$.
- لنفترض أنّ $\Lambda(k)=\Lambda(k')$ حيث k و k' من D_{nm}. عندئذ يكون $k-k'$ مضاعفاً لكلٍّ من n و m ولأنّ هذين العددين أوّليّان فيما بينهما استنتجنا أنّ $(k-k')\mid nm$. ولكن $\left|k-k'\right|<nm$ إذن لا بُدّ أن يكون $k=k'$، والتطبيق Λ متباينٌ.
- ليكن (a,b) من $D_n\times D_m$. لمّا كان $\gcd(n,m)=1$ وجدنا (u,v) في $\mathbb{Z}^2$ يُحقِّق

$$un+vm=1$$

وعندئذ نضع $k=r_{nm}(unb+vma)$.

نجد إذن λ في $\mathbb{Z}$ تُحقّق $k=unb+vma+\lambda nm$. يُحقِّق العددُ k من جهة أولى المساواة

$$k=b(1-vm)+vma+\lambda nm=b+m(\lambda n+va-vb)$$

ومنه $r_m(k)=b$. ويُحقِّق من جهة ثانية

$$k=unb+(1-un)a+\lambda nm=a+n(\lambda m+ub-ua)$$

ومنه $r_n(k)=a$. وأخيراً إنّ $\gcd(k,nm)=1$ لأنّه إذا كان p عدداً أوّليّاً يقسم كلاً من k و nm، قسم p أحدَ العددين n أو m.

- فإذا كان $p\mid n$ استنتجنا أنّ $p\mid\gcd(k,n)$ ومن ثَمّ $p\mid\gcd(r_n(k),n)$ أو $p\mid 1$ لأنّ $\gcd\left(r_n(k),n\right)=\gcd(a,n)=1$ وهذا خُلفٌ.
- وإذا كان $p\mid m$ استنتجنا أنّ $p\mid\gcd(k,m)$ ومن ثَمّ $p\mid\gcd(r_m(k),m)$ أو $p\mid 1$ لأنّ $\gcd(r_m(k),m)=\gcd(b,m)=1$ وهذا خُلفٌ أيضاً.

إذن وجدنا k ينتمي إلى D_{nm} يُحقِّق $\Lambda(k)=(a,b)$، والتطبيق Λ تطبيق غامرٌ. فهو إذن تقابلٌ.

نستنتج من ذلك أنّه في حالة $\gcd(n,m)=1$ لدينا

$$\operatorname{card}(D_{nm})=\operatorname{card}(D_n)\operatorname{card}(D_m)$$

أي

$$\forall (n,m)\in\mathbb{N}^{*2},\quad \gcd(n,m)=1\Rightarrow \varphi(nm)=\varphi(n)\varphi(m)$$

3. ليكن n عدداً من $\mathbb{N}^*$ أكبر أو يساوي 2. وليكن

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$$

تحليل n إلى جداء عوامل أوّليّة. عندئذ نستنتج استناداً إلى ما سبق وبالتدريج على العدد r أنّ

$$\begin{aligned}\varphi(n)&=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}\cdots p_r^{\alpha_r})=\cdots=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_r^{\alpha_r})\\&=p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdots p_r^{\alpha_r}\left(1-\frac{1}{p_r}\right)\\&=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\\&=n\prod_{p|n,p\in\mathcal{P}}\left(1-\frac{1}{p}\right)\end{aligned}$$

وهي النتيجة المرجوّة. ■

التمرين 63. **تابع Euler رؤية أخرى.** نعرّف $\varphi(n)=\operatorname{card}(U(\mathbb{Z}/n\mathbb{Z}))$، أياً كان n من $\mathbb{N}^*$.

1. احسب $\varphi(1)$ و $\varphi(p)$ و $\varphi(p^\alpha)$ في حالة p عدد أولي و α من $\mathbb{N}^*$.
2. أثبت أنّ $\gcd(n,m)=1\Rightarrow\varphi(n\,m)=\varphi(n)\,\varphi(m)$.
3. استنتج أنه $\forall n\in\mathbb{N}\backslash\{0,1\},\quad \varphi(n)=n\cdot\prod_{p\in\mathcal{P},p|n}\left(1-\frac{1}{p}\right)$.
4. ليكن $n\geq 2$، وليكن k من $\mathbb{Z}$ يُحقّق $\gcd(n,k)=1$. أثبت أنّ

$$k^{\varphi(n)}=1\bmod n$$

تسمّى هذه النتيجة مبرهنة Euler.

5. أثبت أنّ $n=\sum_{d|n}\varphi(d)$.
6. **تطبيق.** لتكن $(G,\cdot)$ زمرة منتهية تُحقّق

$$\forall d\in\mathbb{N}^*,\quad \operatorname{card}\left(\left\{x\in G:x^d=1\right\}\right)\leq d$$

أثبت أنّ G زمرة دوّارة.

الحل

لنذكِّر أوّلاً أنّ

$$\begin{aligned} U\big(\mathbb{Z}/n\mathbb{Z}\big) &= \big\{x \in \mathbb{Z}/n\mathbb{Z} : O(x) = n\big\} \\ &= \big\{x \in \mathbb{Z}/n\mathbb{Z} : \langle x\rangle = \mathbb{Z}/n\mathbb{Z}\big\} \\ &= \big\{[x]_n \in \mathbb{Z}/n\mathbb{Z} : \gcd(x,n) = 1\big\} \end{aligned}$$

1. من الواضح أنّ $\varphi(1) = 1$، وإذا كان p عدداً أوّلياً كان

$$U\big(\mathbb{Z}/p\mathbb{Z}\big) = \big(\mathbb{Z}/p\mathbb{Z}\big)\backslash\{0\}$$

إذن $\varphi(p) = p - 1$. وفي حالة α من $\mathbb{N}^*$، لدينا

$$\begin{aligned} (\mathbb{Z}/p^\alpha\mathbb{Z})\backslash U(\mathbb{Z}/p^\alpha\mathbb{Z}) &= \big\{[x] : 0 \le x < p^\alpha, \gcd(x, p^\alpha) > 1\big\} \\ &= \big\{[x] : 0 \le x < p^\alpha, p \mid x\big\} \\ &= \big\{[px] : 0 \le x < p^{\alpha-1}\big\} \end{aligned}$$

إذن $p^\alpha - \varphi(p^\alpha) = p^{\alpha-1}$ ومنه

$$\forall \alpha \in \mathbb{N}^*, \forall p \in \mathcal{P}, \quad \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

2. لنفترض أنّ (n,m) من $\mathbb{N}^{*2}$ تُحقِّق $\gcd(n,m) = 1$. عندئذ نعلم أنّ هناك تشاكل تقابلي حَلَقي بين الحلقتين

$$\mathbb{Z}/nm\mathbb{Z} \quad \text{و} \quad (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

ينتج من ذلك أن هناك تشاكل تقابلي زمري بين الزمرتين

$$U(\mathbb{Z}/nm\mathbb{Z}) \quad \text{و} \quad U(\mathbb{Z}/n\mathbb{Z}) \times U(\mathbb{Z}/m\mathbb{Z})$$

ونستنتج من ذلك أنّ

$$\varphi(nm) = \varphi(n)\varphi(m)$$

3. ليكن n من $\mathbb{N}^*$. عندئذ يُكتب n بالشكل

$$n = \prod_{p\in\mathcal{P}, p\mid n} p^{\alpha_p}$$

فإذا استفدنا من 2. أمكننا أن نكتب

$$\varphi(n) = \prod_{p\in\mathcal{P},p|n} \varphi(p^{\alpha_p})$$

وبناءً على 1. يمكننا أن نكتب

$$\begin{aligned}\varphi(n) &= \prod_{p\in\mathcal{P},p|n} p^{\alpha_p}\left(1-\frac{1}{p}\right)\\ &= \prod_{p\in\mathcal{P},p|n} p^{\alpha_p}\prod_{p\in\mathcal{P},p|n}\left(1-\frac{1}{p}\right)\\ &= n\cdot\prod_{p\in\mathcal{P},p|n}\left(1-\frac{1}{p}\right)\end{aligned}$$

فنكون قد أثبتنا أنّ

$$\forall n\in\mathbb{N}^*,\quad \varphi(n) = n\cdot\prod_{p\in\mathcal{P},p|n}\left(1-\frac{1}{p}\right)$$

4. ليكن $n \geq 2$، وليكن k من $\mathbb{Z}$ يُحقّق $\gcd(n,k)=1$. عندئذ ينتمي صف تكافؤ $[k]$ بالقياس n إلى $U(\mathbb{Z}/n\mathbb{Z})$، ونستنتج من ذلك أنّ $[k]^{\mathrm{card}\left(U\left(\mathbb{Z}/n\mathbb{Z}\right)\right)} = [1]$، وهذا يُكافئ $k^{\varphi(n)} = 1 \bmod n$. تسمّى هذه النتيجة مبرهنة Euler .

$$\forall n\geq 2, \forall k\in\mathbb{Z},\quad \gcd(k,n)=1 \Rightarrow k^{\varphi(n)} = 1 \bmod n$$

وبوجه خاص

$$\forall p\in\mathcal{P}, \forall k\in\mathbb{Z},\quad p\nmid k \Rightarrow k^{p-1} = 1 \bmod p$$

وهذه الحالة الخاصّة تسمّى مبرهنة Fermat .

5. ليكن n عدداً طبيعيّاً أكبر أو يساوي 2 . وليكن d قاسماً للعدد n . عندئذ نعلم أنّه توجد زمرة جزئيّة وحيدة من $\mathbb{Z}/n\mathbb{Z}$ عدد عناصرها d ولتكن H_d . ثُمّ إنّ H_d زمرة دوّارة فهي إذن تشاكل تقابليّاً الزمرة $\mathbb{Z}/d\mathbb{Z}$. لنعرّف المجموعة

$$X_d = \left\{x\in\mathbb{Z}/n\mathbb{Z} : O(x) = d\right\}$$

إذا كان x عنصراً من X_d كان عدد عناصر الزمرة التي يولّدها d فهي إذن H_d، إذن x هو أحد عناصر H_d التي تولّد H_d. وبالعكس إذا كان x عنصراً من H_d يولّد H_d كان x عنصراً من $\mathbb{Z}/n\mathbb{Z}$ رتبته d أي $x \in X_d$. فنكون قد أثبتنا أنّ

$$X_d = \left\{x \in H_d : \langle x \rangle = H_d\right\}$$

ومنه

$$\begin{aligned}\operatorname{card}(X_d) &= \operatorname{card}\left(\left\{x \in \mathbb{Z}/d\mathbb{Z} : \langle x \rangle = \mathbb{Z}/d\mathbb{Z}\right\}\right)\\ &= \operatorname{card}\left(U\left(\mathbb{Z}/d\mathbb{Z}\right)\right) = \varphi(d)\end{aligned}$$

ولكنّ المجموعات $\left(X_d\right)_{d|n}$ تكوّن تجزئة للمجموعة $\mathbb{Z}/n\mathbb{Z}$ إذن

$$n = \operatorname{card}(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} \operatorname{card}(X_d) = \sum_{d|n} \varphi(d)$$

6. لتكن $(G,\cdot)$ زمرة منتهية تُحقّق

$$\forall d \in \mathbb{N}^*, \quad \operatorname{card}(\{x \in G : x^d = 1\}) \leq d$$

نضع $n = \operatorname{card}(G)$، ونعرّف

$$X_d = \left\{x \in G : O(x) = d\right\}$$

في حالة قاسمٍ d للعدد n، كما نعرّف $\psi(d) = \operatorname{card}(X_d)$.

إذا كان $X_d \neq \varnothing$، يوجد a في G رتبته تساوي d. أي $\operatorname{card}(\langle a \rangle) = d$، ومنه

$$\forall y \in \langle a \rangle, \quad y^d = 1$$

ومنه الاحتواء $\langle a \rangle \subset \{x \in G : x^d = 1\}$، ولكن بالاستفادة من الفرْض نجد

$$d = \operatorname{card}(\langle a \rangle) \leq \operatorname{card}(\{x \in G : x^d = 1\}) \leq d$$

إذن

$$\langle a \rangle = \{x \in G : x^d = 1\}$$

وعليه يكون $X_d \subset \langle a \rangle$، ولكن عدد العناصر التي رتبتها تساوي d في الزمرة الدوّارة $\langle a \rangle$ يساوي $\varphi(d)$ إذن $\psi(d) = \varphi(d)$ في هذه الحالة. لقد أثبتنا إذن أنّ

$$\forall d \mid n, \quad (X_d \neq \varnothing) \Rightarrow \left(\psi(d) = \varphi(d)\right)$$

وهذا يبرهن أنّه بوجه عام لدينا

$$\forall d \mid n, \quad \psi(d) \leq \varphi(d)$$

ولكنّ المجموعات $\left(X_d\right)_{d|n}$ منفصلة مثنى مثنى واجتماعها يساوي G إذن $n = \sum_{d|n} \psi(d)$.

ومنه

$$0 = \sum_{d|n} \left(\varphi(d) - \psi(d)\right)$$

وجميع حدود المجموع موجبة، إذن لا بُدّ أن يكون

$$\forall d \mid n, \quad \psi(d) = \varphi(d)$$

وبوجه خاص

$$\psi(n) = \varphi(n) > 0$$

فيوجد في G عنصرٌ رتبته n ، والزمرة G زمرة دوّارة.

ملاحظة. نستنتج من هذا التمرين أنّ زمرة العناصر القلوبة في أي حقل منته تكون دوّارة. ■

التمرين 64. نذكّر بأعداد فِرما : $F_n = 2^{2^n} + 1$ ، أياً كان n من $\mathbb{N}$. وليكن p عدداً أوّليّاً يقسم F_n . أثبت أنّه يوجد λ في $\mathbb{N}^*$ يُحقّق $p = 1 + \lambda 2^{n+1}$.

الحل

نُجري قسمة إقليديّة للعدد $p-1$ على 2^{n+1} ، ليكن λ خارج القسمة وليكن r باقي القسمة. فيكون $0 \leq r < 2^{n+1}$.

لمّا كان $p \mid F_n$ استنتجنا أنّ $2^{2^n} = -1 \bmod p$ ومن ثَمّ $2^{2^{n+1}} = 1 \bmod p$. ولمّا كان p عدداً أوّليّاً فردياً استنتجنا انطلاقاً من مبرهنة Fermat الصغرى أنّ $2^{p-1} = 1 \bmod p$.

ولكن نستنتج من المساواة $p - 1 = \lambda 2^{n+1} + r$ أنّ

$$2^{p-1} = (2^{2^{n+1}})^\lambda 2^r = 2^r \bmod p$$

ومن ثَمّ يكون لدينا $2^r = 1 \bmod p$.

لنفترض أنّ $r > 0$ ، عندئذ يكون p قاسماً مشتركاً للعددين $2^r - 1$ و $2^{2^{n+1}} - 1$ ، فهو قاسم للعدد

$$\gcd(2^{2^{n+1}} - 1, 2^r - 1) = 2^{\gcd(2^{n+1}, r)} - 1$$

ولمّا كان $\gcd(2^{n+1},r)=2^k$ حيث $0\le k\le n$، لأنّ $r<2^{n+1}$، استنتجنا أنّ

$$2^{2^k}=1 \bmod p \quad \text{حيث} \quad 0\le k\le n$$

وهذا يقتضي أنّ $2^{2^n}=(2^{2^k})^{2^{n-k}}=1 \bmod p$، ولكن نعلم من جهة أخرى أنّ $2^{2^n}=-1 \bmod p$ إذن $p \mid 2$ أو $p=2$ وهذا خُلفٌ واضح. إذن لا بُدّ أن يكون $r=0$، وهذا يبرهن أنّ

$$p=1+\lambda 2^{n+1}$$

وهي النتيجة المرجوّة. ■

ملاحظة. يمكن الاستفادة من هذه النتيجة لإثبات أنّ F_3 و F_4 أوّليّان ولإيجاد القاسم 641 للعدد F_5. فمثلاً إذا كان p عدداً أولياً يقسم F_5 وجب أن يكون p من الشكل

$$p_\lambda = 1+\lambda 2^6 = 1+64\lambda$$

فنبدأ بتجريب الأولية من بين هذه الأعداد، فنجرب على التوالي 193، 257، 449، 577، ثمّ 641. فنعثر على القاسم المنشود.

كثيرات الحدود على حقل تبديليّ

1. عموميات

1-1. وصف البنية والمفاهيم الأساسيّة

لتكن A حلقة تبديلية ولنرمز بالرمز $\mathcal{X}$ إلى المجموعة $A^{(\mathbb{N})}$ أي مجموعة المتتاليات $(a_n)_{n\in\mathbb{N}}$ التي حدودها من A والتي يكون عدد حدودها غير الصفريّة منتهياً. أي إنّه إذا كانت $(a_n)_{n\in\mathbb{N}}$ متتالية حدودها من A كان

$$\begin{aligned}(a_n)_{n\in\mathbb{N}} \in \mathcal{X} \quad &\Leftrightarrow \quad \operatorname{card}(\{n \in \mathbb{N} : a_n \neq 0\}) < +\infty \\ &\Leftrightarrow \quad \exists n_0 \in \mathbb{N}, \quad \forall n > n_0 \quad a_n = 0\end{aligned}$$

نعرّف على هذه المجموعة $\mathcal{X}$ القوانين التالية:

① إذا كان $a = (a_n)_{n\in\mathbb{N}}$ و $b = (b_n)_{n\in\mathbb{N}}$ عنصرين من $\mathcal{X}$ كان

$$a + b = (a_n + b_n)_{n\in\mathbb{N}} \in \mathcal{X}$$

② إذا كان $a = (a_n)_{n\in\mathbb{N}}$ عنصراً من $\mathcal{X}$، و λ عنصراً من A كان

$$\lambda \cdot a = (\lambda a_n)_{n\in\mathbb{N}} \in \mathcal{X}$$

③ إذا كان $a = (a_n)_{n\in\mathbb{N}}$ و $b = (b_n)_{n\in\mathbb{N}}$ عنصرين من $\mathcal{X}$ كان

$$a \times b = \left(\sum_{k=0}^{n} a_k b_{n-k}\right)_{n\in\mathbb{N}} \in \mathcal{X}$$

إذ نتحقق بسهولة أنه إذا كانت حدود المتتالية $(a_n)_{n\in\mathbb{N}}$ معدومة بدءاً من الدليل n_0، وكانت حدود المتتالية $(b_n)_{n\in\mathbb{N}}$ معدومة بدءاً من الدليل m_0، كانت حدود المتتالية $a + b$ معدومة بدءاً من الدليل $\max(n_0, m_0)$، وكانت حدود المتتالية $a \times b$ معدومة بدءاً من $n_0 + m_0$. وهذا ما يبيّن صحة تعريف القوانين السابقة.

ثُمّ، لأنّ A حلقة تبديليّة، فإننا نتحقق بسهولة صحّة الخواص التالية:

❶ البنية $(\mathcal{X},+,\times)$ حلقة تبديلية، واحدها العنصر $\mathbb{1}=(1,0,0,\ldots)$ أي المتتالية التي أوّل حد فيها هو حيادي الضرب في A وبقية حدودها أصفار.

❷ أيّاً كان a و b من $\mathcal{X}$، و λ و μ من A كان

❖ $1_A\cdot a=a$

❖ $(\lambda+\mu)\cdot a=\lambda\cdot a+\mu\cdot a$

❖ $\lambda(a+b)=\lambda\cdot a+\lambda\cdot b$

❖ $(\lambda\cdot\mu)\cdot a=\lambda\cdot(\mu\cdot a)$

❸ أيّاً كان a و b من $\mathcal{X}$، و λ من A كان : $\lambda(a\times b)=(\lambda a)\times b$.

فنقول إذن إنّ البنية $(\mathcal{X},+,\times,\cdot)$ جبر تبديلي على الحلقة A.

لنرمز بالرمز δ_k إلى المتتالية $(\delta_{k,n})_{n\in\mathbb{N}}$ من $\mathcal{X}$، المعرّفة كما يأتي:

$$\delta_k=(0,0,\ldots,\underbrace{1}_{k},0,\ldots)\quad \text{أو}\quad \delta_{k,n}=\begin{cases}1 & : \ n=k\\ 0 & : \ n\neq k\end{cases}$$

أي المتتالية التي جميع حدودها أصفار ما عدا الحد الذي دليله k فهو يساوي 1. نلاحظ أنّ δ_0 هو العنصر الحيادي بالنسبة إلى $\times$ ولقد رمزنا إليه سابقاً بالرمز $\mathbb{1}$. أمّا العنصر δ_1 الذي يساوي $(0,1,0,\ldots)$ فنرمز إليه عادة بالرمز X.

لنثبت أنّ $\delta_n\times\delta_1=\delta_{n+1}$. في الحقيقة إذا وضعنا $\delta_n\times\delta_1=(a_p)_{p\in\mathbb{N}}$ كان

$$a_p=\sum_{k=0}^{p}\delta_{n,k}\delta_{1,p-k}=\delta_{n,p-1}=\begin{cases}1 & : \ p=n+1\\ 0 & : \ p\neq n+1\end{cases}$$

ينجم عن ذلك بالتدريج أنّه، أياً كان n من $\mathbb{N}^*$، كان

$$X^n=\underbrace{X\times X\times\cdots\times X}_{n}=\delta_n$$

وإذا كان $a=(a_n)_{n\in\mathbb{N}}$ عنصراً من $\mathcal{X}$، فإنّ a يُكتب بأسلوب وحيد بالصيغة :

$$a=\sum_{n\geq 0}a_n\cdot\delta_n=a_0+\sum_{n\geq 1}a_n\cdot X^n$$

نلاحظ أنّ المجموع السابق منتهٍ لأنّ $a_n=0$ بدءاً من حد معيّن.

نرمز عادة بالرمز $A[X]$ إلى البنية $(\mathcal{X},+,\times,\cdot)$. ونسميها **جبر كثيرات الحدود التي ثوابتها من A بمتحوّل واحد X.**

تنبيه مهم. من الآن فصاعداً سنفترض أنّ A حقل تبديلي وسنرمز إليه بالرمز $\mathbb{K}$ وسنرمز بالرمز $\mathbb{K}[X]$ إلى جبر كثيرات الحدود الموافق.

لنلخّص ما توصّلنا إليه:

- إنّ البنية الجبرية $(\mathbb{K}[X],+,\times,\cdot)$ جبر على الحقل $\mathbb{K}$، وبوجه خاص تكون البنية $(\mathbb{K}[X],+,\times)$ حلقة تبديلية، و $(\mathbb{K}[X],+,\cdot)$ فضاء شعاعي على $\mathbb{K}$.
- وإذا رمزنا بالرمز X إلى العنصر $(0,1,\ldots,0,\ldots)$ من $\mathbb{K}^{(\mathbb{N})}$ واصطلحنا أنّ $X^0 = \mathbb{1} = (1,0,\ldots,0,\ldots)$ فإنّ الجماعة $(X^n)_{n\geq 0}$ تكوّن أساساً للفضاء الشعاعي $(\mathbb{K}[X],+,\cdot)$ على الحقل $\mathbb{K}$. أي إنّ كلّ عنصر P من $\mathbb{K}[X]$ يُكتب وبشكل وحيد على الوجه الآتي:
$$P = \sum_{k\geq 0} a_k X^k$$
ويكون المجموع منتهياً لأنّ $a_k = 0$ بدءاً من حدّ معيّن. ونسمّي الأساس $(X^n)_{n\geq 0}$ الأساس القانوني للفضاء الشعاعي $\mathbb{K}[X]$ على $\mathbb{K}$.

2-1. **ملاحظات** : إذا رمزنا إلى المتحوّل X بالرمز T عوضاً عن X فإنّنا نحصل على الجبر $\mathbb{K}[T]$ عوضاً عن $\mathbb{K}[X]$. لقد جرت العادة، أنّ نكتب PQ دلالة على $P\times Q$ و λP دلالة على $\lambda\cdot P$ في حالة (P,Q,λ) من $(\mathbb{K}[X])^2\times\mathbb{K}$. وذلك لعدم إمكان وقوع التباس بين القانونين فأحدهما داخليّ والآخر خارجيّ. هذا ونطابق بين الحقل $\mathbb{K}$، والحقل الجزئي $\{\lambda 1_{\mathbb{K}[X]} : \lambda\in\mathbb{K}\} = \mathbb{K}\cdot 1_{\mathbb{K}[X]}$ من $\mathbb{K}[X]$.

3-1. **تعريف**. ليكن $P = \sum_{k\geq 0} a_k X^k$ عنصراً من $\mathbb{K}[X]$. إذا كان $P = 0$ قلنا إنّ
$$\operatorname{val}(P) = +\infty \quad \text{و} \quad \deg(P) = -\infty$$
أمّا إذا كان $P \neq 0$ فإنّنا نعرّف :
$$\deg(P) = \max\{k\in\mathbb{N} : a_k \neq 0\}$$
و
$$\operatorname{val}(P) = \min\{k\in\mathbb{N} : a_k \neq 0\}$$
ونسمّي $\deg(P)$ **درجة كثير الحدود** P. يبقى هذا التعريف في حالة كون $\mathbb{K}$ حلقة تبديلية.

1-4. تعريف. إذا كان $P=\sum_{k\geq 0} a_k X^k$ عنصراً من $\mathbb{K}[X]$ وكان $P\neq 0$ أسمينا الحدَّ $a_d X^d$ في حالة $d=\deg(P)$ **الحدّ الأعلى درجة في** P **أو الحد المُسَيْطِر في** P، وإذا كان $a_d=1$ قلنا إنّ P كثير حدود **واحديّ** أو **نظامي**.

1-5. مبرهنة. ليكن كثيرا الحدود P و Q من $\mathbb{K}[X]$. في هذه الحالة :

- $\deg(P+Q)\leq \max(\deg(P),\deg(Q))$. وتقع المساواة في الحالة التي يكون فيها $\deg(P)\neq\deg(Q)$.
- $\operatorname{val}(P+Q)\geq \min(\operatorname{val}(P),\operatorname{val}(Q))$. وتقع المساواة في الحالة التي يكون فيها $\operatorname{val}(P)\neq\operatorname{val}(Q)$.
- $\deg(P\times Q)=\deg(P)+\deg(Q)$.
- $\operatorname{val}(P\times Q)=\operatorname{val}(P)+\operatorname{val}(Q)$.

الإثبات

إنّ الخاصتين الأولى والثانية بسيطتان، والخاصة الرابعة مماثلة في إثباتها للخاصة الثالثة. لنثبت إذن الخاصة الثالثة. من الواضح أنّها صحيحة إذا كان $P=0$ أو $Q=0$. لنفترض إذن أننا لسنا في مثل هذه الحالات، أي إنّ

$$P=\sum_{k=0}^{n} a_k X^k \text{ مع } a_n\neq 0 \text{ و } Q=\sum_{k=0}^{m} b_k X^k \text{ مع } b_m\neq 0.$$

ويكون $P\times Q=\sum_{k\geq 0} c_k X^k$ مع $c_p=\sum_{t+s=p} a_t b_s$.

- إذا كان $n+m<p$ و $t+s=p$ فلا بدّ أن يكون $t>n$ أو $s>m$ ومن ثمّ $a_t=0$ أو $b_s=0$ مما يقتضي أنّ $c_p=0$.
- إذا كان $n+m=p$ و $t+s=p$ فلا بدّ أن يكون $t\geq n$ أو $s\geq m$، ومن ثمّ $(n,m)\neq(t,s)$ يقتضي أيضاً $a_t b_s=0$. نستنتج إذن أنّه يجب أن يكون $c_{n+m}=a_n b_m$، ولكنّ $\mathbb{K}$ حقل تبديليّ فهو حلقة تامّة، ومنه

$$(a_n\neq 0 \text{ و } b_m\neq 0)\Leftarrow c_{n+m}\neq 0$$

إذن $\deg(P\times Q)=\deg(P)+\deg(Q)$. ❐

1-6. **ملاحظة**. واضح من الإثبات السابق، أنّ المبرهنة السابقة تبقى صحيحة في $A[X]$ إذا كانت A حلقة تامّة وتصبح خاطئة إذا حَوَتْ الحلقة A قواسم للصفر.

1-7. **نتيجة**. إنّ الحلقة $(\mathbb{K}[X],+,\times)$ حلقة تامّة. والعناصر القَلوبة فيها هي $\mathbb{K}\backslash\{0\}$ أي $U(\mathbb{K}[X]) = \mathbb{K}\backslash\{0\}$.

الإثبات

في الحقيقة، إنّ الشرط $PQ = 0$ يكافئ $\deg(PQ) = -\infty$ أو

$$\deg(P) + \deg(Q) = -\infty$$

وذلك بمقتضى المبرهنة 1-5.، فإمّا أن يكون $\deg(P) = -\infty$ (أي $P = 0$) أو أن يكون $\deg(Q) = -\infty$ (أي $Q = 0$).

من الواضح أنّ $U(\mathbb{K}[X]) \supset \mathbb{K}\backslash\{0\}$، ومن ناحية أخرى يكون كثير الحدود P من $\mathbb{K}[X]$ قَلوباً إذا وُجِدَ كثير حدود Q في $\mathbb{K}[X]$ يُحقّق $PQ = 1$ وهذا يقتضي أنّ

$$\deg(P) + \deg(Q) = 0$$

ومن ثَمّ $\deg(P) = 0$ أو $P \in \mathbb{K}\backslash\{0\}$. ❐

1-8. **تعريف**. ليكن كثيرا الحدود $P = \sum_{k=0}^{n} a_k X^k$ و $Q = \sum_{k=0}^{m} b_k X^k$ من $\mathbb{K}[X]$. نسمّي **ناتج تركيب كثيري الحدود** P و Q كثير الحدود $P \circ Q$، أو $P(Q)$، المعرّف بالعلاقة

$$P \circ Q = \sum_{k=0}^{n} a_k Q^k$$

نتحقق بسهولة أنّ قانون تركيب كثيرات الحدود تجميعيّ، ولكن ليس تبديلياً، فمثلاً $(1+X)\circ 1 = 2$ في حين نجد أنّ $1 \circ (1+X) = 1$. و نلاحظ من ناحية أخرى أنّ $(P+R)\circ Q = P\circ Q + R\circ Q$، في حين يبيّنُ المثال التالي أنّ تركيب كثيرات الحدود لا يقبل التوزيع على الجمع من اليسار، إذ

$$1\circ(1+X) = 1 \quad \text{و} \quad 1\circ 1 + 1\circ X = 2.$$

1-9. **تعريف** : ليكن كثير الحدود $P=\sum_{k=0}^{n} a_k X^k$ من $\mathbb{K}[X]$. نسمّي التطبيق

$$\widetilde{P}:\mathbb{K}\to\mathbb{K},\quad x\mapsto\sum_{k=0}^{n} a_k x^k$$

التابع الحدودي الموافق لكثير الحدود P . ونتحقق بسهولة أنّ:

$$\forall (P,Q)\in(\mathbb{K}[X])^2,\forall\lambda\in\mathbb{K},\quad \widetilde{P+Q}=\widetilde{P}+\widetilde{Q},\quad \widetilde{P\times Q}=\widetilde{P}\cdot\widetilde{Q},$$

$$\widetilde{\lambda P}=\lambda\widetilde{P},\qquad \widetilde{P\circ Q}=\widetilde{P}\circ\widetilde{Q}.$$

ولقد جرت العادة أن نكتب $P(a)$ عوضاً عن $\widetilde{P}(a)$ أياً كان a من $\mathbb{K}$.

من المهم جداً ملاحظة أنه يمكن لتابعٍ حدوديٍّ موافق لكثير حدود غير الصفر أن يكون تابعاً صفرياً. فمثلاً إذا تأمّلنا كثير الحدود $P=X^2+X$ على الحقل $\mathbb{F}_2=\mathbb{Z}/2\mathbb{Z}$ وجدنا أنّ $P\neq 0$ لأنه من الدرجة الثانية، في حين يكون $\forall x\in\mathbb{F}_2, \widetilde{P}(x)=0$.

2. قابلية القسمة في $\mathbb{K}[X]$

2-1. **تعريف**. لنذكّر في هذه الحالة الخاصّة بالتعاريف العامة.

- إذا كان P و Q عنصرين من $\mathbb{K}[X]$ و $Q\neq 0$. قلنا إنّ Q **يقسم** P وكتبنا $Q|P$ إذا وفقط إذا وُجِدَ R في $\mathbb{K}[X]$ يُحقّق $P=RQ$.
- وإذا كان $P|Q$ و $Q|P$ ، وجدنا λ في $\mathbb{K}^*=\mathbb{K}\backslash\{0\}$ يُحقّق $P=\lambda Q$ ، وعندها نقول إنّ كثيري الحدود P و Q **شريكان**.

2-2. **مبرهنة**. ليكن كثيرا الحدود A و B من $\mathbb{K}[X]$ ، مع $B\neq 0$. عندئذ توجد ثنائية (Q,R) وحيدة من $\mathbb{K}[X]\times\mathbb{K}[X]$ تُحقّق

$$A=QB+R \quad \text{و} \quad \deg R<\deg B$$

الإثبات

- لنثبت أوّلاً الوحدانية. إذا كان $A=QB+R=Q_1B+R_1$ كان

$$R-R_1=(Q_1-Q)B$$

والشرط $Q_1-Q\neq 0$ يقتضي $\deg((Q_1-Q)B)\geq\deg B$ ومنه

$$\deg B\leq\deg(R-R_1)\leq\max(\deg R,\deg R_1)<\deg B$$

وهذا خُلفٌ. إذن $Q=Q_1$ و من ثَمّ $R=R_1$.

❄ لنأتِ إلى إثبات الوجود.

نفترض أنّ $0 \leq d = \deg B$ ونضع $B = \sum_{k=0}^{d} b_k X^k$، مع $b_p \neq 0$. سنثبت النتيجة المطلوبة بالتدريج على درجة A.

- إذا كان $A = 0$، أو كانت $\deg A < d$ وفت الثنائيّة $(Q, R) = (0, A)$ بالغرض.
- ليكن إذن n عدداً أكبر أو يساوي d. ولنفترض أننا أثبتنا صحة الخاصة المطلوبة عند قسمة أيٍّ من كثيرات الحدود A، التي لا تزيد درجتها على $n - 1$، على B.

ليكن $A = \sum_{k=0}^{n} a_k X^k$ من $\mathbb{K}[X]$، يُحقّق $\deg A = n$. ولنعرّف

$$A_1 = A - \frac{a_n}{b_d} X^{n-d} \cdot B$$

إنّ $\deg A_1 \leq n - 1$، واستناداً إلى فرْض التدريج، نجد زوجاً (Q_1, R_1) يُحقّق

$$A_1 = Q_1 B + R_1 \text{ و } \deg R_1 < \deg B$$

عندئذ يكون

$$A = \left(\frac{a_n}{b_d} X^{n-d} + Q_1 \right) B + R_1$$

فتفي الثنائيّة $(Q, R) = \left(\frac{a_n}{b_d} X^{n-d} + Q_1, R_1 \right)$ بالغرض المطلوب، ويتم الإثبات. ❐

3-2. مثال. نبيّن فيما يلي عملية القسمة الإقليدية لكثير الحدود A على كثير الحدود B وقد عرّفنا

$$A = 2X^4 + 5X^3 - X^2 + 2X + 1 \text{ و } B = 2X^2 - 3X + 1$$

$$\begin{array}{rrrrrrrrrr|l}
A \rightarrow & 2X^4 & + & 5X^3 & - & X^2 & + & 2X & + & 1 & 2X^2 - 3X + 1 \leftarrow B \\
\cline{11-11}
 & -2X^4 & + & 3X^3 & - & X^2 & & & & & \\
\cline{2-10}
 & & & 8X^3 & - & 2X^2 & + & 2X & + & 1 & X^2 + 4X + 5 \leftarrow Q \\
 & & - & 8X^3 & + & 12X^2 & - & 4X & & & \\
\cline{3-10}
 & & & & & 10X^2 & - & 2X & + & 1 & \\
 & & & & - & 10X^2 & + & 15X & - & 5 & \\
\cline{5-10}
 & & & & & R & \rightarrow & 13X & - & 4 &
\end{array}$$

فنكتب إذن

$$A(X) = B(X)(X^2 + 4X + 5) + 13X - 4$$

2-4. **مبرهنة**. إنّ الحلقة $(\mathbb{K}[X],+,\times)$ حلقة رئيسية. أي إنّ كلّ مثالي فيها مثاليٌّ رئيسيّ.

الإثبات

ليكن $\mathcal{I}$ مثالياً في $\mathbb{K}[X]$. يمكن أن نفترض أنّه مختلف عن $\{0\}$، إذْ في هذه الحالة ليس هناك ما يجب إثباته، ولنعرّف $\mathcal{N} = \{\deg P : P \in \mathcal{I}\backslash\{0\}\}$. إنّ $\mathcal{N}$ مجموعة جزئية غير خالية في $\mathbb{N}$ فتقبل إذن عنصراً أصغرياً. ونجد P_0 في $\mathcal{I}\backslash\{0\}$ يُحقّق

$$\deg P_0 = \min\left\{\deg P : P \in \mathcal{I}\setminus\{0\}\right\}$$

بالطبع لدينا الاحتواء $\mathcal{I} \supset \{P_0Q : Q \in \mathbb{K}[\mathrm{X}]\} = P_0\,\mathbb{K}[\mathrm{X}]$.

وبالعكس، إذا كان P عنصراً من $\mathcal{I}$، نجد (Q,R) في $(\mathbb{K}[X])^2$ يُحقّق

$$\deg R < \deg P_0 \quad \text{و} \quad P = QP_0 + R$$

ولكن $R = P - QP_0$ ينتمي إلى $\mathcal{I}$، فإذا كان $R \neq 0$ ناقض ذلك تعريف P_0. إذن $R = 0$ ومنه $P \in P_0\mathbb{K}[X]$. فنكون قد أثبتنا أنّ $P_0\mathbb{K}[X] = \mathcal{I}$، والمثالي $\mathcal{I}$ مثالي رئيسي. ❐

2-5. **ملاحظة**. إذا كان $P\,\mathbb{K}[X] = P_0\,\mathbb{K}[X]$ كان P و P_0 شريكين أي يوجد λ في $\mathbb{K}^*$ يُحقّق $P = \lambda P_0$.

لقد درسنا سابقاً قابلية القسمة في حلقة رئيسية بوجه عام وقدّمنا العديد من التعاريف. سنعود للتذكير بها في الحالة الخاصة الموافقة للحلقة الرئيسية $\mathbb{K}[X]$.

2-6. **تعريف**. لتكن كثيرات الحدود $A_1, A_2, \ldots, A_n$ من $\mathbb{K}[X]$. نقول إنّ P **مضاعف مشترك بسيط**، أو أصغر، لكثيرات الحدود $A_1, A_2, \ldots, A_n$ إذا كان :

$$P\mathbb{K}[X] = \bigcap_{i=1}^{n} A_i.\mathbb{K}[X]$$

ونكتب حينئذ $P \in \operatorname{Lcm}(A_1, A_2, \ldots, A_n)$.

ونقول إنّ Q **قاسم مشترك أعظم** لكثيرات الحدود $A_1, A_2, \ldots, A_n$ إذا كان :

$$Q\mathbb{K}[X] = A_1\mathbb{K}[X] + A_2\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$$

وكذلك نكتب عندئذ $Q \in \operatorname{Gcd}(A_1, A_2, \ldots, A_n)$.

لمّا كانت عناصر كلٍ من المجموعتين $\mathrm{Lcm}\,(A_1, A_2, \ldots, A_n)$ و $\mathrm{Gcd}\,(A_1, A_2, \ldots, A_n)$ متناسبة (انظر الملاحظة 2-5.) فإننا نصطلح أن نسمّي المضاعف المشترك الأصغر لكثيرات الحدود $A_1, A_2, \ldots, A_n$ العنصر الواحدي أوالنظامي في المجموعة $\mathrm{Lcm}\,(A_1, A_2, \ldots, A_n)$ ونرمز إليه بالرمز $\mathrm{lcm}\,(A_1, A_2, \ldots, A_n)$. وكذلك نصطلح أن نسمّي القاسم المشترك الأعظم لكثيرات الحدود $A_1, A_2, \ldots, A_n$ ذلك العنصر الواحدي أو النظامي الوحيد في المجموعة $\mathrm{Gcd}\,(A_1, A_2, \ldots, A_n)$ ونرمز إليه بالرمز $\mathrm{gcd}\,(A_1, A_2, \ldots, A_n)$.

2-7. **مبرهنة**. لتكن كثيرات الحدود $A_1, A_2, \ldots, A_n$ من $\mathbb{K}[X]$. عندئذ

$$\mathrm{lcm}\,(A_1, A_2, \ldots, A_n) = \mathrm{lcm}\,(A_1, \mathrm{lcm}\,(A_2, \ldots, A_n))$$
$$\mathrm{gcd}\,(A_1, A_2, \ldots, A_n) = \mathrm{gcd}\,(A_1, \mathrm{gcd}\,(A_2, \ldots, A_n))$$

2-8. **تعريف**. نقول إنّ $A_1, A_2, \ldots, A_n$ كثيرات حدود **أوّليّة فيما بينها** إذا وفقط إذا كان

$$\mathrm{gcd}\,(A_1, A_2, \ldots, A_n) = 1$$

لاحظ أنّ هذا يكافئ قولنا

$$\mathbb{K}[X] = A_1\mathbb{K}[X] + A_2\mathbb{K}[X] + \cdots + A_n\mathbb{K}[X]$$

وهذا بدوره يكافئ وجود كثيرات حدود $P_1, P_2, \ldots, P_n$ من $\mathbb{K}[X]$ تُحقّق المساواة

$$\sum_{i=1}^{n} A_i P_i = 1$$

يسمى هذا التكافؤ مبرهنة Bézout.

2-9. **مبرهنة**

- لتكن كثيرات الحدود A و B و C من $\mathbb{K}[X]$. إذا كان $A \mid BC$ وكان A و C أوليّين فيما بينهما كان $A \mid B$.
- إذا كانت A و $B_1, B_2, \ldots, B_n$ كثيرات حدود من $\mathbb{K}[X]$ وكان B_i و A أوّليين فيما بينهما أياً كان i من $\mathbb{N}_n$، كان $\mathrm{gcd}\,(A, \prod_{i=1}^{n} B_i) = 1$.
- لتكن A و $B_1, B_2, \ldots, B_n$ كثيرات حدود من $\mathbb{K}[X]$. نفترض أنّ كثيرات الحدود $B_1, B_2, \ldots, B_n$ أوّليّة فيما بينها مثنى مثنى، وأنّ $B_i \mid A$ أياً كان i من $\mathbb{N}_n$، عندئذ يكون $\left(\prod_{i=1}^{n} B_i\right) \Big| A$.

الإثبات

- إذا كان A و C أوليّين فيما بينهما، وجدنا كثيري حدود P_1 و P_2 يُحقّقان مساواة بيزو $CP_1 + AP_2 = 1$، ومنه $BCP_1 + BAP_2 = B$ ولأنّ $A \mid BC$ نجد $A|B$.

- يجري إثبات الخاصة بالتدريج على n. لنثبت صحتها في حالة $n = 2$.

$$\exists(P_1, Q_1) \in \mathbb{K}[X], \quad P_1A + Q_1B_1 = 1$$
$$\exists(P_2, Q_2) \in \mathbb{K}[X], \quad P_2A + Q_2B_2 = 1$$

وبضرب العلاقتين طرفاً بطرف، نجد $AP + B_1B_2Q = 1$ وقد عرّفنا

$$Q = Q_1Q_2 \quad \text{و} \quad P = P_1B_2Q_2 + P_2B_1Q_1 + P_1P_2A$$

أي إنّ A و B_1B_2 أوليّان فيما بينهما. ونترك للقارئ مهمة التعميم إلى n.

- سنثبت الخاصة الأخيرة أيضاً في حالة $n = 2$، تاركين مهمة التعميم بالتدريج تمريناً للقارئ.

إنّ $B_1|A$ إذن $A = B_1P_1$، واستناداً إلى الخاصة الأولى $B_2|B_1P_1$ و B_1 و B_2 أوليّان فيما بينهما، إذن $B_2|P_1$ ومنه $P_1 = B_2P_2$، نستنتج إذن أنّ $A = B_1B_2P_2$ أو $(B_1B_2)|A$. ❐

2-10. نتيجة. ليكن a و b عنصرين من $\mathbb{K}$ يُحقّقان $a \neq b$. وليكن (n, m) من $\mathbb{N}^{*2}$. عندئذ يكون

$$\gcd\left((X-a)^n, (X-b)^m\right) = 1$$

الإثبات

نلاحظ أوّلاً أنّ $\gcd(X-a, X-b) = 1$ وذلك لأنّ

$$\lambda(X-a) - \lambda(X-b) = 1$$

حين يكون $\lambda = \dfrac{1}{b-a}$. وإذا طبّقنا النقطة الثانية من المبرهنة السابقة بعد أن نختار

$$A = X - a \quad \text{و} \quad \forall i \in \mathbb{N}_m, \;\; B_i = X - b$$

وجدنا $\gcd(X-a, (X-b)^m) = 1$. وإذا طبّقنا مجدّداً النقطة نفسها بعد أن نختار

$$A = (X-b)^m \quad \text{و} \quad \forall i \in \mathbb{N}_n, \;\; B_i = X - a$$

وجدنا

$$\gcd\left((X-a)^n, (X-b)^m\right) = 1$$ ❐

11-2. خوارزمية إقليدس

يُحسب القاسم المشترك الأعظم لكثيري حدود من $\mathbb{K}[X]$ باتباع ما يسمّى **خوارزمية إقليدس**، وهي مُطابِقة في خطوطها العريضة لتلك الخوارزمية التي تفيد في حساب القاسم المشترك الأعظم لعددين صحيحين، التي درسناها سابقاً. لنذكّر بهذه الخوارزميّة.

تكمن نقطة انطلاق هذه الخوارزمية في الملاحظة التالية:

﴿أياً كان (Q,B,A) من $(\mathbb{K}[X])^3$ كان $\mathrm{Gcd}(A,B) = \mathrm{Gcd}(A-QB,B)$﴾

وذلك لأن مجموعة قواسم A و B هي نفسها مجموعة قواسم B و $A-QB$.

ليكن A و B كثيري حدود من $\mathbb{K}[X]$ مختلفين عن الصفر، يمكننا أن نفترض أنّ $\deg B \leq \deg A$ وذلك دون الإخلال بعموميّة المسألة.

ثُمّ نعرّف المتتالية التدريجية $(R_k)_{k\geq 0}$ من $\mathbb{K}[X]$ على الوجه الآتي :

نضع $R_0 = A$ و $R_1 = B$. وإذا كان $R_k = 0$ وضعنا $R_{k+1} = 0$ وإلاّ عرّفنا R_{k+1} بأنّه باقي القسمة الإقليدية لكثير الحدود R_{k-1} على R_k.

لنثبت، بالتدريج على $1 \leq k$، أنّ

$$\deg R_k \leq \deg B - k + 1$$

في الحقيقة، إذا كان $k = 1$ كانت العلاقة واضحة. وإذا كانت العلاقة صحيحة عند k، فإمّا أن يكون $R_k = 0$، ومن ثَمّ تبقى العلاقة صحيحة عند القيمة $k+1$، و إمّا أن يكون $R_k \neq 0$، وينتج منه أنّ $\deg R_{k+1} < \deg R_k$، إذن

$$\deg R_{k+1} \leq \deg R_k - 1 \leq \deg B - k + 1 - 1 = \deg B - (k+1) + 1$$

والعلاقة صحيحة عند القيمة $k+1$.

ينجم عن ذلك أنّه إذا كان $k_0 = \deg B + 2$ كان $\deg R_{k_0} \leq -1$ أي $R_{k_0} = 0$.

تفيدنا هذه الملاحظة بتعريف العدد الطبيعي N بالعلاقة

$$N = \max\{k \in \mathbb{N} : R_k \neq 0\}$$

وهو، بناءً على ما سبق، يحقق $N \leq \deg B + 1$، ويكون $R_N \neq 0$ و $R_{N+1} = 0$.

مهما يكن k من $\mathbb{N}_N$ نجد Q_k يُحقّق

$$R_{k-1} = Q_k R_k + R_{k+1}$$

وباستعمال الخاصّة المذكورة آنفاً نجد

$$\operatorname{Gcd}(A,B)=\operatorname{Gcd}(R_0,R_1)=\operatorname{Gcd}(R_1,R_2)=\cdots=\operatorname{Gcd}(R_N,0)$$

فيكون إذن $\gcd(A,B)$ و R_N شريكين، ونحصل على $\gcd(A,B)$ من R_N بقسمته على ثابت الحد الأعلى درجة فيه، ليصبح واحدياً.

هذا وإذا عرّفنا المتتاليتين $(S_k)_{0\le k\le N}$ و $(T_k)_{0\le k\le N}$ من $\mathbb{K}[X]$ بالعلاقات

$$\begin{aligned} S_0 &= 1, \quad S_1 = 0, \quad S_{k+1} = S_{k-1} - Q_k S_k \\ T_0 &= 0, \quad T_1 = 1, \quad T_{k+1} = T_{k-1} - Q_k T_k \end{aligned}$$

أمكننا أن نثبت بالتدريج على k من $\{0,1,\ldots,N\}$ أنّ $R_k = S_k A + T_k B$، ومن ثمّ يكون $R_N = S_N A + T_N B$.

