نظرية جالــوا

تأليف

أيــان ســتيوارت
أستاذ مشارك - معهد الرياضيات،
جامعة واريك، كوفنتري

ترجمـة

الدكتور معروف عبدالرحمن سمحان و الدكتور فوزى أحمد الذكير
قسم الرياضيات - كلية العلوم
جامعة الملك سعود

النـشـر الـعـلـمـي والمطـابـع - جـامـعـة الملـك سـعـود
ص.ب ٢٤٥٤ الرياض ١١٤٥١ - المملكة العربية السعودية

مقدمة المترجمين

إن اختيارنا لترجمة كتاب في موضوع نظريّة جالوا كان بسبب عدم توافر كتاب – حسب معرفتنا – مؤلف أو مترجم يغطي هذه المادة المهمة والشيّقة في الرياضيات . ونظرية جالوا تعتبر مثالاً ممتازًا للنظرية الحديثة لوحدة الرياضيّات ، فمن خلالها تستخدم خصائص الحقول والزُمَر في مجال البنى الجبرية لحل مسائل في نظرية المعادلات الكلاسيكية . وقد اكتسبت نظرية جالوا أهمية خاصة في العقود القريبة عندما ظهرت استخدامات نظرية امتدادات الحقول المنتهية في علميْ التشفير والتعمية المستخدمين بصورة واسعة في مجال الاتصالات . وبالإضافة إلى ما تقدم يوجد سبب تاريخي يجعلنا نهتم بترجمة كتاب في موضوع نظرية جالوا ، وهو كون هذا الموضوع امتدادًا لجهود العلماء العرب والمسلمين في عصور نهضتنا الحضارية في مجال حل المعادلات الجبرية ، أمثال الخوارزمي وابن الهيثم وعمر الخيام .

تتوافر كتب عديدة في موضوع نظرية جالوا ، ولكن إعجابنا بكتاب Ian Stewart الذي بين أيدينا يرجع لعدة أسباب منها :

١ ـ اهتمام المؤلف بالناحية التاريخية لتطوّر الموضوع ومعالجته للأفكار بتدرج طبيعي يعطي القاريء فكرة عن كيفية توصل جالوا وغيره إلى بعض النتائج المدرجة في الكتاب .

٢ ـ اعتماد المؤلف أسلوب العرض العفوي (غير الرسمي) مما يجعل الموضوع أكثر تشويقاً للقاريء .

والنقطة الأخيرة أعلاه ميزة للكتاب ولكنها جعلت ترجمته أكثر صعوبة ، حيث إن المؤلف استعمل عبارات وكلمات دارجة وعامية في بعض الأحيان ، مما يجعل

ترجمتها صعبة . ويجدر بنا أن نذكر هنا أننا حاولنا أن تكون ترجمتنا للأفكار وليست ترجمة حرفية، متوخين في ذلك الدقة في نقل ما يقصده المؤلف خاصة في مقدمات الأبواب وفي تعليقه على النتائج الرياضية .

إن كتاب «نظرية جالوا» يصلح كمرجع أو كتاب مقرر لتدريس مادة نظرية جالوا في السنة الأخيرة من مرحلة البكالوريوس أو في أثناء الدراسات العليا لطالب الرياضيات . نأمل أن نكون قد وُفقنا في إضافة عمل مفيد إلى المكتبة العربية العلمية، راجين أن يستفيد منه كل من يهتم بهذه المادة . ونود أن نتقدم بالشكر والتقدير للمحكمين لتقديمهم العديد من المقترحات القيمة واكتشافهم للكثير من الأخطاء المطبعية . والله من وراء القصد .

المترجمان

د . معروف بن عبدالرحمن سمحان

د . فوزي بن أحمد الذكير

المحتويات

صفحة

شكر وعرفان على بعض الصور والأشكال

لقد أعيد طبع الصور التوضيحية التالية بموافقة مصادرها

الأشكال ١ ، ٦ ، ٧ - ٩ ، ١٠ و ٢٠ من كتاب

Ecrits et Memoires Mathematiques d'Evariste Galois, Robert Bourgne and J. P. Azra, Gauthier-Villars, paris 1962

الشكل ٢٣ من

Carl Friedrich Gauss: Verke, Vol X, George Olms Verlag, Hildesheim and New York 1973

الشكل ٤ من

History of Mathematics, David Eugene Smith, Dover Publishing Inc., New York 1951

الشكل ٢٢ من

York and A source Book in Mathematics, David Eugene Smith, McGraw-Hill, New Lodon 1929 .

الشكلان ٣ و ٥ من

The History of Mathematics: an Introduction, David M. Burton, Allyn and Bacon Inc., Boston 1985.

مقدمة الطبعة الأولى

تعتبر نظرية جالوا أنموذجًا تتجلى فيه وحدة علم الرياضيات ، من خلالها تتعاضد فروع مختلفة من الرياضيات لتكون وسيلة فاعلة لدراسة مسائل مهمة تاريخيًا ورياضيًا . إن هذا الكتاب هو محاولة لإبراز نظرية جالوا في هذا الضوء وبأسلوب مناسب لطلاب السنة الثانية والثالثة من مرحلة البكالوريوس (في الجامعات البريطانية) .

يعتبر تطبيق زمرة جالوا على المعادلة من الدرجة الخامسة الخط الأساسي للموضوع ، بالإضافة إلى الطريقة التقليدية عن طريق معادلة كثيرة الحدود العامة ، وهي طريقة مباشرة أشعر بأنها أكثر إقناعًا إذ أوضحت عدم قابلية الحل عن طريق الجذر لمعادلات خاصة من الدرجة الخامسة (معاملاتها أعداد صحيحة) . وقُدّمت نظرية جالوا التجريدية في سياق امتداد الحقول الاختيارية ، بدلاً من الحقول الجزئية للأعداد المركبة ، إن الفائدة من هذا الأسلوب تعوض - بل تزيد على ذلك - عن العمل الإضافي المطلوب . من المواضيع الأخرى المعطاة هي : مسائل مضاعفة المكعب ، تثليث الزاوية ، وتربيع الدائرة ، كذلك إنشاء المضلعات المنتظمة ، حل المعادلات التكعيبية والرباعية ، بناء الحقول المنتهية و «النظرية الأساسية في الجبر» والتي تبرهنها طرق معظمها جبرية بحتة و تعتبر تطبيقًا شيقًا لنظرية سايلو .

لم ألتزم بالمسار الرئيسي للموضوع في بعض الأحيان حرصًا منّا على أن يكون الكتاب جامعاً لكل ما تتطلبه مادته؟ ومن أهم الأمثلة على ذلك برهان تسامي العدد π والذي يجب أن يراه كل مختص في الرياضيات مرة واحدة على الأقل في

حياتــه . وقد ناقشت أعداد فيرما لأبين أن مسألة المضلّعات المنتظمة ليست محلولة تمامًا، بالرغم من اختزالها إلى مسألة تبدو بسيطة ظاهريًا في نظرية الاعداد . وقدمت طريقة لإنشاء ذي سبعة عشر ضلعًا على أساس أن حل مسألة المضلعات المنتظمة يتطلب أكثر من مجرد برهان لكون النتيجة غير محسوسة .

إنّ الدافع الرئيسي لمادة الكتاب ذو جذور تاريخية، مما جعلني أُضَمِّن بعض الملاحظات التاريخية أثناء الشرح ، كلما استدعى الأمر ذلك. وهناك بندان ذوا محتوى تاريخي بحت ؛ أحدهما : لمحة تاريخية لكثيرات الحدود ، والآخر حول حياة افرست جالوا (Evariste Galios) وقد استقيته من مصادر مختلفة (انظر قائمة المراجع)، ومن أهمها وأكثرها فائدة مقالة دوبوي[Dupuy (1896)] .

ولقد حاولت تقديم أمثلة كثيرة أثناء الشرح لتوضيح النظرية العامة، وأفردت بابًا بأكمله لدراسة مفصلة لزُمرة جالوا لامتداد حقلي معيّن. ويوجد ما يقرب من مائتي تمرين ، فضلاً عن عشرين تمرينًا أكثر صعوبة للطلاّب المتقدمين في المستوى .

وأخيرًا أود أن أشكر العديد ممن ساعدوني ونصحوني، وأثروا بي أثناء تأليفي لهذا الكتاب . أشكر منهم على وجه الخصوص رولف شوارتزنبرجر (Rolf Schwarzenberger) و ديفد تول (David Tall) اللذين قرآ مسودات متتابعة من الكتاب . كذلك أشكـــر لين بولمـــر (Len Bulmer) وهيئة مكتبة جامعة وورك (Warwick) لمساعدتهم لي في الحصول على الوثائق المتعلقة بالجزء التاريخي من الموضوع . كما أشكر روني براون (Ronnie Brown) لنصائحه القيّمة ولإرشاداته في التحرير، وأشكر أيضًا المحكّم الذي بيّن لي العديد من الهفوات والزلاّت، والذي سيبقى اسمه أبداً سراً لا أستطيع أن أعرفه بفضل نظام النشر، والذي لولاه لوقع المحكمون في خطر ردود الفعل الغاضبة من المؤلفين .

أيــان ســـتيورات

جامعة وورك - كوفنتري

(إبريل ١٩٧٢م)

مقدمة الطبعة الثانية

لقد مضى ستة عشر عامًا على صدور الطبعة الأولى من كتابي «نظرية جالوا» . ونظرية جالوا الكلاسيكية ليست بالموضوع الذي يمر بتطورات هائلة . لذا فإن أغلب محتوى الطبعة الأولى بقي في هذه الطبعة دون تغيير . ومع ذلك فقد قمت باجراء بعض اللمسات الجمالية والتغييرات الطفيفة ، والتي من شأنها إعادة الشباب للطبعة الأولى .

وأهم التغييرات في هذه الطبعة هي اضافة لمحة عامة عن الموضوع في البداية وباب لحساب زُمَر جالوا ، كما أضفت بعض الأمثلة المحفزة ، وعدّلت بعض التمارين ، وقمت بتصحيح الأخطاء المطبعية التي تمّ استدراكها ، ولكن قد توجد أخطاء جديدة في هذه الطبعة لأن حروفها صفت من جديد ، لذا فإني أدعو القاريء أن يكتشفها بصبره وفطنته . كما طرأت بعض التعديلات على المقدمة التاريخية بناءً على بعض الحقائق المكتشفة مؤخرًا ، ولقد سمح لي الناشر بإضافة ما كنت آمل عمله بالطبعة الأولى ، وهو تضمين صور من مخطوطات جالوا وبعض الصور التاريخية . وقد أجريت بعض التعديلات في البراهين الرياضية أيضاحا لها أو لتصحيح أخطاء فيها وهو قليل . وحذفت بعض المواد التي أعتقد أنها زائدة ، كما حاولت المحافظة على الطريقة العفوية (غير الرسمية) في عرض المادة كما في الطبعة الأولى ، والتي تعتبر الميزة الأولى لهذا الكتاب في رأي العديد من القراء .

وقد استفدت من تعاون العديد من الجهات معي عند إعداد هذه الطبعة ، فلقد وردت إليّ قوائم بأخطاء مطبعية وأخرى رياضية من كل من ستيفن باربر (Stephen Barber) ، أون برسن (Owen Brison) ، بوب كوتس (Bob Coates) ، فيليب هجنز

(Philip Higgins)، ديفيد هولدن (David Holden) ، فرانس أوورت (Frans Oort) ، مايلز ريد (Miles Reid) و س . ف . رايت (C. F. Wright) . وقد استعملت الجامعة المفتوحة (open university) الطبعة الأولى ككتاب أساسي لمقرر M 333 وأرسل إليّ العديد من أعضاء قسم الرياضيات في الجامعة نسخاً من الدروس التي لا تخلو من الأخطاء فأشكرهم وطلاّبهم الذين كانوا حقل تجارب وأعترف لهم بجميلهم .

أيان ستيوارت
جامعة وورك - كوفنتري
(ديسمبر ١٩٨٨م)

ملاحظات للقارئ

لقد رقمت كلاً من النظريات ، والتمهيديات ، والقضايا ،والنتائج وأمثالها تباعًا داخل كل فصل من فصول الكتاب . والرقم المستعمل على الهيئة (ن ، م) ، حيث م هو رقم الفصل و ن الترتيب داخل الفصل .