تفيدنا هذه الخوارزميّة المعمّمة بتعيين U_0 و V_0 من $\mathbb{K}[X]$ يُحقّقان

$$U_0 A + V_0 B = \gcd(A,B)$$

نلاحظ بوجه خاص أنّ عدد عمليات قسمة كثيرات الحدود اللازمة لحساب $\gcd(A,B)$ لا يزيد على $\min(\deg A, \deg B)$.

2-12. مثال. ليكن $A = X^3 + X^2 + 1$ و $B = X^2 + 1$ من $\mathbb{K}[X]$، عيّن القاسم المشترك الأعظم $D = \gcd(A,B)$، ثُمّ أوجد V_0 و U_0 يُحقّقان

$$AU_0 + BV_0 = D$$

لقد بيّنّا نتائج الحساب في الجدول التالي :

k	R_k	Q_k	S_k	T_k
0	X^3+X^2+1	$-$	1	0
1	X^2+1	$X+1$	0	1
2	$-X$	$-X$	1	$-X-1$
3	1	$-X$	$-X$	$-X^2-X+1$
4	0			

و منه $D=1$ و $U_0 = -X$ و $V_0 = 1 - X - X^2$.

2-13. **ملاحظة مهمة**. ليكن كثيرا الحدود A و B من $\mathbb{K}[X]\backslash\{0\}$ ولنفترض أنّه يوجد U_0 و V_0 يُحقّقان $AU_0+BV_0=1$. عندئذ يكون

$$\left\{(u,v)\in(\mathbb{K}[X])^2 : Au+Bv=1\right\}=\left\{(U_0+hB,V_0-hA) : h\in\mathbb{K}[X]\right\}$$

في الحقيقة، إنّ الاحتواء $\supset$ تافه.

وبالعكس، إذا كان $Au+Bv=1$ أي $Au+Bv=AU_0+BV_0$ كان

$$A\,(u-U_0)=B\,(V_0-v) \qquad (*)$$

ولكن A أوليّ مع B من جهة، و A يقسم $B(V_0-v)$ من جهة أخرى. إذن A يقسم V_0-v . أي يوجد h ينتمي إلى $\mathbb{K}[X]$ يُحقّق $v=V_0-hA$. وبالتعويض في $(*)$ والاختصار على A نجد $u=u_0-hB$.

2-14. **ملاحظة**. إذا كان A و B عنصرين من $\mathbb{K}[X]\backslash\{0\}$، وأردنا حساب $\mathrm{lcm}\,(A,B)$ فيمكننا أن نبدأ بحساب $\mathrm{gcd}\,(A,B)$ ، ثم نستنتج المطلوب بالاستفادة من العلاقة التالية :

$$\mathrm{gcd}\,(A,B)\cdot\mathrm{lcm}\,(A,B)\sim A\cdot B\,.$$

2-15. **تعريف**. نقول إنّ كثير الحدود P من $\mathbb{K}[X]$ غير قابل للتحليل، أو غير خزول، إذا وفقط إذا كان

- $\deg P>0$.
- $\forall Q\in\mathbb{K}[X],\;\; Q|P\Rightarrow(\deg Q=\deg P)\vee(\deg Q=0)$.

أو بقول آخر إذا كانت قواسم P هي عناصر $\mathbb{K}^*$ وشركاء P .

ينجم عن هذا التعريف أنّ كثيرات الحدود من الدرجة الأولى في $\mathbb{K}[X]$ تكون غير خزولة، ولكن العكس غير صحيح عموماً.

2-16. **مبرهنة**. إذا كان P كثير حدود غير خزول في $\mathbb{K}[X]$، وكان A عنصراً من $\mathbb{K}[X]$، فهناك تكافؤ بين كوْن كثيرا الحدود A و P أوليين فيما بينهما وبين كوْن P لا يقسم A .

الإثبات

هذا صحيح لأن $\mathrm{gcd}\,(A,P)$ يقسم P . ❐

2-17. **نتيجة**. ليكن P كثير حدود غير خزول في $\mathbb{K}[X]$. إن الشرط اللازم والكافي حتى يقسم P جداء ضرب كثيرات الحدود P_1 و P_2 و$\cdots$ و P_n في $\mathbb{K}[X]$، هو أن يقسم P أحدها.

الإثبات

هذا صحيح لأنه إذا كان P أولياً مع كلٍ من كثيرات الحدود P_1 و P_2 و$\cdots$ و P_n كان أولياً مع جداء ضربها. ❐

لنرمز بالرمز $\mathcal{P}$ إلى مجموعة كثيرات الحدود الواحديّة وغير الخزولة في $\mathbb{K}[X]$. فيكون كل كثير حدود غير خزول في $\mathbb{K}[X]$ شريكاً لعنصر واحدٍ، و واحد فقط من $\mathcal{P}$.

تؤدّي هذه المجموعة، كما سنرى، دوراً مشابهاً للدور الذي تؤدّيه مجموعة الأعداد الأولية في $\mathbb{Z}$.

2-18. **مبرهنة**. ليكن A عنصراً من $\mathbb{K}[X]$. إذا كان $1 \leq \deg A$ فيوجد P في $\mathcal{P}$ يُحقّق $P|A$.

الإثبات

لنتأمّل المجموعة

$$\mathcal{D} = \{Q \in \mathbb{K}[X] : (\deg Q \geq 1) \wedge (Q|A)\}$$

إنّ $\mathcal{D} \neq \varnothing$ لأن $A \in \mathcal{D}$، فالمجموعة $\mathcal{N} = \left\{\deg Q : Q \in \mathcal{D}\right\}$ مجموعة جزئية غير خالية من $\mathbb{N}^*$ فلها أصغر عنصر $m \geq 1$. ليكن Q عنصراً من $\mathcal{D}$ يُحقّق $\deg Q = m$. عندئذ يكون Q قاسماً غير خزول لكثير الحدود A وذلك بمقتضى تعريف m. ❐

2-19. **مبرهنة**. يُكتب كلُّ كثير حدود غير ثابت A من $\mathbb{K}[X]\backslash\mathbb{K}$ بالشكل

$$A = u\, P_1^{\nu_1} P_2^{\nu_2} \cdots P_m^{\nu_m}$$

و $u \in \mathbb{K}^*$، و $P_1, P_2, \ldots, P_m$ عناصر مختلفة مثنى مثنى من $\mathcal{P}$، و $\nu_1, \nu_2, \ldots, \nu_m$ أعداد من $\mathbb{N}^*$. وتكون هذه الكتابة وحيدة إذا لم نأخذ بعين الاعتبار ترتيب حدود الضرب.

الإثبات

- لنثبت جزء الوجود في هذه المبرهنة بالتدريج على $\deg A$.

إذا كان $\deg A = 1$، كان $A = aX + b$ مع $a \neq 0$ أو $A = u(X - \beta)$ حيث $a = u \in \mathbb{K}^*$ و $\beta = -\dfrac{b}{a}$، فيتم الإثبات لأنّ $X - \beta \in \mathcal{P}$.

لنفترض صحة النتيجة المطلوبة في حالة جميع كثير الحدود التي لا تزيد درجاتها على $n - 1$، (مع $2 \leq n$). وليكن A كثير حدود درجته n. يوجد بمُقتضى المبرهنة 2-17. عنصر P_0 ينتمي إلى $\mathcal{P}$ يُحقّق $P_0 | A$، ومن ثَمّ يكون $A = BP_0$ مع $\deg B < n$ و $B \neq 0$.

- فإمّا أن يكون $\deg B = 0$، ومن ثَمّ $B \in \mathbb{K}^*$ ويتم الإثبات.
- وإمّا أن يكون $1 \leq \deg B$، ومن ثَمّ $B = u\, P_1^{\nu_1} P_2^{\nu_2} \cdots P_m^{\nu_m}$ وذلك استناداً إلى فرْض التدريج، إذن $A = u\, P_0 P_1^{\nu_1} P_2^{\nu_2} \cdots P_m^{\nu_m}$، ويتم الإثبات أيضاً في هذه الحالة.

- لنفترض أنّ الجزء المتعلّق بوحدانيّة التفريق السابق غير صحيح، عندئذ يمكننا أن نجد كثير حدودٍ $\tilde{A}$ درجته أصغريّة ويقبل تفريقين مختلفين اختلافاً أساسياً، أي ليس فقط في ترتيب حدود الجداء :

$$\tilde{A} = u\, P_1^{\nu_1} P_2^{\nu_2} \cdots P_m^{\nu_m} = v\, Q_1^{\mu_1} Q_2^{\mu_2} \cdots Q_k^{\mu_k}$$

بمقارنة الحدّين المسَيْطِرين في طرفي المساواة $u\, P_1^{\nu_1} P_2^{\nu_2} \cdots P_m^{\nu_m} = v\, Q_1^{\mu_1} Q_2^{\mu_2} \cdots Q_k^{\mu_k}$ نجد أنّ $u = v$. إنّ P_1 كثير حدود غير خزول ويقسم الجداء $Q_1^{\mu_1} Q_2^{\mu_2} \cdots Q_k^{\mu_k}$ فهو يقسم أحد حدود الجداء. يمكننا إذن أن نفترض أنّ $P_1 | Q_1$، على أن نقوم بإعادة ترتيب حدود الجداء إذا دعت الحاجة، ينجم عن ذلك أنّ

$$\tilde{B} = P_1^{\nu_1 - 1} P_2^{\nu_2} \cdots P_m^{\nu_m} = Q_1^{\mu_1 - 1} Q_2^{\mu_2} \cdots Q_k^{\mu_k}$$

فكثير الحدود $\tilde{B}$ يقبل إذن تفريقين مختلفين اختلافاً أساسياً و $\deg \tilde{A} > \deg \tilde{B}$، وهذا يناقض تعريف $\tilde{A}$، وينهي إثبات المبرهنة. ❐

3. القسمة وفق القوى المتزايدة في $\mathbb{K}[X]$

3-1.مبرهنة. ليكن n من $\mathbb{N}$، وليكن كثيرا الحدود A و B من $\mathbb{K}[X]$ مع $B(0) \neq 0$. توجد في هذه الحالة ثنائية وحيدة (Q, R) من $\mathbb{K}[X] \times \mathbb{K}[X]$ تُحقّق

$$A = BQ + X^{n+1} R \quad \text{و} \quad \deg Q \leq n$$

نسمّي تعيين Q و R عملية القسمة وفق القوى المتزايدة لكثير الحدود A على B حتى المرتبة n، ونسمّيهما على التوالي **خارج**، و**باقي قسمة** A على B، وفق القوى المتزايدة حتى المرتبة n.

الإثبات

- لنبدأ بالوحدانيّة. إذا كان

$$A = BQ + X^{n+1}R = B\tilde{Q} + X^{n+1}\tilde{R}$$

مع $\deg Q \leq n$ و $\deg \tilde{Q} \leq n$. استنتجنا أنّ

$$B(Q - \tilde{Q}) = X^{n+1}(\tilde{R} - R)$$

إذن في حالة $\tilde{R} \neq R$ يكون

$$\begin{aligned} n + 1 &\leq \operatorname{val}(X^{n+1}(\tilde{R} - R)) = \operatorname{val}(B(Q - \tilde{Q})) \\ &= \underbrace{\operatorname{val}(B)}_{0} + \operatorname{val}(Q - \tilde{Q}) \underbrace{\leq}_{Q\neq\tilde{Q}} \deg(Q - \tilde{Q}) \leq n \end{aligned}$$

وهذا خُلفٌ. نستنتج من ذلك أنّ $R = \tilde{R}$ ومن ثَمّ $Q = \tilde{Q}$ لأن $B \neq 0$.

- لنثبت الجزء المتعلّق بالوجود بالتدريج على n. نفترض أنّ

$$A = \sum_{k=0}^{m} a_k X^k \quad \text{و} \quad B = \sum_{k=0}^{r} b_k X^k \text{، مع } b_0 \neq 0$$

  - إذا كانت $n = 0$، وضعنا $Q = a_0/b_0$، فيكون $(A - BQ)(0) = 0$ ومن ثَمّ $X | (A - BQ)$ ويوجد R يُحقّق $A - BQ = XR$، و $\deg Q \leq 0$.
  - لنفترض إذن صحةَ النتيجة عند $0 \leq n - 1$، فيوجد (Q_1, R_1) يُحقّق $A = BQ_1 + X^n R_1$ و $\deg Q_1 \leq n - 1$

واستناداً إلى صحة النتيجة عند $n = 0$ نجد ثنائيّة (Q_2, R_2) تحقّق المساواة

$$R_1 = B\,Q_2 + X\,R_2 \quad \text{مع الشرط} \quad \deg Q_2 \le 0$$

وهكذا نستنتج إذن أنّ

$$A = BQ + X^{n+1}R \quad \text{مع الشرط} \quad \deg Q \le n$$

إذ عرّفنا $Q = Q_1 + X^nQ_2$ و $R = R_2$.

وبذا يتمّ الإثبات. ❐

3-2. مثال. نجد فيما يلي مثالاً على عملية قسمة وفق القوى المتزايدة حتى المرتبة 3 لكثير الحدود $A(X) = 2 + 4X^2 + X^3$ على كثير الحدود $B(X) = 1 + 2X + 3X^2$

$$\begin{array}{rrrrrrr|l}
A \rightarrow & 2 & & +\ 4X^2 & +\ X^3 & & & 1 + 2X + 3X^2 \quad \leftarrow B \\
\cline{8-8}
& -2 & -\ 4X & -\ 6X^2 & & & & \\
\cline{2-5}
& & -\ 4X & -\ 2X^2 & +\ X^3 & & & 2 - 4X + 6X^2 + X^3 \quad \leftarrow Q \\
& & +\ 4X & +\ 8X^2 & +\ 12X^3 & & & \\
\cline{3-5}
& & & 6X^2 & +\ 13X^3 & & & \\
& & & -\ 6X^2 & -\ 12X^3 & -\ 18X^4 & & \\
\cline{4-6}
& & & & X^3 & -\ 18X^4 & & \\
& & & & -\ X^3 & -\ 2X^4 & -\ 3X^5 & \\
\cline{5-7}
& & & & X^4R \rightarrow & -\ 20X^4 & -\ 3X^5 &
\end{array}$$

ومنه

$$A(X) = B(X)(2 - 4X + 6X^2 + X^3) + X^4(-20 - 3X)$$

4. اشتقاق كثيرات الحدود

1-4. تعريف. ليكن كثير الحدود $P = \sum_{n\ge 0} a_n X^n$ من $\mathbb{K}[X]$. نسمّي **مشتق** P كثير الحدود P' من $\mathbb{K}[X]$، المعرّف بالعلاقة

$$P' = \sum_{n\ge 0} (n+1)\,a_{n+1}X^n$$

ونرمز عادة بالرمز $P^{(n)}$ إلى ناتج اشتقاق P، n مرّة، أي :

$$P^{(n)} = \sum_{n\ge 0} (n+k)(n+k-1)\cdots(n+1)\,a_{n+k}X^n$$

4-2. **ملاحظة**. إذا كان العدد المميّز للحقل $\mathbb{K}$ مساوياً الصفر كانت $\deg P'$ مساوية $\deg P - 1$ أياً كان كثير الحدود P الذي يحقق $\deg P \geq 1$، أمّا في حالة $\deg P = 0$ فيكون $P' = 0$.

ولكن في الحالة العامة يكون $\deg P' \leq \deg P - 1$ فمثلاً في حالة الحقل المنتهي $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ يكون $(X^p)' = pX^{p-1} = 0$ لأنّ $p = 0 \mod p$.

تلخّص المبرهنة التالية أهمّ خواص الاشتقاق :

4-3. **مبرهنة** : أياً كان P و Q من $\mathbb{K}[X]$ فلدينا

① $(P+Q)' = P' + Q'$ ② $(\lambda P)' = \lambda P'$

③ $(PQ)' = P'Q + PQ'$ ④ $(P \circ Q)' = P' \circ Q \cdot Q'$

⑤ $$(PQ)^{(n)} = \sum_{k=0}^{n} C_n^k P^{(k)} Q^{(n-k)}$$

الإثبات

- إنّ إثبات الخاصتين ① و ② بسيط ومباشر من التعريف.
- لإثبات الخاصة ③ يكفي استناداً إلى ما سبق أن نتحقق أنّ

$$\begin{aligned}(X^p \cdot X^q)' &= (X^{p+q})' \\ &= (p+q)X^{p+q-1} \\ &= (p\,X^{p-1}) \cdot X^q + X^p \cdot (q\,X^{q-1}) \\ &= (X^p)' \cdot X^q + X^p \cdot (X^q)'\end{aligned}$$

- يمكن تعميم الخاصة ③ على جداء $m \geq 2$ من كثيرات الحدود فتصبح

$$(P_1 P_2 \cdots P_m)' = \sum_{j=1}^{m} P_1 \cdots P_{j-1} P_j' P_{j+1} \cdots P_m$$

- يكفي أنّ نثبت الخاصة ④ في حالة $X^k = P$ ، وبحذف الحالة التافهة $k = 0$، تؤول هذه الخاصة إلى $(Q^k)' = k\,Q^{k-1} \cdot Q'$ وهذه بدورها حالة خاصّة من التعميم السابق.
- يمكن إثبات الخاصة ⑤ بالتدريج ونترك التفاصيل تمريناً للقارئ. ❐

4-4. **مبرهنة. منشور تايلور Taylor** : نفترض أنّ العدد المميّز للحقل $\mathbb{K}$ يساوي 0. ليكن P كثير حدود من $\mathbb{K}[X]$ وليكن a عنصراً من $\mathbb{K}$. عندئذ

$$P(X)=\sum_{k\geq 0}\frac{P^{(k)}(a)}{k\,!}(X-a)^k$$

الإثبات

- حالة $a=0$. لمّا كان $P=\sum_{k\geq 0}\lambda_k X^k$ أمكننا أن نكتب

$$P^{(m)}=\sum_{k\geq 0}\lambda_{m+k}(k+m)(k-1+m)\cdots(1+m)X^m$$

ومن ثَمّ $P^{(m)}(0)=(m\,!)\,\lambda_m$.

ولكنّ العدد المميّز للحقل $\mathbb{K}$ يساوي 0 إذن $m\,!\neq 0$، ومنه

$$\lambda_m=\frac{P^{(m)}(0)}{m\,!}$$

أي $P=\sum_{k\geq 0}\frac{P^{(k)}(0)}{k\,!}X^k$.

- الحالة العامّة. لنضع $Q(X)=P(X+a)$ فيكون $Q^{(k)}(0)=P^{(k)}(a)$، ونستنتج أنّ

$$P(X+a)=\sum_{k\geq 0}\frac{P^{(k)}(a)}{k\,!}X^k$$

أو

$$P(X)=\sum_{k\geq 0}\frac{P^{(k)}(a)}{k\,!}(X-a)^k$$

❒

5. جذور كثيرات الحدود

1-5. **مبرهنة**. ليكن P كثير حدود من $\mathbb{K}[X]$ وليكن a عنصراً من $\mathbb{K}$. هناك تكافؤ بين

❶ $P(a)=0$.

❷ $X-a$ يقسم P.

نقول في هذه الحالة إنّ a **جذر أو صفر** لكثير الحدود P.

الإثبات

بإجراء قسمة إقليدية لكثير الحدود P على $X-a$ نجد

$$P=(X-a)Q+R \quad \text{مع} \quad \deg R<1$$

إذن $R\in\mathbb{K}$. وبحساب قيمة التابع الحدودي السابق عند a نجد أنّ $R=P(a)$ ومنه $P(X)=(X-a)Q(X)+P(a)$. وهذا ما يثبت التكافؤ. ❐

2-5. مبرهنة: ليكن P كثير حدود من $\mathbb{K}[X]$ وليكن a عنصراً من $\mathbb{K}$ ، وأخيراً ليكن k عدداً من $\mathbb{N}^*$. هناك تكافؤ بين

❶ $P=(X-a)^kQ$ و $Q(a)\neq 0$.

❷ $(X-a)^k$ يقسم P و $(X-a)^{k+1}$ لا يقسم P .

ونقول في هذه الحالة إنّ a **جذر مضاعف** من المرتبة k .

الإثبات

❶ ⇐ ❷ من الواضح أنّ $(X-a)^k$ يقسم P ، ومن ناحية أخرى

$$Q=(X-a)Q_1+Q(a)$$

فإذا كان $(X-a)^{k+1}$ يقسم P ، كان $(X-a)^{k+1}$ قاسماً لكثير الحدود $Q(a)(X-a)^k$ واستنتجنا من ثَمّ أنّ $Q(a)=0$ وهذا خُلفٌ.

❷ ⇐ ❶ واضح. ❐

3-5. ملاحظة. نقول إنّ a **جذرٌ بسيط** لكثير الحدود P إذا كان جذراً مرتبته تساوي 1 لكثير الحدود P . أي إذا كان $X-a$ يقسم P و $(X-a)^2$ لا يقسم P .

4-5. مبرهنة. نفترض أنّ العدد المميّز للحقل $\mathbb{K}$ يساوي 0 ، وليكن P كثير حدود من $\mathbb{K}[X]$ ، وليكن a عنصراً من $\mathbb{K}$ ، وأخيراً ليكن k عدداً من $\mathbb{N}^*$. هناك تكافؤ بين الخاصّتين التاليتين:

❶ a جذر مضاعف من المرتبة k لكثير الحدود P .

❷ $P(a)=0, P(a)=0,\ldots,P^{(k-1)}(a)=0$ و $P^{(k)}(a)\neq 0$.

الإثبات

استناداً إلى منشور تايلور يكون

$$P(X) = (X-a)^k \sum_{n\geq k} \frac{P^{(n)}(a)}{n!}(X-a)^{n-k} + \sum_{n=0}^{k-1} \frac{P^{(n)}(a)}{n!}(X-a)^n$$

يكافئ الشرطُ ❶، بناءً على المبرهنة 5-2، الشرطين

$$\sum_{n=0}^{k-1} \frac{P^{(n)}(a)}{n!}(X-a)^n = 0 \quad \text{و} \quad P^{(k)}(a) \neq 0$$

وهذا بدوره يكافئ الشرط ❷. ❐

5-5. مبرهنة. ليكن P كثير حدود من $\mathbb{K}[X]$، ولنفترض أنّ $a_1, a_2, \ldots, a_r$ عناصر مختلفة مثنى مثنى من $\mathbb{K}$، وأخيراً لنفترض أنّ a_i جذر من المرتبة m_i على الأقلّ لكثير الحدود P، وذلك أياً كان i من $\mathbb{N}_r$. حينئذ يقسمُ كثيرُ الحدود $\prod_{i=1}^{r}(X-a_i)^{m_i}$ كثيرَ الحدود P.

الإثبات

لمّا كان $(X-a_i)^{m_i}$ يقسم كثير الحدود P أياً كان i من $\mathbb{N}_r$، ولأنّ كثيرات الحدود $((X-a_i)^{m_i})_{1\leq i\leq r}$ أوّليّة فيما بينها مثنى مثنى، وذلك بمقتضى النتيجة 2-10، استنتجنا أنّ $\prod_{i=1}^{r}(X-a_i)^{m_i}$ يقسم P. ❐

5-6. نتيجة. ليكن P كثير حدود من $\mathbb{K}[X]$ درجته أصغر أو تساوي n، ولنفترض أنّ كثير الحدود P يقبلُ $a_1, a_2, \ldots, a_r$ جذوراً مختلفة مثنى مثنى، وأنّ كلَّ a_i جذرٌ مضاعفٌ من مرتبة أكبر أو تساوي m_i لكثير الحدود P، عندئذ يقتضي الشرطُ $\sum_{i=1}^{r} m_i > n$ النتيجةَ $P = 0$.

الإثبات

هذا صحيح لأنه من جهة أولى يقسمُ كثيرُ الحدود $Q = \prod_{i=1}^{r}(X-a_i)^{m_i}$ كثيرَ الحدود P، ومن جهة ثانية لدينا $\deg Q > \deg P$. ❐

5-7. **نتيجة**. إذا كان P كثير حدود من $\mathbb{K}[X]$ درجته n، فإنّ P يقبل على الأكثر n جذراً مختلفاً، أي

$$\operatorname{card}(\{x \in \mathbb{K} : P(x) = 0\}) \leq n$$

الإثبات :

هذا صحيح لأنه إذا كانت $\mathcal{Z} = \left\{x \in \mathbb{K} : P(x) = 0\right\}$ و $\operatorname{card}(\mathcal{Z}) = m$ قسم كثيرُ الحدود $Q = \prod_{a\in\mathcal{Z}}(X-a)$ كثيرَ الحدود P، وهذا يقتضي أنّ

$$m = \deg Q \leq \deg P = n \qquad \square$$

5-8. **مثال مهم**. **كثيرات حدود لاغرانج Lagrange**

لتكن $x_1, x_2, \ldots, x_{n+1}$ عناصر مختلفة مثنى مثنى في الحقل $\mathbb{K}$. ولتكن $\lambda_1, \lambda_2, \ldots, \lambda_{n+1}$ عناصر من $\mathbb{K}$. في هذه الحالة **يوجد** كثير حدود **وحيد** P درجته أصغر أو تساوي n يُحقِّق

$$\forall i \in \mathbb{N}_{n+1}, \quad P(x_i) = \lambda_i$$

الإثبات

ليكن كثيرا الحدود P و $\tilde{P}$ من $\mathbb{K}[X]$، ولنفترض أنّ درجة كلٍّ منهما أصغر أو تساوي n وأنهما يحقّقان

$$\forall i \in \mathbb{N}_{n+1}, \quad P(x_i) = \lambda_i = \tilde{P}(x_i)$$

عندئذ تكون درجة كثير الحدود $Q = P - \tilde{P}$ أصغر أو تساوي n، وهو يقبل $n+1$ جذراً مختلفاً، وعلى هذا $Q = 0$ أي $P = \tilde{P}$. وهذا يثبت وحدانية كثير الحدود المطلوب إن وُجِدَ.

من ناحية أخرى، لتكن j من $\mathbb{N}_{n+1}$، ولنعرّف

$$\ell_j(X) = \prod_{k\in\mathbb{N}_{n+1}\setminus\{j\}}\left(\frac{X - x_k}{x_j - x_k}\right)$$

نلاحظ أنّ $\deg \ell_j = n$ وأنّ

$$\forall (i,j) \in \mathbb{N}_{n+1}\times\mathbb{N}_{n+1}, \quad \ell_j(x_i) = \delta_{ji} = \begin{cases} 1 & : \quad i = j \\ 0 & : \quad i \neq j \end{cases}$$

لذا نجد بوضع $P = \sum_{k=1}^{n+1}\lambda_k\ell_k$ أنّ $P(x_i) = \lambda_i$ وذلك أياً كان i من $\mathbb{N}_{n+1}$.

نسمّي كثيرات الحدود $(\ell_{n+1},\ldots,\ell_2,\ell_1)$ **كثيرات حدود لاغرانج** Lagrange الموافقة للنقاط $.x_{n+1},\ldots,x_2,x_1$

فمثلاً كثيرات حدود لاغرانج الموافقة للنقاط $x_1=0$ و $x_2=1$ و $x_3=2$ من $\mathbb{R}$ هي

$$\begin{aligned}\ell_1(X) &= \frac{1}{2}X^2 - \frac{3}{2}X + 1\\ \ell_2(X) &= -X^2 + 2X\\ \ell_3(X) &= \frac{1}{2}X^2 - \frac{1}{2}X\end{aligned}$$

ويكون

$$P=\lambda_1\ell_1(X)+\lambda_2\ell_2(X)+\lambda_3\ell_3(X)$$

كثير الحدود الوحيد في $\mathbb{R}[X]$ الذي لا تزيد درجته على 2 ويُحقِّق

$$P(2)=\lambda_3 \text{ و } P(1)=\lambda_2 \text{ و } P(0)=\lambda_1$$

5-9. مثال. مبرهنة ويلسون Wilson

ليكن p عدداً أوليّاً، فيكون $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ حقلاً تبديلياً. ومن ثَمّ تكون $\mathbb{F}_p^*=\mathbb{F}_p\backslash\{0\}$ زمرة عدد عناصرها $p-1$ ومنه

$$\forall a\in\mathbb{F}_p^*,\quad a^{p-1}=1$$

لذلك فإنّ كثير الحدود

$$G(X)=X^{p-1}-1-\prod_{k=1}^{p-1}(X-k)$$

من $\mathbb{F}_p[X]$ يقبل $p-1$ جذراً مختلفاً هي عناصر $\mathbb{F}_p^*$ أمّا درجة G فهي أصغر تماماً من $p-1$ وعليه يجب أن يكون $G=0$ أي

$$X^{p-1}-1=\prod_{k=1}^{p-1}(X-k)$$

وبوجه خاص إذا عوّضنا $X=0$ وجدنا

$$(p-1)!=-1 \bmod p$$

فإذا كان p عدداً أوليّاً كان $(p-1)!=-1\bmod p$. وهذه هي مبرهنة ويلسون.

10-5. تمرين محلول. ليكن a عدداً من $\mathbb{R}$، وليكن n من $\mathbb{N}^*$. والمطلوب حلُّ المعادلة

$$(z+1)^n = \cos 2na + \mathrm{i}\sin 2na \qquad (\mathcal{E})$$

بالنسبة إلى المجهول z في $\mathbb{C}$، واستنتاج قيمة الجداء

$$P_n(a) = \prod_{k=0}^{n-1} \sin\left(a + \frac{k\pi}{n}\right)$$

في الحقيقة،

$$\begin{aligned}
(\mathcal{E}) &\Leftrightarrow z+1 \in \left\{\exp\left(2a\,\mathrm{i} + \frac{2\pi k\,\mathrm{i}}{n}\right) : k \in \{0,1,\ldots,n-1\}\right\}\\
&\Leftrightarrow z \in \left\{\exp\left(2a\,\mathrm{i} + \frac{2\pi k\,\mathrm{i}}{n}\right) - 1 : k \in \{0,1,\ldots,n-1\}\right\}\\
&\Leftrightarrow z \in \left\{2\,\mathrm{i}\sin\left(a + \frac{\pi k}{n}\right)\cdot e^{\mathrm{i}\left(a+\frac{\pi k}{n}\right)} : k \in \{0,1,\ldots,n-1\}\right\}
\end{aligned}$$

لأنّ $e^{2\mathrm{i}\theta} - 1 = 2\,\mathrm{i}(\sin\theta)e^{\mathrm{i}\theta}$. ليكن إذن كثير الحدود

$$Q(X) = (1+X)^n - e^{2na\mathrm{i}} - \prod_{k=0}^{n-1}\left(X - 2\,\mathrm{i}\sin\left(a+\frac{\pi k}{n}\right)e^{\mathrm{i}\left(a+\frac{\pi k}{n}\right)}\right)$$

إنّ $Q = 0$ لأنّه يقبل على الأقّل n جذراً مختلفاً ودرجته أصغر أو تساوي $n-1$.

وهكذا نحصل على المساواة

$$(1+X)^n - e^{2na\mathrm{i}} = \prod_{k=0}^{n-1}\left(X - 2\,\mathrm{i}\sin\left(a+\frac{\pi k}{n}\right)e^{\mathrm{i}\left(a+\frac{\pi k}{n}\right)}\right)$$

ومنه، بتعويض $X = 0$، نجد

$$\begin{aligned}
1 - e^{2na\mathrm{i}} &= \left(-2\,\mathrm{i}\right)^n\left[\prod_{k=0}^{n-1}\sin\left(a+\frac{\pi k}{n}\right)\right]\cdot e^{\mathrm{i}na}\cdot\exp\left(\frac{\mathrm{i}\pi}{n}\sum_{k=0}^{n-1}k\right)\\
&= \left(-2\,\mathrm{i}\right)^n e^{\mathrm{i}na}P_n(a)\exp\left(\frac{\mathrm{i}\pi(n-1)}{2}\right)
\end{aligned}$$

وبالإصلاح نجد

$$P_n(a) = \frac{\sin na}{2^{n-1}}$$

5-11. مبرهنة دالمبير D'Alembert . ليكن P كثير حدود من $\mathbb{C}[X]$ يُحقّق $\deg P > 0$، حينئذ يوجد عددٌ عقدي z_0 يُحقّق $P(z_0) = 0$.

الإثبات

يعتمد الإثبات الذي سنعرضه على مفاهيم في التحليل قد لا يكون القارئ ملمّاً بها، لذلك يمكن للقارئ أن يقبل النتيجة دون إثبات، تاركاً إياه لقراءة ثانية.

لنفترض أنّ $P(z) \neq 0$ أياً كان العدد z من $\mathbb{C}$. ولنعرّف $G(z) = \dfrac{zP'(z)}{P(z)}$ وكذلك $h(r,\theta) = G(re^{i\theta})$. فيكون

$$\frac{\partial h}{\partial r}(r,\theta) = e^{i\theta}G'(re^{i\theta}), \quad \frac{\partial h}{\partial \theta}(r,\theta) = i\, e^{i\theta}G'(re^{i\theta})$$

أي

$$\frac{1}{i\, r}\frac{\partial h}{\partial \theta}(r,\theta) = \frac{\partial h}{\partial r}(r,\theta)$$

من ناحية أخرى، لنعرّف $\gamma(r) = \dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} h(r,\theta)\,d\theta$. من الواضح أنّ

$$\gamma'(r) = \frac{1}{2\pi}\int_0^{2\pi}\frac{\partial h}{\partial r}(r,\theta)\,d\theta = \frac{1}{2\pi\, i\, r}\int_0^{2\pi}\frac{\partial h}{\partial \theta}(r,\theta)\,d\theta$$
$$= \frac{1}{2\pi\, i\, r}[h(r,2\pi) - h(r,0)] = 0$$

ومن ثَمّ $\forall r \in \mathbb{R}_+,\ \gamma(r) = \gamma(0) = 0$. من ناحية أخرى لدينا

$$P(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_0$$

إذن في حالة $|z| \geq 1$ يكون

$$\left|P(z)\right| \geq \left|a_n\right| \cdot |z|^n - \max_{0\leq j<n}\left(\left|a_j\right|\right)|z|^{n-1} = a|z|^n - b|z|^{n-1}$$

وقد عرّفنا $a = |a_n|$ و $b = \max\limits_{0\leq j<n}\left|a_j\right|$. ويكون أيضاً

$$\left|zP'(z) - nP(z)\right| = \left|\sum_{k=0}^{n-1}(k-n)a_k z^k\right|$$
$$\leq \max_{0\leq k<n}\left((n-k)\left|a_k\right|\right)\cdot |z|^{n-1} = c\,|z|^{n-1}$$

وقد عرّفنا أيضاً $c = \max\limits_{0\le k<n} \left((n-k)|a_k|\right)$.

فإذا كان $|z| \ge \max(1, b/a)$ صار لدينا

$$\left|G(z) - n\right| \le \frac{c}{a|z| - b}$$

ومن ثمّ

$$r > \max\left(1, \frac{b}{a}\right) \Rightarrow |\gamma(r) - n| \le \frac{c}{ar - b}$$

وهذا يقتضي، لأنّ $\gamma(r) = 0$، ما يلي

$$r > \max\left(1, \frac{b}{a}\right) \Rightarrow n \le \frac{c}{ar - b}$$

وبجعل r تسعى إلى اللانهاية نجد $n = 0$ وهذا تناقض. إذن لا بدّ أن نجد z_0 في $\mathbb{C}$ يُحقّق $P(z_0) = 0$. ❐

12-5. نتيجة. ليكن P كثير حدود في $\mathbb{C}[X]$. حينئذ يكون P غير خزول إذا وفقط إذا كانت درجته تساوي الواحد، أي $\deg P = 1$.

هذا واضح بناءً على مبرهنة D'Alembert.

تكافئ هذه النتيجة القول إنّ كثيرات الحدود غير الخزولة في $\mathbb{C}[X]$ هي كثيرات الحدود من الصيغة $\lambda(X - \alpha)$ مع $\lambda \in \mathbb{C}^*$ و $\alpha \in \mathbb{C}$.

13-5. مبرهنة. ليكن P كثير حدود في $\mathbb{C}[X]$. ولنفترض أنّ $\deg P > 0$. إذن توجد λ في $\mathbb{C}$، وتوجد أعداد $a_1, a_2, \ldots, a_r$ مختلفة مثنى مثنى في $\mathbb{C}$، وتوجد أعداد طبيعيّة $m_1, m_2, \ldots, m_r$ في $\mathbb{N}^*$ تحقّق

$$P = \lambda \cdot \prod_{k=1}^{r} (x - a_k)^{m_k}$$

وهذه الكتابة وحيدة إذا أغفلنا ترتيب حدود الجداء.

الإثبات

ينتج البرهان مباشرة من المبرهنة 2-18.لأن مجموعة كثيرات الحدود الواحدية وغير الخزولة في $\mathbb{C}[X]$ هي $\mathcal{P}_{\mathbb{C}} = \{X - a : a \in \mathbb{C}\}$. ❐

14-5. مبرهنة. ليكن P كثير حدود في $\mathbb{R}[X]$. هناك تكافؤ بين

❶ إنّ كثير الحدود P واحديٌّ وغير خزول في $\mathbb{R}[X]$.

❷ $P \in \{X - a : a \in \mathbb{R}\} \cup \left\{(X-a)^2 + b^2 : (a,b) \in \mathbb{R} \times \mathbb{R}^*\right\}$.

الإثبات

❶ ⇐ ❷ ليكن كثير الحدود الواحديّ وغير الخزول P في $\mathbb{R}[X]$.

- إذا كان $\deg P = 1$ تمّ الإثبات.
- وإذا كان $\deg P > 1$ كان $\forall x \in \mathbb{R},\ P(x) \neq 0$. ولكن يوجد α في $\mathbb{C}\backslash\mathbb{R}$ يُحقّق $P(\alpha) = 0$ ، ولأنّ P حقيقي كان أيضاً $P(\overline{\alpha}) = 0$. إذن لا بُدّ أن يقسم كثيرُ الحدود $(X-\alpha)(X-\overline{\alpha})$ كثيرَ الحدود P في $\mathbb{C}[X]$، ومنه يوجد Q في $\mathbb{C}[X]$ يُحقّق

$$P(X) = (X^2 - 2(\operatorname{Re}\alpha)X + |\alpha|^2)Q(X)$$

ولكن كلاً من كثيري الحدود P و $X^2 - 2(\operatorname{Re}\alpha)X + |\alpha|^2$ عنصرٌ من $\mathbb{R}[X]$. إذن ينتمي Q ، إلى $\mathbb{R}[X]$ ، ونستنتج، لأنّ P غير خزول وواحدي، أنّ

$$\begin{aligned} P(X) &= X^2 - 2(\operatorname{Re}\alpha)X + |\alpha|^2 \\ &= (X - \operatorname{Re}\alpha)^2 + (\operatorname{Im}\alpha)^2 \end{aligned}$$

وهذا ما يثبت ❷ .

❷ ⇐ ❶ هذا اقتضاءٌ واضح. □

15-5. ملاحظة. يمكننا صياغة النتيجة السابقة على الوجه التالي : ليكن P من $\mathbb{R}[X]$ ، يكون كثير الحدود P غير خزول إذا وفقط إذا كان $P = \alpha X^2 + \beta X + \gamma$ حيث

$$\left(\beta^2 - 4\alpha\gamma < 0\right) \text{ أو } (\beta \neq 0 \text{ و } \alpha = 0)$$

ونستنتج مما سبق النتيجة المهمة الآتية.

5-16. **نتيجة**. ليكن P كثير حدود من $\mathbb{R}[X]$ يُحقّق $\deg P > 0$، إذن يوجد λ في $\mathbb{R}^*$، وتوجد أعداد $\alpha_1,\ldots,\alpha_r$ مختلفة مثنى مثنى من $\mathbb{R}$، وتوجد أيضاً ثنائيات $((\beta_1,\gamma_1),\ldots,(\beta_m,\gamma_m))$ مختلفة مثنى مثنى من $\mathbb{R}^2$ وتحقّق $\beta_i^2 - 4\gamma_i < 0$ أياً كان i من $\mathbb{N}_m$، وأخيراً توجد أعداد طبيعية $s_1,\ldots,s_m$ و $k_1,\ldots,k_r$ من $\mathbb{N}^*$ بحيث يُكتب P بالشكل

$$P = \lambda \cdot \prod_{i=1}^{r}(X - \alpha_i)^{k_i} \cdot \prod_{i=1}^{m}(X^2 + \beta_i X + \gamma_i)^{s_i}$$

وهذه الكتابة وحيدة إذا أغفلنا ترتيب حدود الجداء.

6. العلاقات بين الجذور والأمثال في كثيرات الحدود

6-1. **مبرهنة**. نرمز بالرمز $P_k^{(n)}$ للدلالة على مجموعة أجزاء $\mathbb{N}_n$ التي عدد عناصر كل منها k، مع $n \in \mathbb{N}^*$ و $k \in \mathbb{N}_n \cup \{0\}$. عندئذ أياً كان $(x_1,\ldots,x_n)$ من $\mathbb{K}^n$ كان

$$\prod_{i=1}^{n}(X - x_i) = \sum_{k=0}^{n}(-1)^k\left(\sum_{B\in P_k^{(n)}}\prod_{j\in B}x_j\right)X^{n-k} \qquad (*)$$

مع الاصطلاح أنّ $\prod_{j\in\varnothing}x_j = 1$.

الإثبات

لنتحقق صحةَ هذه المساواة بالتدريج على العدد n. إنّ $(*)$ صحيحة وضوحاً عند $n = 1$. لنفترض إذن صحتها عند قيمة n. وليكن $(x_1,\ldots,x_{n+1})$ من $\mathbb{K}^{n+1}$. عندئذ يكون لدينا استناداً إلى فرْض التدريج ما يلي :

$$\prod_{i=1}^{n}(X - x_i) = \sum_{k=0}^{n}(-1)^k\left(\sum_{B\in P_k^{(n)}}\prod_{j\in B}x_j\right)X^{n-k}$$

وبناءً على العلاقة الآتية :

$$\prod_{i=1}^{n+1}(X - x_i) = X\prod_{i=1}^{n}(X - x_i) - x_{n+1}\prod_{i=1}^{n}(X - x_i)$$

نجد

$$\begin{aligned}\prod_{i=1}^{n+1}(X-x_i) &= \sum_{k=0}^{n}(-1)^k\left(\sum_{B\in P_k^{(n)}}\prod_{j\in B}x_j\right)X^{n+1-k}-\sum_{k=0}^{n}(-1)^k\left(\sum_{B\in P_k^{(n)}}x_{n+1}\prod_{j\in B}x_j\right)X^{n-k}\\
&= \sum_{k=0}^{n}(-1)^k\left(\sum_{B\in P_k^{(n)}}\prod_{j\in B}x_j\right)X^{n+1-k}+\sum_{k=0}^{n}(-1)^{k+1}\left(\sum_{B\in P_k^{(n)}}\prod_{j\in B\cup\{n+1\}}x_j\right)X^{n+1-(k+1)}\\
&= \sum_{k=0}^{n}(-1)^k\left(\sum_{B\in P_k^{(n)}}\prod_{j\in B}x_j\right)X^{n+1-k}+\sum_{k=1}^{n+1}(-1)^k\left(\sum_{B\in P_{k-1}^{(n)}}\prod_{j\in B\cup\{n+1\}}x_j\right)X^{n+1-k}\\
&= X^{n+1}+(-1)^{n+1}\prod_{j\in\mathbb{N}_{n+1}}x_j+\sum_{k=1}^{n}(-1)^k\left(\sum_{B\in P_k^{(n)}}\prod_{j\in B}x_j+\sum_{B\in P_{k-1}^{(n)}}\prod_{j\in B\cup\{n+1\}}x_j\right)X^{n+1-k}\\
&= \sum_{k=0}^{n+1}(-1)^k\left(\sum_{B\in P_k^{(n+1)}}\prod_{j\in B}x_j\right)X^{n+1-k}.\end{aligned}$$

وهو المطلوب إثباته. ❐

2-6. تعريف. نعرّف، أياً كان n من $\mathbb{N}^*$، و k من $\mathbb{N}_n\cup\{0\}$، و $(x_1,\ldots,x_n)$ من $\mathbb{K}^n$، المقدار

$$\Sigma_k^{(n)}(x_1,\ldots,x_n)=\sum_{B\in P_k^{(n)}}\prod_{j\in B}x_j$$

فمثلاً

$$\Sigma_0^{(n)}(x_1,\ldots,x_n)=1,\qquad \Sigma_1^{(n)}(x_1,\ldots,x_n)=x_1+x_2+\cdots x_n,$$
$$\Sigma_2^{(n)}(x_1,\ldots,x_n)=\sum_{1\le i<j\le n}x_ix_j,\quad \Sigma_n^{(n)}(x_1,\ldots,x_n)=x_1x_2\cdots x_n.$$

ونسمّي $(\Sigma_n^{(n)},\ldots,\Sigma_1^{(n)},\Sigma_0^{(n)})$ **التوابع المتناظرة البسيطة ذات n متحوّلاً**. وقد جرت العادة أنّ نكتب فقط Σ_k عوضاً عن $\Sigma_k^{(n)}(x_1,\ldots,x_n)$ إذا لم يكن هناك مجالٌ للالتباس.

يمكننا إذن، بناءً على التعريف السابق، أن نعيد صياغة المبرهنة 6-1 على الوجه الآتي :

'6-1. مبرهنة. أياً كان n من $\mathbb{N}^*$، و $(x_1,\ldots,x_n)$ من $\mathbb{K}^n$ كان

$$\prod_{i=1}^{n}(X-x_i)=\sum_{k=0}^{n}(-1)^k\Sigma_k\,X^{n-k}\qquad(**)$$

3-6. نتيجة. ليكن $P = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + a_n X^n$ كثير حدود من $\mathbb{K}[X]$. عندئذ تكون العناصر $\xi_1, \ldots, \xi_{n-1}, \xi_n$ من $\mathbb{K}$ جذور كثير الحدود P، إذا وفقط إذا تحققت الشروط

$$\forall k \in \mathbb{N}_n, \quad \Sigma_k^{(n)}(\xi_1,\ldots,\xi_n) = (-1)^k \frac{a_{n-k}}{a_n}$$

وذلك لأنّ $P = a_n \prod_{k=1}^{n} (X - \xi_k)$.

4-6. تعريف. ليكن n من $\mathbb{N}^*$، وليكن $f : \mathbb{K}^n \to \mathbb{K}$. نقول إنّ التابع f **متناظرٌ** إذا وفقط إذا تحقّق الشرط

$$\forall \sigma \in S_n, \forall (x_1,\ldots,x_n) \in \mathbb{K}^n, \quad f(x_1,\ldots,x_n) = f(x_{\sigma(1)},\ldots,x_{\sigma(n)})$$

فمثلاً التابعان f و g المعرّفان فيما يلي

$$f(x,y) = x\,y^2 + x^2\,y$$

$$g(x,y,z) = x\,y^2 + y\,z^2 + z\,x^2 + x^2 y + y^2 z + z^2 x$$

تابعان متناظران.

5-6. ملاحظة. إنّ التوابع المتناظرة البسيطة $(\Sigma_0^{(n)}, \Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)})$ توابع متناظرة.

تنبع أهمية التوابع المتناظرة البسيطة من المبرهنة التالية التي نقبلها دون إثبات.

6-6. مبرهنة. ليكن n من $\mathbb{N}^*$، وليكن $f : \mathbb{K}^n \to \mathbb{K}$ تابعاً متناظراً وحدودياً في كلٍ من متحولاته. عندئذ يوجد تابعٌ $h : \mathbb{K}^n \to \mathbb{K}$ يُحقّق

$$\forall (x_1,\ldots,x_n) \in \mathbb{K}^n, \quad f(x_1,x_2,\ldots,x_n) = h(\Sigma_1,\Sigma_2,\ldots,\Sigma_n)$$

فمثلاً يكتب التابع f الوارد آنفاً بالشكل

$$f(x,y) = x^2 y + x y^2 = (x+y)\cdot x\,y = \Sigma_1 \cdot \Sigma_2$$

وأمّا التابع g فيكتب بالشكل:

$$\begin{aligned} g(x,y,z) &= xy^2 + yz^2 + zx^2 + x^2y + y^2z + z^2x \\ &= xy(x+y) + yz(y+z) + zx(\Sigma_1 - z) \\ &= xy(\Sigma_1 - z) + yz(\Sigma_1 - x) + zx(\Sigma_1 - y) \\ &= (xy + yz + zx)\Sigma_1 - 3xyz \\ &= \Sigma_1\Sigma_2 - 3\Sigma_3 \end{aligned}$$

7-6. **مبرهنة**. نعرّف، أياً كان (k,n) من $\mathbb{N}^{*2}$، و $(x_1,\ldots,x_n)$ من $\mathbb{K}^n$، المقدار

$$S_k^{(n)}(x_1,\ldots,x_n) = \sum_{i=1}^{n} x_i^k$$

ونكتب ببساطة S_k إذا لم يكن هناك مجال للالتباس. إنّ التوابع $(S_k^{(n)})_{k\geq 1}$ متناظرة وتربطها بالتوابع المتناظرة البسيطة العلاقات التالية، المعروفة باسم **علاقات نيوتن** Newton:

- في حالة $k \geq n$ تتحقّق المساواة :

$$S_k - S_{k-1}\Sigma_1 + S_{k-2}\Sigma_2 + \cdots + (-1)^{k-1}S_1\Sigma_{k-1} + (-1)^k k\,\Sigma_k = 0$$

- وفي حالة $k < n$ تتحقّق المساواة :

$$S_k - S_{k-1}\Sigma_1 + S_{k-2}\Sigma_2 + \cdots + (-1)^{n-1}S_{k-n-1}\Sigma_{n-1} + (-1)^n S_{k-n}\,\Sigma_n = 0$$

الإثبات

- حالة $k \geq n$. ليكن $P = \prod_{j=1}^{n}(X - x_j)$ نعلم أنّ

$$P = \sum_{k=0}^{n}(-1)^{n-k}\Sigma_{n-k}X^k$$

لمّا كان $P(x_i) = 0$ أمكننا أن نكتب

$$\begin{aligned} P(X) - P(x_i) &= \sum_{m=1}^{n}(-1)^{n-m}\Sigma_{n-m}(X^m - x_i^m) \\ &= (X - x_i)\sum_{m=1}^{n}\left((-1)^{n-m}\Sigma_{n-m}\left(\sum_{k=1}^{m} x_i^{m-k}X^{k-1}\right)\right) \\ &= (X - x_i)\sum_{k=1}^{n}\left(\sum_{m=k}^{n}(-1)^{n-m}\Sigma_{n-m}x_i^{m-k}\right)X^{k-1} \end{aligned}$$

ومنه نستنتج أنّ

$$\prod_{j=1, j\neq i}^{n} (X - x_j) = \sum_{k=1}^{n} \left(\sum_{m=k}^{n} (-1)^{n-m} \Sigma_{n-m} x_i^{m-k} \right) X^{k-1} \qquad (1)$$

ومن ناحية أخرى باشتقاق طرفي المساواة

$$\prod_{j=1}^{n} (X - x_j) = \sum_{k=0}^{n} (-1)^{n-k} \Sigma_{n-k} X^k$$

نجد

$$\sum_{i=1}^{n} \left(\prod_{j=1, j\neq i}^{n} (X - x_j) \right) = \sum_{k=1}^{n} (-1)^{n-k} k\, \Sigma_{n-k} X^{k-1}$$

نستنتج إذن بعد التعويض من (1) أنّ

$$\sum_{k=1}^{n} \left(\sum_{m=k}^{n} (-1)^{n-m} \Sigma_{n-m} S_{m-k} \right) X^{k-1} = \sum_{k=1}^{n} (-1)^{n-k} k\, \Sigma_{n-k} X^{k-1}$$

وقد اصطلحنا أنّ $S_0 = n$، ومنه

$$\forall k \in \mathbb{N}_n, \quad \sum_{m=k}^{n} (-1)^{n-m} \Sigma_{n-m} S_{m-k} = (-1)^{n-k} k\, \Sigma_{n-k}$$

وأخيراً بإجراء تغيير للمتحول بوضع p مكان $n - k$، وبالإصلاح نجد العلاقة المطلوبة.

- أمّا حالة $n < k$ فهي أبسط، إذ لدينا

$$\forall i \in \mathbb{N}_n, \quad 0 = P(x_i) = \sum_{m=0}^{n} (-1)^{n-m} \Sigma_{n-m} x_i{}^m$$

بضرب طرفيّ هذه العلاقة بالمقدار x_i^{k-n} وبالجمع نجد

$$\sum_{m=0}^{n} (-1)^{n-m} \Sigma_{n-m} S_{k+m-n} = 0$$

أو

$$\sum_{m=0}^{n} (-1)^{m} \Sigma_{m} S_{k-m} = 0$$

وهي العلاقة المطلوبة. ❐

8-6. **مثال**. لتكن c, b, a جذور المعادلة $Z^3 + pZ + q = 0$ في $\mathbb{C}$. أوجد معادلة من الدرجة الثالثة جذورها c^2, b^2, a^2.

في الحقيقة، نعلم أنّ $\Sigma_1 = 0$ و $\Sigma_2 = p$ و $\Sigma_3 = -q$. ومن ناحية أخرى

$$\begin{aligned}
a^2 + b^2 + c^2 &= \Sigma_1^2 - 2\Sigma_2 = -2p \\
a^2b^2 + b^2c^2 + c^2a^2 &= \Sigma_2^2 - 2(ab^2c + abc^2 + a^2bc) \\
&= \Sigma_2^2 - 2abc(b + c + a) \\
&= \Sigma_2^2 - 2\Sigma_1\Sigma_3 = p^2 \\
a^2b^2c^2 &= \Sigma_3^2 = q^2
\end{aligned}$$

إذن c^2, b^2, a^2 هي جذور المعادلة

$$X^3 + 2p\,X^2 + p^2X - q^2 = 0$$

تمرينات

إنّ جميع كثيرات الحدود الواردة هي من $\mathbb{C}[X]$ ما لم نذكر خلاف ذلك.

التمرين 1. أثبت صحّة المساواة $C_{2n}^{n}=\sum_{k=0}^{n}(C_n^k)^2$. **مساعدة.** احسب بطريقتين مختلفتين المقدار $(X+1)^{2n}$. ثُمّ عمّم النتيجة.

الحل

في الحقيقة، ليكن (n,m) من $\mathbb{N}^2$ ، نعلم أنّ

$$\begin{aligned}(1+X)^n &= \sum_{k\geq 0} C_n^k X^k,\\ (1+X)^m &= \sum_{k\geq 0} C_m^k X^k,\\ (1+X)^{n+m} &= \sum_{k\geq 0} C_{n+m}^k X^k\end{aligned}$$

فإذا استفدنا من المساواة

$$(1+X)^{n+m}=(1+X)^n(1+X)^m$$

استنتجنا أنّ

$$C_{n+m}^q=\sum_{r+t=q}C_n^rC_m^t=\sum_{r=0}^{q}C_n^rC_m^{q-r}$$

تذكّر أنّ $C_a^b=0$ في حالة $b\notin\{0,1,\ldots,a\}$. وبوجه خاص، في حالة $q=m=n$ نجد

$$C_{2n}^n=\sum_{r=0}^{n}C_n^rC_n^{n-r}=\sum_{r=0}^{n}(C_n^r)^2$$

وهي النتيجة المطلوبة. ■

التمرين 2. قسّم إقليدياً كثير الحدود A على كثير الحدود B في الحالات التالية:

	B	A
①	$2X^2+X+1$	X^4+3X^2+X+1
②	$X^2-2X\cos\varphi+1$	$X^n\sin\varphi-X\sin n\varphi+\sin(n-1)\varphi$
③	$X^2-2X\cos\varphi+1$	$X^{2n}-2X^n\cos n\varphi+1$

الحل

① نجد بحساب مباشر

$$A(X)=B(X)\left(\frac{1}{2}X^2-\frac{1}{4}X+\frac{11}{8}\right)-\frac{1}{8}X-\frac{3}{8}$$

② نلاحظ في حالة $n=2$ أنّ B يقسم A_2 وخارج القسمة هو الثابت $\sin\varphi$. ونلاحظ في حالة $n=3$ أنّ B يقسم A_3 أيضاً، وأنّ خارج القسمة هو $\sin\varphi X+\sin 2\varphi$. وكذلك نجد في حالة $n=4$ أنّ B يقسم A_4 وأنّ خارج القسمة يساوي

$$\sin\varphi X^2+\sin 2\varphi X+\sin 3\varphi\,.$$

يوحي لنا ذلك أنّ B يقسم A_n في الحالة العامّة، وأنّ خارج القسمة يعطى بالعلاقة

$$Q_n(X)=\sum_{p=0}^{n-2}\sin((n-1-p)\varphi)X^p$$

وللتوثُّق من ذلك نبدأ بملاحظة أنّ $X^2-2\cos\varphi X+1=(X-e^{\mathrm{i}\varphi})(X-e^{-\mathrm{i}\varphi})$، وكذلك أنّ

$$\begin{aligned}X^{n+1}-e^{-\mathrm{i}\varphi}X^n-e^{\mathrm{i}n\varphi}X+e^{\mathrm{i}(n-1)\varphi}&=(X^n-e^{\mathrm{i}n\varphi})(X-e^{-\mathrm{i}\varphi})\\&=(X-e^{\mathrm{i}\varphi})(X-e^{-\mathrm{i}\varphi})\left(\sum_{k=0}^{n-1}e^{\mathrm{i}(n-1-k)\varphi}X^k\right)\end{aligned}\quad ❶$$

وإذا استبدلنا $-\varphi$ بالمقدار φ وجدنا أيضاً

$$\begin{aligned}X^{n+1}-e^{\mathrm{i}\varphi}X^n-e^{-\mathrm{i}n\varphi}X+e^{-\mathrm{i}(n-1)\varphi}&=(X^n-e^{-\mathrm{i}n\varphi})(X-e^{\mathrm{i}\varphi})\\&=(X-e^{\mathrm{i}\varphi})(X-e^{-\mathrm{i}\varphi})\left(\sum_{k=0}^{n-1}e^{-\mathrm{i}(n-1-k)\varphi}X^k\right)\end{aligned}\quad ❷$$

فإذا طرحنا المساواة الثانية من الأولى وقسمنا الطرفين على $2\mathrm{i}$، وجدنا

$$A_n=\sin\varphi X^n-\sin n\varphi X+\sin(n-1)\varphi=(X^2-2\cos\varphi X+1)Q_n(X)$$

وعليه نكون قد أثبتنا أنّ $A_n=BQ_n$. وهي النتيجة المرجوّة.

هذا ويمكننا الاستفادة من العلاقة التدريجيّة $Q_{n+1}=XQ_n+\sin n\varphi$ لإثبات أنّ المساواة $A_n=BQ_n$ تقتضي $A_{n+1}=BQ_{n+1}$ والوصول إلى النتيجة المطلوبة بالتدريج. إلاّ أنّ الطريقة السابقة مفيدة في ③ .

③ نلاحظ أنّ

$$X^{2n} - 2\cos n\varphi X^n + 1 = (X^n - e^{\mathrm{i}n\varphi})(X^n - e^{-\mathrm{i}n\varphi})$$

وهنا أيضاً نستفيد من المساواة ❶ فإذا ضربنا طرفيها بالمقدار $X^n - e^{-\mathrm{i}n\varphi}$ وجدنا

$$\begin{aligned} A(X)(X - e^{-\mathrm{i}\varphi}) &= B(X)(X^n - e^{-\mathrm{i}n\varphi})\left(\sum_{k=0}^{n-1} e^{\mathrm{i}(n-1-k)\varphi} X^k\right) \\ &= B(X)\left(\sum_{k=0}^{n-1} e^{\mathrm{i}(n-1-k)\varphi} X^{k+n} - \sum_{k=0}^{n-1} e^{-\mathrm{i}(k+1)\varphi} X^k\right) \\ &= B(X)\left(\sum_{k=n}^{2n-1} e^{\mathrm{i}(2n-1-k)\varphi} X^k - \sum_{k=0}^{n-1} e^{-\mathrm{i}(k+1)\varphi} X^k\right) \\ &= B(X)\left(\sum_{k=n+1}^{2n} e^{\mathrm{i}(2n-k)\varphi} X^{k-1} - \sum_{k=1}^{n} e^{-\mathrm{i}k\varphi} X^{k-1}\right) \end{aligned} \quad ❸$$

وإذا استبدلنا $-\varphi$ بالمقدار φ في هذه المساواة وجدنا

$$A(X)(X - e^{\mathrm{i}\varphi}) = B(X)\left(\sum_{k=n+1}^{2n} e^{-\mathrm{i}(2n-k)\varphi} X^{k-1} - \sum_{k=1}^{n} e^{\mathrm{i}k\varphi} X^{k-1}\right) \quad ❹$$

فإذا طرحنا المساواة ❹ من المساواة ❸ طرفاً من طرف وجدنا

$$A(X)\sin\varphi = B(X)\left(\sum_{k=n+1}^{2n} \sin((2n-k)\varphi) X^{k-1} + \sum_{k=1}^{n} \sin(k\varphi) X^{k-1}\right)$$

وعليه يكون $A(X) = B(X)Q_n(X)$ ، وقد عرّفنا

$$Q_n(X) = \sum_{k=1}^{n} \frac{\sin k\varphi}{\sin\varphi} X^{k-1} + \sum_{k=n+1}^{2n-1} \frac{\sin(2n-k)\varphi}{\sin\varphi} X^{k-1}$$

أو

$$Q_n(X) = \sum_{p=1}^{2n-1} \frac{\sin((n - |n-p|)\varphi)}{\sin\varphi} X^{p-1}$$

وهي النتيجة المطلوبة. ∎

التمرين 3. احسب القاسم المشترك الأعظم D لكثيرَي الحدود A و B في الحالتين التاليتين، ثُمّ أوجد في كلِّ حالة كثيري حدود U و V يُحقِّقان $UA + VB = D$.

	B	A
①	$2X^3 + 5X^2 + 5X + 3$	$2X^4 + 11X^3 + 10X^2 - 2X - 3$
②	$X^4 - 2X^3 + 7X^2 - 4X + 10$	$X^5 - 2X^4 + 2X^3 - 3X^2 + 2$

الحل

نعرّف المتتالية $(R_k)_{0\le k}$ بوضع $R_0 = A$ و $R_1 = B$ و R_{k+1} هو باقي قسمة R_{k-1} على R_k مادام $R_k \neq 0$. عندئذ يكون أيُّ شريك لآخر باقٍ غير معدوم R_N قاسماً مشتركاً أعظم لكثيري الحدود A و B. ثُمّ إذا عرّفنا كثير الحدود Q_k بأنّه خارج قسمة R_{k-1} على R_k في حالة $1 \le k \le N$، أي عرّفناه بالعلاقة $R_{k-1} = Q_k R_k + R_{k+1}$، ثُمّ عرّفنا المتتاليتين $(U_k)_{0\le k}$ و $(V_k)_{0\le k}$ تدريجيّاً كما يلي :

$$\begin{aligned} &U_0 = 1, \quad U_1 = 0, \quad \forall k \in \mathbb{N}_{N-1}, \quad U_{k+1} = U_{k-1} - Q_k U_k \\ &V_0 = 0, \quad V_1 = 1, \quad \forall k \in \mathbb{N}_{N-1}, \quad V_{k+1} = V_{k-1} - Q_k V_k \end{aligned}$$

كان لدينا $U_N A + V_N B = R_N$، ويكفي أن نقسم كلاً من R_N و U_N و V_N على ثابت الحدِّ المُسيْطر في R_N لنحصل على D و U و V على التوالي.

ويمكن تمثيل هذه الحسابات في جدول، وهذا ما سنفعله فيما يلي.

① نجد في الجدول التالي نتائج الحساب السابق.

k	R_k	Q_k	U_k	V_k
0	A		1	0
1	B	$X+3$	0	1
2	$-10X^2 - 20X - 12$	$-\frac{1}{10}(2X+1)$	1	$-X-3$
3	$\frac{3}{5}(X+3)$	$-\frac{50}{3}(X-1)$	$\frac{1}{10}(2X+1)$	$-\frac{1}{10}(2X^2+7X-7)$
4	-42		$\frac{10}{3}X^2 - \frac{5}{3}X - \frac{2}{3}$	$-\frac{10}{3}X^3 - \frac{25}{3}X^2 + \frac{67}{3}X - \frac{44}{3}$
5	0			

إذن

$\gcd(A,B) = 1$ و $U = -\frac{5}{63}X^2 + \frac{5}{126}X + \frac{1}{63}$ و $V = \frac{5}{63}X^3 + \frac{25}{126}X^2 - \frac{67}{126}X + \frac{22}{63}$.

② ونجد في الجدول التالي نتائج الحساب في الحالة الثانية.

k	R_k	Q_k	U_k	V_k
0	A		1	0
1	B	X	0	1
2	$-5X^3+X^2-10X+2$	$-\frac{1}{5}X+\frac{9}{25}$	1	$-X$
3	$\frac{116}{25}(X^2+2)$		$\frac{1}{5}X-\frac{9}{25}$	$-\frac{1}{5}X^2+\frac{9}{25}X+1$
4	0			

إذن

$\gcd(A,B)=X^2+2$ و $U=\frac{5}{116}X-\frac{9}{116}$ و $V=-\frac{5}{116}X^2+\frac{9}{116}X+\frac{25}{116}$. ■

التمرين 4. عيّن باقي القسمة الإقليدية لكثير الحدود $A=(X-3)^{2n}+(X-2)^n-2$ حيث $(n\in\mathbb{N}^*)$، على كثير الحدود B في الحالات التالية:

① $B=(X-3)(X-2)$ ② $B=(X-2)^2$

③ $B=(X-3)^3$ ④ $B=(X-3)^2(X-2)^2$

الحل

① إنّ درجة باقي قسمة A على B تساوي الواحد على الأكثر. إذن يأخذ باقي القسمة المنشود الصيغة $R(X)=aX+b$. فإذا رمزنا إلى خارج قسمة A على B بالرمز Q كان

$$A(X)=Q(X)(X-2)(X-3)+R(X)$$

يكفي لتعيين الثابتين a و b أن نعرف قيمة $R(X)$ عند قيمتين مختلفتين للمتحوّل X . فإذا أردنا الاستفادة من المساواة السابقة اكتفينا بملاحظة أنّ $B\mid(A-R)$ يقتضي أنّ العددين 2 و 3 جذران للفرق $A-R$ أي إنّ $R(2)=A(2)=-1$ و $R(3)=A(3)=-1$.

ولكنّ الشروط $\deg R\leq 1$ و $R(2)=R(3)=-1$ تقتضي أنّ $R(X)=-1$.

② وهنا أيضاً تساوي درجة باقي قسمة A على B الواحد على الأكثر. إذن يأخذ باقي القسمة المنشود الصيغة $R(X)=aX+b$. فإذا رمزنا إلى خارج قسمة A على B بالرمز Q كان

$$A(X)=Q(X)(X-2)^2+R(X)$$

فإذا أردنا الاستفادة من المساواة السابقة اكتفينا بملاحظة أنّ $B\mid(A-R)$ يقتضي أنّ العدد 2 هو جذرٌ مضاعف من المرتبة الثانية على الأقل لكثير الحدود $A-R$ ، أي إنّ العدد 2 هو جذرٌ لكلٍّ من كثير الحدود $A-R$ ولمشتقّه $A'-R'$.

أي $R(2) = A(2) = -1$ و $R'(2) = A'(2) = (\delta_{n,1} - 2)n$. وقد رمزنا بالمقدار $\delta_{n,1}$ للدلالة على العدد 1 في حالة $n = 1$ وعلى العدد 0 في حالة $n > 1$. ونستنتج من الشروط السابقة أنّ $R(X) = n(\delta_{n,1} - 2)(X-2) - 1$.

③ يمكننا في هذه الحالة اتّباع أسلوب الحالة السابقة، ولكن سنتبع أسلوباً آخر. نلاحظ أوّلاً أنّه في حالة $n = 1$ يكون باقي قسمة A على B هو A نفسه، لأنّ $\deg A < \deg B$ في هذه الحالة. لنفترض أنّ $n \geq 2$. عندئذ يُكتب A بالصيغة

$$\begin{aligned} A &= (X-3)^{2n} + (X-3+1)^n - 2 \\ &= (X-3)^{2n} + \sum_{k=0}^{n} C_n^k (X-3)^k - 2 \\ &= -1 + n(X-3) + \frac{n(n-1)}{2}(X-3)^2 + B(X)Q(X) \end{aligned}$$

وقد عرّفنا $Q(X) = (X-3)^{2n-3} + \sum_{k=3}^{n} C_n^k (X-3)^{k-3}$. إذن باقي قسمة A على B في حالة $n \geq 2$ هو $R(X) = -1 + n(X-3) + \frac{n(n-1)}{2}(X-3)^2$.

④ إنّ درجة باقي قسمة A على B في هذه الحالة تساوي 3 على الأكثر. إذن يأخذ باقي القسمة المنشود الصيغة $R(X) = aX^3 + bX^2 + cX + d$. فإذا لاحظنا أنّ $B \mid (A - R)$ يقتضي أنّ كلاً من العددين 2 و 3 هو جذرٌ مضاعف من المرتبة الثانية على الأقل لكثير الحدود $A - R$ ، أي إنّ العددين 2 و 3 جذران لكلٍّ من كثيري الحدود $A - R$ و $A' - R'$. وهذا يُكافئ

$$R(3) = A(3) = -1 \quad \text{و} \quad R(2) = A(2) = -1$$

$$R'(3) = A'(3) = n \quad \text{و} \quad R'(2) = A'(2) = n\left(\delta_{n,1} - 2\right)$$

ولمّا كانت $\deg R \leq 3$ وكلٌّ من $X - 2$ و $X - 3$ يقسم $R(X) + 1$ استنتجنا أنّه يوجد كثير حدود من الدرجة الأولى $\alpha X + \beta$ يُحقّق

$$R(X) + 1 = (X-2)(X-3)(\alpha X + \beta)$$

وعليه يكون

$$R'(3) = 3\alpha + \beta \quad \text{و} \quad R'(2) = -2\alpha - \beta$$

ومنه

$$\begin{aligned}\alpha &= R'(2)+R'(3) &&= n\left(\delta_{n,1}-1\right)\\ \beta &= -3R'(2)-2R'(3) &&= n\left(4-3\delta_{n,1}\right)\end{aligned}$$

وباقي قسمة A على B في هذه الحالة يساوي

$$R(X)=n(X-2)(X-3)\left((\delta_{n,1}-1)X+4-3\delta_{n,1}\right)-1$$

وهو المطلوب. ■

التمرين 5. ما هي قيم n التي تجعل كثير الحدود $B=X^2+X+1$ يقسم كثير الحدود $A=(X^n+1)^n-X^n$ ؟

الحل

لنلاحظ أوّلاً أنّ $B=X^2+X+1=(X-\mathrm{j})(X-\overline{\mathrm{j}})$، مع $\mathrm{j}=\exp\left(\frac{2i\pi}{3}\right)$. فإذا افترضنا أنّ $(X-\mathrm{j})$ يقسم A، كان $A(X)=(X-\mathrm{j})Q(X)$ واستنتجنا بأخذ المرافق، وملاحظة أنّ كثير الحدود A حقيقي، أنّ $A(X)=(X-\overline{\mathrm{j}})\overline{Q(X)}$ وهذا يعني أنّ $(X-\overline{\mathrm{j}})$ يقسم A أيضاً. ولأنّ كثيري الحدود $(X-\mathrm{j})$ و $(X-\overline{\mathrm{j}})$ أوليّان فيما بينهما استنتجنا أنّ $A \mid B$. وبالعكس إذا قسم B كثير الحدود A كان $A \mid (X-\mathrm{j})$. إذن لقد أثبتنا أنّ

$$B \mid A \Leftrightarrow (X-\mathrm{j}) \mid A$$

ونعلم أنّ $A \mid (X-\mathrm{j})$ إذا وفقط إذا كان $A(\mathrm{j})=0$. ولكن

$$A(\mathrm{j})=(\mathrm{j}^n+1)^n-\mathrm{j}^n=\begin{cases}2^n-1 & : \quad n=0 \bmod 3\\ (-1)^n\,\mathrm{j}^2-\mathrm{j} & : \quad n=1 \bmod 3\\ ((-1)^n-1)\,\mathrm{j}^2 & : \quad n=2 \bmod 3\end{cases}$$

وعلى هذا نجد أنّ $A(\mathrm{j})=0$ إذا وفقط إذا كان

$$n=0 \quad \text{أو} \quad n=2 \bmod 6$$

أي

$$(X^2+X+1) \mid \left((X^n+1)^n-X^n\right) \Leftrightarrow (n=0)\vee(n=2 \bmod 6)$$ ■

التمرين 6. ما هي قيم العدد n التي تجعل كثير الحدود $B=(X^2+X+1)^2$ يقسم كثير الحدود $A=(X+1)^n-X^n-1$ ؟

الحل

لنلاحظ أوّلاً أنّ

$$B=(X^2+X+1)^2=(X-\mathrm{j})^2(X-\overline{\mathrm{j}})^2$$

حيث $\mathrm{j}=\exp\left(\frac{2\mathrm{i}\pi}{3}\right)$.

فإذا افترضنا أنّ $(X-\mathrm{j})^2$ يقسم A، كان $A(X)=(X-\mathrm{j})^2Q(X)$ واستنتجنا بأخذ المرافق، وملاحظة أنّ كثير الحدود A حقيقي، أنّ $A(X)=(X-\overline{\mathrm{j}})^2\overline{Q(X)}$ وهذا يعني أنّ $(X-\overline{\mathrm{j}})^2$ يقسم A أيضاً. ولأنّ كثيرَي الحدود $(X-\mathrm{j})^2$ و $(X-\overline{\mathrm{j}})^2$ أوليّان فيما بينهما استنتجنا أنّ $B\mid A$. وبالعكس إذا قسم B كثير الحدود A كان $A\mid(X-\mathrm{j})^2$. إذن لقد أثبتنا أنّ

$$B\mid A\Leftrightarrow(X-\mathrm{j})^2\mid A$$

ونعلم أنّ $A\mid(X-\mathrm{j})^2$ إذا وفقط إذا كان $A(\mathrm{j})=A'(\mathrm{j})=0$. ولكن

$$\begin{aligned}A(\mathrm{j})&=(1+\mathrm{j})^n-\mathrm{j}^n-1=(-1)^n\,\mathrm{j}^{2n}-\mathrm{j}^n-1\\A'(\mathrm{j})&=n\Big((1+\mathrm{j})^{n-1}-\mathrm{j}^{n-1}\Big)=n\,\mathrm{j}\Big(-(-1)^n\,\mathrm{j}^{2n}-\mathrm{j}^{n+1}\Big)\end{aligned}$$

إذن $A\mid(X-\mathrm{j})^2$ إذا وفقط إذا كان $(-1)^n\,\mathrm{j}^{2n}=\mathrm{j}^n+1$ و $(-1)^n\,\mathrm{j}^{2n}=-\mathrm{j}^{n+1}$.

ينتج من الشرط الأخير أنّ $(-\mathrm{j})^{n-1}=1$، ولكن رتبة الجذر $-\mathrm{j}$ في الزمرة الضربيّة $(\mathbb{U},\times)$ تساوي 6، إذن يجب أن يكون $n-1=0\bmod 6$، أو $n=1\bmod 6$. وبالعكس، إذا كان $n=1\bmod 6$ كان $A(\mathrm{j})=A'(\mathrm{j})=0$. إذن

$$(X^2+X+1)^2\mid\Big((X+1)^n-X^n-1\Big)\Leftrightarrow\Big(n=1\bmod 6\Big)$$

وهي النتيجة المرجوّة. ∎

التمرين 7. عيّن باقي القسمة الإقليديّة لكثير الحدود $P=(X+1)^{2n+1}+X^{n+2}$ على $Q=X^2+X+1$.

الحل

إنّ درجة باقي قسمة P على Q تساوي الواحد على الأكثر. إذن يأخذ باقي القسمة المنشود الصيغة $R(X) = aX + b$ وهو ينتمي إلى $\mathbb{R}[X]$. فإذا رمزنا إلى خارج قسمة P على Q بالرمز S كان

$$P(X) = S(X)(X^2 + X + 1) + R(X)$$

ولكن نعلم أنّه في $\mathbb{C}[X]$ لدينا $X^2 + X + 1 = (X - \mathrm{j})(X - \overline{\mathrm{j}})$، حيث $\mathrm{j} = \exp\left(\frac{2\mathrm{i}\pi}{3}\right)$. فإذا تأمّلنا المساواة السابقة في $\mathbb{C}[X]$ استنتجنا أنّ $R(\mathrm{j}) = P(\mathrm{j})$ وهذه المساواة كافية لتعيين الثابتين a و b.

في الحقيقة، لدينا

$$\begin{aligned} P(\mathrm{j}) &= (1 + \mathrm{j})^{2n+1} + \mathrm{j}^{n+2} \\ &= (-\,\mathrm{j}^2)^{2n+1} + \mathrm{j}^{n+2} = -\,\mathrm{j}^{n+2} + \mathrm{j}^{n+2} = 0 \end{aligned}$$

والعلاقة $a\,\mathrm{j} + b = 0$ حيث $(a, b) \in \mathbb{R}^2$ تكافئ $a = b = 0$ أي $R = 0$. ■

التمرين 8. لتكن α و β و γ ثلاثة أعداد طبيعية. أثبت أنّ $B = X^2 + X + 1$ يقسم كثير الحدود $A = (1 + X)^{6\alpha+1} - (1 + X)^{6\beta+2} + (1 + X)^{6\gamma+3}$.

الحل

ليكن $\mathrm{j} = \exp\left(\frac{2\mathrm{i}\pi}{3}\right)$. عندئذ نلاحظ أنّ

$$\begin{aligned} A(\mathrm{j}) &= (1 + \mathrm{j})^{6\alpha+1} - (1 + \mathrm{j})^{6\beta+2} + (1 + \mathrm{j})^{6\gamma+3} \\ &= (-\,\mathrm{j}^2)^{6\alpha+1} - (-\,\mathrm{j}^2)^{6\beta+2} + (-\,\mathrm{j}^2)^{6\gamma+3} \\ &= -\,\mathrm{j}^{12\alpha+2} - \mathrm{j}^{12\beta+1} - \mathrm{j}^{12\gamma} \\ &= -(1 + \mathrm{j} + \mathrm{j}^2) = 0 \end{aligned}$$

إذن $X - \mathrm{j}$ يقسم A، ولأنّ A حقيقي استنتجنا أنّ $X - \overline{\mathrm{j}}$ يقسم A أيضاً. وهذا يقتضي، لأنّ كثيري الحدود $X - \mathrm{j}$ و $X - \overline{\mathrm{j}}$ أوليّان فيما بينهما، أنّ $B \mid A$. وهو المطلوب. ■

التمرين 9. ليكن n و m عددين طبيعيين موجبين تماماً. برهن أنه يوجد كثيرا حدود وحيدان U و V من $\mathbb{R}[X]$، يحققان:

$$\deg U < n, \quad \deg V < m, \quad X^m U(X) + (1-X)^n V(X) = 1$$

واستنتج أنه يوجد عددان حقيقيان α و β يُحقِّقان:

$$(1-X)V'(X) - nV(X) = \alpha X^{m-1},$$
$$XU'(X) + mU(X) = \beta(1-X)^{n-1}$$

وأخيراً عيّن α و β، واستنتج صيغة $V(X)$ و $U(X)$.

الحل

- لنبدأ بإثبات الوجود. نلاحظ انطلاقاً من المساواة $1 = (X+1-X)^{n+m-1}$ أنّ

$$\begin{aligned}
1 &= \sum_{k=0}^{n+m-1} C_{n+m-1}^{k} X^k (1-X)^{n+m-1-k} \\
&= \sum_{k=m}^{n+m-1} C_{n+m-1}^{k} X^k (1-X)^{n+m-1-k} + \sum_{k=0}^{m-1} C_{n+m-1}^{k} X^k (1-X)^{n+m-1-k} \\
&= \sum_{k=0}^{n-1} C_{n+m-1}^{m+k} X^{k+m} (1-X)^{n-1-k} + \sum_{k=0}^{m-1} C_{n+m-1}^{k} X^k (1-X)^{n+m-1-k} \\
&= X^m \underbrace{\sum_{k=0}^{n-1} C_{n+m-1}^{m+k} X^k (1-X)^{n-1-k}}_{U(X)} + (1-X)^n \underbrace{\sum_{k=0}^{m-1} C_{n+m-1}^{k} X^k (1-X)^{m-1-k}}_{V(X)}
\end{aligned}$$

ونرى مباشرة أنّ $\deg U < n$ و $\deg V < m$. وتثبتُ هذه العلاقة أنّ كثيري الحدود $(1-X)^n$ و X^m أوّليّان فيما بينهما.

- لنثبت الآن الوحدانيّة. نفترض أنّ كثيرات الحدود U و V و P و Q تُحقّق الشروط التالية $\deg U < n$ و $\deg P < n$ و $\deg V < m$ و $\deg Q < m$ وأخيراً

$$X^m U + (1-X)^n V = 1 = X^m P + (1-X)^n Q$$

عندئذ نستنتج من ذلك أنّ

$$X^m \left(U - P\right) = (1-X)^n \left(Q - V\right)$$

ولكن $\gcd(X^m,(1-X)^n)=1$ إذن $X^m \mid (Q-V)$. ولكن $\deg(Q-V)<m$ إذن يجب أن يكون $Q-V=0$ أو $Q=V$ وهذا يقتضي أن يكون $U=P$ أيضاً ويثبتُ الوحدانيّة.

■ نستنتج باشتقاق المساواة $X^mU(X)+(1-X)^nV(X)=1$ أنّ

$$(mU+XU')X^{m-1}=(1-X)^{n-1}(nV-(1-X)V') \tag{1}$$

ولأنّ كثيرَ الحدود X^{m-1} يقسم $(1-X)^{n-1}\big(nV-(1-X)V'\big)$، وهو أوّلي مع كثير الحدود $(1-X)^{n-1}$ استنتجنا أنّ X^{m-1} يقسم $\big((1-X)V'-nV\big)$، ولكنّ درجة هذا الأخير تساوي $m-1$ على الأكثر، إذن يوجد ثابتٌ α يُحقّق

$$(1-X)V'-nV=\alpha X^{m-1} \tag{2}$$

وبالتعويض في المساواة (1) نستنتج أنّ

$$XU'+mU=-\alpha(1-X)^{n-1} \tag{3}$$

وعليه $\beta=-\alpha$.

ونستنتج من (2) بتعويض $X=1$ أنّ

$$\alpha=-nV(1)$$

فإذا استفدنا من الصيغة $V(X)=\sum_{k=0}^{m-1}C_{n+m-1}^{k}X^k(1-X)^{m-1-k}$ استنتجنا أنّ

$$\alpha=-nC_{n+m-1}^{m-1}=-\frac{(n+m-1)!}{(n-1)!\cdot(m-1)!}$$

■ لنفترض أنّ $V(X)=\sum_{k=0}^{m-1}\lambda_kX^k$ عندئذ نستنتج من (2) أنّ

$$\sum_{k=0}^{m-2}(k+1)\lambda_{k+1}X^k-\sum_{k=0}^{m-1}k\lambda_kX^k-\sum_{k=0}^{m-1}n\lambda_kX^k=\alpha X^{m-1}$$

أو

$$\sum_{k=0}^{m-2}((k+1)\lambda_{k+1}-(k+n)\lambda_k)X^k-(n+m-1)\lambda_{m-1}X^{m-1}=\alpha X^{m-1}$$

وعليه نستنتج أنّ

$$\lambda_{m-1} = -\frac{\alpha}{n+m-1} \quad \text{و} \quad \lambda_k = \frac{k+1}{k+n}\lambda_{k+1} \quad \text{في حالة} \quad 0 \le k < m-1$$

وهذا يتيح لنا أن نثبت بالتدريج على k أنّ

$$\forall k \in \{0,1,\ldots,m-1\}, \quad \lambda_k = C_{k+n-1}^{k} = \frac{(k+n-1)!}{(n-1)!\cdot k!}$$

ومنه

$$V(X) = \sum_{k=0}^{m-1} C_{k+n-1}^{k} X^k$$

- لنفترض أنّ $U(X) = \sum_{k=0}^{n-1} \mu_k X^k$ عندئذ نستنتج من (3) أنّ

$$\sum_{k=0}^{n-1}(m+k)\mu_k X^k = -\alpha \sum_{k=0}^{n-1} C_{n-1}^{k}(-1)^k X^k$$

ومنه

$$\forall k \in \{0,1,\ldots,n-1\}, \quad \mu_k = \frac{(n+m-1)!}{(n-1)!(m-1)!} \cdot \frac{(-1)^k C_{n-1}^{k}}{(m+k)}$$

وأخيراً

$$U(X) = \frac{(n+m-1)!}{(n-1)!\cdot(m-1)!} \sum_{k=0}^{n-1} \frac{C_{n-1}^{k}}{m+k}(-1)^k X^k$$

وهي النتيجة المطلوبة. ■

التمرين 10. حلّل كثير الحدود $P(X) = (X+\mathrm{i})^n - (X-\mathrm{i})^n$ من $\mathbb{C}[X]$، ثُمّ بسّط الجداء :

$$\mathcal{Z} = \prod_{k=1}^{m}\left(4 + \cot^2\frac{k\pi}{2m+1}\right)$$

الحل

من الواضح أنّ i ليس جذراً لكثير الحدود P إذن

$$P(x) = 0 \Leftrightarrow \left(\frac{x+\mathrm{i}}{x-\mathrm{i}}\right)^n = 1$$

ومن جهة أخرى، إذا عرّفنا أنّ $\omega=\exp\left(\frac{2\pi\,\mathrm{i}}{n}\right)$ ولاحظنا أنّ $\frac{x+\mathrm{i}}{x-\mathrm{i}}\neq 1$ استنتجنا

$$\begin{aligned}\left(\frac{x+\mathrm{i}}{x-\mathrm{i}}\right)^n=1 \quad &\Leftrightarrow \frac{x+\mathrm{i}}{x-\mathrm{i}}\in\left\{\omega^k : k\in\mathbb{N}_{n-1}\right\}\\ &\Leftrightarrow x\in\left\{\mathrm{i}\frac{\omega^k+1}{\omega^k-1} : k\in\mathbb{N}_{n-1}\right\}\\ &\Leftrightarrow x\in\left\{\cot\tfrac{\pi k}{n} : k\in\mathbb{N}_{n-1}\right\}\end{aligned}$$

ولأنّ الأعداد $\left\{\cot\frac{\pi k}{n} : k\in\mathbb{N}_{n-1}\right\}$ مختلفة مثنى مثنى، و $\deg P\leq n-1$ استنتجنا أنّه يوجد عددٌ عقدي λ يُحقِّق

$$P(X)=\lambda\prod_{k=1}^{n-1}\left(X-\cot\frac{\pi k}{n}\right)$$

ولكن أمثال X^{n-1} في P تساوي $2\,\mathrm{i}\,n$ إذن

$$P(X)=(X+\mathrm{i})^n-(X-\mathrm{i})^n=2\,\mathrm{i}\,n\prod_{k=1}^{n-1}\left(X-\cot\frac{\pi k}{n}\right)$$

لنضع $n=2m+1$، ولنلاحظ أنّ

$$\begin{aligned}\prod_{k=m+1}^{2m}\left(X-\cot\frac{\pi k}{2m+1}\right)&=\prod_{k=1}^{m}\left(X-\cot\frac{\pi(2m+1-k)}{2m+1}\right)\\ &=\prod_{k=1}^{m}\left(X+\cot\frac{\pi k}{2m+1}\right)\end{aligned}$$

إذن

$$\begin{aligned}P(X)&=2\,\mathrm{i}\big(2m+1\big)\prod_{k=1}^{2m}\left(X-\cot\frac{\pi k}{2m+1}\right)\\ &=2\,\mathrm{i}\big(2m+1\big)\prod_{k=1}^{m}\left(X-\cot\frac{\pi k}{2m+1}\right)\cdot\prod_{k=m+1}^{2m}\left(X-\cot\frac{\pi k}{2m+1}\right)\\ &=2\,\mathrm{i}\big(2m+1\big)\prod_{k=1}^{m}\left(X-\cot\frac{\pi k}{2m+1}\right)\cdot\prod_{k=1}^{m}\left(X+\cot\frac{\pi k}{2m+1}\right)\\ &=2\,\mathrm{i}\big(2m+1\big)\prod_{k=1}^{m}\left(X^2-\cot^2\frac{\pi k}{2m+1}\right)\end{aligned}$$

فإذا عوّضنا $2\mathrm{i}$ بالمتحوّل X استنتجنا أنّ

$$(2\mathrm{i}+\mathrm{i})^{2m+1}-(2\mathrm{i}-\mathrm{i})^{2m+1}=2\mathrm{i}(2m+1)\prod_{k=1}^{m}\left(-4-\cot^2\frac{\pi k}{2m+1}\right)$$

ومنه

$$\prod_{k=1}^{m}\left(4+\cot^2\frac{\pi k}{2m+1}\right)=\frac{3^{2m+1}-1}{2(2m+1)}$$

وهي النتيجة المطلوبة.

التمرين 11. أثبت أنه أياً كان α من $\mathbb{R}^*$، وأياً كان n من $\mathbb{N}^*$ مع $n\alpha\notin\pi\mathbb{Z}$، كان

$$X^{2n}-2X^n\cos n\alpha+1=\prod_{k=0}^{n-1}\left(X^2-2X\cos\left(\alpha+\frac{2k\pi}{n}\right)+1\right)$$

ثم بسّط الجداء : $\displaystyle\prod_{k=0}^{n-1}\left(\cos\theta-\cos\left(\alpha+\frac{2k\pi}{n}\right)\right)$.

الحل

لنتأمّل كثير الحدود

$$Q(X)=X^{2n}-2X^n\cos n\alpha+1-\prod_{k=0}^{n-1}\left(X^2-2X\cos\left(\alpha+\tfrac{2k\pi}{n}\right)+1\right)$$

ولنعرّف $x_k=\exp\left(\mathrm{i}\alpha+\frac{2\pi\mathrm{i}k}{n}\right)$. عندئذ نستنتج من الشرط $n\alpha\notin\pi\mathbb{Z}$ أنّ

$$\operatorname{card}\left(\left\{x_k:0\le k<n\right\}\cup\left\{\overline{x}_k:0\le k<n\right\}\right)=2n$$

ونتيقّن بالحساب المباشر أنّ $Q(x_j)=0$ في حالة $0\le j<n$، ولأنّ $Q\in\mathbb{R}[X]$ نستنتج أيضاً أنّ $Q(\overline{x}_j)=0$ في حالة $0\le j<n$، وعليه يوجد $2n$ جذراً مختلفاً لكثير الحدود Q. ولكن $\deg Q<2n$، إذن يجب أن يكون $Q=0$. وهذا ما يثبت المساواة المطلوبة. وإذا عوّضنا $e^{\mathrm{i}\theta}$ بالمتحول X استنتجنا مباشرة أنّ :

$$\prod_{k=0}^{n-1}\left(\cos\theta-\cos\left(\alpha+\tfrac{2k\pi}{n}\right)\right)=2^{1-n}\left(\cos n\theta-\cos n\alpha\right).$$

وهي النتيجة المطلوبة.

التمرين 12. أثبت أنه أياً كان العدد الطبيعي الموجب تماماً n، يُكتب كثير الحدود

$$P_n(X)=\left(1+\frac{\mathrm{i}\,X}{2n+1}\right)^{2n+1}-\left(1-\frac{\mathrm{i}\,X}{2n+1}\right)^{2n+1}$$

بالصيغة

$$P_n(X)=2\mathrm{i}\,X\prod_{k=1}^{n}\left(1-\frac{X^2}{(2n+1)^2\tan^2(\frac{\pi k}{2n+1})}\right)$$

ثم احسب كلاً من $\sum_{k=1}^{n}\cot^2(\frac{\pi k}{2n+1})$ و $\sum_{k=1}^{n}\sin^{-2}(\frac{\pi k}{2n+1})$. واستنتج قيمة مجموع المتسلسلة $\sum_{n=1}^{\infty}\frac{1}{n^2}$.

الحل

لنعرّف $x_k=(2n+1)\tan\frac{\pi k}{2n+1}$ في حالة $k\in\mathbb{N}_n$. ولنعرّف كثير الحدود

$$Q(X)=\left(1+\frac{\mathrm{i}\,X}{2n+1}\right)^{2n+1}-\left(1-\frac{\mathrm{i}\,X}{2n+1}\right)^{2n+1}-2\mathrm{i}\,X\prod_{k=1}^{n}\left(1-\frac{X^2}{x_k^2}\right)$$

ولنلاحظ ما يلي :

- في حالة j من $\mathbb{N}_n$ لدينا

$$\begin{aligned}Q(x_j)&=\left(1+\mathrm{i}\tan\tfrac{\pi j}{2n+1}\right)^{2n+1}-\left(1-\tan\tfrac{\pi j}{2n+1}\right)^{2n+1}\\&=\frac{\left(\exp\left(\frac{\pi j}{2n+1}\mathrm{i}\right)\right)^{2n+1}-\left(\exp\left(-\frac{\pi j}{2n+1}\mathrm{i}\right)\right)^{2n+1}}{\cos^{2n+1}\left(\frac{\pi j}{2n+1}\right)}\\&=\frac{(-1)^j-(-1)^j}{\cos^{2n+1}\left(\frac{\pi j}{2n+1}\right)}=0\end{aligned}$$

- ولأنّ $Q(-X)=-Q(X)$ استنتجنا أيضاً أنّ $Q(-x_j)=0$ في حالة j من $\mathbb{N}_n$.
- وأخيراً نلاحظ أنّ $Q(0)=Q'(0)=0$.

نستنتج مما سبق أنّ كثير الحدود Q الذي درجته أصغر أو تساوي $2n+1$ يقبل الأعداد $(x_k)_{k\in\mathbb{N}_n}$ و $(-x_k)_{k\in\mathbb{N}_n}$ جذوراً، ويقبل العدد 0 جذراً مضاعفاً. وهذا يقتضي، لأن مجموع مراتب مضاعفة هذه الجذور أكبر أو يساوي $2n+2$، أنّ $Q=0$. وهي المساواة المطلوبة.

بمقارنة أمثال X^3 في طرفي المساواة

$$\left(1+\frac{\mathrm{i}\,X}{2n+1}\right)^{2n+1}-\left(1-\frac{\mathrm{i}\,X}{2n+1}\right)^{2n+1}=2\,\mathrm{i}\,X\prod_{k=1}^{n}\left(1-\frac{X^2}{x_k^2}\right)$$

نستنتج أنّ

$$-2\,\mathrm{i}\frac{C_{2n+1}^3}{(2n+1)^3}=-2\,\mathrm{i}\sum_{k=1}^{n}\frac{1}{x_k^2}$$

ومنه

$$\sum_{k=1}^{n}\frac{1}{\tan^2\left(\frac{\pi k}{2n+1}\right)}=\frac{n(2n-1)}{3}$$

ولأنّ $\cot^2\theta+1=\dfrac{1}{\sin^2\theta}$ نستنتج أنّ

$$\sum_{k=1}^{n}\frac{1}{\sin^2\left(\frac{\pi k}{2n+1}\right)}=\frac{n(2n-1)}{3}+n=\frac{2n(n+1)}{3}$$

ولكن نعلم أنّه $\sin x\le x\le\tan x\quad ,\left]0,\frac{\pi}{2}\right[\ \in \forall x$ ، إذن

$$\sum_{k=1}^{n}\frac{1}{\tan^2\left(\frac{\pi k}{2n+1}\right)}\le\sum_{k=1}^{n}\frac{(2n+1)^2}{\pi^2k^2}\le\sum_{k=1}^{n}\frac{1}{\sin^2\left(\frac{\pi k}{2n+1}\right)}$$

أو

$$\frac{n(2n-1)}{3}\le\sum_{k=1}^{n}\frac{(2n+1)^2}{\pi^2k^2}\le\frac{2n(n+1)}{3}$$

وبصيغة مكافئة

$$\frac{n(2n-1)}{3(2n+1)^2}\le\frac{1}{\pi^2}\sum_{k=1}^{n}\frac{1}{k^2}\le\frac{2n(n+1)}{3(2n+1)^2}$$

وبجعل n تسعى إلى اللانهاية نجد نستنتج أنّ

$$\lim_{n\to\infty}\sum_{k=1}^{n}\frac{1}{k^2}=\frac{\pi^2}{6}$$

وهي النتيجة المطلوبة. ■

التمرين 13. ليكن n و m عددين طبيعيين موجبين تماماً، وليكن a عنصراً من $\mathbb{C}^*$. نعرّف $\delta = \gcd(n,m)$ و $\mu = \operatorname{lcm}(n,m)$. أثبت أنّ

$$\gcd(X^n - a^n, X^m - a^m) = X^\delta - a^\delta$$

واستنتج أنّ $(X^n - a^n)(X^m - a^m)$ يقسم $(X^\delta - a^\delta)(X^\mu - a^\mu)$.