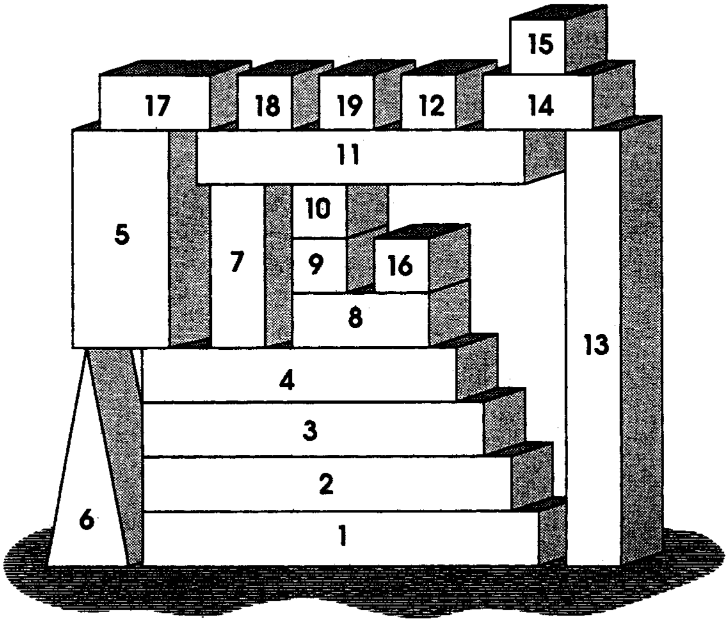
والتمارين في نهاية كل فصل (هناك استثناءان) وترقيمها مشابه لما ذكر أعلاه . وبالنسبة للتمارين الصعبة ميزتها بالإشارة (*) ،كما وضعت حلولاً لبعض التمارين خاصةً القصيرة منها .

وتتمز التعاريف في معظم الأحيان بكلمة **تعريف** بالخط العريض . وبالنسبة للمعادلات التي نحتاج الإشارة إليها فيما بعد فترقم على اليسار بالأسلوب (ن ، م) المشروح أعلاه حيث يبدأ الترقيم من جديد لكل فصل . أما المراجع فلقد وضعتها في نهاية الكتاب ،وهي على الهيئة [William (1066)] .

بناء الكتاب

كل طابوقة (في الشكل ٢) تمثل فصلاً من فصول الكتاب . أما ترابط الفصول ببعضها البعض فهو الترابط المعهود لضمان بقاء البناء قائمًا .

أنصح بالفصول من ١ – ٤ ، من ٧ – ١١ ، ومن ١٣ ـ ١٤ لتقديم مقرر قصير يرمي إلى بيان عدم وجود صيغة لجذور المعادلة من الدرجة الخامسة ، وكبديل لذلك يمكن حذف البند الثالث من الفصل ١٣ مع النصف الأخير من الفصل ١٤ والاستعاضة عن ذلك بالفصل ١٥ .



شكل (٢). بناء الكتاب وفيه كل فصل يعتمد على الفصول التي تسنده .

مقدمـــة تاريخية

إنّ تاريخ معادلات كثيرات الحدود يمتد لفترة طويلة ، فأحد الجداول البابليّة في حوالي ١٦٠٠ ق . م . يثير مسائل يمكن اختزالها إلى حل معادلات تربيعيّة [Midonick, 1965, p. 48] ومن الواضح أن البابليين قد عرفوا طرقًا لحل هذه المعادلات [Bourbaki, 1969, p. 92] وذلك بالرغم من عدم امتلاكهم لأي رموز جبرية يستعينون بها في التعبير عن الحلول . وقد قام الاغريق القدماء بحل المعادلات التربيعية باستخدام الانشاءات الهندسية ، ولكن لم يكن هناك أثر لأي صياغة جبرية إلى العام ١٠٠ م على الأقل [Bourbaki, 1969] . كما قـدم الاغريق طرقًـا لحـل المعـادلات التكعيبية باستخدام نقط تقاطع القطوع المخروطية . وبقيت الطرق الجبرية لحل المعادلات التكعيبية غير معروفة ، وفي عام ١٤٩٤م ذكر باسيولي (Pacioli) في نهاية كتابه (Summa di Arithmetica) (مجمع الحساب ، الشكل ٣) بأن حل المعادلتين :

$$x^3 + mx = n \quad \text{و} \quad x^3 + n = mx$$

هو مسألة تشابه في صعوبتها حل مسألة تربيع الدائرة المستعصية الحل آنذاك .

اكتشف رياضيّو عصر النهضة في بولونيا أن مسألة المعادلة التكعيبية يمكن أن تختزل إلى حل أحد الأنواع الرئيسية الثلاثة :

$$x^3 + px = q \quad ، \quad x^3 = px + q \quad ، \quad x^3 + q = px$$

إنّ فصلهم لهذه الحالات عن بعضها البعض يعود إلى عدم اعترافهم بوجود الأعـداد السالبـة . ويبـدو أن سسيبيـو دل فيرو (Scipio del Ferro) وبتوثيق جيد (Bortolotti, 1925) قد حل كل المعادلات الثلاث أعلاه ، ومن المؤكد أنه قد علّم أحد تلامذته فيور (Fior) طريقة حل إحداها . وقد انتشر خبر حل هذه المعـادلات مما شجع البعض لتجربة طرقهم في الحل . وقد تمّ اكتشاف الحلول مرة أخرى بواسطة نيكولو فونتانا

شكل (٣). صفحة من كتاب *Summa di Arithmetica* جامع الحساب لمؤلفه باسيولي.

(Niccolo Fontan) (ويدعى كذلك Tartaglia الشكل ٤) في العام ١٥٣٥م. وقد بيّن فونتانا طريقته في منافسة عامة مع فيور لكنه رفض إفشاء أي تفاصيل عنها. أخيراً تم اقناعه بأن يعطي تفاصيل الحل إلى الطبيب جيرولامو كاردانو (Girolamo Cardano) بعد أن حصل منه على قسم بكتمانها. لكن كاردانو لم يحفظ قسمه، وعمد إلى كتابة الحل بتفاصيله في كتابه (Ars Magna) الذي ظهر في ١٥٤٥م مع إقراره بأن فونتانا هو مكتشف الحل. وقد ادّعى كاردانو [cardano, 1931] بأنه كان لديه حوافز قوية للوصول إلى الحل مما أزعج فونتانا، وأدّى ذلك إلى العديد من المشاجرات التي جعلت تاريخ هذا الاكتشاف معروفًا للجميع.

شكل (٤). نيكوفوفونتانا (المعروف باسم تارجاليا) Niccolo Fontana (Targalia) مكتشف حل ا لمعادلات التكعيبية.

وهناك طريقة لحل معادلة الدرجة الرابعة عن طريق اختزالها إلى معادلة تكعيبيّة تعود إلى لودوفيكو فيراري (Ludovic Ferrari)، وقد ضمّنها كتاب (Ars Magna) الذي تظهر إحدى صفحاته في شكل (٥) .

HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inscripsit, est in ordine Decimus.

شكل (٥) . صفحة العنوان من كتاب *Ars Magna* لمؤلفه كاردانو .

وهناك خاصية مشتركة لكل الصيغ المكتشفة آنذاك . ويمكن توضيح ذلك من خلال طريقة فونتانا لحل المعادلة :

$$x^3 + px = q$$

وهذا الحل هو :

$$x = \sqrt[3]{\left[\frac{q}{3} + \sqrt{\left(\frac{p^3}{27} + \frac{q^2}{4}\right)}\right]} + \sqrt[3]{\left[\frac{q}{2} - \sqrt{\left(\frac{p^3}{27} + \frac{q^2}{4}\right)}\right]}$$

إنّ الصيغة أعلاه مكوّنة من المعاملات، وذلك بتكرار عمليّات الجمع ، الطرح، الضرب ، القسمة واستخلاص الجذور . إن مثل هذه الصيغة عُرفت باسم الصيغة الجذرية (العبارة الجذرية). ولما كانت جميع المعادلات من الدرجة الرابعة فما دون قد حلّت، فإنّه من الطبيعي السؤال عن كيفية حلّ المعادلة من الدرجة الخامسة عن طريق إيجاد صيغة جذرية لها .

لقد حاول العديد من الرياضيين حل المسألة، ومنهم شرنهاوس (Tschirnhaus) الذي ادّعى حلها ، ولكن لايبنز (Leibnitz) بّين خطأ الادعاء . وحاول أويلر(Euler) حل المسألة ولكنه لم ينجح في ذلك ، إلا أنه اكتشف طريقة جديدة لحل المعادلات الرباعية . وفي عام ١٧٧٠م خطا لاجرانج (Lagrange) خطوة مهمة بإيجاده أسلوبًا يجمع كل الحيل الرياضية التي كانت تستعمل لحل المعادلات من الدرجة الرابعة وما دونها. وقد تبّين أن كل الحيل تعتمد على إيجاد دوال من جذور المعادلات، لا تتغير قيمها عند تبديل مواقع الجذور في صيغة الدوال ، وقد بّين أن هذا الأسلوب لا يصلح في حل المعادلة الخماسية (الدرجة الخامسة) . مما تولد عنه شعور بعدم إمكانية حل معادلة الدرجة الخامسة باستخلاص الجذور ، وحاول روفيني (Ruffini) عام ١٨١٣م أن يبرهن على استحالة الحل، ولقد ظهربحثه في مجلة مغمورة ،وكان برهانه فيها ناقصًا [Bourbaki, p. 103] ولم يثر انتباه أحد. تمّ حل المسألة نهائيًا من قبل أبل (Abel) في عام ١٨٤٢م إذ برهن على استحالة حل المعادلة الخماسية باستخلاص الجذور .

وبرزت بعد ذلك مسألة إيجاد طريقة يمكننا بواسطتها الحكم على إمكانية حلّ

معادلة معطاة ، باستخلاص الجذور . وقد اشتغل عليها أبل إلى أن مات في عام ١٨٢٩م. وفي عام ١٨٣٢م قُتِلَ شاب فرنسي يدعى إفرست جالوا (Evariste Galois) في منازلة (مبارزة) . وقد سعى هذا الشاب لبعض الوقت إلى الحصول على اعتراف بنظرياته الرياضية ، عندما أرسل ثلاث مذكرات إلى أكاديمية العلوم في باريس ، ولكنها رُفضت جميعًا ، وبدا أنّ عمله قد تلاشى عن عالم الرياضيات آنذاك . وبعد ذلك ، وفي ٤ يوليو (تموز) ١٨٤٣م كتب جوزيف ليوفيل (Joseph LiouVille) إلى الاكاديمية مفتتحًا خطابه بما يلي :

آمل أن أجلب انتباه الأكاديمية بالإعلان عن وجود حل دقيق وعميق للمسألة الشيّقة : إمكانية أو عدم إمكانية حل المعادلات بطريقة الجذور وذلك ضمن أوراق إفرست جالوا .

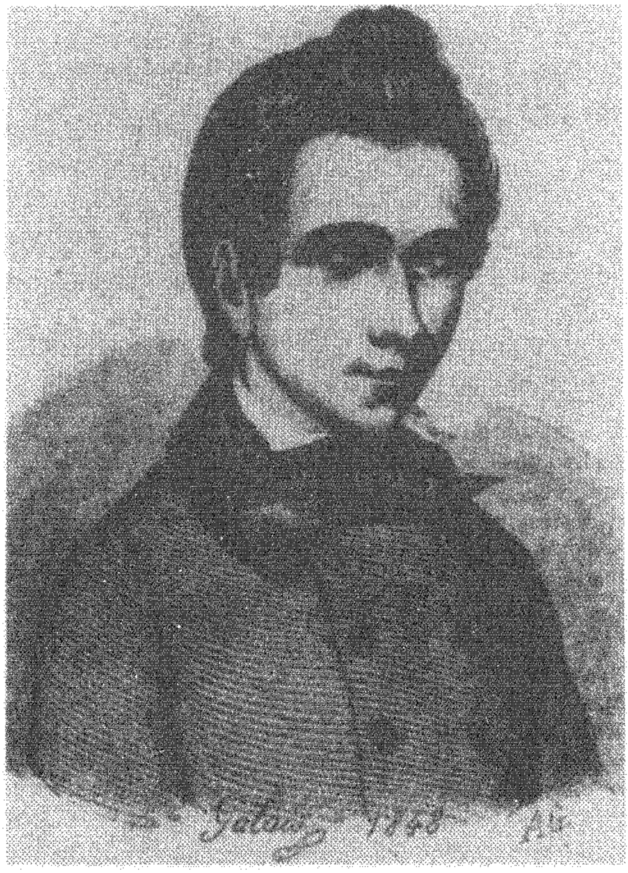
حياة جالوا

ولد إفرست جالوا (Evariste Galois) (الشكل ٦) في بورج لارين (Bourg-La-Reine) قرب باريس في ٢٥ أكتوبر ١٨١١م. وكان أبوه نيكولا جبرائيل جالوا (Nicolas Gabriel Galois) جمهوريًا (Kollros, 1949) ورئيسًا لحزب الأحرار في القرية، ثم أصبح رئيسًا للبلدية بعد عودة لويس الثامن عشر إلى العرش في عام ١٨١٤م. وأما والدة إفرست واسمها أدليد ماري (Adelaide - Marie) فكانت ابنة قاض، وتجيد اللاتينية بطلاقة نتيجة لثقافتها الدينية وللمعارف الكلاسيكية.

استقى جالوا علمه من والدته خلال الاثنتي عشرة سنة الأولى من عمره، حيث درس العلوم الكلاسيكية السائدة آنذاك. وكان سعيدًا في طفولته، ومحط اهتمام شديد من والدته، فقد فضّلت أن يبقى معها في البيت بالرغم من قبوله في كلية رايم (Reims) عندما كان في العاشرة من عمره. وفي أكتوبر ١٨٢٣م دخل جالوا مدرسة لويس العظيم (Louis - le - Grand). وفي أول فصل دراسي له تمرد الطلاب ورفضوا الغناء في كنيسة المدرسة مما أدى إلى طرد مائة منهم.