الحل

لنفترض أنّ α و β عددان طبيعيّان موجبان تماماً وأنّ q و r هما على الترتيب خارج وباقي قسمة α على β أي $\alpha = p\beta + r$ مع $0 \le r < \beta$. عندئذ

$$\begin{aligned} X^\alpha - a^\alpha &= X^{p\beta} X^r - a^{p\beta} a^r \\ &= (X^{p\beta} - a^{p\beta}) X^r + a^{p\beta}(X^r - a^r) \\ &= (X^\beta - a^\beta) \sum_{k=0}^{p-1} a^{\beta(p-1-k)} X^{\beta k + r} + a^{p\beta}(X^r - a^r) \end{aligned}$$

وعليه إذا كان r باقي قسمة α على β، كان $X^r - a^r$ شريك باقي قسمة $X^\alpha - r^\alpha$ على $X^\beta - r^\beta$. ومن ثَمّ

$$\gcd(X^\alpha - a^\alpha, X^\beta - a^\beta) = \gcd(X^\beta - a^\beta, X^r - a^r)$$

لنعرّف إذن $r_0 = n$ و $r_1 = m$، ولنضع، مادام $r_k \ne 0$، r_{k+1} باقي قسمة r_{k-1} على r_k . عندئذ نعلم أنّه عند أوّل قيمة N يكون عندها $r_{N+1} = 0$ يكون $\gcd(n,m) = \delta = r_N$. واستناداً إلى الملاحظة السابقة يكون لدينا

$$\gcd(X^{r_{k-1}} - a^{r_{k-1}}, X^{r_k} - a^{r_k}) = \gcd(X^{r_k} - a^{r_k}, X^{r_{k+1}} - a^{r_{k+1}})$$

في حالة $0 \le k \le N$. ومنه

$$\gcd(X^{r_0} - a^{r_0}, X^{r_1} - a^{r_1}) = \gcd(X^{r_N} - a^{r_N}, X^{r_{N+1}} - a^{r_{N+1}})$$

وهذا يُكافئ قولنا

$$\gcd(X^n - a^n, X^m - a^m) = X^\delta - a^\delta$$

ومن جهة أخرى، لمّا كان كلٌّ من $X^n - a^n$ و $X^m - a^m$ يقسم $X^\mu - a^\mu$ استنتجنا أنّ

$$\operatorname{lcm}(X^n - a^n, X^m - a^m) \mid (X^\mu - a^\mu)$$

وهذا يقتضي أنّ جداء الضرب

$$\gcd(X^n - a^n, X^m - a^m)\,\mathrm{lcm}(X^n - a^n, X^m - a^m)$$

يقسم

$$(X^\delta - a^\delta)(X^\mu - a^\mu)$$

ولكن

$$\gcd(X^n - a^n, X^m - a^m)\,\mathrm{lcm}(X^n - a^n, X^m - a^m) = (X^n - a^n)(X^m - a^m)$$

إذن

$$(X^n - a^n)(X^m - a^m) \mid (X^\delta - a^\delta)(X^\mu - a^\mu)$$

وهي النتيجة المطلوبة. ■

التمرين 14. ليكن P كثير حدود من الدرجة n أمثاله أعداد صحيحة أي $P \in \mathbb{Z}[X]$.
وليكن $N = \gcd(P(0), P(1), \ldots, P(n))$. أثبت أنّ

$$\forall m \in \mathbb{Z}, \quad N \mid P(m)$$

الحل

لنتأمّل $(\ell_0, \ell_1, \ldots, \ell_n)$ كثيرات حدود لاغرانج الموافقة للنقاط $(0, 1, \ldots, n)$. نعلم أنّ

$$\ell_k(X) = \prod_{\substack{j=0 \\ j\neq k}}^{n} \frac{X - j}{k - j}, \qquad k = 0, 1, \ldots, n$$

لنعرّف كثيرات الحدود $\left(C_X^k\right)_{k\in\mathbb{N}}$ بوضع

$C_X^0 = 1$ و $C_X^k = \dfrac{X(X-1)\cdots(X-k+1)}{k!}$ في حالة $k > 0$.

عندئذ نلاحظ مباشرة أنّه في حالة k من $\{0, 1, \ldots, n\}$ لدينا

$$\begin{aligned}\ell_k(X) &= \frac{X}{k} \cdot \frac{X-1}{k-1} \cdot \cdots \cdot \frac{X-k+1}{1} \cdot \frac{X-k-1}{-1} \cdot \cdots \cdot \frac{X-n}{k-n} \\ &= (-1)^{n-k} C_X^k \cdot C_{X-k-1}^{n-k} = C_X^k \cdot C_{n-X}^{n-k}\end{aligned}$$

ولمّا كان

$$\forall k \in \mathbb{N}^*, \quad C_{-X}^k = \frac{-X(-X-1)\cdots(-X-k+1)}{k!} = (-1)^k C_{X+k-1}^k$$

استنتجنا أيضاً أنّ

$$\ell_k(-X) = (-1)^{n-k} C_{-X}^k \cdot C_{n+X}^{n-k} = (-1)^k C_{X+k-1}^k \cdot C_{X+n}^{n-k}$$

ليكن إذن p عدداً صحيحاً، وليكن k من $\{0,1,\ldots,n\}$. نناقش الحالات التالية :

- في حالة $p \in \{0,1,\ldots,n\}$ لدينا $\ell_k(p) = \delta_{p,k}$ ، و $\delta_{p,k}$ هو رمز كرونيكر.
- في حالة $p > n$ ، لدينا $\ell_k(p) = (-1)^{n-k} C_p^k \cdot C_{p-k-1}^{n-k} \in \mathbb{Z}$.
- في حالة $p < 0$ ، لدينا $\ell_k(p) = (-1)^k C_{k-p-1}^k \cdot C_{n-p}^{n-k} \in \mathbb{Z}$.

إذن لقد أثبتنا أنّ

$$\forall k \in \{0,1,\ldots,n\},\ \forall p \in \mathbb{Z},\quad \ell_k(p) \in \mathbb{Z}$$

ليكن P عنصراً من $\mathbb{Z}[X]$ درجته n عندئذ $P(X) = \sum_{k=0}^{n} P(k)\ell_k(X)$. فإذا كان

$$N = \gcd\big(P(0), P(1), \ldots, P(n)\big)$$

وعرّفنا q_k خارج قسمة $P(k)$ على N كان لدينا

$$\forall m \in \mathbb{Z},\quad P(m) = N \cdot \sum_{k=0}^{n} q_k \ell_k(m)$$

ومن ثَمّ $\forall m \in \mathbb{Z},\quad N \mid P(m)$. ■

التمرين 15. ليكن P من $\mathbb{R}[X]$ كثير حدود واحديّاً من الدرجة $n \geq 1$. احسب المقدار

$$\sum_{k=0}^{n} \frac{P(k)}{\prod\limits_{0\leq j\leq n, j\neq k}(k-j)}$$

ثُمّ استنتج أنّ $\max\limits_{0\leq k\leq n} |P(k)| \geq 2^{-n} n!$.

الحل

نستفيد في هذا التمرين أيضاً من $(\ell_0, \ell_1, \ldots, \ell_n)$ كثيرات حدود لاغرانج الموافقة للنقاط $(0,1,\ldots,n)$. نعلم أنّ

$$\ell_k(X) = \prod_{0\leq j\leq n, j\neq k} \frac{X-j}{k-j}, \qquad k = 0,1,\ldots,n$$

فإذا كان P كثير حدود من الدرجة n في $\mathbb{R}[X]$ كان

$$P(x) = \sum_{k=0}^{n} P(k)\ell_k(x) \tag{1}$$

ولكن $\lim_{x\to+\infty} (P(x)/x^n) = 1$ لأنّ P واحدي من الدرجة n، ولدينا مباشرة

$$\lim_{x\to+\infty} \frac{\ell_k(x)}{x^n} = \frac{1}{\prod\limits_{0\le j\le n, j\ne k} (k-j)} = \frac{(-1)^{n-k}}{k!\big(n-k\big)!} = \frac{(-1)^{n-k}}{n!} C_n^k$$

فإذا قسمنا طرفي المساواة (1) على x^n وجعلنا x تسعى إلى اللانهاية وجدنا

$$1 = \sum_{k=0}^{n} \frac{P(k)}{\prod\limits_{0\le j\le n, j\ne k} (k-j)} = \frac{1}{n!}\sum_{k=0}^{n} (-1)^{n-k} C_n^k P(k)$$

- نستنتج من المساواة السابقة أنّ

$$n! \le \sum_{k=0}^{n} C_n^k \left|P(k)\right| \le \left(\sum_{k=0}^{n} C_n^k\right) \max_{0\le k\le n} \left|P(k)\right| = 2^n \max_{0\le k\le n} \left|P(k)\right|$$

وهذا يثبتُ أنّه في حالة كثير حدود واحدي من الدرجة n لدينا

$$\max_{0\le k\le n} \left|P(k)\right| \ge 2^{-n} n!$$

وهي تُكافئ

$$\forall P \in \mathbb{R}_n[X], \quad \left|P^{(n)}(0)\right| \le 2^n \max_{0\le k\le n} \left|P(k)\right|$$

وتتحقّق المساواة في حالة

$$P(X) = \sum_{k=0}^{n} (-1)^k \ell_k(X).$$

- ونستنتج من المساواة نفسها ومن متراجحة كوشي شوارتز أنّ

$$\begin{aligned} n! \le \sum_{k=0}^{n} C_n^k \left|P(k)\right| &\le \sqrt{\sum_{k=0}^{n} (C_n^k)^2}\sqrt{\sum_{k=0}^{n} \left|P(k)\right|^2} \\ &= \sqrt{C_{2n}^n}\sqrt{\sum_{k=0}^{n} \left|P(k)\right|^2} \end{aligned}$$

ومنه

$$\forall P \in \mathbb{R}_n[X], \quad \left|P^{(n)}(0)\right|^2 \leq C_{2n}^n \sum_{k=0}^{n} \left|P(k)\right|^2$$

ويتم إثبات المطلوب. ■

التمرين 16. ليكن P و Q كثيري حدود من الدرجة $n \geq 1$ أمثالهما أعداد عقدية. ولنفترض أن لكثيري الحدود P و Q الجذور نفسها وأيضاً أنّ لكثيري الحدود $P-1$ و $Q-1$ الجذور نفسها. أثبت أن $P = Q$.

الحل

ليكن P كثير حدود من الدرجة n من $\mathbb{N}^*$. ولنعرّف المجموعتين

$$\mathcal{B} = \left\{z \in \mathbb{C} : P(z) = 1\right\} \quad \text{و} \quad \mathcal{A} = \left\{z \in \mathbb{C} : P(z) = 0\right\}$$

عندئذ يكون لدينا

$$P(X) - 1 = \lambda \prod_{\beta \in \mathcal{B}} (X - \beta)^{m_\beta} \quad \text{و} \quad P(X) = \lambda \prod_{\alpha \in \mathcal{A}} (X - \alpha)^{n_\alpha}$$

- من الواضح أنّ $\mathcal{A} \cap \mathcal{B} = \varnothing$.
- ونلاحظ أنّ كلّاً من $\prod_{\alpha \in \mathcal{A}} (X - \alpha)^{n_\alpha - 1}$ و $\prod_{\beta \in \mathcal{B}} (X - \beta)^{n_\beta - 1}$ يقسم $P'(X)$ وهما أوّليّان فيما بينهما لأنّ $\mathcal{A} \cap \mathcal{B} = \varnothing$.

إذن يقسم الجداء $\prod_{\beta \in \mathcal{B}} (X - \beta)^{n_\beta - 1} \prod_{\alpha \in \mathcal{A}} (X - \alpha)^{n_\alpha - 1}$ كثير الحدود $P'(X)$،

ومنه

$$\sum_{\alpha \in \mathcal{A}} (n_\alpha - 1) + \sum_{\beta \in \mathcal{B}} (m_\beta - 1) \leq \deg P' \leq n - 1$$

أي

$$\sum_{\alpha \in \mathcal{A}} n_\alpha + \sum_{\beta \in \mathcal{B}} m_\beta - \operatorname{card}(\mathcal{A}) - \operatorname{card}(\mathcal{B}) \leq n - 1$$

ومنه

$$\operatorname{card}(\mathcal{A} \cup \mathcal{B}) \geq n + 1$$

النتيجة. إذا كان P كثير حدود من $\mathbb{C}[X]$، يُحقّق $\deg(P) > 0$. عندئذ

$$\operatorname{card}\left(\left\{z \in \mathbb{C} : P(z)(P(x)-1) = 0\right\}\right) \geq 1 + \deg P$$

لنفترض أنّ P و Q كثيري حدود عقديّين من الدرجة $n \leq 1$. ولنفترض أنّ Q ينعدم عند جذور P وأنّ $Q-1$ ينعدم عند جذور $P-1$. عندئذ نتأمّل كثير الحدود $R = P - Q$. فنلاحظ أنّ $\deg R \leq n$ وأنّ R ينعدم على المجموعة

$$\left\{z \in \mathbb{C} : P(z)(P(z)-1) = 0\right\}$$

التي عدد عناصرها أكبر تماماً من n . فلا بُدّ أن يكون $R = 0$ أو $P = Q$. ■

التمرين 17. أثبت أنه يوجد في $\mathbb{Q}[X]$ كثير حدود وحيد P_n يُحقّق $P_n - P_n' = X^n$.

الحل

لنفترض أنّ $P = \sum_{k=0}^{m} a_k X^k$ يُحقّق $P - P' = X^n$ عندئذ نجد بالتعويض أنّ

$$\sum_{k=0}^{m} a_k X^k - \sum_{k=0}^{m-1} (k+1) a_{k+1} X^k = X^n$$

أو

$$a_m X^m + \sum_{k=0}^{m-1} (a_k - (k+1) a_{k+1}) X^k = X^n$$

إذن يجب أن يكون $n = m$ ، و $a_n = 1$ ، و $a_k = (k+1) a_{k+1}$ في حالة $0 \leq k < n$.
وهذا يقتضي أن تكون المقادير $\left(k! a_k\right)_{0 \leq k \leq n}$ متساوية وتساوي $n! a_n = n!$. وعليه

$$\forall k \in \left\{0,1,\ldots,n\right\}, \quad a_k = \frac{n!}{k!}$$

ومن ثَمّ يجب أن يكون

$$P = \sum_{k=0}^{n} \frac{n!}{k!} X^k = P_n .$$

وبالعكس، نتيقّن بتحقُّقٍ مباشر أنّ كثير الحدود $P_n = n! \cdot \sum_{k=0}^{n} \frac{X^k}{k!}$ يُحقّق الشرط $P_n - P_n' = X^n$. ■

التمرين 18. كثيرات حدود Tchebychev

1. أثبت أنه يوجد في $\mathbb{R}[X]$ كثير حدود وحيد T_n من الدرجة n، يحقّق، أياً كان العدد الحقيقي θ، العلاقة $T_n(\cos\theta) = \cos n\theta$. ما هو ثابت X^n في T_n؟ نعرّف أيضاً $U_n = \dfrac{1}{n+1}T'_{n+1}$، ما هي قيمة $U_n(\cos\theta)$ بدلالة θ؟

2. عيّن جذور كلٍ من T_n و U_n، وأثبت أنها تنتمي جميعاً إلى المجال $]-1,+1[$.

3. أثبت في حالة $1 \leq n$، العلاقتين التاليتين :
$$T_{n+1} = XT_n - (1-X^2)U_{n-1}$$
$$U_n = XU_{n-1} + T_n$$

4. أثبت أن كثيري الحدود T_n و U_n يحقّقان المعادلتين التفاضليتين :
$$\left(X^2-1\right)T''_n + XT'_n - n^2T_n = 0$$
$$\left(X^2-1\right)U''_n + 3XU'_n - n(n+2)U_n = 0$$
ثم احسب أمثال كثير الحدود T_n.

5. أثبت أن كثيري الحدود T_n و U_n يحققان العلاقتين التدريجيتين التاليتين :
$$T_{n+1} = 2XT_n - T_{n-1} \quad \text{حيث} \quad T_1(X) = X, \quad T_0(X) = 1.$$
$$U_{n+1} = 2XU_n - U_{n-1} \quad \text{حيث} \quad U_1(X) = 2X, \quad U_0(X) = 1.$$

6. نضع $V_n(x) = \dfrac{\mathrm{d}^n}{\mathrm{d}\,x^n}\left((1-x^2)^{n-1/2}\right)$ في حالة x من $[-1,1]$. أثبت أن
$$\frac{n}{2n+1}V_{n+1}(x) = (1-x^2)V'_n(x) - (n+1)xV_n(x)$$
استنتج أنه يمكننا تعيين الثابت λ_n ليكون
$$\forall x \in [-1,1], \quad T_n(x) = \lambda_n\sqrt{1-x^2}V_n(x)$$

7. ليكن f تابعاً يقبل مشتقات مستمرة حتى المرتبة n على المجال $[-1,+1]$. أثبت، بالمكاملة بالتجزئة عدة مراتٍ، أنّ
$$\int_{-1}^{1}\frac{T_n(x)}{\sqrt{1-x^2}}f(x)\,\mathrm{d}\,x = \frac{2^n\cdot n!}{(2n)!}\int_{-1}^{1}\frac{(1-x^2)^n}{\sqrt{1-x^2}}f^{(n)}(x)\,\mathrm{d}\,x$$

واستنتج أن

$$\int_0^\pi f(\cos\theta)\cos n\theta \,\mathrm{d}\,\theta = \frac{2^n \cdot n!}{(2n)!}\int_0^\pi f^{(n)}(\cos\theta)\sin^{2n}\theta \,\mathrm{d}\,\theta$$

ثم طبّق ما سبق في حالة $f = T_m$.

الحل

1. **الوحدانيّة.** لنفترض أنّ P و Q كثيري حدود يُحقّقان $P(\cos\theta) = Q(\cos\theta)$ أيّاً كانت θ من $\mathbb{R}$، عندئذ يقبل كثير الحدود $P - Q$ عدداً لا نهائيّاً من الجذور، ولا بُدَّ أن يكون معدوماً. أي $P = Q$.

الوجود. لنلاحظ أنّ كثيرات الحدود $T_0 = 1$ و $T_1 = X$ و $T_2 = 2X^2 - 1$ تفي بالغرض في حالة $n = 0$ و $n = 1$ و $n = 2$. لإثبات الوجود في الحالة العامّة، نلاحظ أنّ

$$\begin{aligned}
\cos n\theta &= \operatorname{Re}(e^{\mathrm{i}n\theta}) = \operatorname{Re}((\cos\theta + \mathrm{i}\sin\theta)^n) \\
&= \operatorname{Re}\left(\sum_{k=0}^{n} C_n^k\, \mathrm{i}^k \cos^{n-k}\theta \sin^k\theta\right) \\
&= \sum_{0\le 2k\le n} C_n^{2k}(-1)^k \cos^{n-2k}\theta \sin^{2k}\theta \\
&= \sum_{0\le k\le \lfloor n/2\rfloor} C_n^{2k}(-1)^k (1-\cos^2\theta)^k \cos^{n-2k}\theta
\end{aligned}$$

إذن $\cos n\theta = T_n(\cos\theta)$ وقد عرّفنا

$$T_n = \sum_{0\le k\le \lfloor n/2\rfloor} C_n^{2k} X^{n-2k}(X^2-1)^k$$

أمّا ثابتُ X^n في T_n فيساوي $\sum_{0\le k\le \lfloor n/2\rfloor} C_n^{2k} = 2^{n-1}$ في حالة $0 < n$.

ونستنتج باشتقاق طرفَي المساواة في $T_{n+1}(\cos\theta) = \cos(n+1)\theta$ بالنسبة إلى المتحوّل θ:

$$T'_{n+1}(\cos\theta)\sin\theta = (n+1)\sin(n+1)\theta$$

فإذا عرّفنا $U_n = \dfrac{1}{n+1}T'_{n+1}$ كان لدينا

$$U_n(\cos\theta) = \frac{\sin(n+1)\theta}{\sin\theta}$$

نسمّي متتاليتي كثيرات الحدود $\left(T_n\right)_{n\in\mathbb{N}}$ و $\left(U_n\right)_{n\in\mathbb{N}}$، متتاليتي كثيرات حدود تِشِبيشِف من النوع الأول والنوع الثاني بالترتيب.

2. لنعرّف $x_k^{(n)} = \cos\left(\frac{\pi}{2n}(2k-1)\right)$ في حالة k من $\{1,\ldots,n\}$. عندئذ نتيقّن مباشرة بسبب التناقص التام للتابع $\cos$ على المجال $[0,\pi]$ أنّ

$$-1 < x_n^{(n)} < \cdots < x_{k+1}^{(n)} < x_k^{(n)} < \cdots < x_1^{(n)} < 1$$

ونتيقّن مباشرة أنّ

$$T_n\left(x_k^{(n)}\right) = \cos\left(nx_k^{(n)}\right) = \cos\left((2k-1)\frac{\pi}{2}\right) = 0$$

ولأنّ $\deg T_n = n$، نستنتج أنّ T_n يقبل n جذراً بسيطاً هي $\left\{x_k^{(n)} : k\in\mathbb{N}_n\right\}$.

وبأسلوب مماثل إذا عرّفنا $y_k^{(n)} = \cos\left(\frac{\pi k}{n+1}\right)$ في حالة k من $\mathbb{N}_n$. عندئذ نتيقّن مباشرة بسبب التناقص التام للتابع $\cos$ على المجال $[0,\pi]$ أنّ

$$-1 < y_n^{(n)} < \cdots < y_{k+1}^{(n)} < y_k^{(n)} < \cdots < y_1^{(n)} < 1$$

ونتيقّن مباشرة أنّ

$$U_n(y_k^{(n)}) = \frac{\sin\left((n+1)\frac{\pi k}{n+1}\right)}{\sin\frac{\pi k}{n+1}} = \frac{\sin \pi k}{\sin\frac{\pi k}{n+1}} = 0$$

ولأنّ $\deg U_n = n$، نستنتج أنّ U_n يقبل n جذراً بسيطاً هي $\left\{y_k^{(n)} : k\in\mathbb{N}_n\right\}$.

3. لتكن n من $\mathbb{N}^*$. نستنتج من المساواتين :

$$\begin{aligned}\forall\theta\in\mathbb{R},\quad \cos(n+1)\theta &= \cos\theta\cos n\theta - \sin\theta\sin n\theta\\ \sin(n+1)\theta &= \cos\theta\sin n\theta + \sin\theta\cos n\theta\end{aligned}$$

أنّ

$$\begin{aligned}\forall\theta\in\mathbb{R},\quad T_{n+1}(\cos\theta) &= \cos\theta\, T_n(\cos\theta) - (1-\cos^2\theta)U_{n-1}(\cos\theta)\\ U_n(\cos\theta) &= \cos\theta\, U_{n-1}(\cos\theta) + T_n(\cos\theta)\end{aligned}$$

ونستنتج من ذلك مباشرة، بالاستفادة من خاصّة الوحدانيّة في السؤال 1.، أنّ

$$\begin{aligned} T_{n+1} &= XT_n - (1 - X^2)U_{n-1} \\ U_n &= XU_{n-1} + T_n \end{aligned}$$

4. باشتقاق طرفَي المساواة في $T_n(\cos\theta) = \cos n\theta$ بالنسبة إلى المتحوّل θ مرّتين نجد

$$T_n'(\cos\theta)\sin\theta = n\sin n\theta$$

و

$$-T_n''(\cos\theta)\sin^2\theta + T_n'(\cos\theta)\cos\theta = n^2\cos n\theta = n^2 T_n(\cos\theta)$$

أو

$$\forall\theta \in \mathbb{R},\quad T_n''(\cos\theta)(\cos^2\theta - 1) + T_n'(\cos\theta)\cos\theta = n^2 T_n(\cos\theta)$$

وهذا يبرهن أنّ

$$(X^2 - 1)T_n'' + XT_n' - n^2 T_n = 0$$

ونستنتج من هذا أنّ

$$(X^2 - 1)T_{n+1}'' + XT_{n+1}' - (n+1)^2 T_{n+1} = 0$$

فإذا اشتققنا هذه العلاقة وتذكّرنا أنّ $U_n = \dfrac{1}{n+1}T_{n+1}'$ وجدنا

$$(X^2 - 1)U_n'' + 3XU_n' - n(n+2)U_n = 0$$

فنكون بذلك قد وجدنا المعادلتين التفاضليّتين لكثيرات حدود تِشِبيشِف.

▪ لتكن $2 \leq n$. ولنفترض أنّ $T_n = \sum_{k=0}^{n} \lambda_k X^k$ عندئذ نجد بالتعويض في المعادلة التفاضليّة التي يُحقّقها T_n ما يلي :

$$\sum_{k=0}^{n} k(k-1)\lambda_k X^k - \sum_{k=0}^{n-2}(k+2)(k+1)\lambda_{k+2}X^k + \sum_{k=0}^{n} k\lambda_k X^k - \sum_{k=0}^{n} n^2\lambda_k X^k = 0$$

أو

$$-(2n+1)\lambda_{n-1}X^{n-1} + \sum_{k=0}^{n-2}\Big((k^2 - n^2)\lambda_k - (k+2)(k+1)\lambda_{k+2}\Big)X^k = 0$$

وهذا يقتضي أنّ

$$\lambda_{n-1} = 0 \text{ و } \lambda_k = -\frac{(k+2)(k+1)}{n^2 - k^2}\lambda_{k+2} \text{ في حالة } 0 \leq k \leq n-2$$

فإذا تذكّرنا أنّ $\lambda_n = 2^{n-1}$ استنتجنا أنّ

$$\lambda_{n-2p} = (-1)^p 2^{n-2p-1} \frac{n}{n-p} C_{n-p}^p \quad \text{و} \quad \lambda_{n-2p-1} = 0$$

وعليه يكون

$$\forall n \in \mathbb{N}^*, \quad T_n = \sum_{p=0}^{\lfloor n/2 \rfloor} (-1)^p 2^{n-2p-1} \frac{n}{n-p} C_{n-p}^p X^{n-2p}$$

6. لتكن n عدداً طبيعيّاً أكبر أو يساوي 2. نستنتج من المساواتين :

$$\begin{aligned} \forall \theta \in \mathbb{R}, \quad \cos(n+1)\theta + \cos(n-1)\theta &= 2\cos\theta \cos n\theta \\ \sin(n+2)\theta + \sin n\theta &= 2\cos\theta \sin(n+1)\theta \end{aligned}$$

أنّ

$$\begin{aligned} \forall \theta \in \mathbb{R}, \quad T_{n+1}(\cos\theta) + T_{n-1}(\cos\theta) &= 2\cos\theta\, T_n(\cos\theta) \\ U_{n+1}(\cos\theta) + U_{n-1}(\cos\theta) &= 2\cos\theta\, U_n(\cos\theta) \end{aligned}$$

ونستنتج من ذلك مباشرة، بالاستفادة من خاصّة الوحدانيّة في السؤال 1.، أنّ

$$\begin{aligned} T_{n+1} &= 2XT_n - T_{n-1} \\ U_{n+1} &= 2XU_n - U_{n-1} \end{aligned}$$

ونتيقّن مباشرة من أنّ $T_0 = 1$ و $T_1 = X$ و $U_0 = 1$ و $U_1 = 2X$.

7. لنحسب المقدار V_{n+1} بطريقتين، مستفيدين من علاقة لايبنتز. من جهة أولى لدينا

$$\begin{aligned} V_{n+1}(x) &= \left((1-x^2)^{n+½}\right)^{(n+1)} \\ &= -(2n+1)\left(x(1-x^2)^{n-½}\right)^{(n)} \\ &= -(2n+1)\left(x\left((1-x^2)^{n-½}\right)^{(n)} + n\left((1-x^2)^{n-½}\right)^{(n-1)}\right) \\ &= -(2n+1)\left(xV_n(x) + A\right) \end{aligned}$$

وقد عرّفنا $A = n\left((1-x^2)^{n-½}\right)^{(n-1)}$.

ومن جهة ثانية

$$\begin{aligned}V_{n+1}(x) &= \left((1-x^2)^{n+½}\right)^{(n+1)} = \left((1-x^2)(1-x^2)^{n-½}\right)^{(n+1)}\\ &= (1-x^2)\left((1-x^2)^{n-½}\right)^{(n+1)} - 2(n+1)x\left((1-x^2)^{n-½}\right)^{(n)}\\ &\quad -(n+1)A\\ &= (1-x^2)V_n'(x) - 2(n+1)xV_n(x) - (n+1)A\end{aligned}$$

فإذا ضربنا العلاقة الأولى بالمقدار $-\dfrac{n+1}{2n+1}$ وجمعنا الناتج إلى الثانية طرفاً مع طرف وجدنا

$$\frac{n}{2n+1}V_{n+1}(x) = (1-x^2)V_n'(x) - (n+1)xV_n(x)$$

ليكن $Q_n(x) = \lambda_n\sqrt{1-x^2}V_n(x)$ عندئذ نستنتج بالتعويض في العلاقة السابقة أنّ

$$\frac{n}{2n+1}\frac{Q_{n+1}(x)}{\lambda_{n+1}\sqrt{1-x^2}} = \frac{1-x^2}{\lambda_n}\left(\frac{Q_n(x)}{\sqrt{1-x^2}}\right)' - \frac{(n+1)x}{\lambda_n\sqrt{1-x^2}}Q_n(x)$$

ومنه

$$-\frac{\lambda_n}{\left(2n+1\right)\lambda_{n+1}}Q_{n+1}(x) = xQ_n(x) - (1-x^2)\frac{1}{n}Q_n'(x)$$

ولكن، كنّا قد أثبتنا في 3. أنّ

$$T_{n+1} = XT_n - (1-X^2)U_{n-1} = XT_n - (1-X^2)\frac{1}{n}T_n'$$

فإذا اخترنا الثوابت $\left(\lambda_n\right)_{n\geq 0}$ وفق الشروط $\lambda_0 = 1$ و $\forall n\in\mathbb{N},\ \lambda_{n+1} = -\dfrac{\lambda_n}{2n+1}$.
كان لدينا من جهة أولى $T_0(x) = Q_0(x)$ على المجال $]-1,1[$، وكان لدينا

$$Q_{n+1}(x) = xQ_n(x) - (1-x^2)\frac{1}{n}Q_n'(x)$$

وهي، استناداً إلى الملاحظة السابقة، العلاقة التدريجيّة نفسها التي تُحقّقها متتالية كثيرات الحدود $\left(T_n\right)_{n\in\mathbb{N}}$. إذن يمكننا أن نستنتج بالتدريج على العدد n أنّ

$$\forall x\in\,]-1,1[,\quad T_n(x) = Q_n(x).$$

وأخيراً نلاحظ، انطلاقاً من العلاقة التدريجيّة التي تحقّقها المتتالية $\left(\lambda_n\right)_{n\geq 0}$، أنّ

$$\forall n \in \mathbb{N}^*, \quad \lambda_n = \frac{(-1)^n}{1\cdot 3\cdots(2n-1)} = \frac{(-1)^n 2^n n!}{(2n)!}$$

وهكذا نكون قد أثبتنا العلاقة المعروفة باسم علاقة رودرغز Rodrigues :

$$\forall x \in \,]-1,+1[, \quad T_n(x) = \frac{(-1)^n 2^n n!}{(2n)!}\sqrt{1-x^2}\,\frac{\mathrm{d}^n}{\mathrm{d}\,x^n}\left((1-x^2)^{n-½}\right)$$

8. لنضع $g_n(x) = (1-x^2)^{n-½}$ ولنلاحظ أنّ $g_n^{(k)}(-1) = g_n^{(k)}(1) = 0$ في حالة $0 \leq k < n$. عندئذ بإجراء مُكاملة بالتجزئة نجد في حالة $1 \leq k \leq n$:

$$\begin{aligned}\int_{-1}^{1} g_n^{(k)}(t) f^{(n-k)}(t)\,\mathrm{d}\,t &= \left[g_n^{(k-1)}(t) f^{(n-k)}(t)\right]_{-1}^{1} - \int_{-1}^{1} g_n^{(k-1)}(t) f^{(n-k+1)}(t)\,\mathrm{d}\,t \\ &= -\int_{-1}^{1} g_n^{(k-1)}(t) f^{(n-k+1)}(t)\,\mathrm{d}\,t\end{aligned}$$

وعليه نستنتج أنّ المقادير $\left((-1)^k \int_{-1}^{1} g_n^{(k-1)}(t) f^{(n-k+1)}(t)\,\mathrm{d}\,t\right)_{0\leq k\leq n}$ متساوية، ومن ثَمّ

$$(-1)^n \int_{-1}^{1} g_n^{(n)}(t) f(t)\,\mathrm{d}\,t = \int_{-1}^{1} g_n(t) f^{(n)}(t)\,\mathrm{d}\,t$$

وهذا يُكافئ

$$\int_{-1}^{1} T_n(t)\frac{f(t)}{\sqrt{1-t^2}}\,\mathrm{d}\,t = \frac{2^n\cdot n!}{(2n)!}\int_{-1}^{1}(1-t^2)^n\,\frac{f^{(n)}(t)}{\sqrt{1-t^2}}\,\mathrm{d}\,t$$

وبإجراء تغيير المتحوّل $t = \cos\theta$ تُكتب النتيجة السابقة بالشكل

$$\int_{0}^{\pi} f(\cos\theta)\cos n\theta\,\mathrm{d}\,\theta = \frac{2^n\cdot n!}{(2n)!}\int_{0}^{\pi} f^{(n)}(\cos\theta)\sin^{2n}\theta\,\mathrm{d}\,\theta$$

ونجد بتغيير بسيط للمتحوّل أنّ

$$\int_{-1}^{1} T_n(t) T_m(t)\frac{\mathrm{d}\,t}{\sqrt{1-t^2}} = \begin{cases} 0 & : \quad n \neq m \\ \frac{\pi}{2} & : \quad n = m \end{cases}$$

■

التمرين 19. ليكن $A(X) = X^3 + pX + q$ كثير حدود من الدرجة الثالثة في $\mathbb{R}[X]$.

أوجد الشرط اللازم والكافي على p و q حتى يقبل A جذراً حقيقيّاً واحداً فقط.

الحل

لندرس تغيّرات التابع

$$x \mapsto f(x) = x^3 + px + q$$

نلاحظ مباشرة أنّ $f'(x) = 3x^2 + p$ وهنا نناقش الحالات التالية :

- في حالة $p \geq 0$ يكون التابع المشتق موجباً وينعدم في نقطة واحدة على الأكثر، إذن يكون التابع f في هذه الحالة متزايداً تماماً وهو يغيِّر إشارته لأنّ $\lim_{+\infty} f = +\infty$ و $\lim_{-\infty} f = -\infty$، فهو يقبل في هذه الحالة جذراً حقيقيّاً وحيداً فقط.
- في حالة $p < 0$ يكون للتابع f جدول التغيرات التالي :

x	$-\infty$		$-\sqrt{-\frac{p}{3}}$		$\sqrt{-\frac{p}{3}}$		$+\infty$
$f'(x)$		$+$		$-$		$+$	
$f(x)$	$-\infty$	$\nearrow$	$q - \frac{2p}{3}\sqrt{-\frac{p}{3}}$	$\searrow$	$q + \frac{2p}{3}\sqrt{-\frac{p}{3}}$	$\nearrow$	$+\infty$

وعلى هذا ينعدم f مرّة واحدة فقط إذا وفقط إذا كان

$$\left(q - \frac{2p}{3}\sqrt{-\frac{p}{3}} < 0\right) \vee \left(q + \frac{2p}{3}\sqrt{-\frac{p}{3}} > 0\right)$$

وهذا يُكافئ

$$\left(q > -\frac{2p}{3}\sqrt{-\frac{p}{3}}\right) \vee \left(-q > -\frac{2p}{3}\sqrt{-\frac{p}{3}}\right)$$

أو $27q^2 + 4p^3 > 0$.

إذن يقبل كثير الحدود $X^3 + pX + q$ جذراً حقيقيّاً واحداً فقط إذا وفقط إذا كان

$$\left(p \geq 0\right) \text{ أو } 27q^2 + 4p^3 > 0$$

وهذا بدوره يُكافئ

$$27q^2+4p^3>0 \text{ أو } \left(p=q=0\right)$$

ملاحظة. يمكن في هذه الحالة إيجاد هذا الجذر z بالبحث عنه بالشكل $z=u+v$ فنجد بالتعويض في المعادلة $u^3+v^3+(3uv+p)(u+v)+q=0$. وهنا يكفي أن نختار u^3 و v^3 جذرين للمعادلة من الدرجة الثانية: $X^2+qX-\dfrac{p^3}{27}=0$. فنجد

$$z=\frac{1}{\sqrt{3}}\left(\sqrt[3]{\frac{\sqrt{27q^2+4p^3}-3q\sqrt{3}}{2}}-\sqrt[3]{\frac{\sqrt{27q^2+4p^3}+3q\sqrt{3}}{2}}\right)$$

وبذا يتم الإثبات. ■

التمرين 20. عيّن كثير حدود A من $\mathbb{R}[X]$ درجته أصغر ما يمكن، ويقبل القسمة على X^2+1، ويكون $A-1$ مُضاعفاً لكثير الحدود X^3+1.

الحل

ليكن A كثير حدود يقبل القسمة على X^2+1، ويُحقِّق $(A-1)\mid(X^3+1)$. عندئذ يوجد كثير حدود P يُحقِّق $A=(1+X^2)P$، ويوجد كثير حدود Q يُحقّق

$$(1+X^2)P-(1+X^3)Q=1$$

لتعيين P و Q نستعمل خوارزميّة إقليدس المعمّمة، خاصّة لأنّ $1+X^2$ و $1+X^3$ أوّليّان فيما بينهما.

k	R_k	Q_k	S_k	T_k
0	X^3+1		1	0
1	X^2+1	X	0	1
2	$-X+1$	$-X-1$	1	$-X$
3	2		$X+1$	$-X^2-X+1$

ومن ثَمّ يكون

$$(-X^2-X+1)(X^2+1)+(X+1)(X^3+1)=2$$

إذن يكفي أن نختار

$$Q_0 = -\frac{1}{2}X - \frac{1}{2} \text{ و } P_0 = -\frac{1}{2}X^2 - \frac{1}{2}X + \frac{1}{2}$$

ليكون

$$(X^2+1)P_0 - (X^3+1)Q_0 = 1$$

وإذا كان (P,Q) أيّ زوج يُحقّق $(1+X^2)P - (1+X^3)Q = 1$ كان

$$(1+X^2)(P_0 - P) = (1+X^3)(Q - Q_0)$$

واستنتجنا من ذلك، ومن كون $1+X^2$ و $1+X^3$ أوّليّين فيما بينهما، أنّه يوجد كثير حدود R يُحقّق

$$Q_0 - Q = (1+X^2)R \text{ و } P - P_0 = (1+X^3)R$$

ومنه

$$Q = Q_0 - (1+X^2)R \text{ و } P = P_0 + (1+X^3)R$$

وبالعكس، كلُّ زوج (P,Q) من هذا النمط يُحقّق $(1+X^2)P - (1+X^3)Q = 1$ وضوحاً.

وعلى هذا فإنّ مجموعة كثيرات الحدود A التي تحقّق

$$(X^3+1) \mid (A-1) \text{ و } (X^2+1) \mid A$$

هي

$$\left\{(1+X^2)P_0 + (1+X^2)(1+X^3)R : R \in \mathbb{R}[X]\right\}$$

وأصغر كثيرات الحدود هذه درجةً هو

$$\begin{aligned} A_0 &= (1+X^2)P_0 = \frac{1}{2}(1+X^2)(1-X-X^2) \\ &= \frac{1}{2}(1-X-X^3-X^4) \end{aligned}$$

وهو كثير الحدود المطلوب. ∎

التمرين 21. نعرّف، في حالة كثير حدود $P = \sum_{k=0}^{n} a_k X^k$ من $\mathbb{Z}[X]$، المقدار

$$C(P) = \gcd(a_0, a_1, \ldots, a_n)$$

ونقول إنّ P من $\mathbb{Z}[X]$ بدائي إذا وفقط إذا كان $C(P) = 1$.

1. أثبت أنّ جداء ضرب كثيري حدود بدائيّين هو كثير حدود بدائي.
2. أثبت أنّ $\forall (P,Q) \in \mathbb{Z}[X] \times \mathbb{Z}[X],\ \ C(PQ) = C(P)C(Q)$.
3. ليكن P من $\mathbb{Z}[X]$ كثير حدود بدائي. أثبت أنّ P غير خزول في $\mathbb{Q}[X]$ إذا وفقط إذا كان غير خزول في $\mathbb{Z}[X]$، أي إذا لم يكن مساوياً لجداء كثيري حدود من $\mathbb{Z}[X]$ درجة كل منهما أكبر من 1.

الحل

1. لنفترض أنّ $P = \sum_{k=0}^{n} a_k X^k$ و $Q = \sum_{k=0}^{m} b_k X^k$ كثيرا حدود من $\mathbb{Z}[X]$ يُحقّقان

$$C(P) = C(Q) = 1$$

لنعرّف $R = PQ = \sum_{k=0}^{n+m} c_k X^k$، ولنفترض أنّ $C(PQ) \neq 1$. عندئذ يوجد عددٌ أوّلي p يقسم $C(PQ)$. لمّا كان $p \mid a_0 b_0$ أمكننا أن نفترض دون الإخلال بعموميّة الإثبات أنّ $p \mid a_0$، عندئذ نعرّف

$$\kappa = \max\{j \le n : p \mid a_j\}$$

إنّ $\kappa < n$ وإلاّ قَسَمَ p العددَ $C(P)$ وهذا يناقض كون $C(P) = 1$.

لنتأمّل إذن $c_{\kappa+1}$:

$$c_{\kappa+1} = a_0 b_{\kappa+1} + a_1 b_\kappa + \cdots + a_\kappa b_1 + a_{\kappa+1} b_0$$

إنّ p يقسم الأعداد $c_{\kappa+1}$ و $a_0, a_1, \ldots, a_\kappa$ فهو يقسم $a_{\kappa+1} b_0$ ولكنّ p أوّلي مع $a_{\kappa+1}$ استناداً إلى تعريف κ، إذن لا بدَّ أن يقسم p العدد b_0. لنعرّف إذن

$$\tau = \max\{j \le m : p \mid b_j\}$$

إنّ $\tau < m$ وإلاّ قَسَمَ p العددَ $C(Q)$ وهذا يناقض كون $C(Q) = 1$.

لنضع إذن $\sigma = \tau + \kappa + 2$، ولنتأمّل المقدار c_σ، نعلم أنّ

$$c_\sigma = \sum_{i+j=\sigma} a_i b_j = \underbrace{\sum_{i=0}^{\kappa} a_i b_{\sigma-j}}_{i\leq\kappa\Rightarrow p|a_i} + a_{\kappa+1}b_{\tau+1} + \underbrace{\sum_{j=0}^{\tau} a_{\sigma-i} b_j}_{j\leq\tau\Rightarrow p|b_j}$$

ولمّا كان $p \mid c_\sigma$، استنتجنا أنّ $p \mid a_{\kappa+1}b_{\tau+1}$. فإمّا أن يكون $p \mid a_{\kappa+1}$ وهذا يناقض تعريف κ، أو أن يكون $p \mid b_{\tau+1}$ وهذا يناقض تعريف τ. يبيِّن هذا التناقض أنّ افتراضنا $C(PQ) \neq 1$ خطأ، ولا بُدّ أن يكون $C(PQ) = 1$.

2. ليكن P كثير حدود من $\mathbb{Z}[X]$. عندئذ بقسمة أمثال P على قاسمها المشترك الأعظم وهو $C(P)$ نحصل على كثير حدود بدائي P^*، فيكون لدينا $P = C(P)P^*$، و P^* بدائي. فإذا كان P و Q كثيري حدود من $\mathbb{Z}[X]$، كان $PQ = C(P)C(Q)P^*Q^*$، واستناداً إلى ما أثبتناه في 1. يكون P^*Q^* بدائيّاً، إذن $C(PQ) = C(P)C(Q)$.

3. ليكن P كثير حدود من $\mathbb{Z}[X]$ ولنفترض أنّ $C(P) = 1$. من الواضح أنّ كون P غير خزول في $\mathbb{Q}[X]$ يقتضي أنّه غير خزول في $\mathbb{Z}[X]$، لنثبت العكس.

لنفترض أنّ $P = P_1P_2$ حيث $\deg P_1 \geq 1$ و $\deg P_2 \geq 1$ و P_1 و P_2 من $\mathbb{Q}[X]$. فإذا عرّفنا العدد α_k بأنّه المضاعف المشترك الأصغر لمقامات ثوابت كثير الحدود P_k، في حالة $k = 1$ و $k = 2$، انتمى كثيرا الحدود $T_1 = \alpha_1 P_1$ و $T_2 = \alpha_2 P_2$ إلى $\mathbb{Z}[X]$. وكان لدينا $T_1T_2 = \alpha_1\alpha_2 P$. ولأنّ P بدائي استنتجنا أنّ $C(T_1)C(T_2) = \alpha_1\alpha_2$. ولكن $T_1 = C(T_1)T_1^*$ و $T_2 = C(T_2)T_2^*$ وكثيرا الحدود T_1^* و T_2^* ينتميان إلى $\mathbb{Z}[X]$. نستنتج إذن أنّ $P = T_1^*T_2^*$، أي إنّ P خزولٌ في $\mathbb{Z}[X]$.

وهي النتيجة المطلوبة. ■

التمرين 22. أثبت أنّ $P = X^3 + 3X - 1$ غير خزول في $\mathbb{Q}[X]$.

الحل

لنفترض أنّ P خزول في $\mathbb{Q}[X]$، إذن يقبل P جذراً r في $\mathbb{Q}$ لأنّه من الدرجة الثالثة. وعليه يوجد عددان صحيحان p و q أوّليّان فيما بينهما ويُحقّقان $r = \frac{p}{q}$. ومن ثَمّ يكون

$$p^3 + 3pq^2 = q^3$$

نستنتج من هذه المساواة أنّ $p \mid q^3$، ولأنّ $\gcd(p,q) = 1$ استنتجنا أنّ $p \in \{-1,1\}$. ثُمّ نستنتج من المساواة $q^3 - 3pq^2 = p^3$ أنّ $q \mid p^3$، ولأنّ $\gcd(p,q) = 1$ استنتجنا أنّ $q \in \{-1,1\}$. إذن لا بُدّ أن يكون $r \in \{-1,1\}$. ولكن نجد بالحساب المباشر أنّ $P(1) = 3$ و $P(-1) = -5$، إذن لا يقبل كثير الحدود P جذراً في $\mathbb{Q}$، وهو من ثَمّ غير خزول في $\mathbb{Q}[X]$. ■

التمرين 23. فرّق كثير الحدود $P = X^5 + X + 1$ في $\mathbb{Q}[X]$.

الحل

في الحقيقة لدينا

$$P = (X^2 + X + 1)(X^3 - X^2 + 1)$$

وهو التفريق المطلوب! ■

التمرين 24. قسّم وفق القُوى المتزايدة كثير الحدود A على كثير الحدود B حتى المرتبة n في الحالات الآتية:

	A	B	n
①	$2 - 3X^3 + X^4$	$1 + X + X^5$	6
②	$1 - \frac{X^3}{6} + \frac{X^5}{120}$	$1 - \frac{X^2}{2} + \frac{X^4}{24}$	5
③	$1 - abX^2$	$1 - (a+b)X + abX^2$	$\cdots$

الحل

① في الحقيقة، نجد أنّ

$$2 - 3X^3 + X^4 = (1 + X + X^5)Q(X) + X^7 R(X)$$

حيث

$$\begin{aligned} Q(X) &= 1 - X + X^2 - 4X^3 + 5X^4 - 6X^5 + 7X^6 \\ R(X) &= -8 + 4X - 5X^2 + 6X^3 - 7X^4 \end{aligned}$$

② ونجد أنّ

$$1 - \frac{1}{6}X^3 + \frac{1}{120}X^5 = \left(1 - \frac{1}{2}X^2 + \frac{1}{24}X^4\right)Q(X) + X^6 R(X)$$

حيث

$$\begin{aligned} Q(X) &= X + \frac{1}{3}X^3 + \frac{2}{15}X^5 \\ R(X) &= \frac{19}{360}X - \frac{1}{180}X^3 \end{aligned}$$

③ وأخيراً نجد أنّ

$$1 - abX^2 = \left(1 - (a+b)X + abX^2\right)Q_n(X) + X^{n+1}R_n(X)$$

حيث

$$\begin{aligned} Q_n(X) &= -1 + \sum_{k=1}^{n}(a^k + b^k)X^k \\ R_n(X) &= a^{n+1} + b^{n+1} - ab(a^n + b^n)X \end{aligned}$$

وهو المطلوب. ∎

التمرين 25. عيّن كثير حدود P من $\mathbb{R}[X]$ ، درجته أصغر ما يمكن، وباقي قسمته الإقليدية على $X^4 - 2X^3 - 2X^2 + 10X - 7$ يساوي $X^3 + X + 1$ ، وباقي قسمته على $X^4 - 2X^3 - 3X^2 + 13X - 10$ يساوي $2X^2 - 3$.

الحل

لنفترض أنّ M_1 و M_2 و R_1 و R_2 كثيرات حدود من $\mathbb{R}[X]$. نفترض أنّ M_1 و M_2 أوّليّان فيما بينهما، ونرغب في إيجاد كثيرات الحدود P التي تُحقِّق في آن معاً الشرطين $P = R_1 \bmod M_1$ و $P = R_2 \bmod M_2$.