وقد تفوق جالوا في السنتين الأوليين من دراسته في تلك المدرسة، وحصل على الجائزة الأولى في اللاتينية، ولكنه بعد ذلك بدأ يشعر بالملل، ورسب في السنوات التالية، مما زاده ضجرًا. وخلال هذه الفترة بدأ جالوا يهتم بالرياضيات بصورة جدّية، واطّلع على نسخة من كتاب مبادئ الهندسة لمؤلفه لجيندر (Element de Geometrie, by Legendre) الذي اختلف عرضه لمادة الهندسة عما تعود عليه جالوا في مدرسته من خلال دروس الهندسة الإقليدية. ويقال [انظر: Bell, 1965] إنّ جالوا قرأ كتاب لجندر، كما «تقرأ الرواية» وقد ألمّ به في قراءة واحدة

فقط . ووجد جالوا أن مادة الجبر في مدرسته لا ترتقي إلى الأعمال العظيمة للجندر ، مما حدا به لقراءة أعمال لاجرانج و أبل . وعندما بلغ الخامسة عشرة كان يقرأ مواد في مستوى محترفي الرياضيّات ، ولم يعر أهمية لواجباته المدرسية ، ويبدو أنه فقد اهتمامه بها . ولقد أساء مدرسوه فهمه واتهموه بأنه موهوم في طموحاته وأصالته .



شكل (٦). صورة جالـوا وقد حُصِـل عليها من أخيـه الفرد Alfred عام ١٨٤٨م.

ولم يكن جالوا منتظمًا في عمله ، كما يبدو ذلك من بعض مخطوطاته [Bourgne and Azra, 1962] ، وقد كان يعمل بعقله دون أن يسجل شيئًا على الورق إلا النتائج .

ولقد توسّل إليــــه مدرســــه فرنيه (Vernier) أن ينظّم عمله ولكن دون جدوى . وتقدّم جالوا إلى اختبار دخول المدرسة التقنية (Ecole Polytechnique) دون تحضير كاف . ولو أنه نجح في الاختبار لضمن نجاحه كرياضي ، لأن المدرسة التقنية تعتبر الأرضً الخصبة لنمو علماء الرياضيات في فرنسا . ولكن جالوا رسب في الاختبار . وبعد مرور عشرين عامًا كتب تركم (Terquem) محرر (Nouvelle Annelles des Mathematiques) : «لقد أضاع ممتحن ذو ذكاء متواضع مرشحًا ذا ذكاء خارق . لأنهم لا يفهموني ، فأنا بربري . . .» .

وفي عام ١٨٢٨م دخل جالوا مدرسة نورمال (Ecole Normale) (وهي من مستوى يقل عن المدرسة التقنية) وقد حضر درسًا متقدمًا في الرياضيات تحت إشراف ريتشارد (Richard) الذي كان متعاطفًا معه ، وقد كان رأي ريتشارد أن جالوا يجب أن يقبل في المدرسة التقنية دون اختبار . وفي السنة التالية نشر جالوا أوّل بحث له وكان عن الكسور المتواصلة ، وكان بحثًا جيدًا لكنّه لا يدل على عبقرية [انظر Galois, 1897] . وفي تلك الأثناء كان جالوا يكتشف العديد من النتائج في نظرية معادلات كثيرات الحدود وكان يرسلها إليأكاديمة العلوم - كان المحكم هو كوشي (Cauchy) الذي سبق له نشر أبحاث عن سلوك الدوالّ تحت تأثير التباديل لمتغيراتها وهي فكرة رئيسة في نظرية جالوا ، وقد رفض كوشي بحث جالوا كما رفض بحثًا آخر بعد ثمانية أيام ، وقد فقدت مخطوطتا البحثين ولم يرهما أحد منذ ذلك الوقت .

في السنة نفسها أبتلي جالوا بنكبتين ؛ أولاهما انتحار أبيه في ٢ يوليو (تموز) ١٨٢٩م ، بعد نزاع سياسي مرير مع قسيس القرية ، والثانية أنه رسب في اختبار قبول المدرسة التقنية وكانت تلك فرصته الأخيرة . ويوجد روايتان في سبب رسوبه : الأولى تقول إن جالوا فقد صوابه أثناء الاختبار ورمى المسّاحة في وجه الممتحن [Bell, 1965' Dupug, 1896] أما الرواية الثانية وهي لـ[Bertrand,1899] فتقول إن الممتحن كان دنيه (Dinet) وقد سأل جالوا أن يخبره باختصار عن «اللوغاريتمات الحسابية ولكن جالوا أخبره أنه لا يوجد ما يسمى باللوغاريتمات الحسابية ، ولذا رسّبه دنيه . »

وفي فبراير ١٨٣٠م سلم جالوا أبحاثه إلى أكاديمة العلوم ضمن منافسة على الجائزة الكبرى في الرياضيات ، وهي قمة التشريف في هذا المجال ، ومنذ ذلك الحين

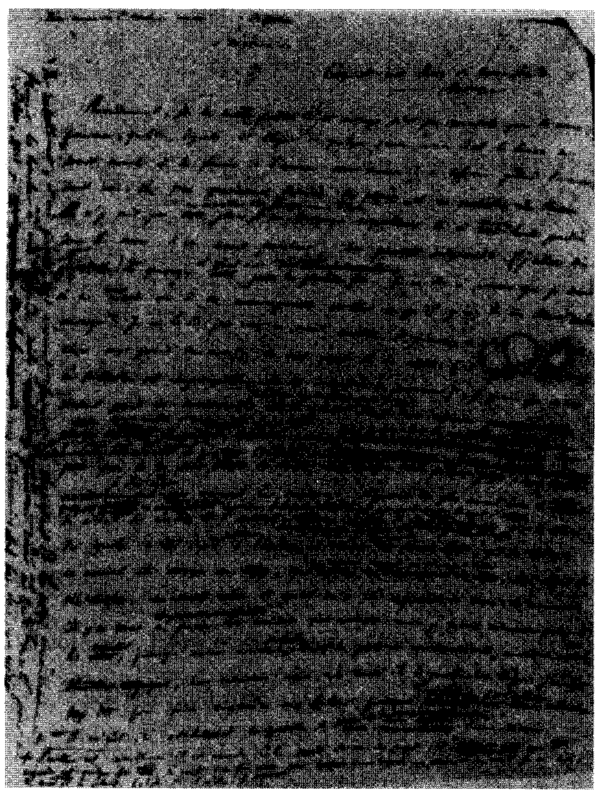
قيّمت أعماله بأنها جديرة بأكثر من هذه الجائزة ، وكان أمين عام الجائزة في ذلك الحين الرياضي فورييه (Fourier) الذي استلم مخطوطة جالوا وأخذها معه للبيت لمتابعتها ، ولكنه مات قبل أن يقرأها ولم يعثر عليها بين الأوراق فيما بعد . يقول دبووي [Dupuy, 1896] أن جالوا لم يعتقد ان الضياع المتكرّر لمخطوطاته مجرد صدفة ، بل نتيجة لتأثير مجتمعه الذي طالما كان يظلم العبقري ويهضمه حقوقه لصالح الأشخاص العاديين . كما كان يلوم عهد بوربون (Bourbon) المبني على الاضطهاد السياسي .

وفي عام ١٨٢٤م خلف شارل العاشر لويس الثامن عشر . وفي ١٨٢٧م حصل المعارضون الليبراليون على بعض الأصوات في الانتخابات، وعندما عقدت جولة أخرى في عام ١٨٣٠م فازوا بالأغلبية مما أجبر شارل على التنحي ، لكنه بدلاً من ذلك عمد إلى عمل انقلاب سياسي . ففي ٢٥ يوليو (تموز) أصدر أوامره لتقييد حرية الصحافة . ولم يستطع الشارع الفرنسي تحمل مثل هذا العمل مما أدى إلى تمرد شعبي دام ثلاثة أيام ، و بعد ذلك تمّ تنصيب دوق أورلينز لويس فيليب (Louis - Philippe) ملكًا كحل مرض للجميع ، وخلال هذه الأيام الثلاثة وبينما كان طلاّب المدرسة التقنية يصنعون التاّريخ في الشوارع كان جالوا وزملاؤه محبوسين من قبل جوينيولت (Guignault) مدير مدرسة نورمال . وكان جالوا غاضبًا لهذا العمل مما جعله يكتب مقالاً لاذعًا ضد المدير في جريدة المدرسة . وقد كتب اسمه كاملاً في نهاية المقال، وقام محرر الجريدة بمحو اسم جالوا ومع ذلك تم طرد جالوا من المدرسة بسبب المقالة التي كتبها «مجهول» . [انظر Dalmas, 1956] وهناك شرح تفصيلي وشيق لهذه الأحداث في [Dupuy, 1896] .

وفي ١٣ يناير (كانون الثاني) ١٨٣١م حاول جالوا العمل كمدرّس رياضيات خاص في مادة الجبر المتقدم لكنه لم يوفق في ذلك . وفي ١٧ يناير (كانون الثاني) أرسل مرة أخرى مقالة إلى أكاديمية العلوم بعنوان «شروط قابلية حل المعادلات باستخلاص الجذور» ، ولم يكن كوشي وقتها في باريس وبدلاً منه تمّ إحالتها إلى المحكمين بواسون (Poisson) ولاكورا (Lacroix) ، و مرّ شهران ولم يسمع من المحكمين مما حدا به إلى كتابة رسالة إلى رئيس الأكاديمية لكن هذا الآخر لم يرد عليها .

انضم جالوا إلى فصيلة من الحرس الوطني وهي منظمة جمهورية ، ولم يمض

طويلاً حتى تمّ أسره مع ضباط الحرس بتهمة التآمر ولكن أسره لم يطل ، وتم إطلاق سراحه بأمر قضائي، وقد تمّ الغاء فصيلة الحرس الوطني بأمر ملكي . وفي ٩ مايو (ايار) كان هناك حفل عشاء احتجاجي تعالت فيه صيحات الاستنكار لما فعله الملك ، ويقال أن جالوا وقف بين الجميع طالبًا شرب نخب الملك وبيده سكين بدلاً من الكأس . وقد فسر رفقاء جالوا هذه الحركة بأنها تهديد لحيـــاة الملك ، فصفقوا له بحماس وراحوا يرقصون ويصرخون بأعلى أصواتهم في الشارع، وفي اليوم التالي تمّ إلقاء القبض على جالوا ، وفي المحكمة اعترف بكل شيء ولكنه ادعى أن النخب كان للويس فيليب "إذن أصبح خائنا" وأن أصوات الحضور في ذلك الحين أخفت عبارته الأخيرة ، و تمت تبرئته وإطلاق سراحه في ١٥ يونيو (حزيران) .



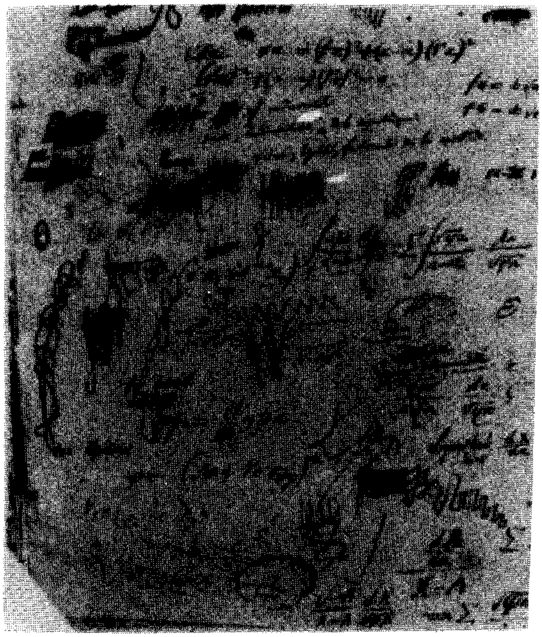
شكل (٧). الصفحة الأولى من مقدمة كتبها جالوا في السجن.

وفي ٤ يوليو (تموز) عرف جالوا مصير مقالته الأخيرة ، فقد أعلن بواسون أنها «غير مفهومة» ، وقد أنهى تقريره [أعيد نشره بأكمله في Taton, 1947] كما يلي :

«لقد فعلنا كل ما في وسعنا لفهم برهان جالوا . فلم تكن حججه واستنتاجاته واضحة ولا مطوّرة بالقدر الكافي الذي يجعلنا نحكم على صحتها ولا يمكننا إعطاء فكرة عنها في هذا التقرير ، وقد نوّه الكاتب بأن القضية الرئيسة في مقالته هي جزء من نظرية عامة لها العديد من التطبيقات . ربما سيتضح فيما بعد بأن الأجزاء المختلفة من هذه النظرية يوضح بعضها بعضًا ، وهي أسهل فهمًا ككل واحد بدلاً من أجزاء منفصلة ، لذا فإننا نقترح أن يقوم المؤلف بنشر عمله كاملاً كي يمكننا الحكم عليه . أما ما يخص الجزء المرسل إلى الاكاديمية فلا يمكننا الاقتراح بقبوله الآن» .