لنلاحظ أوّلاً أنّه إذا كان P_0 حلّاً خاصّاً لهذه المسألة كان $P = P_0 + M_1M_2R$ (حيث R من $\mathbb{R}[X]$) أيضاً حلاً للمسألة نفسها. وبالعكس، إذا كان P أيّ حلٍّ لهذه المسألة قسم كثيرا الحدود M_1 و M_2 الفرقَ $P - P_0$، ولأنّهما أوّليان فيما بينهما كان الجداء M_1M_2 قاسماً للفرق $P - P_0$، أي وُجِدَ R من $\mathbb{R}[X]$ يُحقِّق $P = P_0 + M_1M_2R$. وعليه إذا كان P_0 حلاً خاصّاً لهذه المسألة كانت مجموعة جميع حلولها هي المجموعة

$$\mathcal{S} = \left\{P_0 + M_1M_2R : R \in \mathbb{R}[X]\right\}$$

وللحصول على أصغر هذه الحلول درجةً يكفي أن نختار باقي قسمة أي منها على M_1M_2.

لإيجاد الحل الخاص، نبدأ بتطبيق خوارزميّة إقليدس المعمّمة لتعيين كثيري حدود U_1 و U_2 من $\mathbb{R}[X]$ يُحقّقان

$$U_1M_2 + U_2M_2 = 1$$

وعندئذ يكفي أن نعرّف $P_0 = R_2U_1M_1 + R_1U_2M_2$ فيكون لدينا

$$\begin{aligned}
P_0 &= R_2U_1M_1 + R_1(1 - U_1M_1)\\
&= R_1 + U_1M_1(R_2 - R_1) = R_1 \bmod M_1\\
P_0 &= R_2(1 - U_2M_2) + R_1U_2M_2\\
&= R_2 + U_2M_2(R_1 - R_2) = R_2 \bmod M_2
\end{aligned}$$

وللحصول على أصغر عناصر $\mathcal{S}$ درجةً، نختار P_1 باقي قسمة P_0 على M_1M_2.

في مسألتنا، لدينا

$$\begin{aligned}
M_1 &= X^4 - 2X^3 - 2X^2 + 10X - 7, & R_1 &= X^3 + X + 1\\
M_2 &= X^4 - 2X^3 - 3X^2 + 13X - 10, & R_2 &= 2X^2 - 3
\end{aligned}$$

نبدأ بتطبيق خوارزميّة إقليدس المعمّمة، فنثبت في آن معاً أنّ M_1 و M_2 أوّليان فيما بينهما ونعيِّن كثيري الحدود U_1 و U_2.

k	R_k	Q_k	S_k	T_k
0	M_1		1	0
1	M_2	1	0	1
2	X^2-3X+3	X^2+X-3	1	-1
3	$X-1$	$X-2$	$-X^2-X+3$	X^2+X-2
	1		$\underbrace{X^3-X^2-5X+7}_{U_1}$	$\underbrace{-X^3+X^2+4X-5}_{U_2}$

وبذلك نكون قد أثبتنا أنّ M_1 و M_2 أوّليان فيما بينهما، وعيّنّا كثيري الحدود U_1 و U_2. ثُمّ نحسب كثير الحدود $P_0=R_2U_1M_1+R_1U_2M_2$ فنجد أنّ

$$\begin{aligned}P_0 &= -X^{10}+5X^9-2X^8-40X^7+96X^6+6X^5\\ &\quad -314X^4+401X^3+25X^2-370X+197\end{aligned}$$

وأخيراً نعيِّن P_1 باقي قسمة P_0 على M_1M_2 فنجد

$$P_1=-2X^7+7X^6+8X^5-64X^4+61X^3+115X^2-249X+127$$

وهو كثير الحدود المنشود. ■

التمرين 26. بيِّن أن 1 جذرٌ لكل من كثيرات الحدود التالية وعيِّن رتبة مضاعفته في كلٍّ من الحالات التالية :

$$\begin{aligned}U_n &= X^{2n}-nX^{n+1}+nX^{n-1}-1,\\ V_n &= X^{2n+1}-(2n+1)X^{n+1}+(2n+1)X^n-1,\\ W_n &= X^{2n}-n^2X^{n+1}+2(n^2-1)X^n-n^2X^{n-1}+1.\end{aligned}$$

الحل

① نلاحظ أوّلاً أنّ $U_1=0$ وأنّ

$$U_3=(X-1)^3(X+1)^3 \quad \text{و} \quad U_2=(X-1)^3(X+1)$$

إذن، العدد 1 جذرٌ من المرتبة 3 لكلٍّ من U_2 و U_3. لنفترض أنّ $n\geq 4$ ولنحسب المشتقّات المتتالية لكثير الحدود U_n حتّى المرتبة الثالثة، فنجد أنّ

$$\begin{aligned}
U_n &= X^{2n} - nX^{n+1} + nX^{n-1} - 1,\\
U_n' &= 2nX^{2n-1} - n(n+1)X^n + n(n-1)X^{n-2},\\
U_n'' &= 2n(2n-1)X^{2n-2} - n^2(n+1)X^{n-1} + n(n^2-3n+2)X^{n-3},\\
U_n''' &= 4n(2n^2-3n+1)X^{2n-2} - (n^4-n^2)X^{n-2} + n(n^3-6n^2+11n-6)X^{n-4}
\end{aligned}$$

وعليه نستنتج أنّ

$$U_n(1) = 0 \text{ و } U_n'(1) = 0 \text{ و } U_n''(1) = 0$$

و

$$U_n^{(3)}(1) = 2n(n^2-1) \neq 0$$

إذن العدد 1 جذرٌ مضاعف من المرتبة الثالثة لكثير الحدود U_n أيّاً كانت قيمة n أكبر أو تساوي 2.

② نلاحظ أوّلاً أنّ $V_0 = 0$ وأنّ

$$V_1 = (X-1)^3 \text{ و } V_2 = (X-1)^3(X^2+3X+1)$$

إذن، العدد 1 جذرٌ من المرتبة 3 لكلٍّ من V_1 و V_2. لنفترض أنّ $n \geq 3$ ولنحسب المشتقّات المتتالية لكثير الحدود V_n حتّى المرتبة الثالثة، فنجد أنّ

$$\begin{aligned}
V_n &= X^{2n+1} - (2n+1)X^{n+1} + (2n+1)X^n - 1,\\
V_n' &= (2n+1)\left(X^{2n} - (n+1)X^n + nX^{n-1}\right),\\
V_n'' &= (2n+1)n\left(2X^{2n-1} - (n+1)X^{n-1} + (n-1)X^{n-2}\right),\\
V_n''' &= (2n+1)n\left(2(2n-1)X^{2n-2} - (n^2-1)X^{n-2} + (n^2-3n+2)X^{n-3}\right)
\end{aligned}$$

وعليه نستنتج أنّ

$$V_n(1) = 0 \text{ و } V_n'(1) = 0 \text{ و } V_n''(1) = 0$$

و

$$V_n^{(3)}(1) = n(2n+1)(n+1) \neq 0$$

إذن العدد 1 جذرٌ مضاعف من المرتبة الثالثة لكثير الحدود V_n أيّاً كانت قيمة n من $\mathbb{N}^*$.

③ نلاحظ أوّلاً أنّ $W_1 = 0$. لنفترض أنّ $n \geq 2$، ولنعرّف متحوّلاً جديداً $T = X - 1$.
فيكون

$$\begin{aligned}
W_n &= X^{2n} - 2X^n + 1 - n^2X^{n-1}(X-1)^2 \\
&= (1+T)^{2n} - 2(1+T)^n + 1 - n^2T^2(1+T)^{n-1} \\
&= \sum_{k\geq 2}(C_{2n}^k - 2C_n^k)T^k - n^2T^2\sum_{k\geq 0}C_{n-1}^kT^k \\
&= T^2\sum_{k\geq 0}\left(C_{2n}^{k+2} - 2C_n^{k+2} - n^2C_{n-1}^k\right)T^k \\
&= T^2\sum_{k\geq 0}A_n^{(k)}T^k
\end{aligned}$$

وقد عرّفنا $A_n^{(k)} = C_{2n}^{k+2} - 2C_n^{k+2} - n^2C_{n-1}^k$. وعندئذ نلاحظ ما يلي :

$$\begin{aligned}
A_n^{(0)} &= C_{2n}^2 - 2C_n^2 - n^2 = 0 \\
A_n^{(1)} &= C_{2n}^3 - 2C_n^3 - n^2(n-1) = 0 \\
A_n^{(2)} &= C_{2n}^4 - 2C_n^4 - n^2C_{n-1}^2 = \frac{n^2(n^2-1)}{12}
\end{aligned}$$

وعليه بوضع $Q_n(X) = \sum_{k\geq 2}A_n^{(k)}(X-1)^k$ يكون لدينا

$$Q_n(1) = A_n^{(2)} \neq 0 \quad \text{و} \quad W_n = (X-1)^4Q_n\left(X\right)$$

إذن العدد 1 جذرٌ مضاعف من المرتبة الرابعة لكثير الحدود W_n أيّاً كانت قيمة n أكبر أو تساوي 2. ■

التمرين 27. ليكن كثير الحدود $P = \sum_{k=0}^{n}a_kX^k$ من الدرجة n في $\mathbb{Z}[X]$. ولنفترض أن $\gcd(a_0,\ldots,a_n) = 1$. أثبت أنه إذا كان $(p,q) \in \mathbb{Z}\times\mathbb{N}^*$ وكان العدد $r = \dfrac{p}{q}$ جذراً لكثير الحدود P فإنّ $(\gcd(p,q)=1) \Rightarrow (p \mid a_0)\wedge(q \mid a_n)$.

ثم أوجد الجذور العاديّة لكثيرات الحدود التالية :

$$P = 6X^4 - 11X^3 - X^2 - 4$$

$$Q = 2X^3 + 12X^2 + 13X + 15$$

$$R = 6X^5 + 11X^4 - X^3 + 5X - 6$$

الحل

في الحقيقة لدينا

$$0 = q^n P\left(r\right) = a_0 q^n + p\sum_{k=1}^{n} a_k p^{k-1} q^{n-k} = a_n p^n + q\sum_{k=0}^{n-1} a_k p^k q^{n-k-1}$$

ومنه $p \mid a_0 q^n$ و $q \mid a_n p^n$. ولكن $\gcd(p, q^n) = 1$ و $\gcd(q, p^n) = 1$ إذن $p \mid a_0$ و $q \mid a_n$.

- استناداً إلى ما سبق تنتمي الجذور العاديّة لكثير الحدود $P = 6X^4 - 11X^3 - X^2 - 4$ إلى المجموعة

$$\left\{-4, -2, -\frac{4}{3}, -1, -\frac{2}{3}, -\frac{1}{2}, -\frac{1}{3}, -\frac{1}{6}, \frac{1}{6}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, 1, \frac{4}{3}, 2, 4\right\}$$

وبالتعويض في كثير الحدود نجد الجذرين العاديين 2 و $-\frac{2}{3}$، ويكون

$$P = (X-2)(3X+2)(2X^2 - X + 1)$$

- وكذلك نرى أنّ الجذور العاديّة لكثير الحدود $Q = 2X^3 + 12X^2 + 13X + 15$ سالبة وتنتمي إلى المجموعة

$$\left\{-1, -3, -5, -15, -\frac{1}{2}, -\frac{3}{2}, -\frac{5}{2}, -\frac{15}{2}\right\}$$

وبالتعويض في كثير الحدود نجد الجذر العادي -5، ويكون

$$Q = (X+5)(2X^2 + 2X + 3)$$

- وكذلك نرى أنّ الجذور العاديّة لكثير الحدود $R = 6X^5 + 11X^4 - X^3 + 5X - 6$ تنتمي إلى المجموعة

$$\left\{1, 2, 3, 6, \frac{1}{2}, \frac{3}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{6}, -\frac{1}{6}, -\frac{2}{3}, -\frac{1}{3}, -\frac{3}{2}, -\frac{1}{2}, -6, -3, -2, -1\right\}$$

وبالتعويض في كثير الحدود نجد الجذرين العاديّين $\frac{2}{3}$ و $-\frac{3}{2}$، ويكون

$$R = (2X+3)(3X-3)(X^3 + X^2 + 1)$$

وبذا يتم الإثبات.

التمرين 28. تقبل المعادلة $x^3+px+q=0$ ، في حالة $q\neq 0$ ، ثلاثة جذور a و b و c في $\mathbb{C}^*$. ما عدد القيم التي يأخذها المقدار $\frac{a}{b}+\frac{b}{c}+\frac{c}{a}$ ؟ عيّن المعادلة الجبرية التي تقبل هذه القيم جذوراً.

الحل

لنضع $V(a,b,c)=\frac{a}{b}+\frac{b}{c}+\frac{c}{a}$ عندئذ نلاحظ أنّ

$$\begin{aligned}V(a,b,c)&=V(b,c,a)=V(c,a,b)=v_1\\ V(a,c,b)&=V(b,a,c)=V(c,b,a)=v_2\end{aligned}$$

إذن يأخذ المقدار $V(a,b,c)$ قيمتين v_1 و v_2 على الأكثر. ويكون لدينا

$$\begin{aligned}v_1+v_2&=\frac{a}{b}+\frac{b}{c}+\frac{c}{a}+\frac{a}{c}+\frac{c}{b}+\frac{b}{a}\\ &=\frac{b+c}{a}+\frac{a+c}{b}+\frac{a+b}{c}\\ &=\left(a+b+c\right)\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)-3=\frac{\Sigma_1\Sigma_2}{\Sigma_3}-3=-3\end{aligned}$$

و

$$\begin{aligned}v_1\cdot v_2&=\left(\frac{a}{b}+\frac{b}{c}+\frac{c}{a}\right)\left(\frac{a}{c}+\frac{c}{b}+\frac{b}{a}\right)\\ &=\frac{a^2}{bc}+\frac{c^2}{ab}+\frac{b^2}{ca}+\frac{cb}{a^2}+\frac{ab}{c^2}+\frac{ac}{b^2}+3\\ &=\frac{a^3+b^3+c^3}{abc}+\frac{a^3b^3+c^3b^3+a^3c^3}{(abc)^2}+3\end{aligned}$$

ولكن a و b و c جذورٌ للمعادلة $X^3+pX+q=0$ إذن

$$\begin{aligned}\frac{a^3+b^3+c^3}{abc}&=\frac{-p\cancel{(a+b+c)}-3q}{-q}=3\\ \frac{a^3b^3+c^3b^3+a^3c^3}{(abc)^2}&=\frac{(ap+q)(bp+q)+(cp+q)(bp+q)+(ap+q)(cp+q)}{q^3}\\ &=\frac{p^2(ab+bc+ca)+2pq\cancel{(a+b+c)}+3q^2}{q^2}\\ &=\frac{p^3}{q^2}+3\end{aligned}$$

ومنه

$$v_1v_2 = 9 + \frac{p^3}{q^2}$$

ومن ثَمّ يكون $V(a,b,c)$ و $V(a,c,b)$ جذري المعادلة

$$V^2 - 3V + 9 + \frac{p^3}{q^2} = 0$$

وهي النتيجة المرجوّة. $\blacksquare$

التمرين 29. تقبل المعادلة $x^3 + px + q = 0$، في حالة $q \neq 0$، ثلاثة جذور a و b و c في $\mathbb{C}^*$. احسب المقدار $\frac{a^2+b^2}{c^2} + \frac{b^2+c^2}{a^2} + \frac{c^2+a^2}{b^2}$ بدلالة p و q.

الحل

لمّا كانت a و b و c جذوراً للمعادلة $X^3 + pX + q = 0$ استنتجنا أنّ

$$\begin{aligned}
\frac{a^2+b^2}{c^2} &= \frac{a^2+b^2+c^2}{c^2} - 1 \\
&= \frac{\cancel{(a+b+c)}^2 - 2(ab+bc+ca)}{c^2} - 1 \\
&= -\frac{2p}{q^2}a^2b^2 - 1
\end{aligned}$$

ومن ثَمّ

$$\frac{a^2+b^2}{c^2} + \frac{b^2+c^2}{a^2} + \frac{c^2+a^2}{b^2} = -\frac{2p}{q^2}\left(a^2b^2 + b^2c^2 + c^2a^2\right) - 3$$

ولكن

$$a^2b^2 + b^2c^2 + c^2a^2 = (ab+bc+ca)^2 - 2abc\cancel{(a+b+c)} = p^2$$

إذن

$$\frac{a^2+b^2}{c^2} + \frac{b^2+c^2}{a^2} + \frac{c^2+a^2}{b^2} = -\frac{2p^3}{q^2} - 3$$

وهو المطلوب. $\blacksquare$

التمرين 30. لنتأمّل كثير الحدود $P(X) = X^3 + pX^2 + qX + r$ من $\mathbb{C}[X]$.
ولنفترض أنّ $P(X) = (X-a)(X-b)(X-c)$. أوجد بدلالة (p,q,r) كثير الحدود من الدرجة الثالثة الذي يقبل الأعداد $(1+a^2)$ و $(1+b^2)$ و $(1+c^2)$ جذوراً له.

الحل

في الحقيقة لدينا

$$P(X) = (X-a)(X-b)(X-c)$$

إذن

$$-P(X)P(-X) = (X^2-a^2)(X^2-b^2)(X^2-c^2) = Q(X^2)$$

و Q هو كثير الحدود الواحدي من الدرجة الثالثة الذي جذوره a^2 و b^2 و c^2. وعندئذ يكون $R(X) = Q(X-1)$ هو كثير الحدود الواحدي من الدرجة الثالثة الذي جذوره $1+a^2$ و $1+b^2$ و $1+c^2$.

في الحقيقة، نستنتج من العلاقة $Q(X^2) = -P(X)P(-X)$. أنّ

$$\begin{aligned} Q(X^2) &= (X^3 + pX^2 + qX + r)(X^3 - pX^2 + qX - r) \\ &= X^2(X^2+q)^2 - (pX^2+r)^2 \end{aligned}$$

ومن ثَمّ

$$Q(X) = X(X+q)^2 - (pX+r)^2$$

و

$$\begin{aligned} R(X) = Q(X-1) &= (X-1)(X+q-1)^2 - (pX+r-p)^2 \\ &= X^3 + (2q-3-p^2)X^2 + (q^2-4q+3+2p^2-2pr)X \\ &\quad - (q-1)^2 - (r-p)^2 \end{aligned}$$

إذن $1+a^2$ و $1+b^2$ و $1+c^2$ هي جذور كثير الحدود :

$$X^3 + (2q-3-p^2)X^2 + (q^2-4q+3+2p^2-2pr)X - (q-1)^2 - (r-p)^2$$

وهي النتيجة المرجوّة. ■

التمرين 31. عيّن العدد العقدي λ حتى تقبل المعادلة $Z^4 - 2Z^2 + \lambda Z + 3 = 0$ جذرين جداؤهما يساوي 1. ثُمّ حلّ المعادلة.

الحل

في الحقيقة، لنضع $P(Z) = Z^4 - 2Z^2 + \lambda Z + 3$ عندئذ يكون

$$P(Z) = (Z^2 - aZ + 3 - a^2)(Z^2 + aZ + 1) + (\lambda + 4a - a^3)Z + 6 - a^2$$

وعليه يقبل $P(Z)$ القسمة على $Z^2 + aZ + 1$ إذا وفقط إذا كان

$$a^2 = 6 \quad \text{و} \quad \lambda = (a^2 - 4)a$$

أي إذا وفقط إذا كان $\lambda \in \left\{2\sqrt{6}, -2\sqrt{6}\right\}$ وعندئذ يكون

$$\begin{aligned}
P(Z) &= \left(Z^2 - \frac{\lambda}{2}Z - 3\right)\left(Z^2 + \frac{\lambda}{2}Z + 1\right)\\
&= \left(\left(Z - \frac{\lambda}{4}\right)^2 - \frac{9}{2}\right)\left(\left(Z + \frac{\lambda}{4}\right)^2 - \frac{1}{2}\right)\\
&= \left(Z - \frac{\lambda}{4} - \frac{3\sqrt{2}}{2}\right)\left(Z - \frac{\lambda}{4} + \frac{3\sqrt{2}}{2}\right)\left(Z + \frac{\lambda}{4} - \frac{\sqrt{2}}{2}\right)\left(Z + \frac{\lambda}{4} + \frac{\sqrt{2}}{2}\right)
\end{aligned}$$

وهكذا، تقبل المعادلة $Z^4 - 2Z^2 + \lambda Z + 3 = 0$ جذرين جداؤهما يساوي 1 إذا وفقط إذا تحقّق الشرطان $\lambda = \varepsilon 2\sqrt{6}$ و $\varepsilon \in \{-1, +1\}$، وعندئذ تكون مجموعة جذور المعادلة هي

$$\left\{\frac{\varepsilon\sqrt{6} + 3\sqrt{2}}{2}, \frac{\varepsilon\sqrt{6} - 3\sqrt{2}}{2}, \frac{-\varepsilon\sqrt{6} + \sqrt{2}}{2}, \frac{-\varepsilon\sqrt{6} + \sqrt{2}}{2}\right\}$$

وهي النتيجة المطلوبة. ■

التمرين 32. ليكن لدينا $n+1$ عدداً حقيقياً مختلفاً $x_0, x_1, \ldots, x_n$. نُذكّر أنّ كثير الحدود

$$\ell_i(X) = \prod_{j=0, j\neq i}^{n} \frac{X - x_j}{x_i - x_j}$$

هو كثير الحدود الوحيد الذي درجته أصغر أو تساوي n ويأخذ القيمة 1 عند x_i، والقيمة 0 عند $x_0, x_1, \ldots x_{i-1}, x_{i+1}, \ldots, x_n$. أي، باستعمال رمز Kronecker، $\ell_i(x_j) = \delta_{i,j}$.

1. نبحث، في حالة i من $\{0,1,\ldots,n\}$، عن كثيري حدود U_i و V_i من $\mathbb{R}[X]$ لا تزيد درجة أي منهما على $2n+1$، ويحققان الشروط :

$$\forall k \in \{0,1,\ldots,n\}, \quad U_i(x_k) = \delta_{i,k}, \quad U_i'(x_k) = 0.$$
$$\forall k \in \{0,1,\ldots,n\}, \quad V_i(x_k) = 0, \quad V_i'(x_k) = \delta_{i,k}.$$

① أثبت أنه بالضرورة لدينا

$$V_i(X) = (\ell_i(X))^2 S_i(X) \text{ و } U_i(X) = (\ell_i(X))^2 R_i(X)$$

و R_i و S_i كثيرا حدود من الدرجة الأولى على الأكثر.

② أثبت أنّ المسألة تقبل حلاً، وحلاً وحيداً فقط، عيّن كثيري الحدود R_i و S_i بدلالة x_i و $\ell_i'(x_i)$.

2. ليكن $(\lambda_0,\lambda_1,\ldots,\lambda_n)$ و $(\mu_0,\mu_1,\ldots,\mu_n)$ عنصرين من $\mathbb{R}^{n+1}$، أثبت أنّ كثير الحدود المعرّف بالعلاقة : $H(X) = \sum_{k=0}^{n} \lambda_k U_k(X) + \sum_{k=0}^{n} \mu_k V_k(X)$، هو كثير الحدود الوحيد الذي لا تزيد درجته عن $2n+1$ ويُحقق

$$\forall k \in \{0,1,\ldots,n\}, \quad H(x_k) = \lambda_k, \; H'(x_k) = \mu_k$$

3. نفترض في هذا السؤال أنّ $n=1$ وأنّ $x_1 = 1, x_0 = 0$.

① عيّن كثيرات الحدود V_1, V_0, U_1, U_0.

② أثبت أنه مهما يكن كثير الحدود P الذي لا تزيد درجته على 3 من $\mathbb{R}[X]$ يكن

$$P = P(0)U_0 + P(1)U_1 + P'(0)V_0 + P'(1)V_1$$

③ ليكن $f(x) = \sqrt{1+8x}$. عيِّن كثير حدود P من $\mathbb{R}[X]$ لا تزيد درجته على 3، ويأخذ هو ومشتقُّه عند 0 وعند 1 القيم نفسها التي يأخذها التابع f. قارن عددياً بين $f\left(\frac{3}{8}\right)$ و $P\left(\frac{3}{8}\right)$.

4. نفترض في هذا السؤال أنّ $n=2$ وأنّ $x_2 = 1, x_1 = 0, x_0 = -1$.

① عيّن كثيرات الحدود $V_2, V_1, V_0, U_2, U_1, U_0$.

② أثبت أنه مهما يكن كثير الحدود P الذي لا تزيد درجته على 5 من $\mathbb{R}[X]$ يكن

$$P = P(-1)U_0 + P(0)U_1 + P(1)U_2 + P'(-1)V_0 + P'(0)V_1 + P'(1)V_2$$

③ ليكن P كثير حدود من $\mathbb{R}[X]$ لا تزيد درجته على 4 . أثبت تقارب المتسلسلة

$$\sum_{n\geq 2}\frac{P(n)}{n^2(n^2-1)^2}$$

واحسب مجموعها بدلالة $P(-1),P(0),P(1),P'(-1),P'(0),P'(1)$.

نذكّر أنّ $\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$.

الحل

①.1 لتكن i من $\{0,1,\ldots,n\}$. أيّاً كان k من $\{0,1,\ldots,n\}\backslash\{i\}$ ، كان

$$V_i'(x_k)=0,\quad V_i(x_k)=0 \quad \text{و} \quad U_i'(x_k)=0,\quad U_i(x_k)=0$$

فيكون x_k جذراً مضاعفاً لكلٍّ من U_i و V_i ، وعليه يقسم الجداء $\prod_{0\leq k\leq n,k\neq i}(X-x_k)^2$ كلاً من U_i و V_i . ومن ثَمّ يوجد كثيرا حدود R_i و S_i يُحقّقان المساواتين $U_i=(\ell_i)^2R_i$ و $V_i=(\ell_i)^2S_i$.

ولأنّ $\deg(\ell_i)^2=2n$ و $\deg U_i\leq 2n+1$ و $\deg V_i\leq 2n+1$ استنتجنا أنّ $\deg R_i\leq 1$ و $\deg S_i\leq 1$.

②.1 لتكن i من $\{0,1,\ldots,n\}$. ولنكتب $R_i=a_iX+b_i$ و $S_i=c_iX+d_i$.

- نستنتج من المساواة $U_i=(\ell_i)^2R_i$ والشرطين $U_i(x_i)=1$ و $U_i'(x_i)=0$ أنّ

$$2\ell_i'(x_i)+a_i=0 \quad \text{و} \quad a_ix_i+b_i=1$$

ومنه $a_i=-2\ell_i'(x_i)$ و $b_i=1+2x_i\ell_i'(x_i)$ أي

$$R_i=1-2(X-x_i)\ell_i'(x_i)$$

وهذا يثبت وحدانيّة كثير الحدود U_i . وبالعكس، نتيقّن بالتحقُّق المباشر أنّ كثير الحدود

$$U_i(X)=(\ell_i(X))^2\left(1-2\ell_i'(x_i)(X-x_i)\right)$$

يُحقِّق الشروط :

$$\forall k\in\{0,1,\ldots,n\},\ U_i(x_k)=\delta_{i,k},\ U_i'(x_k)=0 \ \text{و}\ \deg U_i\leq 2n+1$$

- ونستنتج من المساواة $V_i=(\ell_i)^2S_i$ والشرطين $V_i(x_i)=0$ و $V_i'(x_i)=1$ أنّ

$$c_i=1 \quad \text{و} \quad c_ix_i+d_i=0$$

أي $S_i = X - x_i$. وهذا يثبت وحدانيّة كثير الحدود V_i . وبالعكس، نتيقّن بالتحقُّق المباشر أنّ كثير الحدود $V_i(X) = (\ell_i(X))^2(X - x_i)$ يُحقِّق الشروط :

$$\forall k \in \{0,1,\ldots,n\},\ \ V_i(x_k) = 0,\ \ V_i'(x_k) = \delta_{i,k} \text{ و } \deg V_i \leq 2n+1$$

2. ليكن $(\lambda_0, \lambda_1, \ldots, \lambda_n)$ و $(\mu_0, \mu_1, \ldots, \mu_n)$ عنصرين من $\mathbb{R}^{n+1}$ ، ولنتأمّل كثير الحدود المعرّف بالعلاقة

$$H(X) = \sum_{j=0}^{n} \lambda_j U_j(X) + \sum_{j=0}^{n} \mu_j V_j(X)$$

فنلاحظ مباشرة أنّ $\deg H(X) \leq 2n+1$ ، وأنّ

$$\forall k \in \{0,1,\ldots,n\}, \quad H(x_k) = \lambda_k, \quad H'(x_k) = \mu_k.$$

وبالعكس، إذا كان P كثير حدود آخر يُحقّق

$$\forall k \in \{0,1,\ldots,n\}, \quad P(x_k) = \lambda_k, P'(x_k) = \mu_k \ \text{ و } \ \deg P \leq 2n+1$$

استنتجنا أنّ الفرق $Q = H - P$ يقبل جميع الأعداد $\{x_k : 0 \leq k \leq n\}$ جذوراً مضاعفة، ودرجته أصغر أو تساوي $2n+1$ فلا بُدّ أن يكون معدوماً، أي $H = P$.

3. نفترض في هذا السؤال أنّ $n = 1$ وأنّ $x_1 = 1, x_0 = 0$.

①.3 فيكون لدينا

$$\ell_0(X) = 1 - X \text{ و } \ell_1(X) = X \text{ ، و } \ell_0'(x_0) = -1 \text{ و } \ell_1'(x_1) = 1 .$$

وعليه نستنتج أنّ

$$\begin{aligned} U_0(X) &= (X-1)^2(1+2X) & \qquad V_0(X) &= X(X-1)^2 \\ U_1(X) &= X^2(3-2X) & \qquad V_1(X) &= X^2(X-1) \end{aligned}$$

②.3 ليكن P كثير حدود لا تزيد درجته على 3 من $\mathbb{R}[X]$ وليكن كثير الحدود Q المعرّف كما يلي :

$$Q = P - \left(P(0)U_0 + P(1)U_1 + P'(0)V_0 + P'(1)V_1\right)$$

عندئذ نرى مباشرة أنّ $\deg Q \leq 3$ وأنّ الأعداد 0 و 1 جذور مضاعفة لكثير الحدود Q فلا بُدّ أن يكون Q معدوماً، أي

$$P = P(0)U_0 + P(1)U_1 + P'(0)V_0 + P'(1)V_1$$

③.3 يُحقّق التابع f المعرّف بالعلاقة $f(x) = \sqrt{1+8x}$ ما يلي :

$$f(0) = 1, \quad f'(0) = 4, \quad f(1) = 3, \quad f'(1) = \frac{4}{3}$$

وعليه يكون كثير الحدود المطلوب هو

$$\begin{aligned} P &= (X-1)^2(1+2X) + 3X^2(3-2X) + 4X(X-1)^2 + \frac{4}{3}X^2(X-1) \\ &= 1 + 4X - \frac{10}{3}X^2 + \frac{4}{3}X^3 \end{aligned}$$

ونلاحظ بوجه خاص أنّ $f\left(\frac{3}{8}\right) = 2$ و $P\left(\frac{3}{8}\right) = 2 + \frac{13}{128}$. وأنّ

$$P\left(\frac{1}{8}\right) - \sqrt{2} = \frac{557}{384} - \sqrt{2} \approx 0.036$$

و

$$\frac{1}{2}P\left(\frac{7}{8}\right) - \sqrt{2} = \frac{1091}{768} - \sqrt{2} \approx 0.0064$$

4. نفترض في هذا السؤال أنّ $n = 2$ وأنّ $x_2 = 1, x_1 = 0, x_0 = -1$.

①.4 فيكون لدينا

$$\ell_2(X) = \frac{1}{2}(X+1)X \text{ و } \ell_1(X) = 1 - X^2 \text{ و } \ell_0(X) = \frac{1}{2}(X-1)X$$

و

$$\ell_2'(x_2) = \frac{3}{2} \text{ و } \ell_1'(x_1) = 0 \text{ و } \ell_0'(x_0) = -\frac{3}{2} .$$

وعليه نستنتج أنّ

$$\begin{aligned} U_0(X) &= \frac{1}{4}(X-1)^2X^2(3X+4) & V_0(X) &= \frac{1}{4}(X-1)^2X^2(X+1) \\ U_1(X) &= (X^2-1)^2 & V_1(X) &= (X^2-1)^2X \\ U_2(X) &= \frac{1}{4}(X+1)^2X^2(4-3X) & V_2(X) &= \frac{1}{4}(X+1)^2X^2(X-1) \end{aligned}$$

②.4 ليكن P كثير حدود لا تزيد درجته على 5 من $\mathbb{R}[X]$ ، ولنضع تسهيلاً للكتابة

$$P(1)=P_1, P'(1)=P_1', P(0)=P_0, P'(0)=P_0', P(-1)=P_{-1}, P'(-1)=P_{-1}'$$

وليكن كثير الحدود Q المعرّف كما يلي :

$$Q=P-\left(P_{-1}U_0+P_0U_1+P_1U_2+P_{-1}'V_0+P_0'V_1+P_1'V_2\right)$$

عندئذ نرى مباشرة أنّ $\deg Q\le 5$ وأنّ الأعداد -1 و 0 و 1 جذور مضاعفة لكثير الحدود Q فلا بُدّ أن يكون Q معدوماً، أي

$$P=P_{-1}U_0+P_0U_1+P_1U_2+P_{-1}'V_0+P_0'V_1+P_1'V_2$$

③.4 ليكن P كثير حدود من $\mathbb{R}[X]$ لا تزيد درجته على 4 . ولنضع

$$a_n=\frac{P(n)}{n^2(n^2-1)^2}$$

عندئذ يكون $a_n=O(n^{-2})$ والمتسلسلة $\sum_{n\ge 2}a_n$ متقاربة.

لمّا كان $\deg P\le 4$ استنتجنا أنّ ثابت X^5 في كثير الحدود

$$P_{-1}U_0+P_0U_1+P_1U_2+P_{-1}'V_0+P_0'V_1+P_1'V_2$$

يساوي 0 أي

$$\frac{3}{4}\left(P_{-1}-P_1\right)+\frac{1}{4}\left(P_{-1}'+P_1'\right)+P_0'=0$$

ونلاحظ أنّ

$$\frac{V_0(n)}{n^2(n^2-1)^2}=\frac{1}{4(n+1)},\qquad \frac{U_0(n)}{n^2(n^2-1)^2}=\frac{3n+4}{4(n+1)^2}$$
$$\frac{V_1(n)}{n^2(n^2-1)^2}=\frac{1}{n},\qquad \frac{U_1(n)}{n^2(n^2-1)^2}=\frac{1}{n^2}$$
$$\frac{V_2(n)}{n^2(n^2-1)^2}=\frac{1}{4(n-1)},\qquad \frac{U_2(n)}{n^2(n^2-1)^2}=\frac{4-3n}{4(n-1)^2}$$

وعليه يكون

$$a_n=\frac{(3n+4)P_{-1}}{4(n+1)^2}+\frac{P_0}{n^2}+\frac{(4-3n)P_1}{4(n-1)^2}+\frac{P_{-1}'}{4(n+1)}+\frac{P_0'}{n}+\frac{P_1'}{4(n-1)}$$

ولكن

$$P_0' = \frac{3}{4}\left(P_1 - P_{-1}\right) - \frac{1}{4}\left(P_{-1}' + P_1'\right)$$

إذن

$$\begin{aligned} a_n &= \frac{P_{-1}}{4(n+1)^2} + \frac{P_1}{4(n-1)^2} + \frac{P_0}{n^2} \\ &\quad + \left(\frac{1}{n+1} - \frac{1}{n}\right)\frac{3P_{-1} + P_{-1}'}{4} + \left(\frac{1}{n-1} - \frac{1}{n}\right)\frac{P_1' - 3P_1}{4} \end{aligned}$$

وعليه، إذا عرّفنا $S_n = \sum_{k=1}^{n} \frac{1}{k^2}$ كان لدينا

$$\begin{aligned} \sum_{k=2}^{n} a_k &= \frac{P_{-1}}{4}\left(S_n + \frac{1}{(n+1)^2} - \frac{5}{4}\right) + \frac{P_1}{4}\left(S_n - \frac{1}{n^2}\right) + P_0\left(S_n - 1\right) \\ &\quad + \frac{3P_{-1} + P_{-1}'}{4}\left(\frac{1}{n+1} - \frac{1}{2}\right) + \frac{P_1' - 3P_1}{4}\left(1 - \frac{1}{n}\right) \end{aligned}$$

فإذا جعلنا n تسعى إلى اللانهاية استنتجنا أنّ

$$\sum_{n=2}^{\infty} a_n = \frac{\pi^2}{24}\left(P_{-1} + P_1 + 4P_0\right) - \frac{11P_{-1} + 16P_0 + 12P_1 + 2P_{-1}' - 4P_1'}{16}$$

وهي النتيجة المطلوبة. ■

التمرين 33. ليكن λ عدداً حقيقياً من المجال $]0,1[$. نعرّف، في حالة n من $\mathbb{N}^*$، كثير الحدود P_n من $\mathbb{C}[X]$ بالعلاقة :

$$P_n(X) = e^{i\pi\lambda}(X+1)^{2n} - e^{-i\pi\lambda}(X-1)^{2n}$$

1. عيّن درجة $P_n(X)$ وثابت الحد الذي له أعلى درجة فيه.
2. نرمز بالرمز x_k إلى المقدار $i\cot\left(\frac{\pi}{2n}(k+\lambda)\right)$. بيّن أن $(x_k)_{0\le k\le 2n-1}$ هي جذور لكثير الحدود $P_n(X)$.
3. بحساب مجموع الجذور السابقة، استنتج أنّ

$$\cot(\pi\lambda) = \frac{1}{2n}\sum_{k=0}^{n-1}\cot\frac{\pi(k+\lambda)}{2n} - \frac{1}{2n}\sum_{k=0}^{n-1}\cot\frac{\pi(k+1-\lambda)}{2n}$$

4. أثبت باشتقاق العلاقة السابقة بالنسبة إلى λ أنّ

$$\frac{1}{\sin^2 \pi\lambda} = \frac{1}{4n^2}\sum_{k=0}^{n-1}\left(\sin^{-2}\frac{\pi(k+\lambda)}{2n} + \sin^{-2}\frac{\pi(k+1-\lambda)}{2n}\right)$$
$$\frac{1}{\sin^2 \pi\lambda} = \frac{1}{4n^2}\sum_{k=0}^{n-1}\left(\cot^2\frac{\pi(k+\lambda)}{2n} + \cot^2\frac{\pi(k+1-\lambda)}{2n}\right) + \frac{1}{2n}$$

5. استنتج مما سبق وجود النهاية : $\lim\limits_{N\to\infty}\sum\limits_{k=-N}^{N}\frac{1}{(k+\lambda)^2}$ ، واحسب قيمتها بدلالة λ،

واستنتج تقارب المتسلسلتين : $\sum\limits_{k=1}^{\infty}\frac{1}{(2k+1)^2}$ و $\sum\limits_{k=1}^{\infty}\frac{1}{k^2}$. ثُمّ احسب مجموعيهما.

6. أثبت أنّ المتسلسلة $\sum\limits_{k=1}^{\infty}\frac{k^2+\lambda^2}{\left(k^2-\lambda^2\right)^2}$ متقاربة وأنّ :

$$\sum_{k=1}^{\infty}\frac{k^2+\lambda^2}{\left(k^2-\lambda^2\right)^2} = \frac{\pi^2}{2\sin^2\pi\lambda} - \frac{1}{2\lambda^2}$$

الحل

ليكن λ عدداً حقيقياً من المجال $]0,1[$. ولنعرّف، في حالة n من $\mathbb{N}^*$، كثير الحدود P_n من $\mathbb{C}[X]$ بالعلاقة : $P_n(X) = e^{\mathrm{i}\pi\lambda}(X+1)^{2n} - e^{-\mathrm{i}\pi\lambda}(X-1)^{2n}$.

1. في الحقيقة، إنّ $\deg P_n \le 2n$، وثابت X^{2n} فيه يساوي $2\mathrm{i}\sin\pi\lambda$. إذن $\deg P_n = 2n$.

2. نرمز بالرمز x_k إلى المقدار $\mathrm{i}\cot\left(\frac{\pi}{2n}(k+\lambda)\right)$. عندئذ نجد بالتعويض في P_n أنّ

$$\begin{aligned}
P_n(x_k) &= e^{\mathrm{i}\pi\lambda}\left(\mathrm{i}\cot\frac{\pi(k+\lambda)}{2n}+1\right)^{2n} - e^{-\mathrm{i}\pi\lambda}\left(\mathrm{i}\cot\frac{\pi(k+\lambda)}{2n}-1\right)^{2n}\\
&= \frac{(-1)^n}{\sin^{2n}\frac{\pi(k+\lambda)}{2n}}\left(e^{\mathrm{i}\pi\lambda}\left(e^{-\frac{\pi\mathrm{i}(k+\lambda)}{2n}}\right)^{2n} - e^{-\mathrm{i}\pi\lambda}\left(e^{\frac{\pi\mathrm{i}(k+\lambda)}{2n}}\right)^{2n}\right)\\
&= \frac{(-1)^n}{\sin^{2n}\frac{\pi(k+\lambda)}{2n}}\left(e^{\mathrm{i}\pi\lambda}e^{-\mathrm{i}\pi(k+\lambda)} - e^{-\mathrm{i}\pi\lambda}e^{\mathrm{i}\pi(k+\lambda)}\right)\\
&= \frac{(-1)^n}{\sin^{2n}\frac{\pi(k+\lambda)}{2n}}\left((-1)^k - (-1)^k\right) = 0
\end{aligned}$$

وعلى هذا تكون الأعداد $\{x_k : 0 \le k < 2n\}$ جذوراً لكثير الحدود P_n . ولأنّ هذه الأعداد مختلفة مثنى مثنى نستنتج أنّها تمثّل جميع جذور P_n . ويكون من ثَمّ

$$P_n(X) = 2\,\mathrm{i}(\sin\pi\lambda)\prod_{k=0}^{2n-1}(X - x_k)$$

3. نستنتج إذن أنّ ثابت X^{2n-1} في P_n يساوي $-2\,\mathrm{i}(\sin\pi\lambda)\sum_{k=0}^{2n-1} x_k$ أو

$$2n\cot\pi\lambda = -\mathrm{i}\sum_{k=0}^{2n-1} x_k = \sum_{k=0}^{2n-1}\cot\frac{\pi(k+\lambda)}{2n}$$

وعليه

$$\begin{aligned}
2n\cot\pi\lambda &= \sum_{k=0}^{n-1}\cot\frac{\pi(k+\lambda)}{2n} + \sum_{k=n}^{2n-1}\cot\frac{\pi(k+\lambda)}{2n}\\
&= \sum_{k=0}^{n-1}\cot\frac{\pi(k+\lambda)}{2n} + \sum_{k=0}^{n-1}\cot\frac{\pi(2n-1-k+\lambda)}{2n}\\
&= \sum_{k=0}^{n-1}\cot\frac{\pi(k+\lambda)}{2n} + \sum_{k=0}^{n-1}\cot\left(\pi - \frac{\pi(k+1-\lambda)}{2n}\right)
\end{aligned}$$

ومنه

$$\cot\pi\lambda = \frac{1}{2n}\sum_{k=0}^{n-1}\cot\frac{\pi(k+\lambda)}{2n} - \frac{1}{2n}\sum_{k=0}^{n-1}\cot\frac{\pi(k+1-\lambda)}{2n}$$

4. نتأمّل طرفي المساواة السابقة بوصفها توابع للمتحوّل λ على المجال $]0,1[$ فنجد بالاشتقاق بالنسبة إلى λ أنّ

$$\frac{1}{\sin^2\pi\lambda} = \frac{1}{4n^2}\sum_{k=0}^{n-1}\left(\sin^{-2}\frac{\pi(k+\lambda)}{2n} + \sin^{-2}\frac{\pi(k+1-\lambda)}{2n}\right)$$

وبالاستفادة من العلاقة $\dfrac{1}{\sin^2\theta} = 1 + \cot^2\theta$ نستنتج أنّ

$$\frac{1}{\sin^2\pi\lambda} = \frac{1}{4n^2}\sum_{k=0}^{n-1}\left(\cot^2\frac{\pi(k+\lambda)}{2n} + \cot^2\frac{\pi(k+1-\lambda)}{2n}\right) + \frac{1}{2n}$$

5. وبالاستفادة من المتراجحة المألوفة

$$\forall x \in \left]0,\frac{\pi}{2}\right[,\quad \sin x \le x \le \tan x$$

نستنتج أنّ

$$\begin{aligned}\frac{1}{\sin^2\pi\lambda}-\frac{1}{2n}&=\frac{1}{4n^2}\sum_{k=0}^{n-1}\left(\cot^2\frac{\pi(k+\lambda)}{2n}+\cot^2\frac{\pi(k+1-\lambda)}{2n}\right)\\&\leq\frac{1}{4n^2}\sum_{k=0}^{n-1}\left(\frac{4n^2}{\pi^2(k+\lambda)^2}+\frac{4n^2}{\pi^2(\lambda-1-k)^2}\right)\\&\leq\frac{1}{4n^2}\sum_{k=0}^{n-1}\left(\sin^{-2}\frac{\pi(k+\lambda)}{2n}+\sin^{-2}\frac{\pi(k+1-\lambda)}{2n}\right)\\&=\frac{1}{\sin^2\pi\lambda}\end{aligned}$$

أو

$$\frac{1}{\sin^2\pi\lambda}-\frac{1}{2n}\leq\frac{1}{\pi^2}\sum_{k=0}^{n-1}\left(\frac{1}{(k+\lambda)^2}+\frac{1}{(\lambda-1-k)^2}\right)\leq\frac{1}{\sin^2\pi\lambda}$$

وهذا يُكافئ

$$\frac{1}{\sin^2\pi\lambda}-\frac{1}{2n}\leq\frac{1}{\pi^2}\sum_{k=-n}^{n-1}\frac{1}{(\lambda+k)^2}\leq\frac{1}{\sin^2\pi\lambda}$$

ونستنتج من ذلك أنّ

$$\lim_{N\to\infty}\sum_{k=-N}^{N}\frac{1}{(k+\lambda)^2}=\frac{\pi^2}{\sin^2\pi\lambda}$$

- فعلى سبيل المثال، باختيار $\lambda=\frac{1}{2}$ نستنتج أنّ $\lim_{N\to\infty}\sum_{k=-N}^{N}\frac{4}{(2k+1)^2}=\pi^2$ ومنه

$$\lim_{N\to\infty}\left(\sum_{k=0}^{N}\frac{1}{(2k+1)^2}+\sum_{k=1}^{N}\frac{1}{(2k-1)^2}\right)=\frac{\pi^2}{4}$$

أو

$$\lim_{N\to\infty}\sum_{k=0}^{N}\frac{1}{(2k+1)^2}=\frac{\pi^2}{8}$$

وهذا يثبت تقارب المتسلسلة $\sum_{n=0}^{\infty}\frac{1}{(2n+1)^2}$ ويثبتُ أنّ مجموعها يساوي $\frac{\pi^2}{8}$.

- ومن جهة أخرى، بملاحظة أنّ $\frac{1}{(2n+1)^2} \leq \frac{1}{4n^2}$ في حالة $n \geq 1$، نستنتج أيضاً تقارب المتسلسلة $\sum_{n=1}^{\infty} \frac{1}{n^2}$ فإذا رمزنا بالرمز S إلى مجموعها كان لدينا

$$S = \sum_{n=0}^{\infty} \frac{1}{(2n+1)^2} + \sum_{n=1}^{\infty} \frac{1}{(2n)^2} = \frac{\pi^2}{8} + \frac{1}{4} S$$

ومن ثَمّ $S = \frac{\pi^2}{6}$.

6. لنلاحظ أنّ

$$\begin{aligned}
\sum_{k=-N}^{N} \frac{1}{(k+\lambda)^2} &= \frac{1}{\lambda^2} + \sum_{k=1}^{N} \frac{1}{(k+\lambda)^2} + \sum_{k=1}^{N} \frac{1}{(-k+\lambda)^2} \\
&= \frac{1}{\lambda^2} + \sum_{k=1}^{N} \left(\frac{1}{(k+\lambda)^2} + \frac{1}{(k-\lambda)^2} \right) \\
&= \frac{1}{\lambda^2} + 2\sum_{k=1}^{N} \frac{k^2+\lambda^2}{(k^2-\lambda^2)^2}
\end{aligned}$$

إذن اعتماداً على نتيجة السؤال السابق نستنتج تقارب المتسلسلة $\sum_{k=1}^{\infty} \frac{k^2+\lambda^2}{(k^2-\lambda^2)^2}$ وأنّ

$$\sum_{k=1}^{\infty} \frac{k^2+\lambda^2}{(k^2-\lambda^2)^2} = \frac{\pi^2}{2\sin^2 \pi\lambda} - \frac{1}{2\lambda^2}$$

وهي النتيجة المرجوّة. ■

التمرين 34. ليكن (a,b) من $\mathbb{R}^2$، ولنتأمّل $P(X) = X^4 + aX + b$.

1. أوجد، بدراسة التابع $x \mapsto P(x)$، الشرط اللازم والكافي على (a,b) حتّى لا يكون لكثير الحدود $P(X)$ جذور حقيقيّة.
2. أثبت أنّه يوجد كثيرا حدود حقيقيّان

$$R(X) = X^2 + \lambda X + \mu \quad \text{و} \quad Q(X) = X^2 + \alpha X + \beta$$

يُحقّقان $P(X) = Q(X) \cdot R(X)$.