وفي ١٤ يوليو (تموز) كان جالوا على رأس تظاهرة للجمهوريين مرتديًا زي فصيلة الحرس الوطني المنحلّة ويحمل بيده سكينًا وبندقية . وقد ألقي القبض عليه في بونت نُف (الجسر التاسع) (Pont-Neuf) واتهم بارتدائه زياً ممنوعاً وحكم عليه بالسجن ستة أشهر في محل يدعى سنت بلاجي (القسيسة - بلاجي) (Sainte - Pelagie) . وأثناء وجوده في السجن استمر جالوا في شغله في الرياضيات شكل (٧) . وعندما انتشر وباء الكوليرا عام ١٨٣٢م تم نقله إلى المستشفى ، وبعد ذلك تمّ إطلاق سراحه .

وبعد أن عادت له حريته ، التقى مع فتاة تدعى مي ستيفاني د . (Mlle Stephanie D.) . وقد وقع في حبها وكانت هذه تجربته العاطفيةالأولى والأخيرة في حياته ، و لم يكن اسم عائلة محبوبته معروفًا حتى وقت قريب مما يدعم الصورة الرومانسية لما كان معروفًا آنذاك بـ (Femme Fatale) (المرأة القاتلة) . وقد وجد اسمها مطموسًا في واحدة من مخطوطات جالوا ، وتمّ فحص هذه المخطوطة بصورة دقيقة من قبل كارلوس انفنتوزي (Carlos Infantozzi) والذي كان أنجح من سابقيه في كشف اسم الفتاة كاملاً وهو ستيفاني - فليسي بوتران دو موتيل(Stephanie-Felicie Poterin du Motel) وهي ابنة محترمة لطبيب يعيش في المنطقة نفسها [انظر : Rothman, 1982] . وقد اكتنف الغموض هذه الفترة من حياة جالوا مما أخفى الكثير مما سيكون له تأثير على ما سيجري له من أحداث . لقد بينت بقايا رسائله (انظر [Bourgne and Azra, 1962] بأن الفتاة رفضت جالوا وأنه تأثر بذلك كثيرًا . لم يمض وقت طويل حتى أن شخصًا تحداه ونازله بسبب علاقته بالفتاة فيما يبدو (شكا ٨)



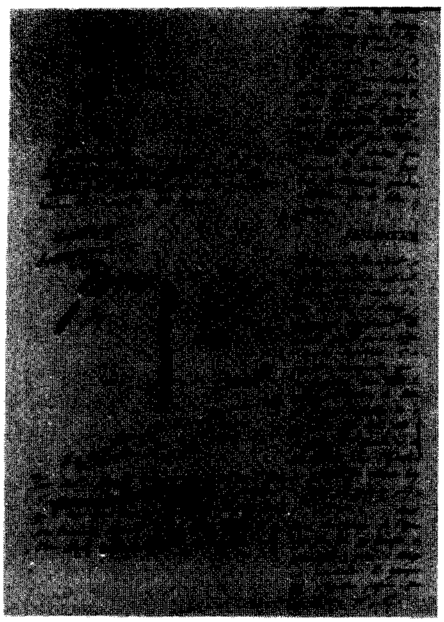
شكل (٨) بعض ماكتبه ورسمه جالوا قبل ذهابه إلى المنازلة القاتلة لاحظ كلمة "Une femme" مع كلمة ثانية مشطوبة في أسفل يسار الورقة.

ومرة أخرى هناك غموض محيط بهذا الحدث؛ يقول البعض [Bell, 1965; Kollros, 1949] أنّ الفتاة قد استعملت كعذر فقط، وأن السبب الحقيقي للمنازلة هو تصفية حساب متعلق بانتماءات سياسية مختلفة. ويؤيد وجهةالنظر هذه ألكسندر دوما (Alexandre Dumas) (في مؤلفه Memoires) فيقول أن أحد خصوم جالوا السياسيين كان بيشو دربنفيل (Pecheux DHerbinville)، ولكن دالما [Dalmas, 1956]، يرى أن المُنَازل الآخر كان جمهوريًا مستشهدًا بتقرير الشرطة، ومن المحتمل أن يكون أحد رفقاء جالوا الثوريين وأن سبب المنازلة هي الفتاة، و يدعم هذا الرأي الأخير كلمات جالوا نفسه [Bourgne and Azra, 1962] إذ يقول :

«إنني أتوسل إلى الوطنيين وأصدقائي جميعًا بأن لا يلوموني إذ لم يكن موتى فداء لبلدي – إني أموت ضحيّة لمغناج شائنة السمعة . وشمعة حياتي يطفئها شجار يأس، آه لماذا أموت

في سبيل شئ تافه وحقير! . . . العفو للّذين سيقتلوني فإنّ نواياهم حسنة» .

في اليوم نفسه، ٢٨ (آيار) وفي ليلة المنازلة كتب رسالته المشهورة إلى صديقه أوجست شفالييه (Auguste Chevalier) ملخصًا فيها اكتشافاته . وقد نشرها شفالييه في (Revue Encyclopedique)، وفي هذه الرسالة يبيّن جالوا الخطوط العريضة للارتباط ما بين الزمر ومعادلات كثيرات الحدود، وذكر أن المعادلة قابلة للحل بطريقة الجذور شريطة أن تكون زمرتها قابلة للحل . كما ذُكر، إضافة إلى افكار أخرى، بعض الشيء عن الدوال الناقصية وتكامل الدوال الجبرية وأمور أخرى بدت غامضة ويصعب معرفة مقصوده منها . و رسالته هذه تثير الشفقة عليه ، فقد كان يخربش بتعليقاته في الهامش وكتب في أحدها : لم يبق لدي وقت (شكل ٩) .

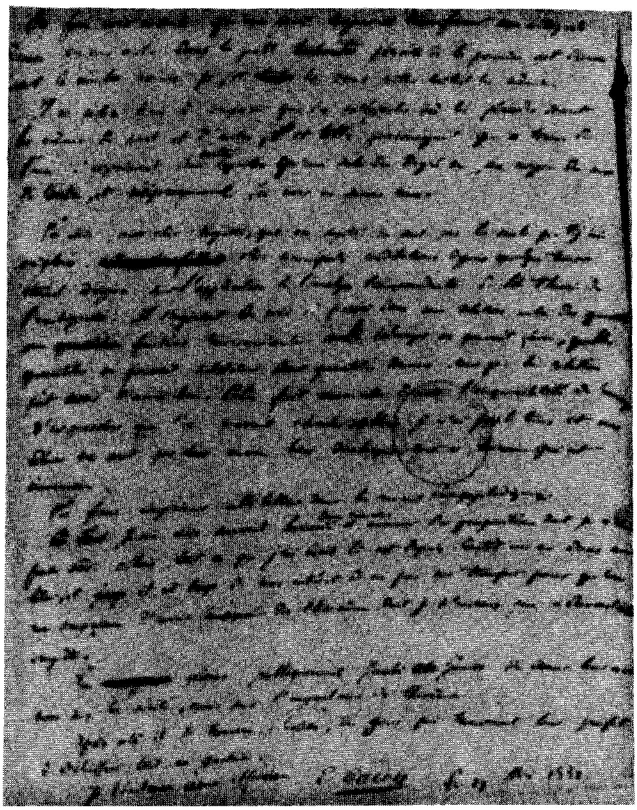


شكل(٩). لم يبق لدي وقت (Je nai pas temps) تجدها فوق الفقرة المشطوبة فى أسفل اليسار.

لقد كانت المنازلة بالمسدسات بخمس وعشرين خطوة . أصيب جالوا في بطنه ومات في اليوم التالي ، ٣١ مايو (آيار) من التهاب في الصفاق وقد رفض رؤية أي قسيس قبل موته ، في ٢ يونيو (حزيران) ١٨٣٢م دفن جالوا في خندق مشترك في

مقبرة مونتبارناس(Montparnasse) .

ولقد أنهى رسالته إلى شفالييه بالكلمات التالية : اسأل جاكوبي (Jacobi) أو جاوس (Gauss) ليعطوك رأيهم علانيـــةً ، ليس في صواب هذه النظريات بل في أهميتها . آمل في المستقبل أن يجد بعض الناس الفائدة من فك مغالق هذه اللخبطة (شكل ١٠).



شكل (١٠). فك مغالق هذه اللخبطة (dechiffrer tout ce gachis) تجدها فى السطر قبل الأخير . هذه آخر صفحة كتبها جالوا قبل المنازلة.

نظرة شاملة
Over view

تعتبر نظرية جالوا مزيج مبهر من الرياضيات التقليدية والرياضيات المعاصرة، وتأخذ كثيراً من الجهد قبل أن تصل إلى إدراك ماهيتها. وفي هذا الفصل سنقدم نظرة عامة سريعة للمباديء الأساسية للموضوع، ونشرح كيفية تطور المعالجة المجردة من الأفكار التي قدمها جالوا.

إن هدف نظرية جالوا هو دراسة حلول معادلات كثيرات الحدود

$$f(t) = t^n + a_{n-1} t^{n-1} + \dots + a_0 = 0$$

وعلى وجه الخصوص تحديد المعادلات التي يمكن حلها بواسطة «صيغة» وتلك التي لا يمكن ايجاد صيغة لحلها. الصيغة هنا تعني عبارة جذرية (أي شئ يمكن الحصول عليه من المعاملات a_i باستخدام عمليات الجمع، والطرح، والضرب، والقسمة، وأخذ الجذر النوني حيث $n = 2,3,4,\dots\dots$). إن الهدف الأساسي لهذا الكتاب هو البرهان على أنه بالرغم من إمكانية حل المعادلات التربيعية والتكعيبيّة وذات الدرجة الرابعة فإنه بصفة عامة لا يمكن حل المعادلة من الدرجة الخامسة بواسطة الجذور.

وبصيغة معاصرة فإن الفكرة الأساسية لجالوا هي دراسة تناظرات كثيرة الحدود $f(t)$، وهذه التناظرات تكون زمرة (زمرة جالوا)، وإمكانية حل معادلة كثيرة الحدود يتم بواسطة دراسة خواص زمرة جالوا. إن كثيراً من المسائل يمكن دراستها بدراسة حلول معادلات كثيرات الحدود. ونتيجة لذلك فإن لنظرية جالوا تطبيقات كثيرة في مجالات الرياضيات المختلفة، وسنركز اهتمامنا هنا على العلاقة بين نظرية جالوا والإنشاءات الهندسية، حيث سنبرهن على استحالة تقسيم الزاوية إلى ثلاثة أقسام

متساوية، ومضاعفة المكعب وتربيع الدائرة وذلك بواسطة المسطرة والفرجار، وكذلك سوف نصف النتيجة التي حصل عليها جاوس وهي : إمكانيـة إنشاء مضلع منتظم ذو 17 ضلعًا باستخدام المسطرة والفرجار. وفي الفصل الأخير سنستخدم نظرية جالوا لإعطاء برهان للنظرية الأساسية في الجبر (أي كثيرة حدود بمعاملات مركبة يجب أن يكون لها حلاً مركبًا) .

زمر جالوا كما اكتشفها جالوا
وكيفية استخدامها

لقد اكتشف جالوا ماهية الزمرة بطريقة مجردة وليس فقط بالنظر إليها من منظار علاقتها مع معادلات كثيرات الحدود. ويعتبر الأسلوب الذي اتبعه في ذلك أقل تجريدًا مقارنة بالاسلوب الحديث ولكنه يعتبر أسلوبًا على درجة كبيرة من التجريد في تلك الأيام. وفي الحقيقة فإن جالوا يعتبر أحد الرواد الذين أسسوا الجبر المجرد المعاصر. ولكي نفهم الأسلوب المعاصر فإنه يكون من المناسب أن نلقي نظرة على الطريقة التي كان يفكر فيها جالوا. فعلى سبيل المثال ليكن لدينا معادلة كثيرة الحدود :

$$f(t) = t^4 - 4t^2 - 5 = 0$$

ويمكن تحليل هذه المعادلة كالتالي :

$$(t^2 + 1)(t^2 - 5) = 0$$

ولهذه المعادلة أربعة أصفار هي $t = i, -i, \sqrt{5}, -\sqrt{5}$. من الواضح أن هذه الأصفار تنقسم إلى زوجين من الأصفار : $i, -i$ و $\sqrt{5}, -\sqrt{5}$. وفي الحقيقة أنّه من المستحيل التمييز جبريًا بين i و $-i$ ، $\sqrt{5}$ و $-\sqrt{5}$ بالمفهوم التالي : اكتب أي معادلة كثيرة حدود بمعاملات كسرية بحيث تكون أصفارها i و $-i$ ، $\sqrt{5}$ و $-\sqrt{5}$ بأي ترتيب كان، فإذا وضعنا :

$$\alpha = i, \quad \beta = -i, \quad \gamma = \sqrt{5}, \quad \delta = -\sqrt{5}$$

فإن بعض هذه المعادلات :

$$\alpha^2 + 1 = 0, \quad \alpha + \beta = 0, \quad \delta^2 - 5 = 0$$

$$\gamma + \delta = 0, \quad \alpha\gamma - \beta\delta = 0$$

وهلم جرّا . وفي الحقيقة يوجد عدد غير منته من المعادلات الصحيحة التي تكون على الصورة أعلاه . ومن ناحية أخرى فإنّه يوجد عدد غير منته من المعادلات الخاطئة مثل $\alpha + \gamma = 0$. فلو أخذنا أي معادلة صحيحة وبدّلنا α و β فإننا نحصل على معادلة صحيحة أيضًا . وهذا صحيح أيضاً إذا بدلنا γ و δ. فعلى سبيل المثال تصبح المعادلات أعلاه باستخدام هذه الطريقة كالتالي :

$$\beta^2 + 1 = 0, \quad \beta + \alpha = 0, \quad \gamma^2 - 5 = 0,$$
$$\delta + \gamma = 0, \quad \beta\gamma - \alpha\delta = 0, \quad \alpha\delta - \beta\gamma = 0,$$
$$\beta\delta - \alpha\gamma = 0$$

وجميع هذه المعادلات صحيحة . وفي المقابل إذا بدّلنا α و γ فإنّنا نحصل على المعادلة الخاطئة أيضًا $\gamma + \beta = 0$.