3. أوجد علاقات بسيطة بين $\alpha, \beta, \lambda, \mu$ والعددين a و b. واستنتج أنّ $Z = \lambda^2$ هو حلٌّ لمعادلة من الدرجة الثالثة يُطلب تعيينها.

4. حلّ في $\mathbb{C}$ المعادلة $X^4 + 2X + \frac{1}{2} = 0$.

الحل

1. لنتأمّل التابع $f : x \mapsto P(x)$. يقبل التابع f جدول التغيرات التالي

x	$-\infty$		$-\sqrt[3]{2a}\,/2$		$+\infty$
$f'(x)$		$-$	0	$+$	
$f(x)$	$+\infty$	$\searrow$	$b - 3a\sqrt[3]{2a}\,/8$	$\nearrow$	$-\infty$

إذن الشرط اللازم والكافي حتّى لا يكون لكثير الحدود $P(X)$ جذور حقيقيّة هو $b - \frac{3}{8}a\sqrt[3]{2a} > 0$ وهذا يُكافئ $256b^3 > 27a^4$.

2. نعلم أنّ كثيرات الحدود غير الخزولة في $\mathbb{R}[X]$ هي تلك التي تكون من الدرجة الأولى، أو من الدرجة الثانية وليس لها جذور حقيقيّة. ولمّا كان P كثير حدود واحدياً من الدرجة الرابعة، استنتجنا أنّه يُكتب بالضرورة جداء كثيرات حدود واحديّة غير خزولة من الدرجة الأولى والدرجة الثانية. فإذا كان أحدها من الدرجة الثانية أسميناه Q وأسمينا R خارج قسمة P عليه، وإذا كانت جميعها من الدرجة الأولى أسمينا Q جداء ضرب اثنين منها، وأسمينا R خارج قسمة P عليه. وهكذا نستنتج أنّه يوجد كثيرا حدود :

$$R(X) = X^2 + \lambda X + \mu \quad \text{و} \quad Q(X) = X^2 + \alpha X + \beta$$

يُحقّقان $P = Q \cdot R$.

3. وعندئذ يكون

$$QR = X^4 + (\alpha + \lambda)X^3 + (\beta + \mu + \alpha\lambda)X^2 + (\lambda\beta + \mu\alpha)X + \beta\mu$$

وتتحقّق المساواة $P = Q \cdot R$ إذا وفقط إذا كان

$$\alpha + \lambda = 0, \quad \beta + \mu + \alpha\lambda = 0, \quad \lambda\beta + \mu\alpha = a, \quad \beta\mu = b$$

وهذه الشروط تُكافئ

$$\alpha = -\lambda, \quad \beta + \mu = \lambda^2, \quad \lambda(\beta - \mu) = a, \quad \beta\mu = b$$

نستنتج من الشرطين الثاني والثالث أنّ

$$\lambda\beta + \lambda\mu = \lambda^3, \quad \lambda\beta - \lambda\mu = a,$$

ومن ثَمّ

$$2\lambda\beta = \lambda^3 + a, \quad 2\lambda\mu = \lambda^3 - a,$$

وإذا استفدنا من الشرط $\beta\mu = b$ استنتجنا أنّ $4\lambda^2 b = \lambda^6 - a^2$. وأخيراً إذا عرّفنا $Z = \lambda^2$ كان لدينا

$$Z^3 - 4bZ - a^2 = 0$$

4.لنتأمّل الحالة الخاصّة الموافقة لكثير الحدود $P(X) = X^4 + 2X + \frac{1}{2}$ ، أي $a = 2$ و $b = \frac{1}{2}$. في هذه الحالة تكون $Z = \lambda^2$ حلاً للمعادلة $Z^3 - 2Z - 4 = 0$. وعليه يمكننا أنّ نختار مثلاً $\lambda = \sqrt{2}$. فيكون عندئذ

$$\alpha = -\sqrt{2}, \quad \beta + \mu = 2, \quad \sqrt{2}(\beta - \mu) = 2, \quad \beta\mu = \frac{1}{2}$$

ومن ثَمّ

$$\alpha = -\sqrt{2}, \quad \beta = 1 + \frac{1}{\sqrt{2}}, \quad \mu = 1 - \frac{1}{\sqrt{2}}$$

ومنه

$$\begin{aligned} P(X) &= X^4 + 2X + \frac{1}{2} \\ &= \left(X^2 + \sqrt{2}X + 1 - \frac{1}{\sqrt{2}}\right)\left(X^2 - \sqrt{2}X + 1 + \frac{1}{\sqrt{2}}\right) \end{aligned}$$

فجذور P في $\mathbb{C}$ هي

$$\left\{\frac{1 + \mathrm{i}\sqrt{\sqrt{2}+1}}{\sqrt{2}}, \frac{1 - \mathrm{i}\sqrt{\sqrt{2}+1}}{\sqrt{2}}, \frac{1 - \sqrt{\sqrt{2}-1}}{\sqrt{2}}, \frac{1 + \sqrt{\sqrt{2}-1}}{\sqrt{2}}\right\}$$

وهو المطلوب. ■

الحقول

سنستعرض فيما يلي تقنيتين مهمّتين تفيدان في بناء الحقول هما حقل الكسور الموافق لحلقة تامة، وحقل خارج قسمة حلقة تبديليّة بمثالي أعظمي.

1. حقل الكسور الموافق لحلقة تامّة

لتكن A حلقة تامّة ولنضع $A^* = A\backslash\{0\}$. ثُمّ لنعرِّف على المجموعة $A \times A^*$ العلاقة الثنائية $\mathcal{R}$ كما يلي :

$$(a,b)\,\mathcal{R}\,(a',b') \Leftrightarrow ab' = ba'$$

وقانوني التشكيل الداخليين $(+)$ و $(\cdot)$ الآتيين

$$(a,b) + (a',b') = (ab' + a'b, bb')$$
$$(a,b) \cdot (a',b') = (aa', bb')$$

إنّ القانونين $(+)$ و $(\cdot)$ تجميعيّان وتبديليان ويقبلان على التوالي العنصرين الحياديين $(0,1)$ و $(1,1)$ ، ثُم إنّهما متجانسان مع علاقة التكافؤ $\mathcal{R}$ أي مهما يكن X و Y و Z و T من $A \times A^*$ يكن

$$\big(X\,\mathcal{R}\,Y\big) \wedge \big(Z\,\mathcal{R}\,T\big) \Rightarrow \begin{cases} (X+Z)\,\mathcal{R}\,(Y+T), \\ (X \cdot Z)\,\mathcal{R}\,(Y \cdot T). \end{cases}$$

تفيد هذه الخاصة في تزويد مجموعة صفوف التكافؤ $\mathcal{FR}(A) = A \times A^* / \mathcal{R}$ بقانوني الجمع والضرب المتوافقين مع ما سبق، فنحصل على حقل تبديلي نسمّيه **حقل كسور الحلقة التامة** A. وقد جرت العادة أن نرمز إلى صف التكافؤ $[(a,b)]$ بالرمز $\dfrac{a}{b}$، ونسمّيه كسراً بسطُه أو صورته a ومقامه أو مخرجه b. ويكون التطبيق $j : A \to \mathcal{FR}(A), a \mapsto \frac{a}{1}$ تشاكلاً حلقيّاً متبايناً، يفيدنا بالمطابقة بين عناصر A وعناصر $j(A)$ فنقول تجاوزاً إنّ A حلقة جزئية من $\mathcal{FR}(A)$.

فمثلاً إذا كانت A هي حلقة الأعداد الصحيحة $\mathbb{Z}$ كان حقل كسور الحلقة $\mathbb{Z}$ هو حقل الكسور العادية $\mathbb{Q}$. سندرس فيما يلي بالتفصيل مثالاً مهماً على الإنشاء السابق.

2. حقل الكسور العاديّة على حقل تبديليّ

ليكن $\mathbb{K}$ حقلاً تبديلياً. ولتكن $\mathbb{K}[X]$ حلقة كثيرات الحدود بمتحوّل واحد على $\mathbb{K}$. لقد وجدنا عند دراسة كثيرات الحدود أنّ الحلقة $\mathbb{K}[X]$ حلقة تامّة، ومن ثَمّ نحصلُ انطلاقاً منها على حقل تبديليّ، هو حقل كسورها، عند تطبيق الإنشاء السابق. ومنه التعريف التالي :

2-1. تعريف. نسمّي **حقل الكسور العاديّة** على حقل تبديليّ $\mathbb{K}$، حقل كسور الحلقة التامّة $\mathbb{K}[X]$، ونرمز إليه بالرمز $\mathbb{K}(X)$.

وإذا كان F عنصراً من $\mathbb{K}(X)$. قلنا إنّ $\dfrac{P}{Q}$ تمثيل غير خزول للكسر F إذا وفقط إذا حقّق العنصر (P,Q) من $\mathbb{K}[X]\times(\mathbb{K}[X]\backslash\{0\})$، الشرطين :

$$\gcd(P,Q)=1 \quad \text{و} \quad F=\frac{P}{Q}$$

ومن الواضح أنّ لكل كسر عاديّ من $\mathbb{K}(X)$ تمثيلاً غير خزول.

2-2. مبرهنة وتعريف. ليكن F من $\mathbb{K}(X)$. عندئذ لا يتعلّق المقدار $\deg P-\deg Q$ من $\mathbb{Z}\cup\{+\infty\}$ بالممثِّل $\dfrac{P}{Q}$ للكسر F. ونسمّيه **درجة الكسر** F ونرمز إليه بالرمز $\deg F$.

وكما في حالة كثيرات الحدود تتحقَّق الخاصّتان المبيّنتان في المبرهنة التالية، التي نترك إثباتها البسيط تمريناً للقارئ.

2-3. مبرهنة. ليكن الكسران $\dfrac{A}{B}$ و $\dfrac{C}{D}$ من $\mathbb{K}(X)$. عندئذ يكون :

$$\deg\left(\frac{A}{B}+\frac{C}{D}\right)\leq\max\left(\deg\frac{A}{B},\deg\frac{C}{D}\right)$$
$$\deg\left(\frac{A}{B}\cdot\frac{C}{D}\right)=\deg\frac{A}{B}+\deg\frac{C}{D}$$

2-4. **تعريف**. ليكن F من $\mathbb{K}(X)$. وليكن $\frac{P}{Q}$ تمثيلاً غير خزول للكسر F . نقول إنّ a من $\mathbb{K}$ ، **قطبٌ** للكسر F ، إذا وفقط إذا كان a جذراً لكثير الحدود Q . ونقول إنّ a **قطبٌ مضاعف** من المرتبة m إذا وفقط إذا كان a جذراً مضاعفاً من المرتبة m لكثير الحدود Q.

2-5. **مبرهنة وتعريف**. ليكن F من $\mathbb{K}(X)$. عندئذ لا يتعلّق الكسر $\frac{Q\cdot P'-P\cdot Q'}{Q^2}$ بالممثِّل $\frac{P}{Q}$ للكسر F . ونسمّيه **مشتق الكسر** F ونرمز إليه بالرمز F' . وتتحقّق الخواص الآتية :

$$(F+G)'=F'+G'$$
$$(\alpha F)'=\alpha F'$$
$$(F\cdot G)'=F'\cdot G+F\cdot G'$$

وذلك مهما يكن F و G من $\mathbb{K}(X)$ و α من $\mathbb{K}$.

2-6. **المبرهنة الأساسيّة في تفريق الكسور**. ليكن F من $\mathbb{K}(X)$. وليكن $\frac{P}{Q}$ تمثيلاً غير خزول للكسر F . نفترض أنّ $Q=\prod_{i=1}^{p}(Q_i)^{\alpha_i}$ ، و Q_1 و Q_2 و $\cdots$ و Q_p كثيرات حدود غير خزولة ومختلفة مثنى مثنى. عندئذ يوجد كثير حدود وحيد E وجماعة وحيدة من كثيرات الحدود $(A_{ij})_{(i,j)\in\Delta}$ مجموعة أدلّتها هي $\Delta=\bigcup_{k=1}^{p}\left(\{k\}\times\mathbb{N}_{\alpha_k}\right)$ يُحقّقان ما يلي :

1. $\forall(i,j)\in\Delta,\ \ \deg A_{ij}<\deg Q_i$
2. $F=E+\sum_{i=1}^{p}\left(\sum_{j=1}^{\alpha_i}\frac{A_{ij}}{(Q_i)^j}\right)$

الإثبات

يجري إثبات هذه المبرهنة بتجزئته إلى مراحل كلُّ مرحلة منها بسيطة في ذاتها، وتعطي في مجموعها الحالة العامّة.

① ليكن الكسر $F = \dfrac{P}{Q}$ عندئذ يوجد في $\mathbb{K}[X]$ كثير حدود وحيد E يحقّق

$$\deg(F-E) < 0$$

في الحقيقة، إذا كان E_1 و E_2 يحقّقان الخاصّة المطلوبة كان

$$\begin{aligned}\deg(E_1 - E_2) &= \deg\big((F-E_2)-(F-E_1)\big)\\ &\le \max\big(\deg(F-E_2), \deg(F-E_1)\big) < 0\end{aligned}$$

وهذا يثبت أنّ $E_1 = E_2$.

ومن ناحية أخرى، إذا أخذنا E خارج القسمة الإقليديّة لكثير الحدود P على Q، وكان R هو باقي هذه القسمة، كان $\deg(F-E) = \deg\left(\dfrac{R}{Q}\right) < 0$.

② ليكن $F = \dfrac{P}{Q_1 Q_2}$ كسراً فيه $\deg F < 0$ و $\gcd(Q_1, Q_2) = 1$. عندئذ توجد ثنائيّة وحيدة (U_1, U_2) من $(\mathbb{K}[X])^2$ تُحقِّق :

$$F = \frac{U_1}{Q_1} + \frac{U_2}{Q_2} \quad \text{و} \quad \deg U_1 < \deg Q_1 \quad \text{و} \quad \deg U_2 < \deg Q_2$$

في الحقيقة، لنفترض أوّلاً أنّ الثنائيتين (U_1, U_2) و (U_1^*, U_2^*) تُحقِّقان المطلوب، عندئذ ينتج من المساواة

$$\frac{U_1}{Q_1} + \frac{U_2}{Q_2} = \frac{U_1^*}{Q_1} + \frac{U_2^*}{Q_2}$$

أنّ $(U_2^* - U_2)Q_1 = (U_1 - U_1^*)Q_2$، أي إنّ Q_1 يقسِمُ $(U_1 - U_1^*)Q_2$ وهو أوّلي مع Q_2. فلا بدَّ أن يقسِمَ $U_1 - U_1^*$. وهذا يقتضي أنّ $U_1 - U_1^* = 0$ لأنّ $\deg(U_1 - U_1^*)$ أصغر تماماً من $\deg Q_1$. بذا نكون قد أثبتنا أنّ $U_1 = U_1^*$ ومن ثَمّ $U_2 = U_2^*$. وبذا يتمّ إثبات الجزء المتعلّق بالوحدانيّة.

ومن ناحية أخرى، نجد استناداً إلى مبرهنة Bézout ثنائيّة (T_1, T_2) من $(\mathbb{K}[X])^2$ تحقّق

$$T_2 Q_1 + T_1 Q_2 = 1$$

ومن ثَمّ يكون $P = P T_2 Q_1 + P T_1 Q_2$. ثُمّ نُجري قسمة إقليديّة لكثير الحدود $P T_2$ على Q_2 لنجد

$$P T_2 = S Q_2 + U_2 \quad \text{مع} \quad \deg U_2 < \deg Q_2$$

ونعرّف $U_1 = PT_1 + SQ_1$، فيكون لدينا من جهة أولى $P = U_2Q_1 + U_1Q_2$ أو

$$F = \frac{P}{Q_1Q_2} = \frac{U_1}{Q_1} + \frac{U_2}{Q_2}$$

ومن جهة ثانية،

$$\deg \frac{U_1}{Q_1} = \deg\left(F - \frac{U_2}{Q_2}\right) \leq \max\left(\deg F, \deg \frac{U_2}{Q_2}\right) < 0$$

أو $\deg U_1 < \deg Q_1$.

بالطبع يمكن تعميم الخاصّة السابقة بالتدريج على الوجه الآتي :

③ ليكن $F = \dfrac{P}{Q_1Q_2\cdots Q_r}$ كسراً فيه $\deg F < 0$، وكثيرات الحدود Q_1 و $\cdots$ و Q_r، أوّليّة فيما بينها مثنى مثنى. عندئذ يوجد عنصر وحيد $(U_1, \ldots, U_r)$ من $(\mathbb{K}[X])^r$ يُحقّق :

$$\forall i \in \mathbb{N}_r, \;\; \deg U_i < \deg Q_i \quad \text{و} \quad F = \frac{U_1}{Q_1} + \frac{U_2}{Q_2} + \cdots + \frac{U_r}{Q_r}$$

④ ليكن الكسر $F = \dfrac{P}{Q^\alpha}$ حيث $\deg F < 0$ و α من $\mathbb{N}^*$. عندئذ يوجد عنصر وحيد $(P_1, \ldots, P_\alpha)$ من $(\mathbb{K}[X])^\alpha$ يُحقّق:

$$\forall i \in \mathbb{N}_\alpha, \;\; \deg P_i < \deg Q \quad \text{و} \quad F = \frac{P_1}{Q} + \frac{P_2}{Q^2} + \cdots + \frac{P_\alpha}{Q^\alpha}$$

في الحقيقة، لا يوجد ما يجب إثباته في حالة $\alpha = 1$. لنفترض أنّ $\alpha > 1$، وأنّ النتيجة صحيحة عند القيمة $\alpha - 1$. عندئذ نُجري قسمة إقليديّة لكثير الحدود P على Q فنجد أنّ

$$P = TQ + P_\alpha \quad \text{مع} \quad \deg P_\alpha < \deg Q$$

فإذا عرّفنا $F_1 = \dfrac{P}{Q^\alpha} - \dfrac{P_\alpha}{Q^\alpha}$، كان $\deg F_1 \leq \max(\deg F, \deg \dfrac{P_\alpha}{Q^\alpha}) < 0$ ومن جهة ثانية $F_1 = \dfrac{T}{Q^{\alpha-1}}$، لذلك يوجد بمُقتضى فرْض التدريج عنصر $(P_1, \ldots, P_{\alpha-1})$ من $(\mathbb{K}[X])^{\alpha-1}$ يُحقّق

$$\forall i \in \mathbb{N}_{\alpha-1}, \;\; \deg P_i < \deg Q \quad \text{و} \quad F_1 = \frac{P_1}{Q} + \frac{P_2}{Q^2} + \cdots + \frac{P_{\alpha-1}}{Q^{\alpha-1}}$$

وهذا يُكمل إثبات الوجود في حالة α. أمّا إثبات الوحدانيّة فهو سهل ونتركه تمريناً للقارئ.

لنأتِ إلى إثبات المبرهنة الأساسيّة، ولنفترض أنّ $F=\dfrac{P}{Q_1^{\alpha_1}Q_2^{\alpha_2}\cdots Q_p^{\alpha_p}}$ و Q_1 و $\cdots$ و Q_p كثيرات حدود غير خزولة مختلفة مثنى مثنى. عندئذ نجد بالاستفادة من الخاصّتين ① و ③ كثيرات الحدود E و U_1 و $\cdots$ و U_p من $\mathbb{K}[X]$، تُحقّق

$$F=E+\sum_{i=1}^{p}\frac{U_i}{(Q_i)^{\alpha_i}} \qquad (*)$$

ويكون $\forall i\in\mathbb{N}_p,\ \deg\dfrac{U_i}{(Q_i)^{\alpha_i}}<0$، لأنّ كثيرات الحدود $Q_1^{\alpha_1}$ و $\cdots$ و $Q_p^{\alpha_p}$ أوليّة فيما بينها مثنى مثنى. ثُمّ نستعمل الخاصّة ④ لنجد، أياً كان i من $\mathbb{N}_p$، $(A_{i1},A_{i2},\ldots,A_{i\alpha_i})$ من $(\mathbb{K}[X])^{\alpha_i}$ تحقّق الشروط

$$\forall j\in\mathbb{N}_{\alpha_i},\ \deg A_{ij}<\deg Q_i \quad \text{و} \quad \frac{U_i}{Q_i^{\alpha_i}}=\sum_{j=1}^{\alpha_i}\frac{A_{ij}}{(Q_i)^j}$$

وهذا بعد التعويض في العلاقة $(*)$ يُكمل الإثبات. ❐

2-7. نتيجة وتعريف. ليكن F من $\mathbb{C}(X)$. وليكن $\dfrac{P}{Q}$ تمثيلاً غير خزول للكسر F. يمكننا أن نفترض أنّ $Q=\prod\limits_{i=1}^{p}(X-a_i)^{\alpha_i}$ حيث a_1 و a_2 و $\cdots$ و a_p هي أقطاب F، و α_1، α_2، $\cdots$، α_p هي رتب مضاعفة كلٍّ منها بالترتيب. عندئذ يوجد كثير حدود وحيد E، وجماعة وحيدة $(\lambda_{ij})_{(i,j)\in\Delta}$ من $\mathbb{C}$ مجموعة أدلّتها $\Delta=\bigcup\limits_{k=1}^{p}(\{k\}\times\mathbb{N}_{\alpha_k})$ يُحقّقان

$$F=E+\sum_{i=1}^{p}\left(\sum_{j=1}^{\alpha_i}\frac{\lambda_{ij}}{(X-a_i)^j}\right)$$

نسمّي E **الجزء الصحيح** في الكسر F، ونسمّي المقدار

$$\frac{\lambda_{i1}}{(X-a_i)}+\frac{\lambda_{i2}}{(X-a_i)^2}+\cdots+\frac{\lambda_{i\alpha_i}}{(X-a_i)^{\alpha_i}}$$

الجزء القطبيّ الموافق للقطب a_i في الكسر F، وأخيراً نسمّي العدد λ_{i1} **راسب** الكسر F عند القطب a_i.

2-8. نتيجة وتعريف. ليكن F من $\mathbb{R}(X)$. وليكن $\frac{P}{Q}$ تمثيلاً غير خزول للكسر F . يمكننا أن نفترض أنّ

$$Q = \prod_{i=1}^{p}(X - a_i)^{\alpha_i} \cdot \prod_{i=1}^{q}(X^2 + b_i X + c_i)^{\beta_i}$$

حيث a_1 و a_2 و $\cdots$ و a_p هي أقطاب F ، و α_1 و α_2 و $\cdots$ و α_p هي رتب مضاعفة كلٍّ منها بالترتيب. والثنائيات $((b_i, c_i))_{i\in\mathbb{N}_q}$ مختلفة مثنى مثنى، وتحقّق في حالة i من $\mathbb{N}_q$ المتراجحة $b_i^2 - 4c_i < 0$. عندئذ يوجد كثير حدود وحيد E وجماعة وحيدة $(\lambda_{ij})_{(i,j)\in\Delta}$ من الأعداد الحقيقيّة مجموعة أدلّتها هي $\Delta = \bigcup_{k=1}^{p}(\{k\}\times\mathbb{N}_{\alpha_k})$ ، وجماعتان وحيدتان $(\mu_{ij})_{(i,j)\in\Gamma}$ و $(\nu_{ij})_{(i,j)\in\Gamma}$ من الأعداد الحقيقيّة مجموعة أدلّتهما هي $\Gamma = \bigcup_{k=1}^{q}(\{k\}\times\mathbb{N}_{\beta_k})$ ، بحيث يكون :

$$F = E + \sum_{i=1}^{p}\left(\underbrace{\sum_{j=1}^{\alpha_i}\frac{\lambda_{ij}}{(X-a_i)^j}}_{\text{عناصر بسيطة من النوع الأول}}\right) + \sum_{i=1}^{q}\left(\underbrace{\sum_{j=1}^{\beta_i}\frac{\mu_{ij}X + \nu_{ij}}{(X^2 + b_i X + c_i)^j}}_{\text{عناصر بسيطة من النوع الثاني}}\right)$$

2-9. بعض الطرائق العمليّة في تفريق الكسور من $\mathbb{C}(X)$ أو $\mathbb{R}(X)$ إلى عناصر بسيطة

① للحصول على الجزء الصحيح نُجري قسمة إقليديّة للبسط على المقام.

② بعد تفريق المقام إلى جداء كثيرات حدود غير خزولة، نكتب التفريق المطلوب بدلالة ثوابت مجهولة، ثُمّ يجري تعيين الثوابت. فإذا كانت الأقطاب بسيطة، أو مضاعفة، ولكن رتب مضاعفتها صغيرة (1 أو 2)، يمكننا تعيين هذه الثوابت بتوحيد المقامات والمطابقة، إذ نحصل على جملة معادلات خطيّة. ولكن بوجه عام تعتبر هذه الطريقة آخر ما نلجأ إليه، وذلك لطول ما تتطلّبه من حسابات.

مثال 1. لنتأمّل الكسر العادي $F(X) = \frac{1}{X^2(X-1)^2}$.

نعلم من الدراسة العامّة أنّ F يقبل تفريقاً إلى عناصر بسيطة من الشكل

$$F(X) = \frac{a}{X} + \frac{b}{X-1} + \frac{c}{X^2} + \frac{d}{(X-1)^2} \qquad (*)$$

نلاحظ أنّ $F(1-X)=F(X)$ إذن

$$\begin{aligned}F(X)&=\frac{a}{X}+\frac{b}{X-1}+\frac{c}{X^2}+\frac{d}{(X-1)^2}\\&=\frac{-a}{X-1}+\frac{-b}{X}+\frac{c}{(X-1)^2}+\frac{d}{X^2}\end{aligned}$$

ولمّا كان التفريق وحيداً وجب أن يكون $d=c$ و $a=-b$.

من جهة أخرى بضرب طرفيّ المساواة $(*)$ بالمقدار X^2 ثُمّ تعويض $X=0$ نجد $c=1$. وأخيراً بحساب $F(-1)$ بطريقتين نجد $\frac{1}{4}=-a+\frac{a}{2}+1+\frac{1}{4}$ أو $a=2$. إذن يكون

$$\frac{1}{X^2(1-X)^2}=\frac{2}{X}-\frac{2}{X-1}+\frac{1}{X^2}+\frac{1}{(X-1)^2}$$

③ حالة قطب بسيط. إذا كان a قطباً بسيطاً للكسر $F=\frac{P}{Q}$، كان الجزء القطبيّ الموافق للقطب a في الكسر F هو $\frac{P(a)}{(X-a)Q'(a)}$.

في الحقيقة، نعلم أنّ $Q(X)=(X-a)R(X)$ حيث $R(a)=Q'(a)\neq 0$. لذلك يكون a جذراً لكثير الحدود $P-\frac{P(a)}{Q'(a)}R$ فهو يقبل القسمة على $X-a$ أي يوجد كثير حدود $T(X)$ يُحقّق

$$P(X)-\frac{P(a)}{Q'(a)}R(X)=(X-a)T(X)$$

وهذا يثبت أنّ

$$F(X)=\frac{P(X)}{Q(X)}=\frac{P(a)}{(X-a)Q'(a)}+\frac{T(X)}{R(X)}$$

ويُثبت المطلوب لأنّ a ليس قطباً للكسر $\frac{T(X)}{R(X)}$.

مثال 2. ليكن n من $\mathbb{N}^*$، وليكن P من $\mathbb{C}[X]$ كثير حدود يُحقّق $\deg P<n$. لنتأمّل الكسر العادي

$$F(X)=\frac{P(X)}{X^n-1}$$

إنّ أقطاب F بوجه عام هي الجذور من المرتبة n للواحد أي $\{\omega^k : 0 \leq k < n\}$ حيث $\omega = \exp\left(\frac{2\pi\,\mathrm{i}}{n}\right)$، وهي جميعها بسيطة.

إذن

$$F(X) = \sum_{k=0}^{n-1} \frac{\lambda_k}{X - \omega^k}$$

واستناداً إلى ما سبق، تُحسب λ_k بالصيغة

$$\lambda_k = \frac{P(\omega^k)}{n(\omega^k)^{n-1}} = \frac{1}{n}\omega^k \cdot P(\omega^k)$$

نستنتج إذن أنّ

$$\frac{P(X)}{X^n - 1} = \frac{1}{n}\sum_{k=0}^{n-1} \frac{\omega^k \cdot P(\omega^k)}{X - \omega^k}$$

وبوجه خاص

$$\frac{1}{X^n - 1} = \frac{1}{n}\sum_{k=0}^{n-1} \frac{\omega^k}{X - \omega^k}$$

مثال 3. ليكن n من $\mathbb{N}^*$، وليكن P من $\mathbb{C}[X]$ كثير حدود يُحقّق $\deg P < n$. لنتأمّل الكسر العادي

$$F(X) = \frac{P(X)}{X(X-1)(X-2)\cdots(X-n)}$$

إنّ أقطاب F بوجه عام هي الأعداد $\{0,1,\ldots,n\}$، وهي جميعها بسيطة. إذن

$$F(X) = \sum_{k=0}^{n} \frac{\lambda_k}{X - k}$$

أمّا λ_k فتساوي

$$\lambda_k = \frac{P(k)}{k(k-1)\cdots 1\cdot(-1)\cdots(k-n)} = \frac{(-1)^{n-k}P(k)}{k!\cdot(n-k)!}$$

ومنه

$$\frac{P(X)}{X(X-1)(X-2)\cdots(X-n)} = \frac{1}{n!}\sum_{k=0}^{n} \frac{(-1)^{n-k}C_n^k P(k)}{X - k}$$

④ حالة قطب مضاعف. لنفترض أنّ a قطبٌ مضاعفٌ من المرتبة m للكسر $F = \frac{P}{Q}$، أي $Q(X) = (X-a)^m \cdot Q_1(X)$ و $Q_1(a) \neq 0$.

نقوم في هذه الحالة بإجراء تغيير للمتحوّل $X = T + a$ فنجد

$$F(T+a) = \frac{A(T)}{T^m \cdot B(T)}$$

و $A(T) = P(T+a)$ و $B(T) = Q_1(T+a)$. ولمّا كان الشرط

$$B(0) = Q_1(a) \neq 0$$

محقَّقاً أمكننا أن نُجري قسمة وفق القوى المتزايدة لكثير الحدود $A(T)$ على $B(T)$ حتّى المرتبة $m-1$ فنجد

$$A(T) = B(T) \cdot (\lambda_m + \lambda_{m-1} T + \cdots + \lambda_1 T^{m-1}) + T^m R(T)$$

ومن ثَمّ يكون

$$F(T+a) = \frac{\lambda_m}{T^m} + \cdots + \frac{\lambda_1}{T} + \frac{R(T)}{B(T)}$$

أو بالعودة إلى المتحوّل X:

$$F(X) = \frac{\lambda_m}{(X-a)^m} + \cdots + \frac{\lambda_1}{X-a} + \frac{R(X-a)}{Q_1(X)}$$

وهذا يبيِّن أنّ الجزء القطبيّ للكسر F الموافق للقطب a هو $\sum_{k=1}^{m} \frac{\lambda_k}{(X-a)^k}$، لأنّ a ليس قطباً للكسر $\frac{R(X-a)}{Q_1(X)}$.

مثال 4. لنتأمّل الكسر العادي

$$F(X) = \frac{1}{(X-1)^3(X+1)^2}$$

فإذا وضعنا $X = T + 1$ وجدنا

$$F(T+1) = \frac{1}{T^3 \cdot (2+T)^2} = \frac{1}{T^3 \cdot (4 + 4T + T^2)}$$

وبإجراء قسمة وفق القوى المتزايدة للعدد 1 على $4 + 4T + T^2$ حتى المرتبة 2 نجد

$$1 = (4 + 4T + T^2) \cdot \left(\tfrac{1}{4} - \tfrac{1}{4}T + \tfrac{3}{16}T^2\right) - T^3 \left(\tfrac{1}{2} + \tfrac{3}{16}T\right)$$

ومنه

$$F(1+T)=\frac{1}{4T^3}-\frac{1}{4T^2}+\frac{3}{16T}-\frac{\frac{1}{2}+\frac{3}{16}T}{(T+2)^2}$$

وبالعودة إلى المتحوّل X نجد

$$F(X)=\frac{1}{4(X-1)^3}-\frac{1}{4(X-1)^2}+\frac{3}{16(X-1)}-\frac{5+3X}{16(X+1)^2}$$

وأخيراً بملاحظة أنّ $5+3X=2+3(X+1)$ نجد

$$F(X)=\frac{1}{4(X-1)^3}-\frac{1}{4(X-1)^2}+\frac{3}{16(X-1)}-\frac{1}{8(X+1)^2}-\frac{3}{16(X+1)}$$

⑤ حالة العناصر البسيطة من النوع الثاني في $\mathbb{R}(X)$. يمكننا في مثل هذه الحالة إجراء الحسابات في $\mathbb{C}(X)$ ثُمّ الانتقال إلى $\mathbb{R}(X)$ بجمع العناصر المترافقة. وكذلك يُمكن اتّباع طريقة الثوابت غير المعيّنة. سنعرض في المثال التالي تقنية أخرى قد تكون مفيدة في بعض الحالات.

مثال 5. لنتأمّل الكسر العادي

$$F(X)=\frac{1}{(X-1)^2(X^2+1)^3}$$

والمطلوب تفريقه إلى عناصر بسيطة في $\mathbb{R}(X)$. لنضع $T=X^2+1$ ولنضرب بسط ومقام الكسر السابق بكثير الحدود $(X+1)^2$ فيكون

$$F(X)=\frac{(X+1)^2}{T^3\cdot(2-T)^2}=\frac{2X+T}{T^3\cdot(4-4T+T^2)}$$

ثُمّ نقوم بإجراء قسمة وفق القوى المتزايدة في $\mathbb{R}(X)[T]$ لكثير الحدود $2X+T$ على $4-4T+T^2$ حتى المرتبة 2 فنجد

$$\begin{aligned}2X+T=(4-4T+T^2)\cdot\left(\frac{X}{2}+\frac{2X+1}{4}T+\frac{3X+2}{8}T^2\right)\\+T^3\left(\frac{4X+3}{4}-\frac{3X+2}{8}T\right)\end{aligned}$$

ومنه نستنتج أنّ

$$F(X)=\frac{X}{2T^3}+\frac{2X+1}{4T^2}+\frac{3X+2}{8T}+\frac{8X+6-(3X+2)T}{8(2-T)^2}$$

ولكن

$$\begin{aligned} 8X+6-(3X+2)T &= -3X^3-2X^2+5X+4 \\ &= (X+1)^2(-3X+4) \end{aligned}$$

و

$$(2-T)^2 = (X+1)^2(X-1)^2$$

إذن

$$F(X) = \frac{X}{2\left(X^2+1\right)^3} + \frac{2X+1}{4\left(X^2+1\right)^2} + \frac{3X+2}{8\left(X^2+1\right)} + \frac{-3X+4}{8(X-1)^2}$$

وأخيراً بملاحظة أنّ $-3X+4 = -3(X-1)+1$ نجد

$$F(X) = \frac{X}{2(X^2+1)^3} + \frac{2X+1}{4(X^2+1)^2} + \frac{3X+2}{8(X^2+1)} + \frac{1}{8(X-1)^2} - \frac{3}{8(X-1)}$$

3. حقل خارج قسمة حلقة تبديليّة على مثالي أعظمي

لتكن $(A,+,\cdot)$ حلقة تبديلية. وليكن $\mathcal{I}$ مثالياً في A. نعرّف العلاقة الثنائية $\mathcal{R}_{\mathcal{I}}$ على A على الوجه الذي بات مألوفاً لدينا أي

$$\forall (x,y) \in A^2, \quad x\,\mathcal{R}_{\mathcal{I}}\,y \Leftrightarrow x-y \in \mathcal{I}$$

يثبت القارئ بسهولة أنّ هذه العلاقة علاقة تكافؤ على A، ونرمز عادة إلى صفوف تكافُئها بالرمز $A/\mathcal{I}$. و إذا كان X و Y عنصرين من $A/\mathcal{I}$، كانت المجموعات التالية

$$X+Y = \{x+y : (x,y) \in X \times Y\}$$

و

$$-X = \{-x : x \in X\}$$

و

$$X \cdot Y = \{x \cdot y : (x,y) \in X \times Y\}$$

صفوف تكافؤ، أي عناصر من $A/\mathcal{I}$. تتيح لنا هذه الملاحظة تعريف قانونيَ تشكيل داخليين $(+)$ و $(\cdot)$ على $A/\mathcal{I}$، يجعلان منها حلقة تبديلية، حيادي الجمع فيها هو $[0] = \mathcal{I}$، ونظير X بالنسبة إلى الجمع هو $-X$، وحيادي الضرب فيها هو $[1]$. تُسمّى هذه الحلقةُ **حلقة خارج قسمة الحلقة A على المثالي $\mathcal{I}$**.

3-1. **تعريف**. نقول عن مثاليٍّ $\mathcal{M}$ في حلقة تبديلية $(A,+,\cdot)$، إنّه **مثالي أعظميّ** إذا كان $\mathcal{M} \neq A$ وكان A و $\mathcal{M}$ هما المثاليّان الوحيدان في A اللذان يحويان $\mathcal{M}$، أو بقول آخر إذا تحقَّق، أياً كان المثالي $\mathcal{I}$ في A، الشرط

$$\mathcal{M} \subset \mathcal{I} \Rightarrow (\mathcal{I} = \mathcal{M}) \vee (\mathcal{I} = A)$$

3-2. **مبرهنة**. ليكن $\mathcal{M}$ مثاليّاً في حلقة تبديلية $(A,+,\cdot)$، هنالك تكافؤ بين

❶ المثالي $\mathcal{M}$ مثالي أعظميّ في A.

❷ حلقةُ خارج القسمة $A/\mathcal{M}$ حقلٌ تبديلي.

الإثبات

لنفترض أولاً أنّ $\mathcal{M}$ مثالي أعظميّ في A. وليكن $X = [x]$ عنصراً من المجموعة $(A/\mathcal{M})\backslash\{0\}$. لمّا كان المثالي $\mathcal{M} + x \cdot A$ يحوي $\mathcal{M}$ ومختلفاً عن $\mathcal{M}$، (وإلّا كان $x \in \mathcal{M}$ و $(X = [0]$)، وجب أن يكون $\mathcal{M} + x \cdot A = A$. فيوجد في A عنصرٌ a ويوجد في $\mathcal{M}$ عنصرٌ m يُحقّقان $m + x\,a = 1$، أو $[x]\cdot[a] = [1]$ في $A/\mathcal{M}$. إذن العناصر غير المعدومة في $A/\mathcal{M}$ قَلوبة و $A/\mathcal{M}$ حقل.

وبالعكس، لنفترض أنّ $A/\mathcal{M}$ حقل، وليكن $\mathcal{I}$ مثالياً في A، يُحقّق

$$\mathcal{M} \subset \mathcal{I} \quad \text{و} \quad \mathcal{M} \neq \mathcal{I}$$

نأخذ حينئذٍ عنصراً x من $\mathcal{I}\backslash\mathcal{M}$، فيكون $[x] \neq [0]$، إذن في A عنصرٌ a يُحقّق $[x]\cdot[a] = [1]$ في $A/\mathcal{M}$. فمن جهة أولى، يكون $x\,a \in \mathcal{I}$، ومن جهة ثانية، يكون $(1 - x) \in \mathcal{M} \subset \mathcal{I}$. إذن $1 \in \mathcal{I}$، ومن ثَمّ $A = \mathcal{I}$. فالمثالي $\mathcal{M}$ مثالي أعظميّ في الحلقة A. ❐

3-3. **تعريف**. نقول إنّ مثالياً $\mathcal{P}$ في حلقة تبديلية $(A,+,\cdot)$، **مثالي أوليّ** إذا وفقط إذا كان $\mathcal{P} \neq A$، وتحقق الشرط

$$\forall (x,y) \in A^2, \quad x \cdot y \in \mathcal{P} \Rightarrow (x \in \mathcal{P}) \vee (y \in \mathcal{P})$$

3-4. **مبرهنة**. ليكن $\mathcal{P}$ مثاليّاً في حلقة تبديلية $(A,+,\cdot)$، هنالك تكافؤ بين

❶ المثالي $\mathcal{P}$ مثالي أوليّ في A.

❷ حلقةُ خارج القسمة $A/\mathcal{P}$ تامة.

الإثبات

الإثبات واضح من التعريف السابق، ونترك التفاصيل تمريناً للقارئ. ❐

3-5. **مبرهنة**. لتكن $(A,+,\cdot)$ حلقة تبديلية.

- إنّ كل مثالي أعظميّ في A مثاليٌّ أولي.
- إذا كانت A حلقة رئيسية، فكل مثالي أوليّ مختلف عن $\{0\}$ في A مثاليٌّ أعظمي.
- إذا كانت A حلقة رئيسية، و p عنصراً غير خزول في A فإن المثالي pA أوليّ.

الإثبات

▪ ليكن $\mathcal{M}$ مثالياً أعظميّاً في A. إذن الحلقةُ $A/\mathcal{M}$ حقلٌ، فهي حلقة تامةٌ؛ واستناداً إلى المبرهنة السابقة يكون المثالي $\mathcal{M}$ مثالياً أوليّاً في A.

▪ ليكن $\mathcal{P}$ مثاليّاً أولياً في الحلقة الرئيسية A مختلفاً عن $\{0\}$. يوجد حينئذ في A عنصرٌ p يُحقّق $\mathcal{P}=pA$ و $p\neq 0$. وليكن $\mathcal{M}=mA$ مثالياً في A يحوي $\mathcal{P}$. إذن $p\in mA$ ومن ثَمّ يوجد في A عنصرٌ a يُحقّق $p=ma\in\mathcal{P}$.

- فإذا كان $m\in\mathcal{P}$، أصبح لدينا $mA\supset\mathcal{P}\supset\mathcal{M}$، أو $\mathcal{M}=\mathcal{P}$.
- وإذا كان $a\in\mathcal{P}$ وجدنا b في A يُحقّق $a=pb$، ويكون لدينا من ثَمّ $p(1-mb)=0$، ولكن الحلقة A تامّة لأنها رئيسية، إذن $1=mb\in\mathcal{M}$، ومنه $A=\mathcal{M}$.

وهكذا نكون قد أثبتنا أنّ المثالي $\mathcal{P}$ أعظمي.

▪ ليكن p عنصراً غير خزول في A، وليكن $xy\in pA$. نعرّف $z=\gcd(p,x)$.

- إمّا أن يكون $z\in U(A)$ ومن ثَمّ يكون p و x أوليّين فيما بينهما و $p|xy$ إذن $p|y$ أو $y\in pA$.
- وإمّا أن يكون $z\sim p$ ومن ثَمّ $p\mid x$ أو $x\in pA$. فالمثالي pA أوليّ. ❐

3-6. **نتيجة مهمّة**. لتكن $(A,+,\cdot)$ حلقة رئيسية، و ليكن p عنصراً غير خزول في A، حينئذ تكون حلقة خارج القسمة A/pA حقلاً تبديلياً.

3-7. **مثال**. لتكن A الحلقة الرئيسيّة $\mathbb{R}[X]$ ولنتأمّل في $\mathbb{R}[X]$ كثير الحدود غير الخزول $P(X) = X^2 + 1$. نعلم، بناءً على ما سبق، أنّ الحلقةَ A/PA، التي نرمز إليها في هذه الحالة $\mathbb{R}[X]/(X^2+1)$، هي حقلٌ تبديلي. في الحقيقة إنّ التطبيق

$$\varphi : \mathbb{C} \to \mathbb{R}[X]/(X^2+1),\ a + \mathrm{i}\, b \mapsto [a + bX]$$

تقابلٌ، وتشاكلٌ حقليّ.

فإذا كان $z_1 = a_1 + \mathrm{i}\, b_1$ و $z_2 = a_2 + \mathrm{i}\, b_2$ من $\mathbb{C}$، كان، من جهة أولى :

$$\begin{aligned}\varphi(z_1 + z_2) &= [a_1 + a_2 + (b_1 + b_2)X] \\ &= [(a_1 + b_1 X) + (a_2 + b_2 X)] \\ &= [a_1 + b_1 X] + [a_2 + b_2 X] = \varphi(z_1) + \varphi(z_2)\end{aligned}$$

ومن جهة ثانية،

$$\begin{aligned}\varphi(z_1 \cdot z_2) &= [a_1 a_2 - b_1 b_2 + (a_1 b_2 + b_1 a_2)X] \\ &= [(a_1 + b_1 X)(a_2 + b_2 X) - b_1 b_2 (1 + X^2)] \\ &= [(a_1 + b_1 X)(a_2 + b_2 X)] \\ &= [(a_1 + b_1 X)] \cdot [(a_2 + b_2 X)] = \varphi(z_1) \cdot \varphi(z_2)\end{aligned}$$

ليكن $z = a + \mathrm{i}\, b$ عنصراً من $\ker \varphi$ أي $\varphi(z) = 0$. عندئذ يكون لدينا $[a + bX] = [0]$، وهذا يقتضي أنّ $X^2 + 1$ يقسم $a + bX$. ويكون $a + bX$ كثير الحدود الصفريّ أي $a = b = 0$ أو $z = 0$. فالتشاكل φ متباينٌ.

وأخيراً ليكن $\mathcal{T}$ عنصراً من $\mathbb{R}[X]/(X^2+1)$ عندئذ يوجد T في $\mathbb{R}[X]$ يُحقّق $\mathcal{T} = [T]$. ولمّا كانت درجة باقي القسمة الإقليدية لكثير الحدود T على $X^2 + 1$ أصغر أو تساوي 1، أمكننا تسمية هذا الباقي $a + bX$. وعندئذ يقسم كثير الحدود $X^2 + 1$ كثير الحدود $(T - a - bX)$، ومن ثَمّ $\mathcal{T} = [T] = [a + bX] = \varphi(a + \mathrm{i}\, b)$. فالتطبيق φ غامرٌ.

بذا نكون قد أثبتنا أنّ حقل الأعداد العقديّة $\mathbb{C}$ يُشاكل تقابلياً حقل خارج القسمة $\mathbb{R}[X]/(X^2+1)$.

4. توسيع الحقل

1-4. تعريف. ليكن $\mathbb{K}$ حقلاً يشاكل تقابلياً حقلاً جزئياً من حقل $\mathbb{L}$. نقول في هذه الحالة إنّ $\mathbb{L}$ **توسيع للحقل** $\mathbb{K}$.

فمثلاً $\mathbb{R}$ توسيع للحقل $\mathbb{Q}$ و $\mathbb{C}$ توسيع للحقل $\mathbb{R}$.

2-4. مبرهنة. إذا كان $\mathbb{K}$ حقلاً عدده المميِّز 0، كان $\mathbb{K}$ توسيعاً للحقل $\mathbb{Q}$، وإذا كان العدد المميّز للحقل $\mathbb{K}$ هو العدد الأوليّ p كان $\mathbb{K}$ توسيعاً للحقل $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

الإثبات

إذا كان العدد المميِّز للحقل $\mathbb{K}$ هو 0، فهذا يعني أنّ التشاكل الحلقي

$$\varphi : \mathbb{Z} \to \mathbb{K},\ n \mapsto n \cdot 1_{\mathbb{K}}$$

متباين، ومن ثَمّ فإنّ $\operatorname{Im}\varphi$ حلقة جزئية من $\mathbb{K}$ تشاكل تقابلياً $\mathbb{Z}$، إذن يحوي الحقل $\mathbb{K}$ حقل الكسور الموافق للحلقة $\operatorname{Im}\varphi$ وهو يشاكل تقابلياً $\mathbb{Q}$. فالحقل $\mathbb{K}$ توسيع للحقل $\mathbb{Q}$.

وإذا كان العدد المميِّز للحقل $\mathbb{K}$ هو العدد الأولي p، كانت $p\mathbb{Z}$ نواة التشاكل $\varphi : \mathbb{Z} \to \mathbb{K}, n \mapsto n \cdot 1_{\mathbb{K}}$ وكان

$$\tilde{\varphi} : \mathbb{F}_p \to \mathbb{K},\ [n] \mapsto n \cdot 1_{\mathbb{K}}$$

تشاكلاً حلقياً متبايناً، بذا يكون $\operatorname{Im}\varphi$ حقلاً جزئياً من $\mathbb{K}$ وهو يشاكل تقابلياً $\mathbb{F}_p$. ❐

3-4. تذكِرة. سنحتاج في التعريف اللاحق إلى بعض الخواص البسيطة للفضاءات الشعاعيّة التي يمكن للقارئ أن يقبلها، علماً أننا سنعود إليها بتفصيل كامل أثناء دراستنا للجبر الخطيّ.

ليكن E فضاءً شعاعياً على حقل $\mathbb{K}$. يكون E منتهي البعد إذا وجدت فيه جملة منتهية من الأشعة تفيد بالتعبير عن أي شعاع منه بعبارة خطية في عناصرها، وفي مثل هذه الحالة توجد في الفضاء E جملة $(v_1,\ldots,v_n)$ تكون أساساً للفضاء E أي يمكن كتابة كل عنصر x من E بطريقة وحيدة عبارة خطية $x = x_1v_1 + \cdots + x_nv_n$ حيث x_1 و $\ldots$ و x_n من $\mathbb{K}$. ونبرهن أنه إذا وُجِدَ في فضاء شعاعي E أساس عدد عناصره n فعدد عناصر كل أساس للفضاء E هو أيضاً n، نسمّي هذا العددَ بُعدَ الفضاء الشعاعي E، ونكتب $\dim E = n$ وفي هذه الحالة يوجد تشاكل تقابلي بين الفضاءين الشعاعيين E و $\mathbb{K}^n$.

4-4. **تعريف**. ليكن $\mathbb{L}$ توسيعاً للحقل $\mathbb{K}$. يمكننا في هذه الحالة اعتبار $\mathbb{L}$ فضاءً شعاعياً على الحقل $\mathbb{K}$. فإذا كان $\mathbb{L}$ فضاءً شعاعياً منتهي البعد وبعده n على $\mathbb{K}$، قلنا إنّ $\mathbb{L}$ **توسيع بسيط من الدرجة n للحقل $\mathbb{K}$**، وكتبنا $[\mathbb{L} : \mathbb{K}] = n$.

فمثلاً حقل الأعداد العقدية $\mathbb{C}$ توسيع بسيط من الدرجة الثانية للحقل $\mathbb{R}$، إذ نعلم أنّ $(1, \mathrm{i})$ أساس للفضاء الشعاعي $\mathbb{C}$ على $\mathbb{R}$. في حين أنّ الحقل $\mathbb{R}$ ليس توسيعاً بسيطاً لحقل الأعداد العاديّة $\mathbb{Q}$.

5-4. **ملاحظة**. سنعتمد في بقية هذا البحث بعض الرموز المتعارفة والتي سنذكرها فيما يلي تثبيتاً للأفكار :

- إذا كان $(\mathbb{K},+,\cdot)$ حقلاً فإننا نرمز بالرمز $\mathbb{K}^*$ إلى الزمرة الضربيّة $(\mathbb{K}\backslash\{0\},\cdot)$.

- أياً كان كثير الحدود P من $\mathbb{K}[X]$ فإننا نرمز إلى المثالي الرئيسي الذي يولده P بالرمز (P) أي $(P) = P\cdot\mathbb{K}[X] = \{P\cdot Q : Q \in \mathbb{K}[X]\}$.

- أياً كان كثير الحدود المعطى P في $\mathbb{K}[X]$، وأياً كان A من $\mathbb{K}[X]$، فإننا نسمّي العنصرَ من $\mathbb{K}[X]/(P)$ الذي يقبلُ A ممثلاً له، صفَّ تكافؤ A بالقياس P ونرمز إليه بالرمز $[A]$. ونصطلح أن نكتبَ c عوضاً عن $[c]$ أياً كان العنصر c من $\mathbb{K}$.

5. الحقول المنتهية

سنهتم في هذه الفقرة بالحقول المنتهية، أي الحقول التي عدد عناصرها منته. لا نشير عادة عند حديثنا عن حقول منتهية إلى مسألة كونها تبديلية، وذلك بسبب المبرهنة المهمة التالية التي نذكرها دون إثبات، لخروج الإثبات عن إطار هذا الكتاب.

1-5. **مبرهنة ودربرن – Wedderburn**. إنّ كلّ حقلٍ منته تبديليٌّ.

تُلقي المبرهنة التالية ضوءاً على بنية الزمر الجزئية المنتهية من الزمرة الضربيّة في حقل تبديليّ.

5-2. مبرهنة. ليكن $\mathbb{K}$ حقلاً تبديلياً، ولتكن G زمرة جزئية منتهية من $(\mathbb{K}^*,\cdot)$. حينئذ تكون الزمرة G زمرة دوّارة.

الإثبات

- لنلاحظ أولاً أنّه إذا كان x و y عنصرين من G وكانت n رتبة x و m رتبة y (أي $O(x) = n$ و $O(y) = m$) حيث $\gcd(n,m) = 1$ فإنّ رتبة xy تساوي $n\,m$.

في الحقيقة، إذا كان $p \geq 1$ و $(x\,y)^p = 1$ كان x^p عنصراً من الزمرة $\langle y\rangle$ المولّدة بالعنصر y والتي رتبتها m إذن $x^{pm} = (x^p)^m = 1$، ومن ثَمَّ يقسم n العددَ pm (لأنّ $O(x) = n$). ولكنّ n و m أوليّان فيما بينهما إذن يقسم n العددَ p. ونبرهن بأسلوب مماثل أنّ العددَ m يقسم p. ونستنتج مجدّداً، لأنّ n و m أوليّان فيما بينهما، أنّ p مضاعف للعدد $n\,m$. وبالعكس، من الواضح أنّ

$$(x\,y)^{nm} = (x^n)^m \cdot (y^m)^n = 1$$

وهذا يثبت أنّ $O(x\,y) = n\,m$.

- لنعرّف $r = \max\{O(x) : x \in G\}$. سنثبتُ أنّ العددَ r يقسم $\operatorname{card}(G)$ وأنّ رتبة كل عنصر من G تقسم r.

في الحقيقة، يوجد، بمقتضى تعريف r، عنصر x_0 من G يُحقّق $r = O(x_0)$ ولكن $\langle x_0\rangle$ زمرة جزئية من G فعدد عناصرها يقسم عدد عناصر G. إذن r يقسم $\operatorname{card}(G)$.

من ناحية أخرى، ليكن y من G، ولنضع $O(y) = q$. إذا كان q لا يقسم r، يمكننا أن نجد (بتفريق كل من r و q إلى عوامله الأولية) عدداً أوليّاً p يُحقّق، من جهة أولى، $r = p^\alpha r'$ و $\gcd(p,r') = 1$، ومن جهة ثانية، $q = p^\beta q'$ مع $\gcd(p,q') = 1$ و $0 \leq \alpha < \beta$. إنّ رتبة $a = x_0^{p^\alpha}$ هي r'، ورتبة $b = y^{q'}$ هي p^β واستناداً إلى الملاحظة التي بدأنا منها يكون $O(a\,b) = p^\beta r' > r$، وهذا يناقض تعريف r.

- نستنتج مما سبق أنّ $G \subset \{x \in \mathbb{K} : x^r - 1 = 0\}$، ولكن كثير الحدود $X^r - 1$ يقبل على الأكثر r جذراً في $\mathbb{K}$ لأنّ $\mathbb{K}$ حقل تبديليّ، ومن ثَمَّ $\operatorname{card}(G) \leq r$. ينجم عن ذلك أنّ $\operatorname{card}(G) = r$ وأنّ الزمرة G زمرة دوّارة، لأن العنصر x_0 يولّدها. ❐

5-3. **نتيجة**. إذا كان $\mathbb{K}$ حقلاً منتهياً كانت الزمرة $\mathbb{K}^*$ زمرة دوّارة.

تعطينا المبرهنة التالية معلومة مهمّة عن عدد عناصر حقل منته، فمثلاً لا توجد حقول منتهية عدد عناصرها 12 أو 15.

5-4. **مبرهنة**. إذا كان $\mathbb{K}$ حقلاً منتهياً فإنّ عدده المميّز عدد أوليّ p، ويوجد n في $\mathbb{N}^*$ يُحقّق $\operatorname{card}(\mathbb{K}) = p^n$.

الإثبات

لو كان العدد المميّز للحقل $\mathbb{K}$ صفراً لكان $\mathbb{K}$ توسيعاً للحقل $\mathbb{Q}$ وهذا يناقض كونه منتهياً. ليكن إذن p العددَ المميّز للحقل $\mathbb{K}$. إنّ p عدد أولي لأنّ $\mathbb{K}$ حقل كما نعلم. ولقد رأينا في المبرهنة 4-2. أنّ $\mathbb{K}$ توسيع للحقل $\mathbb{F}_p$، وهذا التوسيع بسيط لأن عدد عناصر $\mathbb{K}$ منته. ليكن إذن $n = \dim_{\mathbb{F}_p} \mathbb{K} = [\mathbb{K} : \mathbb{F}_p]$. فيكون الفضاء الشعاعي $\mathbb{K}$ على $\mathbb{F}_p$ مُشاكِلاً تقابلياً للفضاء الشعاعيّ $\mathbb{F}_p^n$ على الحقل نفسه، ومنه

$$\operatorname{card}(\mathbb{K}) = \operatorname{card}(\mathbb{F}_p^n) = p^n \qquad \square$$

5-5. **مثال**. سننشئ حقلاً منتهياً عدد عناصره 4 انطلاقاً من الحقل $\mathbb{F}_2$ وذلك بإجراء توسيع بسيط لهذا الأخير. نلاحظ أنّ

$$\forall x \in \mathbb{F}_2,\ \ x(x+1) = 0$$

ومن ثَمّ فإنّ كثير الحدود $P = X^2 + X + 1$ غير خزول في $\mathbb{F}_2[X]$ والمثالي

$$(P) = P \cdot \mathbb{F}_2[X] = \{P \cdot Q : Q \in \mathbb{F}_2[X]\}$$

مثاليّ أعظميّ في $\mathbb{F}_2[X]$ بمقتضى المبرهنة 3-5.، ومن ثَمّ تكون حلقة خارج القسمة $\mathbb{K} = \mathbb{F}_2[X]/(P)$ حقلاً وذلك استناداً إلى المبرهنة 3-2.

لنأتِ إلى وصف الحقل $\mathbb{K}$. نرمز بالرمز j إلى العنصر $[X]$ من $\mathbb{K}$ أي إلى صف تكافؤ العنصر X بالقياس لعلاقة التكافؤ المعرّفة بالمثاليّ (P)، أو ببساطة بالقياس P، ليكن A كثير حدودٍ ما من $\mathbb{F}_2[X]$، لا تزيد درجة باقي القسمة الإقليدية لكثير الحدود A على P على 1 لذلك نجد عنصراً وحيداً (Q, a, b) من $\mathbb{F}_2[X] \times \mathbb{F}_2 \times \mathbb{F}_2$، يُحقّق

$$A = Q \cdot P + a\,X + b$$

ومن ثَمّ يكتب صف تكافؤ A بالقياس P بطريقة وحيدة بالشكل

$$[A] = [a][X] + [b] = a\,j + b$$

حيث (a,b) من $\mathbb{F}_2 \times \mathbb{F}_2$. واتفقنا أن نكتب c عوضاً عن $[c]$ عندما يكون c من $\mathbb{F}_2$. نستنتج إذن أنّ

$$\mathbb{K} = \{0,1,j,1+j\}$$

فعدد عناصر الحقل $\mathbb{K}$ هو 4، ونتحقق بسهولة أنّ قوانين الجمع والضرب في $\mathbb{K}$ معطاة بالجدولين الآتيين:

$+$	0	1	j	$j+1$
0	0	1	j	$j+1$
1	1	0	$j+1$	j
j	j	$j+1$	0	1
$j+1$	$j+1$	j	1	0

$\times$	0	1	j	$j+1$
0	0	0	0	0
1	0	1	j	$j+1$
j	0	j	$j+1$	1
$j+1$	0	$j+1$	1	j

فمثلاً

$$\begin{aligned}(j+1)(j+1) &= [1+X][1+X] = [1+2X+X^2]\\ &= [X+P] = [X] = j\end{aligned}$$

ونترك للقارئ مهمة إنشاء حقل عدد عناصره 8 وذلك باستعمال كثير الحدود غير الخزول $P = X^3 + X^2 + 1$ من $\mathbb{F}_2[X]$.

نجد في المبرهنة التالية تعميماً للمثال السابق.

6-5. مبرهنة. ليكن p عدداً أولياً، وليكن كثير الحدود غير الخزول A من الدرجة d في $\mathbb{F}_p[X]$. إنّ الحقل $\mathbb{K} = \mathbb{F}_p[X]/(A)$ حقل منته عدد عناصره p^d.

الإثبات

لنرمز بالرمز α إلى صفّ تكافؤ X بالقياس A أي $[X] = \alpha$. سنثبتُ أنّ التطبيق التالي هو تقابلٌ

$$\Phi : \underbrace{\mathbb{F}_p \times \cdots \times \mathbb{F}_p}_{d} \to \mathbb{K},\ (x_0, x_1, \ldots, x_{d-1}) \mapsto \sum_{k=0}^{d-1} x_k \alpha^k$$

▪ **التباين**. لنفترض أنّ $\Phi(x_0,\ldots,x_{d-1}) = \Phi(y_0,\ldots,y_{d-1})$. ولنعرّف كثير الحدود

$$G = \sum_{k=0}^{d-1}(x_k - y_k)X^k \in \mathbb{F}_p[X]$$

إنّ $[G] = 0_{\mathbb{K}}$ لأنّ $\Phi(x_0,\ldots,x_{d-1}) = \Phi(y_0,\ldots,y_{d-1})$ وهذا يعني أنّ $G \in (A)$ أو أنّ A يقسم G وهذا يقتضي أنّ $G = 0$ لأنّ $\deg G < \deg A$. ولكن

$$(x_0,\ldots,x_{d-1}) = (y_0,\ldots,y_{d-1}) \Leftrightarrow G = 0$$

نستنتج أنّ Φ متباين.

▪ **الغمر**. ليكن $[P]$ من $\mathbb{K}$. إنّ درجة باقي القسمة الإقليدية لكثير الحدود P على A أصغر تماماً من $d = \deg A$، ومن ثَمّ يوجد Q في $\mathbb{F}_p[X]$، ويوجد $(x_0,\ldots,x_{d-1})$ في $(\mathbb{F}_p)^d$ يُحقّقان

$$P = A\cdot Q + \sum_{k=0}^{d-1} x_k X^k$$

فإذا أخذنا صف تكافؤ P بالقياس A وجدنا أنّ $[P] = \sum_{k=0}^{d-1} x_k\alpha^k \in \operatorname{Im}\Phi$، ونستنتج من ثَمّ أنّ Φ غامر.

ينجم عن ذلك أنّ $\operatorname{card}(\mathbb{K}) = \operatorname{card}\left(\mathbb{F}_p^d\right) = p^d$. ❐

نلاحظ من هذه المبرهنة أنّ كثيرات الحدود غير الخزولة تؤدّي دوراً مهمّاً في دراسة الحقول المنتهية، وسيزداد وضوح هذا الأمر لاحقاً.

5-7. مبرهنة. ليكن $\mathbb{K}$ حقلاً منتهياً عدده المميِّز p . حينئذ يكون

$$\forall R \in \mathbb{F}_p[X], \forall n \in \mathbb{N}, \forall x \in \mathbb{K}, \quad R(x^{p^n}) = \big(R(x)\big)^{p^n}$$

الإثبات

لنلاحظ أولاً أنه إذا كان p عدداً أولياً فإنّ p يقسم C_p^k وذلك أياً كان k من $\mathbb{N}_{p-1}$. لأن

$$C_p^k = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

و p يقسم بسط الكسر السابق ولا يقسم مقامه. إذن

$$\forall k \in \mathbb{N}_{p-1},\ C_p^k = 0 \bmod p$$

ينجم عن ذلك واستناداً إلى دستور ثنائي الحد أنّ

$$\forall (x,y) \in \mathbb{K},\ (x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} C_p^k x^k y^{p-k} = x^p + y^p$$

نستنتج من ذلك، بالتدريج على n ، أنّ

$$\forall n \in \mathbb{N}, \forall (x,y) \in \mathbb{K}^2, \quad (x+y)^{p^n} = x^{p^n} + y^{p^n}$$

ومن ثَمّ نستنتج، أيضاً بالتدريج ولكن على المتحوّل ℓ ، أنّ

$$\forall n \in \mathbb{N}, \forall (x_1,\ldots,x_\ell) \in \mathbb{K}^\ell, \quad (x_1 + \cdots + x_\ell)^{p^n} = x_1^{p^n} + \cdots + x_\ell^{p^n}$$

من ناحية أخرى، إنّ عدد عناصر $\mathbb{F}_p^*$ هو $p-1$ ومنه $\forall a \in \mathbb{F}_p^*, a^{p-1} = 1$. نستنتج إذن أنّه مهما تكن a من $\mathbb{F}_p$ يكن $a^p = a$. ومن ثَمّ نجد، بالتدريج على n :

$$\forall a \in \mathbb{F}_p,\ a^{p^n} = a$$

فإذا كان $R = \sum_{k=1}^{d} a_k X^k$ عنصراً من $\mathbb{F}_p[X]$ أمكننا أن نكتب، أياً كان x من $\mathbb{K}$ و n من $\mathbb{N}$ ، ما يلي:

$$\big(R(x)\big)^{p^n} = \left(\sum_{k=0}^{d} a_k x^k\right)^{p^n} = \sum_{k=0}^{d} a_k^{p^n} (x^k)^{p^n} = \sum_{k=0}^{d} a_k (x^{p^n})^k = R(x^{p^n})$$

وهو المطلوب إثباته. ❐

8-5. مبرهنة. ليكن p عدداً أولياً. وليكن كثير الحدود غير الخزول Q من الدرجة d في $\mathbb{F}_p[X]$. عندئذ يكون لدينا التكافؤ التالي: $Q \mid (X^{p^n} - X) \Leftrightarrow d \mid n$ وذلك أياً كان n من $\mathbb{N}^*$.

الإثبات

لمّا كان Q غير خزول فإنّ عدد عناصر الحقل $\mathbb{K} = \mathbb{F}_p[X]/(Q)$ يساوي p^d ورتبة الزمرة $\mathbb{K}^*$ هي $p^d - 1$ ، إذن يكون لدينا $\forall x \in \mathbb{K}^*, x^{p^d-1} = 1$ ، ونستنتج من ذلك أنّ $\forall x \in \mathbb{K},\ x^{p^d} = x$ ، وينجم عن ذلك بالتدريج على k أنّ

$$\forall k \in \mathbb{N}, \forall x \in \mathbb{K}, \quad x^{p^{dk}} = x \qquad (*)$$

لنثبت الآن التكافؤ المطلوب.

($\Rightarrow$) لمّا كان d يقسم n، يوجد k يُحقّق $n = d\,k$ وبناءً على $(*)$ يكون

$$\forall x \in \mathbb{K},\ \ x^{p^n} = x$$

وإذا عرّفنا كثير الحدود $G = X^{p^n} - X$ من $\mathbb{F}_p[X]$ كان صف تكافؤ G بالقياس Q عنصراً من $\mathbb{K}$ ويحقق استناداً إلى ما سبق $[G] = ([X])^{p^n} - [X] = 0$. وبذا يكون $G \in (Q)$ أو Q يقسم G.

($\Leftarrow$) لنرمز بالرمز α إلى العنصر $[X]$ من $\mathbb{K}$، إذن $Q(\alpha) = 0$، ولأن Q يقسم كثير الحدود $X^{p^n} - X$ فإنّ $\alpha^{p^n} = \alpha$. ليكن y من $\mathbb{K}$، يوجد R في $\mathbb{F}_p[X]$ يُحقّق $y = [R]$ (أي إنّ y هو صف تكافؤ R بالقياس Q)، ومنه $R(\alpha) = y$. وينتج بمقتضى المبرهنة 5-7. أنّ

$$y^{p^n} = (R(\alpha))^{p^n} = R(\alpha^{p^n}) = R(\alpha) = y$$

نكون قد أثبتنا أنّ $\forall y \in \mathbb{K}^*,\ \ y^{p^n - 1} = 1$. ولكن $\mathbb{K}^*$ زمرة دوّارة رتبتها $p^d - 1$ فيوجد عنصر y_0 في $\mathbb{K}^*$ رتبته $p^d - 1$، ومن ثَمّ تقتضي العلاقةُ $y_0^{p^n - 1} = 1$ أنّ $p^d - 1$ يقسم $p^n - 1$. بإجراء قسمة إقليدية للعدد n على d نجد (q, r) يُحقّق $n = q\,d + r$ و $d > r \geq 0$. ولكن

$$\begin{aligned} p^n - 1 &= p^r(p^{qd} - 1) + p^r - 1 \\ &= p^r \cdot (p^d - 1) \cdot \left(\sum_{k=0}^{q-1} p^{dk} \right) + p^r - 1 \end{aligned}$$

ومنه $p^d - 1$ يقسم $p^r - 1$، و $p^d - 1 > p^r - 1$ إذن $0 = p^r - 1$ ومن ثَمّ $r = 0$ و $n = qd$. وهذا ما يثبت المطلوب. ❐

5-9. **مبرهنة**. ليكن p عدداً أولياً، ولتكن n من $\mathbb{N}^*$. نرمز بالرمز K_p^n إلى مجموعة كثيرات الحدود الواحديّة وغير الخزولة من الدرجة n في $\mathbb{F}_p[X]$. فيكون

$$X^{p^n} - X = \prod_{d|n} \Big(\prod_{Q \in K_p^d} Q \Big)$$

أي إنّ $X^{p^n} - X$ هو جداء ضرب جميع كثيرات الحدود الواحدية وغير الخزولة من درجة تقسم n.

الإثبات

نلاحظ أولاً أنّ كثير الحدود $X^{p^n} - X$ من $\mathbb{F}_p[X]$ لا يقبل قاسماً على شكل مربّع كثير حدود درجته أكبر أو تساوي 1، وذلك لأنّه إذا كان $X^{P^n} - X = Q^2R$ وجدنا بالاشتقاق أنّ

$$\left(2Q'R + QR'\right)Q = p^n X^{p^n-1} - 1 = -1$$

فكثير الحدود Q يقسم -1 وهذا يناقض كون درجته تزيد على 1. ينتج ممّا سبق أنّ تفريق $X^{p^n} - X$ إلى جداء كثيرات حدود واحدية غير خزولة يكتب كما يلي

$$X^{p^n} - X = \prod_{i=1}^{k} Q_i$$

و $Q_1, \ldots, Q_k$ كثيرات حدود واحدية غير خزولة ومختلفة مثنى مثنى. وينتمي كلُّ Q_i (عملاً بالمبرهنة 5-9.) إلى إحدى المجموعات K_p^d و d قاسم للعدد n. إذن

$$X^{p^n} - X = \prod_{i=1}^{k} Q_i \quad \text{يقسم} \quad \prod_{d|n}\Big(\prod_{Q\in K_p^d} Q\Big)$$

وبالعكس، أياً كان القاسم d للعدد n، يقسمُ كلُّ Q من K_p^d كثيرَ الحدود $X^{p^n} - X$ ولكن عناصر $\bigcup_{d|n} K_p^d$ أوليّة فيما بينها مثنى مثنى، إذن يقسم الجداءُ $\prod_{d|n}\Big(\prod_{Q\in K_p^d} Q\Big)$ كثيرَ الحدود $X^{p^n} - X$. ونستنتج أنّ

$$X^{p^n} - X = \prod_{d|n}\Big(\prod_{Q\in K_p^d} Q\Big)$$

لأنّ الطرفين واحديان. ❒

5-10. نتيجة. ليكن p عدداً أولياً ولتكن n من $\mathbb{N}^*$. نذكّر بأنّ K_p^n هي مجموعة كثيرات الحدود الواحديّة وغير الخزولة من الدرجة n في $\mathbb{F}_p[X]$، نرمز إلى $\mathrm{card}\left(K_p^n\right)$ بالرمز I_p^n. فيكون $p^n = \sum_{d|n} dI_p^d$.

الإثبات

تكفي مقارنة الحدين المُسيطرين في طرفي العلاقة $X^{p^n} - X = \prod_{d|n}\Big(\prod_{Q\in K_p^d} Q\Big)$. ❒

5-11. مثال. لنفترض أنّ $p = 2$، ولنكتب العلاقات السابقة حين يكون $n = 1, 2, 3, 4$.

فنجد

$$\begin{aligned} 2^1 &= I_2^1 \\ 2^2 &= 2I_2^2 + I_2^1 \\ 2^3 &= 3I_2^3 + I_2^1 \\ 2^4 &= 4I_2^4 + 2I_2^2 + I_2^1 \end{aligned}$$

ومن ثَمّ فإنّ

$$I_2^1 = 2 \text{ و } I_2^2 = 1 \text{ و } I_2^3 = 2 \text{ و } I_2^4 = 3$$

ونترك القارئ يتحقّق أنّ

$$\begin{aligned} K_2^1 &= \{X, X+1\}, \\ K_2^2 &= \{X^2 + X + 1\}, \\ K_2^3 &= \{X^3 + X + 1, X^3 + X^2 + 1\}, \\ K_2^4 &= \{X^4 + X + 1, X^4 + X^3 + 1, X^4 + X^3 + X^2 + X + 1\}. \end{aligned}$$

5-12. مبرهنة. ليكن p عدداً أولياً. عندئذ مهما تكن n من $\mathbb{N}^*$، يوجد في $\mathbb{F}_p[X]$ كثيرُ حدودٍ غير خزول من الدرجة n.

الإثبات

نستفيد من النتيجة 5-10. والرموز الواردة فيها. ينتج من العلاقة $\sum_{d|n} dI_p^d = p^n$ أنّ $p^n \geq n\, I_p^n$ وذلك أياً كان n. ومن ثم

$$\begin{aligned} nI_p^n &= p^n - \sum_{d|n, d\neq n} dI_p^d \\ &\geq p^n - \sum_{d=1}^{n-1} p^d = p^n - \frac{p^n - 1}{p-1} = \frac{p^n(p-2)+1}{p-1} > 0 \end{aligned}$$

نستنتج أنّ $I_p^n > 0$ ومن ثمّ، لأنّه عددٌ صحيحٌ يكون $I_p^n \geq 1$ أي $K_p^n \neq \varnothing$. ❐

5-13. نتيجة. يوجد حقل منته عدد عناصره ℓ إذا وفقط إذا كان $\ell = p^n$ و p عدد أوليّ و n من $\mathbb{N}^*$.

الإثبات

لقد أثبتنا لزوم الشرط في المبرهنة 5-4. وبالعكس، إذا كان p عدداً أوليّاً وكان n عدداً من $\mathbb{N}^*$، نختار في $\mathbb{F}_p[X]$ كثير حدودٍ غير خزولٍ P من الدرجة n، وهو موجود بمقتضى المبرهنة 5-12. فيكون $\mathbb{K} = \mathbb{F}_p\,[X]/(P)$ حقلاً عدد عناصره p^n. ❐

5-14. مبرهنة. ليكن p عدداً أوّلياً، و A كثيرَ حدودٍ واحديّاً غير خزول في $\mathbb{F}_p[X]$ من الدرجة n. إذا كان $\mathbb{K}$ حقلاً منتهياً عدد عناصره p^n فيوجد تشاكل تقابليّ حقليّ بين $\mathbb{K}$ و $\mathbb{F}_p\,[X]/(A)$ و $\mathbb{K} =$.

الإثبات

لنلاحظ أنّ العدد المميِّز للحقل $\mathbb{K}$ هو p. لأنّ العدد المميّز للحقل $\mathbb{K}$ عددٌ أوليّ يقسم عدد عناصر الزمرة $(\mathbb{K},+)$ الذي يساوي p^n. فالحقل $\mathbb{K}$ هو إذن توسيع للحقل $\mathbb{F}_p$ ويمكننا اعتبار هذا الأخير حقلاً جزئياً من $\mathbb{K}$. ولمّا كانت رتبة الزمرة $(\mathbb{K}^*,\cdot)$ هي $p^n - 1$ كان

$$\forall x \in \mathbb{K}^*,\ \ x^{p^n-1} = 1$$

ومنه نستنتج أنّ $\forall x \in \mathbb{K},\ \ x^{p^n} = x$. ينجم عن ذلك أنّ عناصر $\mathbb{K}$ هي جذور لكثير الحدود $X^{p^n} - X$ ودرجة هذا الأخير تساوي $\operatorname{card}(\mathbb{K})$. إذن جذور $X^{p^n} - X$ هي تماماً عناصر $\mathbb{K}$. أي $X^{p^n} - X = \prod_{\alpha\in\mathbb{K}} (X-\alpha)$، ولكن A يقسم $X^{p^n} - X$ إذن يوجد α ينتمي إلى $\mathbb{K}$ ويُحقّق $A(\alpha) = 0$.

لنضع $\mathcal{I} = \{Q \in \mathbb{F}_p[X] : Q(\alpha) = 0\}$، إنّ $\mathcal{I}$ مثاليّ من $\mathbb{F}_p[X]$ مختلف عن $\mathbb{F}_p[X]$ (لأنّ $1 \notin \mathcal{I}$) ثُمّ إنّه يحتوي على المثالي الأعظمي (A) (لأنّ A غير خزول) إذن $\mathcal{I} = (A)$. ومنه

$$\forall Q \in \mathbb{F}_p[X],\ \ Q(\alpha) = 0 \Rightarrow Q \in (A) \qquad (*)$$

لنعرّف إذن التطبيق التالي : $\Phi : \mathbb{F}_p\,[X]/(A) \to \mathbb{K},\ [Q] \mapsto Q(\alpha)$

إنّ هذا التعريف جيدٌ، لأنه إذا كان $[Q'] = [Q]$، عنى هذا أنّ كثير الحدود A يقسم $Q - Q'$ وكان من ثَمّ $Q'(\alpha) = Q(\alpha)$. ونتحقق بسهولة أنّ

$$\Phi([Q] + [P]) = \Phi([Q]) + \Phi([P])$$

$$\Phi([Q] \cdot [P]) = \Phi([Q]) \cdot \Phi([P])$$

أياً كان $[Q]$ و $[P]$ من $\mathbb{F}_p[X]/(A)$ ، فالتطبيق Φ تشاكل حقليّ.

إنّ التطبيق Φ متباين لأنه إذا كان $Q(\alpha) = 0$ كان $[Q] = 0$ عملاً بالخاصّة $(*)$ ومنه $\ker \Phi = \{0\}$. من ناحية أخرى $\operatorname{card}(\mathbb{F}_p[X]/(A)) = \operatorname{card}(\mathbb{K}) = p^n$. ومن ثَمّ لا بدّ أن يكون Φ تقابلاً وهذا يثبت المطلوب. ❐

5-15. نتيجة وتعريف. ليكن p عدداً أولياً ولتكن n من $\mathbb{N}^*$. يوجد حقل منته وحيدٌ عدد عناصره p^n نرمز إليه عادة بالرمز $\mathbb{F}_{p^n}$ أو $GF(p^n)$.

نقصد بالوحدانية أنه إذا كان $\mathbb{K}$ و $\mathbb{K}'$ حقلين منتهيين عدد عناصر كل منهما p^n فيوجد تشاكل تقابلي حقليّ بينهما.

نأمل في نهاية هذا الفصل أن نكون قد قدّمنا إلى القارئ نظرية الحقول والحقول المنتهية، التي حظيت باهتمام كبير من قبل الباحثين التطبيقيين منذ نحو خمسين عاماً، لتطبيقاتها الواسعة في مجالات عديدة كنظرية ترميز المعلومات وفي الدارات المنطقية.

تمرينات

التمرين 1. حلّل إلى عناصر بسيطة في $\mathbb{C}(X)$ كلّاً من الكسور العادية الآتية في حالة n و m عددان طبيعيّان موجبان تماماً.

$$\frac{1}{(X-a)^n(X-b)^m},\quad \frac{1}{(X-2)^2(X-3)^3},\quad \frac{1}{(X^2-1)^2},$$
$$\frac{1}{(X+1)^7-X^7-1}.\quad \frac{1}{(X-1)(X-2)\cdots(X-n)},\quad \frac{X^{2n}}{(X^2+1)^n},$$

الحل

❶ حالة الكسر $F(X)=\dfrac{1}{(X^2-1)^2}$. لمّا كان $\dfrac{1}{X^2-1}=\dfrac{1}{2}\left(\dfrac{1}{X-1}-\dfrac{1}{X+1}\right)$ استنتجنا أنّ

$$\begin{aligned}\frac{1}{(X^2-1)^2}&=\frac{1}{4}\left(\frac{1}{(X-1)^2}-\frac{2}{X^2-1}+\frac{1}{(X+1)^2}\right)\\&=\frac{\frac14}{(X-1)^2}-\frac{\frac14}{X-1}+\frac{\frac14}{(X+1)^2}+\frac{\frac14}{X+1}\end{aligned}$$

❷ حالة الكسر $F(X)=\dfrac{1}{(X-2)^2(X-3)^3}$. في الحقيقة، يُكتب F بالشكل F_2+F_3 وقد رمزنا بالرمز F_2 إلى الجزء القطبي الموافق للقطب 2 وبالرمز F_3 إلى الجزء القطبي الموافق للقطب 3.

- لحساب F_3 نُجري تغيير المتحوّل $Y=X-3$ فيكون لدينا

$$F(X)=\frac{1}{Y^3(1+Y)^2}$$

ولكن، بالاستفادة من العلاقة $1=1+Y-Y$ يمكننا أنّ نكتب

$$F(X)=\frac{1+Y-Y}{Y^3(1+Y)^2}=\frac{1}{Y^3(1+Y)}-\frac{1}{Y^2(1+Y)^2}$$

ونتابع بالأسلوب ذاته.

$$\begin{aligned}F(X) &= \frac{1+Y-Y}{Y^3(1+Y)} - \frac{1+Y-Y}{Y^2(1+Y)^2}\\ &= \frac{1}{Y^3} - \frac{2}{Y^2(1+Y)} + \frac{1}{Y(1+Y)^2}\\ &= \frac{1}{Y^3} - \frac{2(1+Y-Y)}{Y^2(1+Y)} + \frac{1+Y-Y}{Y(1+Y)^2}\\ &= \frac{1}{Y^3} - \frac{2}{Y^2} + \frac{3}{Y(1+Y)} - \frac{1}{(1+Y)^2}\\ &= \frac{1}{Y^3} - \frac{2}{Y^2} + \frac{3(1+Y-Y)}{Y(1+Y)} - \frac{1}{(1+Y)^2}\\ &= \frac{1}{Y^3} - \frac{2}{Y^2} + \frac{3}{Y} - \frac{3}{1+Y} - \frac{1}{(1+Y)^2}\end{aligned}$$

ومنه

$$F(X) = \frac{1}{(X-3)^3} - \frac{2}{(X-3)^2} + \frac{3}{X-3} - \frac{3}{X-2} - \frac{1}{(X-2)^2}$$

❸ حالة الكسر $F_{n,m}(X) = \dfrac{1}{(X-a)^n(X-b)^m}$. هذا تعميم للحالة السابقة، نفترض أنّ $a \neq b$ وإلّا كانت المسألة تافهة. نجري تغيير المتحوّل $Y = \dfrac{X-a}{b-a}$ فيكون لدينا

$$F_{n,m}(X) = \frac{1}{(b-a)^{n+m}} \cdot \frac{1}{Y^n(Y-1)^m} = \frac{(-1)^m}{(b-a)^{n+m}} \cdot G_{n,m}(Y)$$

وقد عرّفنا $G_{n,m}(Y) = \dfrac{1}{Y^n(1-Y)^m}$. وهنا نلاحظ أنّ

$$\frac{1}{1-Y} - \sum_{k=0}^{n+m-2} Y^k = \frac{Y^{n+m-1}}{1-Y}$$

وباشتقاق طرفي هذه العلاقة $m-1$ مرّة ثُمّ القسمة على $(m-1)!$ نجد

$$\frac{1}{(1-Y)^m}-\sum_{k=m-1}^{n+m-2}C_k^{m-1}Y^{k-m+1}=\frac{1}{(m-1)!}\sum_{k=0}^{m-1}C_{m-1}^k(Y^{n+m-1})^{(k)}\left(\frac{1}{1-Y}\right)^{(m-1-k)}$$
$$=Y^n\sum_{k=0}^{m-1}\frac{C_{n+m-1}^k}{(m-1-k)!}Y^{m-1-k}\left(\frac{1}{1-Y}\right)^{(m-1-k)}$$

وقد استفدنا من علاقة لايبنتز في مشتق الجداء. ومنه

$$\frac{1}{(1-Y)^m}-\sum_{k=1}^{n}C_{n+m-1-k}^{m-1}Y^{n-k}=Y^n\cdot\sum_{p=0}^{m-1}\frac{C_{n+m-1}^{n+p}}{p\,!}Y^p\left(\frac{1}{1-Y}\right)^{(p)}$$

ومن ثَمّ فإنّ الكسر

$$H_{n,m}(Y)=G_{n,m}(Y)-\sum_{k=1}^{n}\frac{C_{n+m-1-k}^{m-1}}{Y^k}$$

يُكتب بالصيغة المُكافئة

$$H_{n,m}(Y)=\sum_{p=0}^{m-1}\frac{C_{n+m-1}^{n+p}}{p\,!}Y^p\left(\frac{1}{1-Y}\right)^{(p)}$$

وهو إذن لا يقبل الصفر قطباً. والجزء القطبي الموافق للقطب 0 في $G_{n,m}(Y)$ هو $\sum_{k=1}^{n}\frac{C_{n+m-1-k}^{m-1}}{Y^k}$. وبملاحظة أنّ $G_{n,m}(Y)=G_{m,n}(1-Y)$ نستنتج أنّ الجزء القطبي الموافق للقطب 1 في $G_{n,m}(Y)$ هو $\sum_{k=1}^{m}\frac{C_{n+m-1-k}^{n-1}}{(1-Y)^k}$. وهكذا نستنتج أنّ

$$G_{n,m}(Y)=\frac{1}{Y^n(1-Y)^m}=\sum_{k=1}^{n}\frac{C_{n+m-1-k}^{m-1}}{Y^k}+\sum_{k=1}^{m}\frac{C_{n+m-1-k}^{n-1}}{(1-Y)^k}$$

وبالعودة إلى $F_{n,m}$ نجد أنّ

$$\frac{1}{(X-a)^n(X-b)^m}=\sum_{k=1}^{n}\frac{A_{n,m}^{(k)}(a,b)}{(X-a)^k}+\sum_{k=1}^{m}\frac{A_{m,n}^{(k)}(b,a)}{(X-b)^k}$$

وقد عرّفنا $A_{n,m}^{(k)}(a,b)=(-1)^mC_{n+m-1-k}^{m-1}(b-a)^{k-n-m}$. ولعلّ أجمل هذه الصيغ هي التالية :

$$\frac{(b-a)^{n+m}}{(X-a)^n(b-X)^m}=\sum_{k=1}^{n}C_{n+m-1-k}^{m-1}\left(\frac{b-a}{X-a}\right)^k+\sum_{k=1}^{m}C_{n+m-1-k}^{n-1}\left(\frac{a-b}{X-b}\right)^k$$

❹ حالة الكسر $F_n(X)=\dfrac{X^{2n}}{(X^2+1)^n}$. نلاحظ هنا أنّ

$$F_n(X)=\frac{X^{2n}}{(X^2+1)^n}=\left(1-\frac{1}{X^2+1}\right)^n=1+\sum_{m=1}^{n}(-1)^m C_n^m\frac{1}{(X^2+1)^m}$$

ولكن استناداً إلى ❸ يمكننا أن نكتب

$$\frac{1}{(X^2+1)^m}=\frac{1}{(X-\mathrm{i})^m(X+\mathrm{i})^m}=\sum_{k=1}^{m}\frac{A_{m,m}^{(k)}(\mathrm{i},-\mathrm{i})}{(X-\mathrm{i})^k}+\sum_{k=1}^{m}\frac{A_{m,m}^{(k)}(-\mathrm{i},\mathrm{i})}{(X+\mathrm{i})^k}$$

حيث

$$A_{m,m}^{(k)}(-\mathrm{i},\mathrm{i})=2^{k-2m}\,\mathrm{i}^k\,C_{2m-1-k}^{m-1}\quad \text{و}\quad A_{m,m}^{(k)}(\mathrm{i},-\mathrm{i})=2^{k-2m}(-\mathrm{i})^k C_{2m-1-k}^{m-1}$$

ومنه

$$\frac{1}{(X^2+1)^m}=\sum_{k=1}^{m}2^{k-2m}\,\mathrm{i}^k\,C_{2m-1-k}^{m-1}\left(\frac{(-1)^k}{(X-\mathrm{i})^k}+\frac{1}{(X+\mathrm{i})^k}\right)$$

وبالعودة إلى F_n نجد

$$F_n(X)=1+\sum_{m=1}^{n}(-1)^m C_n^m\left(\sum_{k=1}^{m}2^{k-2m}\,\mathrm{i}^k\,C_{2m-1-k}^{m-1}\left(\frac{(-1)^k}{(X-\mathrm{i})^k}+\frac{1}{(X+\mathrm{i})^k}\right)\right)$$

أو

$$\begin{aligned}F_n(X)&=1+\sum_{1\le k\le m\le n}\left((-1)^m 2^{k-2m}\,\mathrm{i}^k\,C_n^m C_{2m-1-k}^{m-1}\left(\frac{(-1)^k}{(X-\mathrm{i})^k}+\frac{1}{(X+\mathrm{i})^k}\right)\right)\\&=1+\sum_{k=1}^{n}\left(\sum_{m=k}^{n}(-1)^m 2^{k-2m}\,\mathrm{i}^k\,C_n^m C_{2m-1-k}^{m-1}\right)\left(\frac{(-1)^k}{(X-\mathrm{i})^k}+\frac{1}{(X+\mathrm{i})^k}\right)\\&=1+\sum_{k=1}^{n}\left(\frac{\overline{\lambda_k^{(n)}}}{(X-\mathrm{i})^k}+\frac{\lambda_k^{(n)}}{(X+\mathrm{i})^k}\right)\end{aligned}$$

حيث

$$\lambda_k^{(n)}=(2\,\mathrm{i})^k\sum_{m=k}^{n}(-1)^m 2^{-2m}C_n^m C_{2m-1-k}^{m-1}$$

في حالة $1\le k\le n$.

❺ حالة الكسر $F_n(X)=\dfrac{1}{(X-1)(X-2)\cdots(X-n)}$. نلاحظ أنّ الأقطاب بسيطة، ومن ثَمّ

$$F_n(X)=\sum_{k=1}^{n}\frac{a_k}{X-k}$$

حيث

$$a_k=\frac{1}{(k-1)(k-2)\cdots 1(-1)(-2)\cdots(k-n)}=\frac{k(-1)^{n-k}}{k!(n-k)!}$$

إذن

$$F_n(X)=\frac{1}{n!}\sum_{k=1}^{n}\frac{k(-1)^k C_n^k}{X-k}$$

❻ حالة الكسر $F(X)=\dfrac{1}{(X+1)^7-1-X^7}$. نبحث أوّلاً عن أقطاب هذا الكسر. أي عن جذور كثير الحدود $Q(X)=(X+1)^7-1-X^7$. نلاحظ أوّلاً أنّ

$$\begin{aligned}\gcd\left(Q,Q'\right)&=\gcd\left(Q,(X+1)^6-X^6\right)\\&=\gcd\left(Q-(X+1)\left((X+1)^6-X^6\right),(X+1)^6-X^6\right)\\&=\gcd\left(X^6-1,(X+1)^6-X^6\right)\end{aligned}$$

ولكن

$$\begin{aligned}X^6-1&=(X^2-1)(X^2+X+1)(X^2-X+1)\\(X+1)^6-X^6&=(2X+1)(X^2+X+1)(3X^2+3X+1)\end{aligned}$$

إذن

$$\gcd\left(Q(X),Q'(X)\right)=X^2+X+1$$

وكلٌّ من $\mathrm{j}=\exp\left(\frac{2i\pi}{3}\right)$ و j^2 جذرٌ مُضاعفٌ لكثير الحدود $Q(X)$ وهو يقبل وضوحاً العددين 0 و -1 جذوراً. ولأنّ أمثال X^6 في $Q(X)$ هي 7 استنتجنا أنّ

$$Q(X)=7X(X+1)(X-\mathrm{j})^2(X-\mathrm{j}^2)^2$$

ومنه

$$F(X)=\frac{a}{X}+\frac{b}{X+1}+\frac{\alpha}{X-\mathrm{j}}+\frac{\beta}{(X-\mathrm{j})^2}+\frac{\gamma}{X-\mathrm{j}^2}+\frac{\delta}{(X-\mathrm{j}^2)^2}$$

ولكن $F(X)=\overline{F(X)}$ لأنّ $F(X)$ ينتمي إلى $\mathbb{R}(X)$ إذن

$$F(X)=\frac{a}{X}+\frac{b}{X+1}+\frac{\alpha}{X-\mathrm{j}}+\frac{\beta}{(X-\mathrm{j})^2}+\frac{\bar{\alpha}}{X-\mathrm{j}^2}+\frac{\bar{\beta}}{(X-\mathrm{j}^2)^2}$$

القطبان 0 و -1 بسيطان إذن $a=\dfrac{1}{Q'(0)}=\dfrac{1}{7}$ و $b=\dfrac{1}{Q'(-1)}=-\dfrac{1}{7}$، ثُمّ إنّ

$$\beta=\left[(X-\mathrm{j})^2F(X)\right]_{X\leftarrow\mathrm{j}}=\frac{1}{7\,\mathrm{j}\big(1+\mathrm{j}\big)(\mathrm{j}-\mathrm{j}^2)^2}=\frac{1}{21}$$

وأخيراً لتعيين α نحسب $F(-\mathrm{j})$ بطريقتين فنجد أنّ

$$\frac{1}{7(\mathrm{j}^2-\mathrm{j})(4\,\mathrm{j}^2)}=\frac{1}{7}\left(-\frac{1}{\mathrm{j}}-\frac{1}{1-\mathrm{j}}-\frac{7\alpha}{2\,\mathrm{j}}+\frac{1}{12\,\mathrm{j}^2}+7\bar{\alpha}+\frac{1}{3}\right)$$

ومنه $\dfrac{5}{21}=2\,\mathrm{j}\,\bar{\alpha}-\alpha$، وعليه يكون $\alpha=\dfrac{5}{21\sqrt{3}}\mathrm{i}$. وأخيراً

$$F\big(X\big)=\frac{1}{7}\left(\frac{1}{X}-\frac{1}{X+1}+\frac{\frac{5}{3\sqrt{3}}\mathrm{i}}{X-\mathrm{j}}+\frac{\frac{1}{3}}{(X-\mathrm{j})^2}-\frac{\frac{5}{3\sqrt{3}}\mathrm{i}}{X-\mathrm{j}^2}+\frac{\frac{1}{3}}{(X-\mathrm{j}^2)^2}\right)$$

وهي النتيجة المطلوبة. ■

التمرين 2. حلّل إلى عناصر بسيطة في $\mathbb{R}(X)$ الكسور العادية التالية، في حالة $n\in\mathbb{N}^*$:

$$\frac{1}{(X^4-1)^2},\quad \frac{X^6-X^2+1}{(X-1)^3},\quad \frac{X^5+64}{(X^2+2X+4)^3},$$
$$\frac{1}{(X^3-1)^3},\quad \frac{1}{X^8+X^4+1},\quad \frac{1}{(X^2-1)^n},$$
$$\frac{X^2}{X^4-2\cos\alpha X^2+1},\ \alpha\in\mathbb{R},\quad \frac{X^7+5}{(X+2)^3(X^2+X+1)^2},$$
$$\frac{X^2-X+4}{(X-1)^4(X^2+X+1)^2},\quad \sum_{k=0}^{n}\frac{k\,!}{X(X+1)\cdots(X+k)}.$$

الحل

❶ حالة الكسر $F(X)=\dfrac{1}{(X^4-1)^2}$. لنبدأ بملاحظة أنّ

$$\left(\frac{X}{X^4-1}\right)'=\frac{-1-3X^4}{(X^4-1)^2}=\frac{-4-3(X^4-1)}{(X^4-1)^2}=-\frac{4}{(X^4-1)^2}-\frac{3}{X^4-1}$$

فإذا عرّفنا $H(X)=\dfrac{1}{X^4-1}$ كان لدينا

$$F(X)=-\frac{1}{4}\Big(\big(XH(X)\big)'+3H(X)\Big)$$

ولكن

$$H(X)=\frac{1}{2}\left(\frac{1}{X^2-1}-\frac{1}{X^2+1}\right)=\frac{1/4}{X-1}-\frac{1/4}{X+1}-\frac{1/2}{X^2+1}$$

و

$$\begin{aligned}XH(X)&=\frac{X-1+1}{4(X-1)}-\frac{X+1-1}{4(X+1)}-\frac{X}{2(X^2+1)}\\&=\frac{1}{4(X-1)}+\frac{1}{4(X+1)}-\frac{X}{2(X^2+1)}\end{aligned}$$

ومن ثَمّ

$$\begin{aligned}\big(XH(X)\big)'&=-\frac{1}{4(X-1)^2}-\frac{1}{4(X+1)^2}-\frac{1-X^2}{2(X^2+1)^2}\\&=-\frac{1}{4(X-1)^2}-\frac{1}{4(X+1)^2}-\frac{2-X^2-1}{2(X^2+1)^2}\\&=-\frac{1}{4(X-1)^2}-\frac{1}{4(X+1)^2}+\frac{1}{2(X^2+1)}-\frac{1}{(X^2+1)^2}\end{aligned}$$

وعليه

$$F(X)=-\frac{\frac{3}{16}}{X-1}+\frac{\frac{1}{16}}{(X-1)^2}+\frac{\frac{3}{16}}{X+1}+\frac{\frac{1}{16}}{(X+1)^2}+\frac{\frac{1}{4}}{X^2+1}+\frac{\frac{1}{4}}{(X^2+1)^2}$$

وهو التفريق المطلوب في $\mathbb{R}(X)$.