إنّ العمليات التي نستخدمها هنا هي تباديل الأصفار α ، β ، γ ، δ . وفي الحقيقة إذا استخدمنا الرمز المتبع للتباديل فإن تبديل α و β هو :

$$R = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \gamma & \delta \end{pmatrix}$$

وتبديل γ و δ هو:

$$S = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \alpha & \beta & \delta & \gamma \end{pmatrix}$$

وهذان عنصران في زمرة التباديل S_4 التي تحتوي على جميع تباديل المجموعة $\{\alpha, \beta, \gamma, \delta\}$ وهي 24 تبديلاً .

إذا كان كل من هذين التبديلين يحول معادلة صحيحة إلى معادلة صحيحة فإنّ المعادلة التي نحصل عليها من التبديل الناتج من هذين التبديلين على التوالي يجب أن تكون أيضًا صحيحة ، وهذا التبديل هو :

$$T = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \delta & \gamma \end{pmatrix}$$

هل هناك تبديلات أخرى تتمتع بهذه الخاصية ألا وهي المحافظة على المعادلات الصحيحة ؟ بالتأكيد ، وهو التبديل المحايد :

$$I = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \alpha & \beta & \gamma & \delta \end{pmatrix}$$

من السهل على القاريء أن يتأكد من أن التبديلات الأربعة أعلاه هي فقط التبديلات التي تحوّل معادلة صحيحة إلى معادلة صحيحة ، إمّا العشرين تبديلاً الباقية فإنها تحوّل معادلة صحيحة إلى معادلة خاطئة .

هناك حقيقة عامة سهلة البرهان تنص على أن التحويلات القابلة للانعكاس على عنصر رياضي والتي تحافظ على بعض الخواص تكون زمرة . سنسمي هذه الزمرة بزمرة التناظرات للعنصر . وهذا الاصطلاح شائع خاصة إذا كان هذا العنصر الرياضي هو شكل هندسي والتحويلات هي حركة صلبة ، ومن الممكن أيضًا تعميم هذه الفكرة . وعليه فإن التبديلات الأربعة تكون لنا زمرة ولنرمز لها بالرمز G .

لقد لاحظ جالوا أن تركيب هذه الزمرة ينظّم لنا لحد ما طريقة التفكير لحل المعادلات . فمثلاً لنأخذ الزمرة الجزئية :

$$H = \{I, R\}$$

إن بعض العبارات في $\alpha, \beta, \gamma, \delta$ تكون عبارات ثابتة تحت تأثير التباديل في هذه الزمرة . فعلى سبيل المثال إذا أثرت R على :

$$\alpha^2 + \beta^2 - 5\gamma\delta^2$$

فإننا نحصل على :

$$\beta^2 + \alpha^2 - 5\gamma\delta^2$$

وهي العبارة السابقة نفسها . وفي الحقيقة فإن العبارة تبقى ثابتة تحت تأثير R إذا وفقط إذا كان متناظرة في α و β .

إنّه ليس من الصعب أن نبرهن على أنّ كثيرة حدود في α ، β ، γ ، δ التي تكون متناظرة في α و β يمكن كتابتها على صورة كثيرة حدود في $(\alpha+\beta)$ ، $\alpha\beta$ ، γ ، δ ، فعلى سبيل المثال يمكن كتابة العبارة السابقة على الصورة :

$$(\alpha+\beta)^2 - 2\alpha\beta - 5\gamma\delta^2 .$$

ولكننا نعلم أن $\alpha = i$ ، $\beta = -i$ ومنه نجد :

$$\alpha+\beta = 0 , \quad \alpha\beta = 1 .$$

وعليه فإن العبارة تختصر إلى :

$$-2 - 5\gamma\delta^2$$

الآن تم حذف α و β معًا.

دعنا نفترض الآن عدم معرفتنا للقيم $i, -i, \sqrt{5}, -\sqrt{5}$ ولكننا بدلاً من ذلك نعرف زمرة جالوا G . في الحقيقة لنفرض أن $g(t)$ كثيرة حدود من الدرجة الرابعة حيث زمرة جالوا لها هي نفس زمرة جالوا لكثيرة الحدود $f(t)$ المعطية في مثالنا السابق، وبذلك فإننا لا يمكن أن نعرف أصفار كثيرة الحدود هذه، لنفرض أن هذه الأصفار هي $\alpha, \beta, \gamma, \delta$ ، وليكن لدينا ثلاث مجموعات عناصرها عبارات رياضية في $\alpha, \beta, \gamma, \delta$ وبالتحديد:

$$\mathbb{Q} \subseteq \mathbb{Q}(\gamma,\delta) \subseteq \mathbb{Q}(\alpha,\beta,\delta)$$

حيث $\mathbb{Q}(\gamma,\delta)$ هي مجموعة جميع العبارات الرياضية في γ ، δ بمعاملات كسرية، $\mathbb{Q}(\alpha,\beta,\gamma,\delta)$ هي مجموعة جميع العبارات الرياضية في $\alpha, \beta, \gamma, \delta$ بمعاملات كسرية، لتكن $H = \{I,R\} \subseteq G$ ولنفرض أننا نعلم الحقيقتين التاليتين :

(١) جميع العبارات التي تبقى ثابتة تحت تأثير H هي بالضبط عناصر $\mathbb{Q}(\gamma,\delta)$.

(٢) جميع العبارات التي تبقى ثابتة تحت تأثير G هي بالضبط عناصر $\mathbb{Q}$.

مما سبق نستطيع أن نقدّم وصفًا لحل المعادلة $g(t) = 0$ كما يلي :

من الواضح أن العبارتين $\alpha+\beta$ و $\alpha\beta$ تبقيان ثابتتين تحت تأثير H. باستخدام الحقيقة (١) نجد أن $\alpha+\beta$ و $\alpha\beta$ عنصرين في $\mathbb{Q}(\gamma,\delta)$. ولكن

$$(t-\alpha)(t-\beta) = t^2 - (\alpha+\beta)t + \alpha\beta$$

وهذا يعني أن α و β تحقّقان معادلة من الدرجة الثانية معاملاتها تنتمي إلى المجموعة $Q(\gamma,\delta)$. أي أنّنا نستطيع حل هذه المعادلة ونجد α , β بدلالة عبارات رياضية في γ و δ تحتوي في أسوأ حالاتها على جذور تربيعية، وبالتالي فإنّنا نحصل على α و β كعبارات جذرية في γ و δ .

ونستطيع أن نستخدم الأسلوب نفسه للحصول على γ و δ، والعبارتان $\gamma+\delta$ و $\gamma\delta$ تبقيان ثابتتين تحت تأثير G، ومن الواضح أنهما تبقيان ثابتتين تحت تأثير كل من R و S ، وهاتان تولدان G . باستخدام الحقيقة (٢) $\gamma+\delta\ ,\ \gamma\delta \in Q$. وعليه فإنّ γ و δ تحققان معادلة من الدرجة الثانية بمعاملات في Q، وبالتالي يمكن أن نجدهما كعبارات جذرية بمعاملات كسرية. وبالتعويض في الصيغ التي وجدت لكل من α و γ نستطيع إيجاد الأصفار الأربعة كعبارات جذرية بمعاملات كسرية .

إنّنا لم نستطع ايجاد هذه الجذور ولكنّنا وجدنا أنّ معرفتنا لبعض المعلومات عن زمرة جالوا ضمنت لنا وجود هذه الأصفار، ولو كان لدينا معلومات أكثر لاستطعنا إنهاء المسألة .

إن المثال السابق يوضّح لنا مدى العلاقة بين تركيب الزمرة الجزئية لزمرة جالوا G وبين احتمال حل المعادلة $g(t) = 0$، و لقد اكتشف جالوا أن هذه العلاقة عميقة جدًا . فعلى سبيل المثال، إن برهانه على استحالة حل المعادلة من الدرجة الخامسة بواسطة الجذور يترجم على أن زمرة جالوا لهذه المعادلة هي زمرة ذات طبيعة معينة .

الشكل المجرد

The Abstract Setting

لقد اتبع أسلوب المعالجة الحديث أسلوب جالوا من حيث المبدأ، ولكنه اختلف عنه في الناحية التطبيقية، والمجموعة $Q(\alpha,\beta,\gamma,\delta)$ التي قدمت سابقًا هي عبارة عن حقل جزئي من حقل الأعداد المركبة $\mathbb{C}$ مُوَلّد بأصفار g . وتباديل الأصفار $\alpha,\beta,\gamma,\delta$ التي تحافظ على العلاقات الجبرية فيما بينها ، وهي عبارة عن زمرة التناظرات للحقل $Q(\alpha,\beta,\gamma,\delta)$ ، وبصورة أدق هي زمرة التماثلات الذاتية لهذا الحقل، وما هذا إلا

اسم مزخرف للشيء نفسه.

بالإضافة إلى ذلك نريد دراسة كثيرات حدود بمعاملات مأخوذة من حقل K وليس فقط أعداد صحيحة أو كسرية . إنّ أصفار كثيرة حدود $f(t)$ بمعاملات في K تعين لنا حقلاً آخر L يحتوى K . فعليه يكون اهتمامنا منصبًا مبدئيًا على زوج من الحقول $K \subset L$ أو بصورة أعم على امتداد حقلي $L : K$. إذن عندما يتكلم جالوا عن كثيرات حدود يكون هذا مكافئًا للكلام عن امتدادات الحقول بالأسلوب الحديث. وزمرة جالوا لكثيرة حدود تصبح زمرة تماثلات ذاتية للحقل L التي تثبت الحقل K ، بكلام آخر زمرة دوال $\theta : L \to L$ بحيث لكل $x, y \in L$ ، $k \in K$ يكون:

$$\theta(x + y) = \theta(x) + \theta(y)$$

$$\theta(x\, y) = \theta(x)\, \theta(y)$$

$$\theta(k) = k$$

وبالتالي فإنّ معظم نظريّة جالوا تتم دراستهـا باستخـــدام امتدادات الحقول وزمر تماثلاتها الذاتية التي تُثبِّت K .

إن الطريقة التي اتّبعت لحلّ $g(t) = 0$ تعتمد اعتمادًا كليًا على الحقيقتين (١) و(٢)، ولكن هل بإمكاننا أن نعرّف هذه الحقائق دون معرفتنا المسبقة لأصفار g ؟ والجواب هو نعم (ولكن بقدر من الصعوبة) إذا استطعنا أن نضع دراسة عامة لزمر التماثلات الذاتية لامتداد الحقول ، زمرها الجزئية ، والحقول الجزئية التي تبقى ثابتة تحت تأثير هذه الزمر الجزئية . وهذا يؤدي إلى تقابل جالوا بين زمر جالوا الجزئية وبين الحقول الجزئية M من L التي تحوي K .

الفصول من (١-٤) و (٧-١١) توضّح لنا هذا التقابل وتبرهن لنا خواصه المهمة . الفصلين الخامس والسادس يبعدانا قليلاً لنغطي بعض التطبيقات الهندسية .

الفصل الثاني عشر يزوّدنا بمثال لترسيخ الأفكار التي تم دراستها. الفصول (١٣ - ١٩) تبرهن لنا بعض النتائج الشيّقة جدًا.

الفصل الأول

مفاهيم أساسية
Background

إنّ الهدف من هذا الفصل هو تزويد القاريء ببعض المفاهيم الأساسية التي تعتمد عليها نظرية جالوا وبالتحديد: مفهوم الحلقة، والحقل ، والمجال الكامل، والمثالية ، وكثيرة الحدود، والقاسم المشترك الأعظم. وسنغطي أيضًا خوارزمية إقليدس التي تستخدم لايجاد القاسم المشترك الأعظم لكثيرتي حدود. ويستطيع القاريء الذي عنده دراية عن هذه المواضيع الاستغناء عن هذا الفصل.

سنفترض هنا أن القاريء على دراية بتحليل الأعداد الصحيحة إلى عواملها الأوّلية، ويعرّف على الأقل مفهوم حلقة الخارج من نظريّة الحلقات. وأثناء قيامنا بعرض هذه المفاهيم الأساسية سنقدم بعض الترميزات الشائعة الاستخدام.