❷ حالة الكسر $F(X) = \dfrac{X^6 - X^2 + 1}{(X-1)^3}$. لنضع $T = X - 1$ فيكون

$$\begin{aligned} F(X) = \frac{X^6 - X^2 + 1}{(X-1)^3} &= \frac{(T+1)^6 - (T+1)^2 + 1}{T^3} \\ &= \frac{1}{T^3}\left(T^6 + 6T^5 + 15T^4 + 20T^3 + 14T^2 + 4T + 1\right) \\ &= T^3 + 6T^2 + 15T + 20 + \frac{14}{T} + \frac{4}{T^2} + \frac{1}{T^3} \\ &= (X-1)^3 + 6(X-1)^2 + 15X + 5 + \frac{14}{X-1} + \frac{4}{(X-1)^2} + \frac{1}{(X-1)^3} \end{aligned}$$

وأخيراً

$$F(X) = X^3 + 3X^2 + 6X + 10 + \frac{14}{X-1} + \frac{4}{(X-1)^2} + \frac{1}{(X-1)^3}$$

❸ حالة الكسر $F(X) = \dfrac{X^5 + 64}{(X^2 + 2X + 4)^3}$. لنضع $Q(X) = X^2 + 2X + 4$

فيكون لدينا بإجراء قسمة إقليديّة لكثير الحدود $X^5 + 64$ على $Q(X)$ نجد

$$X^5 + 64 = Q(X)(X^3 - 2X^2 + 8) - 16X + 32$$

وكذلك

$$X^3 - 2X^2 + 8 = Q(X)(X - 4) + 4X + 24$$

ومن ثَمّ

$$X^5 + 64 = Q^2(X)(X-4) + Q(X)(4X + 24) - 16X + 32$$

إذن

$$F(X) = \frac{X - 4}{X^2 + 2X + 4} + \frac{4X + 24}{(X^2 + 2X + 4)^2} + \frac{-16X + 32}{(X^2 + 2X + 4)^3}$$

❹ حالة الكسر $F(X) = \dfrac{1}{(X^3 - 1)^3}$. لنضع $T = X^2 + X + 1$ ولنلاحظ أنّ

$$(X-1)(X+2) = T - 3$$

وهذا يفيدنا في كتابة $F(X)$ بالشكل الآتي

$$F(X) = \frac{(X+2)^3}{T^3(T-3)^3}$$

وبإجراء قسمة إقليديّة لكثير الحدود $(X+2)^3$ على X^2+X+1 نجد

$$(X+2)^3 = (X^2+X+1)(X+5) + 6X + 3$$

ومن ثَمّ

$$F(X) = -\frac{6X+3+(X+5)T}{T^3(3-T)^3}$$

بإجراء قسمة وفق القوى المتزايدة في $\mathbb{R}(X)[T]$ لكثير الحدود $6X+3+(X+5)T$ على كثير الحدود $(3-T)^3$ نجد أنّ

$$6X+3+(X+5)T = Q_X(T)(3-T)^3 + T^3 R_X(T)$$

حيث

$$Q_X(T) = \frac{1+2X}{9} + \frac{8+7X}{27}T + \frac{7+5X}{27}T^2$$
$$R_X(T) = \frac{40+26X}{9} - \frac{55+38X}{27}T + \frac{7+5X}{27}T^2$$

فيكون لدينا

$$F(X) = -\frac{1+2X}{9T^3} - \frac{8+7X}{27T^2} - \frac{7+5X}{27T} + \frac{R_X(T)}{(T-3)^3}$$

فإذا تذكّرنا أنّ $(X+2)^3$ يقسم $(T-3)^3$ وأنّ -2 ليس قطباً للكسر F استنتجنا أنّ المقدار $(X+2)^3$ يجب أن يقسم كثير الحدود $R_X(X^2+X+1)$ وهذا ما نتحقّق منه مباشرة بإجراء قسمة إقليديّة لكثير الحدود $R_X(X^2+X+1)$ على $(X+2)^3$ إذ نجد أنّ

$$R_X(X^2+X+1) = \frac{1}{27}(X+2)^3\left(5X^2-13X+9\right)$$

ومنه

$$F(X) = -\frac{1+2X}{9T^3} - \frac{8+7X}{27T^2} - \frac{7+5X}{27T} + \frac{5X^2-13X+9}{27(X-1)^3}$$

ولكن $5X^2-13X+9=5(X-1)^2-3(X-1)+1$ إذن

$$F(X)=\frac{1}{27}\left(\frac{5}{X-1}-\frac{3}{(X-1)^2}+\frac{1}{(X-1)^3}-\frac{7+5X}{T}-\frac{8+7X}{T^2}-\frac{3+6X}{T^3}\right)$$

حيث $T=X^2+X+1$.

❺ حالة الكسر $F(X)=\dfrac{1}{X^8+X^4+1}$.

لنلاحظ أنّ أقطاب هذا الكسر في $\mathbb{C}$ هي الأعداد $\{\omega^k:k\in\Delta\}\cup\{\overline{\omega}^k:k\in\Delta\}$ حيث $\omega=\exp\left(\frac{i\pi}{6}\right)$ و $\Delta=\{1,2,4,5\}$. وهي جميعاً أقطاب بسيطة، إذن في $\mathbb{C}(X)$ يمكننا أن نكتب، بعد ملاحظة أنّ $F(X)\in\mathbb{R}(X)$، ما يلي

$$\begin{aligned}F(X)&=\sum_{k\in\Delta}\left(\frac{a_k}{X-\omega^k}+\frac{\overline{a}_k}{X-\overline{\omega}^k}\right)\\&=\sum_{k\in\Delta}\left(\frac{(a_k+\overline{a}_k)X-\omega^k\overline{a}_k-\overline{\omega}^k a_k}{X^2-(\omega^k+\overline{\omega}^k)X+1}\right)\end{aligned}$$

يُحسب العدد a_k بالصيغة $a_k=\dfrac{1}{8\omega^{7k}+4\omega^{3k}}$. وعندئذ

k	$2\operatorname{Re}(\omega^k)$	$2\operatorname{Re}(a_k)$	$2\operatorname{Re}(\overline{\omega}^k a_k)$
1	$\sqrt{3}$	$-\dfrac{1}{2\sqrt{3}}$	$-\dfrac{1}{4}$
2	1	0	$-\dfrac{1}{4}$
4	-1	0	$-\dfrac{1}{4}$
5	$-\sqrt{3}$	$\dfrac{1}{2\sqrt{3}}$	$-\dfrac{1}{4}$

ومن ثَمّ

$$F(X)=\frac{-\frac{1}{2\sqrt{3}}X+\frac{1}{4}}{X^2-\sqrt{3}X+1}+\frac{\frac{1}{2\sqrt{3}}X+\frac{1}{4}}{X^2+\sqrt{3}X+1}+\frac{\frac{1}{4}}{X^2-X+1}+\frac{\frac{1}{4}}{X^2+X+1}$$

❻ حالة الكسر $F_n(X)=\dfrac{1}{(X^2-1)^n}$. هذه حالة خاصّة من التمرين ❸.1 إذ نجد

$$\frac{1}{(X^2-1)^n}=\sum_{k=1}^{n}\frac{(-1)^{k-n}2^{k-2n}C_{2n-1-k}^{n-1}}{(X-1)^k}+\sum_{k=1}^{n}\frac{(-1)^{n}2^{k-2n}C_{2n-1-k}^{n-1}}{(X+1)^k}$$

❼ حالة الكسر $F(X)=\dfrac{X^2}{X^4-2\cos\alpha X^2+1}$، مع $\alpha\in\mathbb{R}\backslash(\pi+2\pi\mathbb{Z})$. في الحقيقة لدينا

$$\begin{aligned}F(X)&=\frac{X^2}{X^4-2\cos\alpha X^2+1}=\frac{X^2}{(X^2-e^{i\alpha})(X^2-e^{-i\alpha})}\\&=\frac{1}{2\,i\sin\alpha}\left(\frac{e^{i\alpha}}{X^2-e^{i\alpha}}-\frac{e^{-i\alpha}}{X^2-e^{-i\alpha}}\right)\end{aligned}$$

ولكن، بوضع $\alpha=2\beta$، والاستفادة من كون

$$\begin{aligned}\frac{e^{i\alpha}}{X^2-e^{i\alpha}}&=\frac{1}{2}\left(\frac{e^{i\beta}}{X-e^{i\beta}}-\frac{e^{i\beta}}{X+e^{i\beta}}\right),\\\frac{e^{-i\alpha}}{X^2-e^{-i\alpha}}&=\frac{1}{2}\left(\frac{e^{-i\beta}}{X-e^{-i\beta}}-\frac{e^{-i\beta}}{X+e^{-i\beta}}\right)\end{aligned}$$

نستنتج

$$\begin{aligned}F(X)&=\frac{1}{4\,i\sin\alpha}\left(\frac{e^{i\beta}}{X-e^{i\beta}}-\frac{e^{i\beta}}{X+e^{i\beta}}-\frac{e^{-i\beta}}{X-e^{-i\beta}}+\frac{e^{-i\beta}}{X+e^{-i\beta}}\right)\\&=\frac{1}{4\,i\sin\alpha}\left(\frac{e^{i\beta}}{X-e^{i\beta}}-\frac{e^{-i\beta}}{X-e^{-i\beta}}-\frac{e^{i\beta}}{X+e^{i\beta}}+\frac{e^{-i\beta}}{X+e^{-i\beta}}\right)\\&=\frac{1}{4\cos\beta}\left(\frac{X}{X^2-2\cos\beta X+1}-\frac{X}{X^2+2\cos\beta X+1}\right)\end{aligned}$$

أمّا في حالة $\alpha\in\pi+2\pi\mathbb{Z}$ فلدينا ببساطة

$$F(X)=\frac{X^2}{(X^2+1)^2}=\frac{1}{X^2+1}-\frac{1}{(X^2+1)^2}.$$

❽ حالة الكسر $F(X) = \dfrac{X^7+5}{(X+2)^3(X^2+X+1)^2}$. نضع $T = X+2$ فيكون لدينا

$$F(X) = \frac{(T-2)^7+5}{T^3(T^2-3T+3)^2} = \frac{A(T)}{T^3(B(T))^2}$$

حيث

$$\begin{aligned} A(T) &= (T-2)^7+5 \\ &= -123+448T-672T^2+560T^3-280T^4+84T^5-14T^6+T^7 \\ B(T) &= 3-3T+T^2 \\ (B(T))^2 &= 9-18T+15T^2-6T^3+T^4 \end{aligned}$$

وبإجراء قسمة وفق القوى المتزايدة حتّى المرتبة 2 لكثير الحدود $A(T)$ على $(B(T))^2$ نجد

$$A(T) = (B(T))^2Q(T) + T^3R(T)$$

حيث

$$\begin{aligned} Q(T) &= -\frac{41}{3} + \frac{202}{9}T - 7T^2 \\ R(T) &= \frac{46}{3} - \frac{80}{3}T + \frac{176}{9}T^2 - 7T^3 + T^4 \end{aligned}$$

وأخيراً نلاحظ بإجراء قسمة إقليديّة لكثير الحدود $R(T)-(B(T))^2$ على $B(T)$ أنّ

$$R(T)-(B(T))^2 = B(T)\left(\frac{14}{9}-T\right) + \left(\frac{5}{3}-T\right)$$

وهكذا نكون قد أثبتنا أنّ

$$A(T) = (B(T))^2Q(T) + T^3\left((B(T))^2 + B(T)\left(\frac{14}{9}-T\right) + \left(\frac{5}{3}-T\right)\right)$$

ومن ثَمّ

$$\begin{aligned} F(X) &= \frac{A(T)}{T^3(B(T))^2} = \frac{Q(T)}{T^3} + 1 + \frac{\frac{14}{9}-T}{B(T)} + \frac{\frac{5}{3}-T}{(B(T))^2} \\ &= 1 - \frac{7}{T} + \frac{202}{9T^2} - \frac{41}{3T^3} + \frac{\frac{14}{9}-T}{B(T)} + \frac{\frac{5}{3}-T}{(B(T))^2} \end{aligned}$$

وبالعودة إلى المتحوّل X نجد

$$F(X)=1-\frac{7}{X+2}+\frac{\frac{202}{9}}{(X+2)^2}-\frac{\frac{41}{3}}{(X+2)^3}-\frac{\frac{4}{9}+X}{X^2+X+1}-\frac{\frac{1}{3}+X}{(X^2+X+1)^2}$$

❾ حالة الكسر $F(X)=\dfrac{X^2-X+4}{(X-1)^4(X^2+X+1)^2}$. نضع $T=X-1$ فيكون لدينا

$$F(X)=\frac{T^2+T+4}{T^4(T^2+3T+3)^2}=\frac{A(T)}{T^3(B(T))^2}$$

حيث

$$\begin{aligned}A(T)&=T^2+T+4\\B(T)&=3+3T+T^2\\(B(T))^2&=9+18T+15T^2+6T^3+T^4\end{aligned}$$

وبإجراء قسمة وفق القوى المتزايدة حتّى المرتبة 3 لكثير الحدود $A(T)$ على $(B(T))^2$ نجد

$$A(T)=(B(T))^2Q(T)+T^4R(T)$$

حيث

$$\begin{aligned}Q(T)&=\frac{4}{9}-\frac{7}{9}T+\frac{25}{27}T^2-\frac{23}{27}T^3\\R(T)&=\frac{17}{3}+8T+\frac{113}{27}T^2+\frac{23}{27}T^3\end{aligned}$$

وأخيراً نلاحظ بإجراء قسمة إقليديّة لكثير الحدود $R(T)$ على $B(T)$ أنّ

$$R(T)=B(T)\left(\frac{44+23T}{27}\right)+\left(\frac{7+5T}{9}\right)$$

وهكذا نكون قد أثبتنا أنّ

$$A(T)=(B(T))^2Q(T)+T^4\left(B(T)\left(\frac{44+23T}{27}\right)+\left(\frac{7+5T}{9}\right)\right)$$

ومن ثَمّ

$$F(X)=\frac{A(T)}{T^4(B(T))^2}=\frac{Q(T)}{T^4}+\frac{\frac{44}{27}+\frac{23}{27}T}{B(T)}+\frac{\frac{7}{9}+\frac{5}{9}T}{(B(T))^2}$$

$$=-\frac{23}{27T}+\frac{25}{27T^2}-\frac{7}{9T^3}+\frac{4}{9T^4}+\frac{\frac{44}{27}+\frac{23}{27}T}{B(T)}+\frac{\frac{7}{9}+\frac{5}{9}T}{(B(T))^2}$$

وبالعودة إلى المتحوّل X نجد

$$\begin{aligned}F(X)=&-\frac{\frac{23}{27}}{X-1}+\frac{\frac{25}{27}}{(X-1)^2}-\frac{\frac{7}{9}}{(X-1)^2}+\frac{\frac{4}{9}}{(X-1)^2}\\&+\frac{\frac{7}{9}+\frac{23}{27}X}{X^2+X+1}+\frac{\frac{2}{9}+\frac{5}{9}X}{(X^2+X+1)^2}\end{aligned}$$

❿ حالة الكسر $F_n(X)=\sum_{k=0}^{n}\frac{k!}{X(X+1)\cdots(X+k)}$. نلاحظ أوّلاً أنّ

$$\frac{k!}{X(X+1)\cdots(X+k)}=\sum_{p=0}^{k}\frac{A_k^p}{X+p}$$

ونعيّن الثابت A_k^p بالعلاقة

$$\begin{aligned}A_k^p&=\left[(X+p)\frac{k!}{X(X+1)\cdots(X+k)}\right]_{X\leftarrow -p}\\&=\frac{k!}{(-p)(1-p)\cdots(-1)(1)(2)\cdots(k-p)}\\&=\frac{(-1)^p k!}{p!(k-p)!}=(-1)^p C_k^p\end{aligned}$$

إذن

$$\frac{k!}{X(X+1)\cdots(X+k)}=\sum_{p=0}^{k}\frac{(-1)^p C_k^p}{X+p}$$

ومن ثمّ

$$F_n(X)=\sum_{k=0}^{n}\frac{k!}{X(X+1)\cdots(X+k)}=\sum_{k=0}^{n}\left(\sum_{p=0}^{k}\frac{(-1)^pC_k^p}{X+p}\right)$$
$$=\sum_{0\le p\le k\le n}\frac{(-1)^pC_k^p}{X+p}=\sum_{p=0}^{n}\frac{(-1)^p}{X+p}\left(\sum_{k=p}^{n}C_k^p\right)$$

ولكن

$$\sum_{k=p}^{n}C_k^p=\sum_{k=p}^{n}\left(C_{k+1}^{p+1}-C_k^{p+1}\right)=C_{n+1}^{p+1}$$

إذن

$$F_n(X)=\sum_{p=0}^{n}\frac{(-1)^pC_{n+1}^{p+1}}{X+p}$$

وهي النتيجة المطلوبة.

التمرين 3. احسب المشتق من المرتبة n لكلٍ من الكسور العادية التالية من $\mathbb{C}(X)$:

$$\frac{1}{X(X+1)\cdots(X+m)},\quad \frac{1}{X^2-2\cos\alpha X+1},\quad \frac{1}{X^2-2\operatorname{sh}\alpha X-1}$$

الحل

❶ حالة الكسر $F_m(X)=\dfrac{1}{X(X+1)\cdots(X+m)}$. وجدنا في التمرين السابق أنّ

$$F_m(X)=\frac{1}{X(X+1)\cdots(X+m)}=\frac{1}{m!}\sum_{p=0}^{m}\frac{(-1)^pC_m^p}{X+p}$$

ومن ثمّ

$$F_m^{(n)}(X)=\frac{1}{m!}\sum_{p=0}^{m}(-1)^pC_m^p\left(\frac{1}{X+p}\right)^{(n)}$$
$$=\frac{n!}{m!}\sum_{p=0}^{m}\frac{(-1)^{p+n}C_m^p}{\left(X+p\right)^{n+1}}$$

❷ حالة الكسر $F(X)=\dfrac{1}{X^2-2\cos\alpha X+1}$ حيث $\alpha\in\,]0,\pi[$. من الواضح أنّ

$$F(X)=\frac{1}{(X-e^{\mathrm{i}\alpha})(X-e^{-\mathrm{i}\alpha})}=\frac{1}{2\mathrm{i}\sin\alpha}\left(\frac{1}{X-e^{\mathrm{i}\alpha}}-\frac{1}{X-e^{-\mathrm{i}\alpha}}\right)$$

ومن ثَمّ

$$\begin{aligned}F^{(n)}(X)&=\frac{1}{2\mathrm{i}\sin\alpha}\left(\left(\frac{1}{X-e^{\mathrm{i}\alpha}}\right)^{(n)}-\left(\frac{1}{X-e^{-\mathrm{i}\alpha}}\right)^{(n)}\right)\\&=\frac{1}{2\mathrm{i}\sin\alpha}\left(\frac{(-1)^n n!}{(X-e^{\mathrm{i}\alpha})^{n+1}}-\frac{(-1)^n n!}{(X-e^{-\mathrm{i}\alpha})^{n+1}}\right)\\&=\frac{(-1)^n n!}{2\mathrm{i}\sin\alpha}\left(\frac{(X-e^{-\mathrm{i}\alpha})^{n+1}-(X-e^{\mathrm{i}\alpha})^{n+1}}{(X^2-2\cos\alpha X+1)^{n+1}}\right)\end{aligned}$$

ولكن

$$(X-e^{-\mathrm{i}\alpha})^{n+1}-(X-e^{\mathrm{i}\alpha})^{n+1}=2\mathrm{i}\sum_{k=0}^{n+1}(-1)^k C_{n+1}^k(\sin k\alpha)X^{n+1-k}$$

إذن

$$F^{(n)}(X)=\frac{n!\cdot\sum_{k=1}^{n+1}(-1)^{n+1-k}C_{n+1}^k\dfrac{\sin k\alpha}{\sin\alpha}X^{n+1-k}}{(X^2-2\cos\alpha X+1)^{n+1}}$$

❸ حالة الكسر $F(X)=\dfrac{1}{X^2-2\operatorname{sh}\alpha X-1}$. من الواضح أنّ

$$F(X)=\frac{1}{(X-e^{\alpha})(X+e^{-\alpha})}=\frac{1}{2\operatorname{ch}\alpha}\left(\frac{1}{X-e^{\alpha}}-\frac{1}{X+e^{-\alpha}}\right)$$

ومن ثَمّ

$$\begin{aligned}F^{(n)}(X)&=\frac{1}{2\operatorname{ch}\alpha}\left(\left(\frac{1}{X-e^{\alpha}}\right)^{(n)}-\left(\frac{1}{X+e^{-\alpha}}\right)^{(n)}\right)\\&=\frac{1}{2\operatorname{ch}\alpha}\left(\frac{(-1)^n n!}{(X-e^{\alpha})^{n+1}}-\frac{(-1)^n n!}{(X+e^{-\alpha})^{n+1}}\right)\\&=\frac{(-1)^n n!}{2\operatorname{ch}\alpha}\left(\frac{(X+e^{-\alpha})^{n+1}-(X-e^{\alpha})^{n+1}}{(X^2-2\operatorname{sh}\alpha X-1)^{n+1}}\right)\end{aligned}$$

وهي النتيجة المرجوّة. ■

التمرين 4. بسّط كلّاً من الكسور العادية التالية:

$$\sum_{k=0}^{n}\frac{1}{(X+k)(X+k+1)},$$

$$\sum_{k=0}^{n}\frac{1}{(X+k)(X+k+1)(X+k+2)},$$

$$\sum_{k=0}^{n}\frac{2^k}{(X+2^k)(X+2^{k+1})},$$

الحل

❶ حالة المجموع $S_n(X)=\sum_{k=0}^{n}\frac{1}{(X+k)(X+k+1)}$. نلاحظ أنّ

$$\begin{aligned}S_n(X)&=\sum_{k=0}^{n}\left(\frac{1}{X+k}-\frac{1}{X+k+1}\right)\\&=\frac{1}{X}-\frac{1}{X+n+1}=\frac{n+1}{X(X+n+1)}\end{aligned}$$

❷ حالة المجموع $S_n(X)=\sum_{k=0}^{n}\frac{1}{(X+k)(X+k+1)(X+k+2)}$. نلاحظ أنّ

$$\begin{aligned}S_n(X)&=\frac{1}{2}\sum_{k=0}^{n}\left(\frac{1}{(X+k)(X+k+1)}-\frac{1}{(X+k+1)(X+k+2)}\right)\\&=\frac{1}{2}\left(\frac{1}{X(X+1)}-\frac{1}{(X+n+1)(X+n+2)}\right)\\&=\frac{2(n+1)X+(n+1)(n+2)}{2X(X+1)(X+n+1)(X+n+2)}\end{aligned}$$

❸ حالة المجموع $S_n(X)=\sum_{k=0}^{n}\frac{2^k}{(X+2^k)(X+2^{k+1})}$. نلاحظ أنّ

$$\begin{aligned}S_n(X)&=\sum_{k=0}^{n}\left(\frac{1}{X+2^k}-\frac{1}{X+2^{k+1}}\right)\\&=\frac{1}{X+1}-\frac{1}{X+2^{n+1}}=\frac{2^{n+1}-1}{(X+1)(X+2^{n+1})}\end{aligned}$$

وهي النتيجة المرجوّة.

التمرين 5. حلّل إلى عناصر بسيطة في $\mathbb{R}(X)$ الكسر العادي الآتي

$$F(X) = \frac{X^3 + 2X + 1}{(X-1)^2(X^2+1)^4}$$

الحل

نعرّف متحوّلاً جديداً $T = X^2 + 1$، ونلاحظ أنّ $(X+1)(X-1) = T - 2$، وأنّ

$$\begin{aligned}(X+1)^2(X^3+2X+1) &= (T+2X)(XT+X+1)\\ &= XT^2 + (2X^2+X+1)T + 2X^2 + 2X\\ &= XT^2 + (2T+X-1)T + 2T + 2X - 2\\ &= (X+2)T^2 + (X+1)T + 2(X-1)\end{aligned}$$

ومن ثمّ

$$F(X) = \frac{X^3+2X+1}{(X-1)^2(X^2+1)^4} = \frac{A_X(T)}{T^4(2-T)^2}$$

وقد عرّفنا $A_X(T) = (X+2)T^2 + (X+1)T + 2(X-1)$.

نُجري في $\mathbb{R}(X)[T]$ قسمة وفق القوى المتزايدة لكثير الحدود $A_X(T)$ على $(2-T)^2$ حتى المرتبة الثالثة فنجد أنّ

$$A_X(T) = (2-T)^2 Q_X(T) + T^4 R_X(T)$$

حيث

$$\begin{aligned}Q_X(T) &= \frac{X-1}{2} + \frac{3X-1}{4}T + \frac{7X+3}{8}T^2 + \frac{11X+7}{16}T^3\\ R_X(T) &= \frac{1}{16}\big((30X+22) - (11X+7)T\big) = \frac{15-11X}{16}(X+1)^2\end{aligned}$$

وعندئذ يكون لدينا

$$\begin{aligned}F(X) &= \frac{Q_X(T)}{T^4} + \frac{R_X(T)}{(2-T)^2}\\ &= \frac{1}{T^4}\left(\frac{X-1}{2} + \frac{3X-1}{4}T + \frac{7X+3}{8}T^2 + \frac{11X+7}{16}T^3\right) + \frac{1}{16}\cdot\frac{15-11X}{(X-1)^2}\end{aligned}$$

أو

$$F(X)=\frac{X-1}{2T^4}+\frac{3X-1}{4T^3}+\frac{7X+3}{8T^2}+\frac{11X+7}{16T}+\frac{1}{16}\cdot\frac{4-11(X-1)}{(X-1)^2}$$

وأخيراً

$$F(X)=\frac{\frac{1}{2}X-\frac{1}{2}}{(X^2+1)^4}+\frac{\frac{3}{4}X-\frac{1}{4}}{(X^2+1)^3}+\frac{\frac{7}{8}X+\frac{3}{8}}{(X^2+1)^2}+\frac{\frac{11}{16}X+\frac{7}{16}}{X^2+1}+\frac{\frac{1}{4}}{(X-1)^2}-\frac{\frac{11}{16}}{X-1}$$

وهي النتيجة المرجوّة. ■

التمرين 6. ليكن n من $\mathbb{N}^*$، وليكن k من $\mathbb{N}$. نضع $\alpha_k=\exp\left(\frac{2\,\mathrm{i}\,\pi k}{n}\right)$.

❖ تحقَّق أنّ

$$\sum_{k=1}^{n}\frac{1}{X-\alpha_k}=\frac{nX^{n-1}}{X^n-1}$$

وأنّ

$$\sum_{k=1}^{n}\frac{\alpha_k}{X-\alpha_k}=\frac{n}{X^n-1}$$

❖ اختصر المجموعين :

$F(X)=\sum_{k=1}^{n}\frac{X^3}{(X-\alpha_k)^2}$ و $G(X)=\sum_{k=1}^{n}\frac{X^2-\alpha_{k-2}X+\alpha_{k+2}}{(X-\alpha_k)^2}$.

الحل

❶ ليكن P كثير حدود من $\mathbb{C}[x]$ درجته أصغر تماماً من n. إنّ أقطاب الكسر $F(X)=\frac{P(X)}{X^n-1}$ هي الأعداد $\alpha_1,\ldots,\alpha_n$ وهي أقطاب بسيطة. إذن توجد أعداد $\lambda_1,\lambda_2,\ldots,\lambda_n$ في $\mathbb{C}$ تُحقّق

$$F(X)=\frac{P(X)}{X^n-1}=\sum_{k=1}^{n}\frac{\lambda_k}{X-\alpha_k}$$

ويتعيّن الثابتُ λ_k بالعلاقة $\lambda_k=\frac{P(\alpha_k)}{n\alpha_k^{n-1}}=\frac{1}{n}\alpha_k P(\alpha_k)$.

ومن ثَمَّ

$$\forall P \in \mathbb{C}[x], \quad \deg P < n \Rightarrow \frac{P(X)}{X^n - 1} = \frac{1}{n}\sum_{k=1}^{n}\frac{\alpha_k P(\alpha_k)}{X - \alpha_k}$$

وبأخذ $P(X) = nX^{n-1}$ و $P(X) = n$ نجد

$$\frac{nX^{n-1}}{X^n - 1} = \sum_{k=1}^{n}\frac{1}{X - \alpha_k}, \qquad \frac{n}{X^n - 1} = \sum_{k=1}^{n}\frac{\alpha_k}{X - \alpha_k}$$

❷ نلاحظ أنّ

$$\begin{aligned}F(X) &= \sum_{k=1}^{n}\frac{X^3}{(X - \alpha_k)^2} = -X^3\left(\sum_{k=1}^{n}\frac{1}{X - \alpha_k}\right)' \\ &= -X^3\left(\frac{nX^{n-1}}{X^n - 1}\right)' = \frac{n^2X^{2n+1} - n(n-1)X^{n+1}(X^n - 1)}{(X^n - 1)^2} \\ &= \frac{nX^{2n+1} + n(n-1)X^{n+1}}{(X^n - 1)^2}\end{aligned}$$

وأنّ

$$\begin{aligned}G(X) &= \sum_{k=1}^{n}\frac{X^2 - \alpha_{k-2}X + \alpha_{k+2}}{(X - \alpha_k)^2} \\ &= X^2 \cdot \sum_{k=1}^{n}\frac{1}{(X - \alpha_k)^2} + \left(\alpha_2 - \alpha_{-2}X\right)\cdot\sum_{k=1}^{n}\frac{\alpha_k}{(X - \alpha_k)^2} \\ &= -X^2\left(\sum_{k=1}^{n}\frac{1}{X - \alpha_k}\right)' - \left(\alpha_2 - \alpha_{-2}X\right)\left(\sum_{k=1}^{n}\frac{\alpha_k}{X - \alpha_k}\right)' \\ &= -X^2\left(\frac{nX^{n-1}}{X^n - 1}\right)' - \left(\alpha_2 - \alpha_{-2}X\right)\left(\frac{n}{X^n - 1}\right)' \\ &= n\frac{X^{2n} + (n - 1 - n\alpha_{-2})X^n + n\alpha_2X^{n-1}}{(X^n - 1)^2}\end{aligned}$$

وهي النتيجة المرجوّة. ∎

التمرين 7. أثبت أنّ كثير الحدود $P = X^3 - 2$ هو كثيرُ حدود غير خزول في $\mathbb{Q}[X]$. ثُمّ صِف الحقل $\mathbb{Q}[X]/(P)$. مبيّناً أنه يمكن تزويد المجموعة $\mathbb{Q}^3$ بقانوني تشكيل داخليين $\oplus$ و $\otimes$ بحيث يصبح التطبيق

$$\varphi : \mathbb{Q}^3 \to \mathbb{Q}[X]/(P), (a,b,c) \mapsto [a + bX + cX^2]$$

تشاكلاً تقابلياً حقلياً. كيف تحسب مقلوب عنصر غير صفري في الحقل $(\mathbb{Q}^3, \oplus, \otimes)$؟

الحل

❶ إنّ درجة كثير الحدود $P = X^3 - 2$ تساوي 3 فإذا كان خزولاً في $\mathbb{Q}[x]$ كان له قاسم من الدرجة الأولى في $\mathbb{Q}[x]$ ، وقَبِلَ، من ثَمّ، جذراً ρ ينتمي إلى $\mathbb{Q}$. وهذا يقتضي أن يكون العدد $\sqrt[3]{2}$ عدداً عاديّاً، وهذا خُلفٌ صارخٌ. إذن P كثير حدود غير خزول في $\mathbb{Q}\big[X\big]$.

❷ لنرمز بالرمز α إلى صف التكافؤ $[X]$ في الحقل $\mathbb{K} = \mathbb{Q}[X]/(P)$. عندئذ يكون لدينا بملاحظة أنّ $\alpha^3 = 2$ في $\mathbb{K}$ ما يلي :

$$(a + b\alpha + c\alpha^2)(a' + b'\alpha + c'\alpha^2) = A + B\alpha + C\alpha^2$$

حيث

$$\begin{aligned} A &= aa' + 2bc' + 2cb', \\ B &= ab' + ba' + 2cc', \\ C &= ac' + bb' + ca'. \end{aligned}$$

فإذا عرّفنا على $\mathbb{Q}^3$ قانوني التشكيل $\oplus$ و $\otimes$ بالعلاقتين :

$$(a,b,c) \oplus (a',b',c') = (a + a', b + b', c + c')$$
$$(a,b,c) \otimes (a',b',c') = (aa' + 2bc' + 2cb', ab' + ba' + 2cc', ac' + bb' + ca')$$

عرّفَ التطبيق

$$\varphi : \left(\mathbb{Q}^3, \oplus, \otimes\right) \to \mathbb{K}, (a,b,c) \mapsto a + b\alpha + c\alpha^2$$

تشاكلاً حقليّاً تقابليّاً.

ويُعطى $(a,b,c)^{-1}$ مقلوبُ العنصر (a,b,c) من $\mathbb{Q}^3 \backslash \{(0,0,0)\}$ بالعلاقة

$$\left(\frac{a^2 - 2bc}{a^3 + 2b^3 + 4c^3 - 6abc}, \frac{2c^2 - ab}{a^3 + 2b^3 + 4c^3 - 6abc}, \frac{b^2 - ac}{a^3 + 2b^3 + 4c^3 - 6abc}\right)$$

حيث نترك التحقُّق من ذلك تمريناً للقارئ. ■

التمرين 8. بيّن أنه في حقل منته $\mathbb{K}$ مختلف عن $\mathbb{F}_2$ يكون $\sum_{x\in\mathbb{K}} x = 0$.

الحل

لنفترض أنّ $q = \operatorname{card}(\mathbb{K})$. نعلم أنّ عناصر $\mathbb{K}$ هي جذور كثير الحدود $X^q - X$. ويساوي مجموع هذه الجذور نظير مَثَل X^{q-1} في كثير الحدود هذا. ولمّا كان $q-1>1$ لأنّ $\mathbb{K}\neq\mathbb{F}_2$ استنتجنا أنّ هذه الأمثال معدومة، أي $\sum_{x\in\mathbb{K}} x = 0$. ■

التمرين 9. ليكن a و b عنصرين من $\mathbb{F}_{2^n}$ و n عدد فرديّ. أثبت أنّ

$$a^2+ab+b^2=0 \Rightarrow a=b=0$$

الحل

ليكن a و b عنصرين من $\mathbb{F}_{2^n}$ يُحقّقان $a^2+ab+b^2=0$. ولنناقش الحالتين الآتيتين:

- في حالة $b \neq a$ ، يكون بالضرورة $b\neq 0$ ، لأنّ $b=0$ يقتضي $a^2=0$ ومن ثَمّ $a=0$ وهذا يناقض كون $a\neq b$. نعرّف إذن $x=ab^{-1}$ وهو عنصرٌ مختلفٌ عن 1 في $\mathbb{F}_{2^n}$ ويُحقّق استناداً إلى الفرض $x^2+x+1=0$ ومن ثَمّ يكون

$$x^3=1 \quad \text{و} \quad x\neq 1$$

إذن رتبة العنصر x في الزمرة الضربيّة $\mathbb{F}_{2^n}\backslash\{0\}$ تساوي 3 ، والعدد 3 يقسم 2^n-1 .

ولكن

$$(n \text{ عددٌ فردي}) \Rightarrow 2^n=(-1)^n=-1 \bmod 3$$

وهذا يناقض كون $2^n = 1 \bmod 3$. وهذه الحالة لا يمكن أن تقع.

- إذن لا بُدّ أن يكون $a=b$ فنستنتج عندئذ أنّ $3a^2=0$ ولأنّ العدد المميِّز للحقل $\mathbb{F}_{2^n}$ هو 2 نتج من ذلك أنّ $a^2=0$ ومنه يكون $a=b=0$. ■

التمرين 10. أثبت أنه إذا كان $\mathbb{K}=\mathbb{F}_{p^n}$ قَبِلَ كلُّ عنصر من $\mathbb{K}$ جذراً من المرتبة p .

الحل

في الحقيقة، إذا كان x عنصراً من $\mathbb{F}_{p^n}$ عرّفنا $y=x^{p^{n-1}}$. وعندئذ يكون $y^p=x^{p^n}=x$.

إذن y هو جذرٌ من المرتبة p للعنصر x . ■

التمرين 11. ليكن الحقل $\mathbb{F}_q = \mathbb{K}$ مع $q = p^n$ و p عدد أوليّ فرديّ. أثبت أن العنصر a من $\mathbb{K}^*$ يقبل جذراً تربيعياً إذا وفقط إذا كان $a^{(q-1)/2} = 1$.

الحل

- لنفترض أنّ العنصر a من $\mathbb{K}^*$ يقبل جذراً تربيعيّاً b، أي أنّ $a = b^2$. فيكون b عنصراً من $\mathbb{K}^*$، ويكون $a^{(q-1)/2} = b^{q-1} = 1$.
- وبالعكس، لمّا كانت $(\mathbb{K}^*,\cdot)$ زمرة دوّارة، اخترنا عنصراً z من $\mathbb{K}^*$ يكون مولّداً لهذه الزمرة. فيوجد k يُحقِّق $a = z^k$. ولمّا كان $a^{(q-1)/2} = 1$ كان $z^{k(q-1)/2} = 1$ أي إنّ $k(q-1)/2$ من مضاعفات رتبة z أي $q-1$. فلا بُدّ أن يكون k عدداً زوجيّاً: $k = 2\ell$. والعدد $b = z^\ell$ جذرٌ تربيعيٌّ للعدد a. ■

التمرين 12. ليكن الحقل $\mathbb{K} = \mathbb{F}_q$ حيث $q = p^n$ و p عدد أوليّ، وليكن k من $\mathbb{N}^*$ و a من $\mathbb{K}^*$. أثبت صحة التكافؤ

$$\left(\exists b \in \mathbb{K}^*,\;\; a = b^k\right) \Leftrightarrow a^{(q-1)/d} = 1$$

وقد عرّفنا $d = \gcd(q-1, k)$.

الحل

لمّا كان $d = \gcd(q-1, k)$ استنتجنا أنّ $q - 1 = d\lambda$ و $k = d\ell$ حيث $\gcd(\lambda, \ell) = 1$.

- لنفترض أنّ العنصر a من $\mathbb{K}^*$ يقبل جذراً b من المرتبة k، أي إنّ $a = b^k$. فيكون b عنصراً من $\mathbb{K}^*$، ويكون $a^{(q-1)/d} = b^{k\lambda} = b^{d\ell\lambda} = (b^{q-1})^\ell = 1$.
- وبالعكس، لمّا كانت $(\mathbb{K}^*,\cdot)$ زمرة دوّارة، اخترنا عنصراً z من $\mathbb{K}^*$ يكون مولّداً لهذه الزمرة. فيوجد r يُحقِّق $a = z^r$. ولمّا كان $a^{(q-1)/d} = 1$ كان $z^{r\lambda} = 1$ أي إنّ $r\lambda$ من مضاعفات رتبة z أي $q - 1 = d\lambda$. وعليه يوجد عدد r' يُحقّق $r = dr'$. وعليه $a = z^{dr'}$.

ولكن، $d = \gcd(q-1, k)$ إذن يوجد u و v يُحقّقان $d = vk + u(q-1)$ ومن ثَمّ $z^d = z^{vk}(z^{q-1})^u = z^{vk}$. وعليه يكون $a = z^{dr'} = z^{vkr'} = (z^{vr'})^k$ والعدد $b = z^{vr'}$ جذرٌ من المرتبة k للعدد a. ■

التمرين 13. ليكن الحقل $\mathbb{K}=\mathbb{F}_q$ حيث $q=p^n$ و p عدد أوليّ، وليكن k من $\mathbb{N}^*$.

أثبت صحة التكافؤ

$$(\forall a\in\mathbb{K}^*,\exists b\in\mathbb{K}^*,\ a=b^k)\Leftrightarrow \gcd(q-1,k)=1$$

الحل

لنضع $d=\gcd(q-1,k)$. بالاستفادة من التمرين السابق لدينا

$$\left(\forall a\in\mathbb{K}^*,\exists b\in\mathbb{K}^*,\ a=b^k\right)\Leftrightarrow\left(\forall a\in\mathbb{K}^*,\ a^{(q-1)/d}=1\right)$$

- فإذا كان $d=1$ تحقَّق الشرط $\forall a\in\mathbb{K}^*, a^{q-1}=1$ لأنّ رتبة الزمرة $(\mathbb{K}^*,\cdot)$ هي $q-1$.
- وإذا كان $\forall a\in\mathbb{K}^*,\ a^{(q-1)/d}=1$، اخترنا a أيّ مولِّد للزمرة الدوّارة $(\mathbb{K}^*,\cdot)$، فنستنتج من الخاصّة السابقة أنّ العدد $(q-1)/d$ هو أحد مضاعفات العدد $q-1$، ومن ثَمّ أنّ $d=1$.

بذا نكون قد أثبتنا التكافؤ المطلوب. ■

التمرين 14. أثبت أنّ $\mathbb{F}_{p^m}$ حقل جزئيّ من $\mathbb{F}_{p^n}$ إذا وفقط إذا كان m يقسم n.

الحل

- إذا كان $\mathbb{F}_{p^m}$ حقلاً جزئيّاً من $\mathbb{F}_{p^n}$ كانت الزمرة $(\mathbb{F}_{p^m}^*,\cdot)$ زمرة جزئيّة من $(\mathbb{F}_{p^n}^*,\cdot)$ وكان من ثَمّ p^m-1 قاسماً للعدد p^n-1 ولا بُدَّ أن يكون $m\mid n$.
- وبالعكس، لنفترض أنّ $m\mid n$ عندئذ يقسم كثيرُ الحدود $X^{p^m}-X$ كثيرَ الحدود $X^{p^n}-X$. إذن تنتمي جميع جذور $X^{p^m}-X$ إلى الحقل $\mathbb{F}_{p^n}$. فالحقل $\mathbb{F}_{p^m}$ حقلٌ جزئي من $\mathbb{F}_{p^n}$. ■

التمرين 15. أثبت أنّ X^4+X^3+1 كثير حدود غير خزول في $\mathbb{F}_2[X]$، واستعمله لإنشاء $\mathbb{F}_{16}$، معيّناً جداول الجمع والضرب في $\mathbb{F}_{16}$ بعد أن تقترح تمثيلاً مُناسباً لعناصره.

الحل

- من الواضح أن ليس لكثير الحدود $P(X) = X^4 + X^3 + 1$ جذورٌ في $\mathbb{F}_2$. فإذا كان خزولاً وجب أن يُكتب جداءَ كثيري حدود غير خزولَين من الدرجة الثانية. ولكن في $\mathbb{F}_2[x]$ هناك كثير حدود غير خزول وحيد من الدرجة الثانية هو $X^2 + X + 1$. وعليه إذا كان $P(X)$ خزولاً وجب أن يكون
$$P(X) = (X^2 + X + 1)^2 = X^4 + X^2 + 1$$
وهذا خُلفٌ. إذن لا بُدَّ أن يكون $P(X)$ غير خزول في $\mathbb{F}_2[x]$.

- إذن $\mathbb{F}_2[x]/(P)$ حقلٌ عددُ عناصره 16 وبسبب الوحدانيّة يكون $\mathbb{F}_{16} = \mathbb{F}_2[x]/(P)$.

- ليكن α صفّ تكافؤ $[x]$ في $\mathbb{F}_{16} = \mathbb{F}_2[x]/(P)$. ولنحسب رتبة العنصر α في الزمرة $(\mathbb{F}_{16}^*, \cdot)$ التي عدد عناصرها 15. في الحقيقة، لدينا

k	α^k
0	1
1	α
2	α^2
3	α^3
4	$1+\alpha^3$
5	$1+\alpha+\alpha^3$
6	$1+\alpha+\alpha^2+\alpha^3$
7	$1+\alpha+\alpha^2$

k	α^k
8	$\alpha+\alpha^2+\alpha^3$
9	$1+\alpha^2$
10	$\alpha+\alpha^3$
11	$1+\alpha^2+\alpha^3$
12	$1+\alpha$
13	$\alpha+\alpha^2$
14	$\alpha^2+\alpha^3$

فالعنصر α يولِّد الزمرة الضربيّة $(\mathbb{F}_{16}^*, \cdot)$. ويمكن تمثيل عناصر الحقل $\mathbb{F}_{16}$ بالمجموعة
$$\left\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\right\}$$
وفي هذا التمثيل يكون
$$0 \times x = 0 \text{ و } \alpha^k \times \alpha^\ell = \alpha^{(k+\ell) \bmod 15}.$$

أمّا قانون الجمع فهو مبيَّن في الجدول التالي :

$+$	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
0	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
1	1	0	α^{12}	α^9	α^4	α^3	α^{10}	α^8	α^{13}	α^6	α^2	α^5	α^{14}	α	α^7	α^{11}
α	α	α^{12}	0	α^{13}	α^{10}	α^5	α^4	α^{11}	α^9	α^{14}	α^7	α^3	α^6	1	α^2	α^8
α^2	α^2	α^9	α^{13}	0	α^{14}	α^{11}	α^6	α^5	α^{12}	α^{10}	1	α^8	α^4	α^7	α^9	α^3
α^3	α^3	α^4	α^{10}	α^{14}	0	1	α^{12}	α^7	α^6	α^{13}	α^{11}	α	α^9	α^5	α^8	α^2
α^4	α^4	α^3	α^5	α^{11}	1	0	α	α^{13}	α^8	α^7	α^{14}	α^{12}	α^2	α^{10}	α^6	α^9
α^5	α^5	α^{10}	α^4	α^6	α^{12}	α	0	α^2	α^{14}	α^9	α^8	1	α^{13}	α^3	α^{11}	α^7
α^6	α^6	α^8	α^{11}	α^5	α^7	α^{13}	α^2	0	α^3	1	α^{10}	α^9	α	α^{14}	α^4	α^{12}
α^7	α^7	α^{13}	α^9	α^{12}	α^6	α^8	α^{14}	α^3	0	α^4	α	α^{11}	α^{10}	α^2	1	α^5
α^8	α^8	α^6	α^{14}	α^{10}	α^{13}	α^7	α^9	1	α^4	0	α^5	α^2	α^{12}	α^{11}	α^3	α
α^9	α^9	α^2	α^7	1	α^{11}	α^{14}	α^8	α^{10}	α	α^5	0	α^6	α^3	α^{13}	α^{12}	α^4
α^{10}	α^{10}	α^5	α^3	α^8	α	α^{12}	1	α^9	α^{11}	α^2	α^6	0	α^7	α^4	α^{14}	α^{13}
α^{11}	α^{11}	α^{14}	α^6	α^4	α^9	α^2	α^{13}	α	α^{10}	α^{12}	α^3	α^7	0	α^8	α^5	1
α^{12}	α^{12}	α	1	α^7	α^5	α^{10}	α^3	α^{14}	α^2	α^{11}	α^{13}	α^4	α^8	0	α^9	α^6
α^{13}	α^{13}	α^7	α^2	α^9	α^8	α^6	α^{11}	α^4	1	α^3	α^{12}	α^{14}	α^5	α^9	0	α^{10}
α^{14}	α^{14}	α^{11}	α^8	α^3	α^2	α^9	α^7	α^{12}	α^5	α	α^4	α^{13}	1	α^6	α^{10}	0

وهذا التمثيل مناسبٌ لإجراء عمليّة الضرب أكثر منه لإجراء عمليّة الجمع. ■

دليل مفردات الجزء الأوّل

يشير الرقم إلى الصفحة التي يظهر فيها المفهوم المشار إليه ظهوراً معنوياً.

احتلَّ الدكتور عمران قوبا المركز الثاني في مسابقة انتقاء أساتذة التعليم العالي على مستوى الجمهورية الفرنسية "أغرغاسيون" في عام 1985، وحصل على شهادة الدكتوراه في الرياضيات البحتة في اختصاص التحليل التابعي من جامعة بيير وماري كوري في باريس عام 1990.

يدرّس الدكتور قوبا الرياضيات في المعهد العالي للعلوم التطبيقية والتكنولوجيا منذ عام 1990. وقد وضع في هذه السلسلة من الكتب العلميّة أغلب الموضوعات التي درّسها في المعهد العالي في مجالات الجبر العام، والجبر الخطّي، والتحليل، والمعادلات التفاضلية، والتحليل العقدي، والتحويلات التكامليَّة وغيرها، وقد أغنى السلسلة بالعديد من الأمثلة والتطبيقات والمسائل والتمرينات.

تمثّل هذه السلسلة أداة مهمّة لكلِّ الراغبين في دراسة الرياضيّات بصفتها علماً وفنّاً قائمَيْن بذاتهما، أو لأولئك الراغبين في استعمال الرياضيّات بصفتها أداة مهمّة ومفيدة في جميع العلوم الحديثة.

في هذا الجزء الأوّل من سلسلة الجبر، يبدأ القارئ بدراسة مقدمات في المنطق الرياضي ولغة المجموعات، والبنى الجبرية من زمر وحلقات وحقول، حقل الأعداد العقدية، وحلقة الأعداد الصحيحة، وحلقة كثيرات الحدود، ومقدمات في نظرية الحقول.

ISBN 978-9933-9228-9-4

المعهد العالي للعلوم التطبيقية والتكنولوجيا
Higher Institute for Applied Sciences and Technology
www.hiast.edu.sy