(١,١) الخواص العامة للحلقات
General Properties of Rings

نذكّر القاريء بأن الحلقة هي عبارة عن مجموعة R معرفًا عليها عمليتان ثنائيتان + (الجمع) و x (الضرب) بحيث يكون $(R, +)$ زمرة ابدالية ، وعملية الضرب تجميعية وتحقق خاصيتي التوزيع:

$$(a + b) \times c = (a \times c) + (b \times c)$$

$$a \times (b + c) = (a \times b) + (a \times c)$$

لكل $a,b,c \in R$. سنرمز للمحايد الجمعي في R بالرمز 0 ونكتب ab بدلاً من $a \times b$.

تسمى الحلقة D مجالاً كاملاً إذا تحقق ما يلي:

(١) $ab = ba$ لكل $a,b \in D$.

(٢) يوجد عنصر $1 \in D$ بحيث يكون $a1 = 1a = a$ لكل $a \in D$.

(٣) إذاكان $a,b \in D$ بحيث $ab = 0$ فإن $a = 0$ أو $b = 0$.

الحقل هو عبارة عن حلقة F بحيث يكون $(F\backslash\{0\}, x)$ زمرة ضربية إبدالية . وبالتالي لكل عنصر $a \in F$ ، $a \neq 0$ يوجد له نظير ضربي a^{-1} . في الغالب نكتب a/b أو $\frac{a}{b}$ بدلاً من ab^{-1} . كل حقل يجب أن يكون مجالاً كاملاً . سنرمز للمحايد الضربي بالرمز 1 .

من الأمثلة المهمة لهذه الأنظمة : المجال الكامل للأعداد الصحيحة$\mathbb{Z}$، الحقول $\mathbb{C}$ ، $\mathbb{R}$ ، Q حيث Q هي مجموعة الأعداد النسبية ، $\mathbb{R}$ مجموعة الأعداد الحقيقية و $\mathbb{C}$ مجموعة الأعداد المركبة .

تسمى المجموعة الجزئية غير الخالية S من الحلقة R حلقة جزئية من R إذا كان $a+b \in S$ ، $a-b \in S$ ، $ab \in S$ لكل $a,b \in S$. **الحقل الجزئي** من الحقل F هو مجموعة جزئية S من F تحتوي على العنصرين 0، 1 وتحقق الشروط التالية :

- إذا كان $a,b \in S$ فإن $a+b \in S$ ، $a-b \in S$ ، $ab \in S$.
- وإذا كان $a \neq 0$ فإن $a^{-1} \in S$.

المثالية من الحلقة R هي حلقة جزئية I من R بحيث يكون $ir \in I$ و ri لكل $i \in I$ ، $r \in R$. فعلى سبيل المثال $\mathbb{Z}$ حلقة جزئية من Q و $\mathbb{R}$ حقل جزئي من $\mathbb{C}$ ، ومجموعة الأعداد الصحيحة الزوجية $2\mathbb{Z}$ مثالية من $\mathbb{Z}$.

إذا كانت I مثالية من الحلقة R فإننا نستطيع ايجاد حلقة الخارج R/I التي عناصرها المجموعات المشاركة من I في R وعمليتا الجمع والضرب معرفة كما يلي

$$(I + r) + (I + s) = I + (r + s)$$

$$(I + r)(I + s) = I + (rs)$$

حيث $r, s \in R$ ، $I+r$ هي المجموعة المشاركة $\{i+r : i \in I\}$. فعلى سبيل المثال إذا كانت $n\mathbb{Z}$ هي مجموعة الأعداد الصحيحة التي تقبل القسمة على العدد الصحيح n . فإنه من الواضح أن $n\mathbb{Z}$ مثالية من $\mathbb{Z}$ وأن حلقة الخارج $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ هي حلقة الأعداد الصحيحة قياس n .

سنحتاج إلى الخاصية التالية للحلقة $\mathbb{Z}_n$:

نظرية (١,١)

تكون الحلقة $\mathbb{Z}_n$ حقلاً إذا وفقط إذا كان n عددًا أوليًا .

البرهان

لنفرض أولاً أن n ليس أوليًا . إذا كان $n = 1$ فإن $\mathbb{Z}_n=\mathbb{Z}/\mathbb{Z}$ وهذه المجموعة تحتوي على عنصر واحد فقط وبالتالي لا يمكن أن تكون حقلا . إذا كان $n > 1$ فإن $n = r s$ حيث $1 < r , s < n$. وبوضع $I = n\mathbb{Z}$ نحصل على :

$$(I + r) (I + s) = I + r s = I \ .$$

ولكن I هو العنصر الصفري للحلقة $\mathbb{Z}/I$ ، $I + r \neq I$ و $I + s \neq I$ وهذا يؤدي إلى أنه لا يمكن أن يكون $\mathbb{Z}/I$ حقلاً لأنه في الحقل يجب أن يكون حاصل ضرب عنصرين غير صفريين عنصرًا غير صفري .

ولبرهان العكس نفرض أن n عدد أولي . وليكن $I + r$ عنصر غير صفري في $\mathbb{Z}/I$. وبما أن r و n أوليان نسبيًا فإنه باستخدام بعض الخواص الأساسية للمجموعة $\mathbb{Z}$ نستطيع إيجاد عددين صحيحين a و b بحيث يكون $a r + b n = 1$. ومنه

$$(I + a)(I + r) = (I + 1) - (I + n)(I + b) = I + 1$$

وبالمثل

$$(I + r)(I + a) = I + 1$$

وبما أن $I + 1$ هو العنصر المحايد في $\mathbb{Z}/I$ فإننا نكون قد وجدنا نظيرًا ضربيًا للعنصر $I + r$. و من ثم فإن كل عنصر غير صفري في $\mathbb{Z}/I$ له نظير ضربي ومنه فإن $\mathbb{Z}_n=\mathbb{Z}/I$ حقل . Δ

من الآن فصاعدا عندما نتكلم عن $\mathbb{Z}_n$ فإننا نعتبر عناصرها $0,1,2,..., n - 1$ بدلاً من

$$I, I + 1, I + 2 ,..., I + n -1$$

(١,٢) مميّز الحقل

Characteristic of the Field

تعريف

يعرّف الحقل الجزئي الأوّلي للحقل K بأنّه تقاطع جميع الحقول الجزئية للحقل K .

من السهل أن نرى أن تقاطع أي مجموعة من الحقول الجزئية للحقل K يكون حقلاً جزئياً (التقاطع هنا ليس خاليًا لأن أي حقل جزئي يجب أن يحتوي على العنصرين $0 , 1$) وعليه فإن الحقل الجزئي الأولي للحقل K هو أصغر حقل جزئي للحقل K وهو وحيد أيضا . الآن الحقلين Q و $\mathbb{Z}_p$ (p أولي) ليس لها حقول جزئية فعلية ومن ثم فإن كلا منهما يساوي حقله الجزئي الأولي . والنظرية التالية تبرهن لنا أنّ هذين الحقلين هما الحقلان الجزئيان الأوليان الوحيدان .

نظرية (١,٢)

إنّ كل حقل جزئي أوّلي إمّا أن يكون متماثلاً مع الحقل Q أو أن يكون متماثلاً مع الحقل $\mathbb{Z}_p$ (p أولي) .

البرهان

ليكن K حقلاً و P حقله الجزئي الأولي . بما أن P يحتوي العنصرين 0 ، 1 فإنه يحتوي على جميع العناصر n^* $(n \in \mathbb{Z})$ المعرفة كما يلي :

$n^* = 1 + 1 + ... + 1$ ، n من المرّات $(n > 0)$.

$$0^* = 0$$

$n^* = -(-n)^*$ إذا كان $n < 0$.

وبحسابات بسيطة مستخدمين خاصيّة التوزيع نجد أنّ الدّالة $* : \mathbb{Z} \to P$ تعرف لنا تشاكل حلقي . وتكون لدينا الحالتان التاليتان :

(أ) **الحالة الأولى:** $n^* = 0$ حيث $n \neq 0$.

بما أن $(-n)^* = 0$ فإنه يوجد أصغر عدد صحيح موجب p بحيث $p^* = 0$.

إذا كان p مؤلفًا ، وليكن $p = r\,s$ ، $1 < r, s < p$ فإن $0 = p^* = r^* s^*$ ، ومنه $r^* = 0$ أو $s^* = 0$ وهذا يناقض اختيار p . وعليه فإن p أولي . العناصر n^* تكون حلقة تماثل $\mathbb{Z}_p$ وهو حقل باستخدام نظرية (١ , ١) . وهذا الحقل يجب أن يكون مساوياً للحقل P لأن P هو أصغر حقل جزئي من K .

(ب) الحالة الثانية: $n^* \neq 0$ حيث $n \neq 0$.

وفي هذه الحالة P يجب أن يحتوي على جميع العناصر m^* / n^* حيث $m, n \in \mathbb{Z}$ ، $n \neq 0$. وهذا يكوّن حقلاً جزئيًا متماثلاً مع Q (صورة العنصر m^* / n^* هو m / n وهذا الحقل يجب أن يكون مساويا للحقل P . ∆

تعريف

نقول إن مميز الحقل K صفرًا إذا كان الحقل الجزئي الأولي له يشاكل Q ، وأما إذا كان حقله الجزئي الأولي يشاكل $\mathbb{Z}_p$ فنقول إنّ مميزه p .

على سبيل المثال مميّز كل من الحقول Q ، $\mathbb{R}$ ، $\mathbb{C}$ صفر لأن الحقل الجزئي الأوّلي لكل منها هو Q ، ومميز $\mathbb{Z}_p$ (p أولي) هو p . سوف نرى أنه يوجد حقول أخرى غير $\mathbb{Z}_p$ لها مميز p [تمرين (٦ , ١)].

وسيكون للعناصر n^* المعرفة في نظرية (٢ , ١) أهمية كبرى فيما بعد ولقد اتفق على أن يكتب n بدلاً من n^* وسوء الترميز هذا لن يسبب أي إرباك للقاريء طالما وضع في عين الاعتبار أنه من الممكن أن يكون n صفراً في حقل ما دون أن يكون صفراً كعدد صحيح . ففي الحقل $\mathbb{Z}_5$ لدينا $2 = 7 = -3$. ونلاحظ أن هذه المشكلة لا تظهر في الحقول ذات المميزات الصفرية ، وبهذا الاستخدام يكون هناك معنى لحاصل الضرب $n\,k\ (n \in K, n \in \mathbb{Z})$ وهذا يعني :

$$n\,k = \pm(k + k + \ldots + k)$$

تمهيدية (٣, ١)

إذا كان K حقلاً جزئيًا من L فإن K و L يجب أن يكون لهما المميز نفسه .

البرهان

K و L لهما الحقل الجزئي الأولي نفسه . Δ

تمهيدية (١,٤)

إذا كان k عددًا غير صفري في الحقل K ، وكان n عددًا صحيحًا بحيث $n\,k = 0$ فإنّ n هو مضاعف لمميز K .

البرهان

يجب أن يكون $n = 0$ في الحقل K وهذا يعني بالترميز القديم أن $n^* = 0$. إذا كان المميز 0 فإن $n = 0$ (كعدد صحيح) . أما إذا كان المميز $p > 0$ فإن n يجب أن يكون مضاعفًا للعدد p . Δ

(١,٣) حقول الكسور

Fields of Fractions

في بعض الأحيان يمكن أن نطمر حلقة R في حقل ، أي أن نجد حقلاً يحتوي على حلقة جزئية تماثل R . إنه من الممكن طمر الأعداد الصحيحة $\mathbb{Z}$ في الأعداد الكسرية Q . وهذا المثال له الخاصية التالية : ان كل عنصر في Q هو عبارة عن كسر بسطه ومقامه عناصر في $\mathbb{Z}$. ونريد هنا تعميم هذا الوضع .

تعريف

حقل الكسور للحلقة R هو حقل K يحوي حلقة جزئية R' تماثل R بحيث نستطيع كتابة كل عنصر في K على الصورة r/s ، حيث $r, s \in R'$ ، $s \neq 0$.

قبل أن نعطي الحالة العامة لبناء حقل الكسور للحلقة R لنرى كيف تمّ بناء الأعداد الكسرية Q من الأعداد الصحيحة $\mathbb{Z}$. من الممكن أن نعتبر أن العدد الكسري r/s هو عبارة عن الزوج (r,s) حيث $r, s \in \mathbb{Z}$. ولكن كل عدد كسري يقابل عدداً من الكسور

المختلفة ، فعلى سبيل المثال $\frac{10}{15} = \frac{4}{6} = \frac{2}{3}$ وهكذا ، ولذلك يجب علينا أن ننظر إلى الأزواج المرتبة $(4,6)$ و $(2,3)$ و $(10,15)$ على أنها متساوية . ولكي نصل إلى هذا فإننا نعرف علاقة تكافؤ على $\mathbb{Z}$ بحيث تكون جميع هذه الأزواج المرتبة متكافئة ، وبصورة عامة (r,s) و (t,u) يقابلان العدد الكسري نفسه إذا وفقط إذا كان $r / s = t / u$. أي أن $r u = s t$. وبتعميم ذلك نحصل على :

نظرية (٥,١)

يوجد لكل مجال كامل حقل كسور .

البرهان

لنفرض أنّ R مجال كامل ولنفرض أن S هي مجموعة جميع الأزواج المرتبة (r,s) حيث $r,s \in R$ ، $s \neq 0$. لنعرف العلاقة ~ على S كالتالي :

$$(r,s) \sim (t,u) \iff r u = s t \ .$$

من السهل أن نبرهن أنّ ~ علاقة تكافؤ على S ، لنرمز لفصل تكافؤ (r,s) بالرمز $[r,s]$. لتكن F هي مجموعة فصول التكافؤ . سنبرهن على أن F هو حقل كسور R . لنعرف أولاً عمليتي الضرب والجمع على F كالتالي :

$$[r,s] + [t,u] = [r u + t s, s u]$$

$$[r,s]\,[t,u] = [r t, s u] \ .$$

وبعد ذلك يجب علينا أن نجري حسابات طويلة نوعًا ما لكي نثبت أن F يحقق جميع خواص حقل الكسور ، وبما أن هذه الحسابات روتينية فإننا لن نجريها هنا ولكننا نحث القاريء الذي لم يسبق له إجراؤها أن يجريها . والمطلوب برهانه هو التالي :

(١) عمليتي الجمع والضرب حسنة التعريف . أي أنــه إذا كـان

$$(r,s) \sim (r',s') \text{ و } (t,u) \sim (t',u')$$

فإن :

$$[r,s]+[t,u] = [r',s']+[t',u'] \text{ و } [r,s][t,u] = [r',s'][t',u'] \ .$$

(٢) F مجموعة مغلقة تحت تأثير عمليتي الجمع والضرب .

(٣) F حقل .

(٤) الدالة $F \to R$ المعرّفة بـ $[r,1] \to r$ تشاكل متباين .

(٥) $[r,s] = [r,1] / [s,1]$. Δ

يمكن أن نبرهن أنه إذا كان R مجالاً كاملاً معطى فإن جميع حقوله الكسرية متماثلة (انظر تمرين ١٦ , ١) . وعليه فإننا نستطيع القول أن حقل الكسور الذي حصلنا عليه أعلاه ، هو حقل الكسور الوحيد للمجال الكامل R . لقد جرت العادة ألا نميز بين العنصر $r \in R$ وصورته $[r,1] \in F$ ونكتب $[r,s] = r / s$.

(١,٤) كثيرات الحدود

Polynomials

من المهم جدًا أن نعرّف طبيعة وخواص كثيرات الحدود في بداية هذا الكتاب، وجميعنا يعلم أن كثيرة الحدود هي عبارة جبرية مثل $t^2 - 2t + 6$ أو $2t^5 + 7t^2 - 11$.

لقد تعودنا في الحقيقة أن نفكّر في كثيرة الحدود كدالّة في t ، فمثلاً : إنّ كثيرة الحدود الأولى تعرّف لنا دالة f بحيث $f(t) = t^2 - 2t + 6$ ، ولكن عندما تكون معاملات كثيرة الحدود تنتمي إلى حقل أو حلقة معيّنة ، فإنّه من الممكن أن نحصل على عبارات جبرية مختلفة في t بحيث تعرف جميعها نفس الدالة، وعلى سبيل المثال ليكن $\mathbb{Z}_2=\{0,1\}$ هو حقل الأعداد الصحيحة قياس 2 وليكن لدينا كثيرتا الحدود :

$$f(t) = t, \quad g(t) = t^2$$

لأسباب كثيرة فإنّه من المهم أن نعتبر أن كثيرتي الحدود أعلاه مختلفتان ، ومن هذه الأسباب أن كثيرة الحدود الثانية هي مربع الأولى ولكن الأولى ليست مربعًا للثانية .

ولكن لو فكّرنا في كثيرتي الحدود كدالتين من $\mathbb{Z}_2$ إلى $\mathbb{Z}_2$ فإننا نجد أنّ

$$f(0) = 0 = g(0)$$

$$f(1) = 1 = g(1)$$

أي أن $f = g$. ولتجنب هذه المشكلة فإنّنا سوف نعتبر أنّ كثيرتي حدود تكونان مختلفتين إذا كانتا مختلفتين في الشكل، ولكن أي كثيرة حدود تعرّف لنا دالة بتعويض قيم

للمتغيّر ، وهذه الدالة مهمة أيضًا .

لتكن R حلقة إبدالية . نعرّف كثيرة الحدود على R في المجهول t كالتالي :

$$r_0 + r_1 t + \ldots + r_n t^n$$

حيث $r_0, r_1, \ldots, r_n \in R$ ، $t, 0 \le n \in \mathbb{Z}$ مجهول . وإذا ابتغينا التقيّد بلغة المجموعات نستطيع أن نمثّل هذا التعبير بالمتتالية $(r_0, r_1, \cdots, r_n)$ ، [أنظر تمرين (١٧ , ١)]. تسمى العناصر $r_0, r_1, \cdots, r_n$ بمعاملات كثيرة الحدود . في العادة الحدود $0t^m$ إما أن تسقط أو تكتب 0 والحدود $1t^m$ تستبدل بـ t^m . نقول إن كثيرتي الحدود متساويتان إذا وفقط إذا كانت المعاملات المتقابلة متساوية (على اعتبار أن معاملات قوى t غير الظاهرة في كثيرة الحدود هي الصفر).

سنستخدم الترميز

$$\sum r_i t^i$$

بدلاً من

$$r_0 + r_1 t + \ldots + r_n t^n$$

حيث $i \ge 0$ أعدادًا صحيحة ، $r_k = 0$ إذا كانت $k \ge n$.

وإذا كانت

$$r = \sum r_i t^i$$

$$s = \sum s_i t^i$$

كثيرتي حدود فإنّنا نعرّف حاصل الجمع وحاصل الضرب كالتالي

$$r + s = \sum (r_i + s_i) t^i$$

$$r s = \sum q_j t^j$$

حيث

$$q_j = \sum_{h+i=j} r_h s_i$$

وباستخدام التعريفين السابقين يكون من السهل البرهان على أنّ مجموعة جميع كثيرات الحدود على R في المجهول t تكوّن حلقة تسمى بحلقة كثيرات الحدود على R

في المجهول t ويرمز لها بالرمز$R[t]$. إذا كانت ....u,v,w, مجاهيل مختلفة فإنّنا نحصل على حلقات ,...$R[u], R[v], R[w]$ وهذه جميعها متماثلة . ونستطيع أيضًا أن نعرف كثيرة حدود في أكثر من مجهول $t_1, t_2, \cdots$ ونحصل على حلقة كثيرة الحدود

$$R[t_1, t_2, \cdots]$$

بطريقة متماثلة .

في العادة نرمز لعنصر في الحلقة $R[t]$ بحرف واحد مثل f إذا كان المجهول واضحًا أما إذا كان هناك غموض فإننا نرمز للعنصر بالرمز $f(t)$. ولسوء الحظ فإن هذا الترميز يظهر لنا f على أنها دالّة في متغير t وهذا ليس صحيحًا . وإن أي كثيرة حدود $f \in R[t]$ تعرف لنا دالة من R إلى R كالتالي : إذا كانت

$$f = \Sigma r_i t^i$$

وكان $\alpha \in R$ فإن صورة α هي :

$$\Sigma r_i \alpha^i$$

وهذا الأخير ما هو إلا عنصر في R وليس كثيرة حدود . ولقد جرت العادة على أن تستخدم الرمز f نفسه ليعبر عن هذه الدالة ، وعليه فإن $f(\alpha) = \Sigma r_i \alpha^i$. ويعتبر سوء استخدام الترميز هذا عرفًا ولكن بشيء من الحذر سوف لا يشكل إرباكًا للقارىء .

وسوء استخدام آخر للترميز هو استبدال المجهولين في كثيرة حدود بمجهول آخر ؛ أي أنه إذا كان t,u مجهولين وكان $f(t) = \Sigma r_i t^i$ فإنّنا يمكن أن نكتب $f(u) = \Sigma r_i u^i$. ومن الواضح أيضًا ما نعنيه بـ $f(t+1)$ وهكذا . من المهم دائمًا أن نتذكر أنه من الممكن لكثيرتي حدود مختلفتين على R أن نعرف لنا دالة واحدة . فعلى سبيل المثال لقد رأينا أن كثيرتي الحدود t و t^2 على $\mathbb{Z}_2$ تعرف لنا دالّة واحدة وهي دالة الوحدة ، وهذا هو أحد الأسباب التي تجعل من غير الحكمة تعريف كثيرة الحدود كدالة ، وسبب آخر هو أننا نريد أن نعرف ماذا نعني بقولنا كثيرة حدود تقسم كثيرة حدود أخرى وهذا المفهوم ليس واضحاً للدوال المعرفة على R وخاصة إذا كان R حقلاً حيث إنه في هذه الحالة أي عنصر لا يساوي صفرًا يقسم أي عنصر في الحقل .

تمهيدية (١,٦)

إذا كان R مجالاً كاملاً وكان t مجهولا فإنّ $R[t]$ مجال كامل .

البرهان

لنفرض أن

$$f = f_0 + f_1 t + ... + f_n t^n, \quad g = g_0 + g_1 t + ... + g_m t^m$$

حيث $f_n \neq 0 \neq g_m$ وجميع المعاملات تنتمي إلى R. معامل t^{m+n} في fg هو $f_n g_m$ وبما أن R مجال كامل فإنّ $f_n g_m \neq 0$. وعليه إذا كان $f \neq 0$ و $g \neq 0$ فإن $fg \neq 0$. هذا يؤدّي إلى أن $R[t]$ مجال كامل . Δ

من نظرية (٥ , ١) نستطيع أن نحصل على حقل كسور للمجال الكامل $R[t]$. نسمى هذا الحقل بحقل العبارات الكسرية في t على R ونرمز له بالرمز $R(t)$. وعناصر هذا الحقل تكون على الصورة $p(t)/q(t)$ حيث p و q كثيرتي حدود ، q غير صفرية . بالمثل فإنّ حقل الكسور الجزئية للمجال الكامل $R[t_1, ..., t_n]$ هو $R(t_1, ..., t_n)$.

(١,٥) خوارزمية إقليدس

Euclidean Algorithm

سنحتاج إلى التعريف التالي :

تعريف

إذا كانت f كثيرة حدود على حلقة ابدالية R ، $f \neq 0$ فإن درجة f هي أعلى قوة للمجهول t التي تظهر في f بمعامل غير صفري .

وبكلام آخر إذا كانت $f = \sum r_i t^i$ وكان $r_n \neq 0$ و $r_m = 0$ حيث $m > n$ فإن درجة f هي n . سنرمز لدرجة f بالرمز ∂f. إذا كانت $f = 0$ فإنّنا سنعتبر $\partial f = -\infty$ حيث الرمز ∞ - يتمتع بالخواص التالية :

$n > -\infty$ لكل عدد صحيح n ، $-\infty + n = -\infty$ ، $-\infty \times n = -\infty$ ، $(-\infty)^2 = -\infty$.

النتائج التالية نحصل عليها مباشرةً من التعريف السابق :

قضية (١,٧)

إذا كان R مجالاً كامــلاً وكانت f، g كثيرتي حــدود على R فإن :

$$\partial (f + g) \leq \max (\partial f, \partial g)$$

$$\partial (f g) = \partial f + \partial g$$

[وجود المتباينة في السطر الأول يرجع لإمكانية اختصار الحدود العليا ، أنظر تمرين (١ , ٨)].

إنّ كثيرًا من النتائج المهمة في نظرية كثيرات الحدود يمكن الحصول عليها من ملاحظة إمكانية قسمة كثيرة حدود معينة على كثيرة حدود أخرى مع السماح لظهور باق لهذه القسمة .

قضية (١,٨)

لتكن f و g كثيرتي حدود على الحقل K ولنفرض أن $f \neq 0$. عندئذ يوجد كثيرتا حدود وحيدتان q و r على K بحيث يتحقق :

$$g = f q + r \text{ و } \partial r < \partial f$$

البرهان

نستخدم الاستنتاج الرياضي على ∂g .

إذاكانت $\partial g = -\infty$ فإن $g = 0$ وبهذه الحالة نأخذ $q = r = 0$.

إذاكانت $\partial g = 0$ و $\partial f = 0$ فإن $g = k \in K$ و $f = j \in K$. وفي هذه الحالة نأخذ $q = k / j$ و $r = 0$.

أما إذاكانت $\partial g = 0$ و $\partial f > 0$ نأخذ $q = 0$ و $r = g$.

نفرض الآن أن العبارة صحيحة لجميع كثيرات الحدود التي درجتها أقل من n ولنفرض أن $\partial g = n > 0$. إذا كانت $\partial f > \partial g$ فإننا نأخذ في هذه الحالة $q = 0$ و $r = g$. أما إذا كانت $\partial f \leq \partial g$ فلدينا في هذه الحالة :

$$f = a_m t^m + \ldots + a_0$$

$$g = b_n t^n + \ldots + b_0$$

حيث $a_m \neq 0 \neq b_n$ و $m \leq n$. لندع

$$g_1 = b_n a_m^{-1} t^{n-m} f - g$$

وبما أن الحدود ذات الدرجات العليا تختصر فإنّ $\partial g_1 < \partial g$. باستخدام الاستنتاج الرياضي نستطيع أن نجد كثيرتي حدود q_1 و r_1 بحيث يتحقق :

$$g_1 = f q_1 + r_1 \quad ، \quad \partial r_1 < \partial f$$

وإذا فرضنا الآن أنّ:

$$q = b_n a_m^{-1} t^{n-m} - q_1$$

$$r = - r_1$$

نحصل على :

$$g = f q + r \quad ، \quad \partial r < \partial f .$$

ولبرهان الوحدانية نفرض أن :

$$g = f q_1 + r_1 = f q_2 + r_2 \quad ، \quad \partial r_1 , \partial r_2 < \partial f$$

ومنه نجد أن :

$$f(q_1 - q_2) = r_2 - r_1$$

وباستخدام قضية (٧ , ١) نجد أن درجة كثيرة الحدود في الطرف الأيسر أكبر من درجة كثيرة الحدود في الطرف الأيمن إلا إذا كان كلاهما صفرًا. وبما أنّ $f \neq 0$ يجب أن يكون $q_1 = q_2$ و $r_1 = r_2$. Δ

في القضية (٨ , ١) تسمى q بخارج القسمة وتسمى r الباقي ، ولإيجاد q و r نستخدم طريقة تعرف بخوارزمية القسمة .

نقدم الآن مفهوم الانقساميّة لكثيرات الحدود وعلى الأخص مفهوم القاسم المشترك الأعظم الذي سيكون له دور مهم في حساب كثيرات الحدود في الفصل الثاني .

تعريف

لتكن f و g كثيرتي حدود على الحقل K نقول إنّ f تقسم g (أو f قاسم لـ g أو g مضاعف لـ f) ونكتب $f \mid g$ إذا وجدت كثيرة حدود h على K بحيث $g = fh$ ، أما إذا

كانت f لا تقسم g فإننا نكتب $f \nmid g$. ونقول إنّ كثيرة الحدود d على الحقل K هي قاسم مشترك أعظم لكثيرتي الحدود f و g (ونكتب $h\,c\,f$) إذا تحقق التالي :

(١) $d \mid f$ و $d \mid g$

(٢) *إذا كان $e \mid f$ و $e \mid g$ فإن $e \mid d$.*

لاحظ أنّنا قلنا قاسم مشترك أعظم وليس القاسم المشترك الأعظم ، وذلك لأنه ليس من الضروري أن يكون وحيدًا. التمهيدية التالية تبرهن لنا وحدانية h c f باستثناء القواسم الثابتة (أي كثيرات الحدود التي لها درجة صفر) .

تمهيدية (١,٩)

إذا كان d هو $h\,c\,f$ لكثيرتي الحدود f و g على الحقل K وكان $0 \neq k \in K$ فإن $k\,d$ هو $h\,c\,f$ لكثيرتي الحدود f و g . وإذا كان كل d و e هما $h\,c\,f$ لكثيرتي الحدود f و g فإنه يوجد $k \in K$ ، $k \neq 0$ بحيث $e = k\,d$.

البرهان

من الواضح أن $kd \mid f$ و $kd \mid g$ ، وإذا كان $e \mid f$ و $e \mid g$ فإنّ $e \mid d$ وعليه فإن $e \mid kd$ ، وبالتالي فإنّ $k\,d$ هو h c f .

إذا كان كل من d و e هو h c f فإن $e \mid d$ و $d \mid e$ ؛ وعليه فإن $e = kd$ حيث k كثيرة حدود على K . وبما أن $e \mid d$ فإنّ $\partial e \leq \partial d$ وعليه فإنّ $\partial k \leq 0$. إذن $k \in K$. وبما أن $0 \neq e = k\,d$ فإنه يجب أن تكون $k \neq 0$. Δ

سنبرهن الآن على أنّه يجب أن يكون لكل كثيرتي حدود غير صفريتين على حقل ما قاسم مشترك أعظم واحد وذلك بتقديم طريقة لحساب h c f . وهذه الطريقة هي تعميم للطريقة التي قدّمها إقليدس (c. 600 BC) لحساب القاسم المشترك الأعظم لعددين صحيحين ولذلك فإنها تعرف بخوارزمية إقليدس .

خوارزمية (١,١٠)

(أ) المعطيات : كثيرتا حدود f و g كل منهما لا تساوي صفرًا على حقل K .

(ب) الطريقة : للتبسيط دع $f = r_{-1}$ ، $g = r_0$. *استخدم خوارزمية القسمة لتحصل على التوالي على كثيرتي حدود* q_i و r_i *على* K *بحيث يتحقق التالي :*

$$
\begin{aligned}
r_{-1} &= q_1 r_0 + r_1 \quad ، \quad \partial r_1 < \partial r_0 \\
r_0 &= q_2 r_1 + r_2 \quad ، \quad \partial r_2 < \partial r_1 \\
r_1 &= q_3 r_2 + r_3 \quad ، \quad \partial r_3 < \partial r_2 \qquad (١,١) \\
&\vdots \\
r_i &= q_{i+2} r_{i+1} + r_{i+2} \quad ، \quad \partial r_{i+2} < \partial r_{i+1} \\
&\vdots
\end{aligned}
$$

بما أنّ درجات كثيرات الحدود r_i تتناقص فإنّنا يجب أن نصل إلى مرحلة نتوقف عندها وهذا يحدث عندما يكون لدينا كثيرة حدود r_{s+2} بحيث $r_{s+2} = 0$ وبالتالي فإنّ آخر معادلة تكون :

$$r_s = q_{s+2} r_{s+1} \; . \qquad (١,٢)$$

نظرية (١,١١)

اعتمادًا على الترميز السابق r_{s+1} *هي قاسم مشترك أعظم لكثيرتي الحدود* f *و* g *على* K.

البرهان

سنبرهن أولاً على أنّ r_{s+1} تقسم كل من f و g، وسنستخدم الاستنتاج التناقصي للبرهان $r_{s+1} \mid r_i$ لكل i.

من الواضح أنّ $r_{s+1} \mid r_{s+1}$. باستخدام المعادلة (١,٢) نجد أنّ $r_{s+1} \mid r_s$.

وباستخدام (١,١) نستنتج أنّه إذا كان $r_{s+1} \mid r_{i+2}$ و $r_{s+1} \mid r_{i+1}$ فإنّ $r_{s+1} \mid r_i$.

وبالتالي فإنّ $r_{s+1} \mid r_i$ لكل i ، وعلى وجه الخصوص $g = r_0 \mid r_{s+1}$ و $f = r_{-1} \mid r_{s+1}$.

الآن نفرض أنّ $e \mid g$ و $e \mid f$. باستخدام (١,١) نحصل على $e \mid r_i$. ومنه

$e \mid r_{s+1}$. وبالتالي فإن r_{s+1} قاسم مشترك أعظم لكثيرتي الحدود f و g . Δ

مثال

لتكن $f = 2t^7 + t^3 - 1$ و $g = t^3 + 4$

على Q . نحسب قاسم مشترك أعظم كالتالي :

$$2t^7 + t^3 - 1 = (t^3 + 4)(2t^4 - 8t + 1) + (32t - 5)$$

$$t^3 + 4 = (32t - 5)\left(\frac{t^3}{32} + \frac{5t}{1024} + \frac{25}{32768}\right) + \frac{131197}{32768}$$

$$32t - 5 = \frac{131197}{32768}\left(\frac{32768}{131197}(32t - 5)\right) + 0$$

وبالتالي فإنّ hcf هو 131197/32768 .

كذلك فإنّ أي مضاعف كسري (وعلى وجه الخصوص 1) هو hcf لكثيرتي الحدود f و g .

سننهي هذا الفصل بتقديم خاصيّة للقاسم المشترك الأعظم لكثيرتي حدود مستخدمين لذلك خوارزمية إقليدس .

نظرية (١,١٢)

لتكن f و g كثيرتي حدود غير صفريتين على الحقل K وليكن d هو hcf لهما .
عندئذ يوجد كثيرتي حدود a و b على K بحيث تتحقق المساواة :

$$.d = af + bg$$

البرهان

بما أنّ hcf وحيد باستثناء القواسم الثابتة فإنّنا نستطيع أن نفرض أنّ $d = r_{s+1}$ حيث المعادلتين (١ , ١) و (٢ , ١) متحققتين ، و ندعى كفرضية للاستنتاج وجود كثيرتي حدود a_i و b_i بحيث :

$$.d = a_i r_i + b_i r_{i+1}$$

من الواضح أن هذا صحيح إذا كان $i = s + 1$ حيث نأخذ $a_i = 1, \ b_i = 0$. الآن باستخدام (١ , ١) نجد :

$$r_{i+1} = r_{i-1} - q_{i+1} r_i \ .$$

وباستخدام الاستنتاج نجد :

$$d = a_i r_i + b_i (r_{i-1} - q_{i+1} r_i) \ .$$

وإذا وضعنا

$$a_{i-1} = b_i$$
$$b_{i-1} = a_i - b_i \ q_{i+1}$$

فإننا نحصل على :

$$d = a_{i-1} r_{i-1} + b_{i-1} r_i \ .$$

وباستخدام الاستنتاج التناقصي

$$d = a_{-1} r_{-1} + b_{-1} r_0$$
$$= a f + b g$$

حيث $a = a_{-1}$ و $b = b_{-1}$. Δ

تزودنا خطوة الاستنتاج في البرهان السابق بطريقة عملية لحساب كثيرتي الحدود a و b.

تمـارين

(١ , ١) أثبت أنّ $15 \ \mathbb{Z}$ مثالية من $5 \ \mathbb{Z}$ وأن $5 \ \mathbb{Z} / 15 \ \mathbb{Z}$ يماثل $\mathbb{Z}_3$.

(١ , ٢) هل الحلقتان $\mathbb{Z}$ و $2 \ \mathbb{Z}$ متماثلتان ؟

(١ , ٣) اكتب جدولي الجمع والضرب لكل من $\mathbb{Z}_6$ ، $\mathbb{Z}_7$ و $\mathbb{Z}_8$. أي من هذه الحلقات مجال كامل ؟ وأيّ منها حقل ؟

(١ , ٤) لماذا جدولا الضرب والجمع في تمرين (١ , ٣) متناظرة حول القطر ؟

(١ , ٥) يعرف الحقل الأولي بأنه الحقل الذي ليس له حقول جزئية غير تافهة . أثبت أنه إذا كان K حقلاً أوليًا فإنه إما أن يماثل Q أو $\mathbb{Z}_p$. حيث p عددًا أوليًا .

(١,٦) أثبت أنّ الجدولين التاليين يمثلان حقلاً

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

.	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

جد الحقول الجزئية الأولية ومميّز هذا الحقل . هل هو يماثل $\mathbb{Z}_4$ ؟ كم عدد الحقول التي عناصرها أربعة ؟

(١,٧) أكمل التفاصيل التي تركت في برهان نظرية (٥ , ١)

(١,٨) بين أن الجزء الثاني من القضية (٧ , ١) غير صحيح إذا كان R حلقة وليس مجالاً كاملاً وذلك بأخذ $f = 3t$ و $g = 2t$ على $\mathbb{Z}_6$. هل يبقى الجزء الأول صحيحًا في هذه الحالة ؟

(١,٩) جد خارج قسمة g على f والباقي لكل مما يلي :

(أ) $g = t^7 - t^4 + 5$ ، $f = t^3 + 7$ على Q .

(ب) $g = t^2 + 1$ ، $f = t^2$ على Q .

(ج) $g = 4t^3 - 17t^2 + t - 3$ ، $f = 2t + 5†$ على $\mathbb{R}$.

(د) $g = t^3 + 2t^3 - t + 1$ ، $f = t + 2$ على $\mathbb{Z}_3$.

(هـ) $g = t^7 - 4t^6 + t^3 - 3t + 5$ ، $f = 2t^3 - 2$ على $\mathbb{Z}_7$.

(١,١٠) جد h c f لكل زوج من كثيرات الحدود في التمرين (٩ , ١) .

(١,١١) اكتب h c f على الصورة a f + b g لكل زوج من كثيرات الحدود في التمرين (٩ , ١) .

(١,١٢) لتكن R حلقة تحتوي على محايد ضربي 1 . نقول أن $x \in R$ عنصر وحدة إذا كان له نظير ضربي في R . لتكن U هي مجموعة جميع عناصر الوحدة في R . أثبت أن (. , U) زمرة .

(١٣ ,١) ادرس زمرة عناصر الوحدة لكل من $\mathbb{Z}_5$ ، $\mathbb{Z}_6$ ، $\mathbb{Z}_{12}$ و $\mathbb{Z}_{24}$.

(١٤ ,١) جد قيم n بحيث تكون رتبة كل عنصر في زمرة عناصر الوحدة لـ $\mathbb{Z}_n$ تقسم 2 .

(١٥ ,١) ضع علامة صح أو خطأ أمام كل من العبارات التالية :

(أ) لم يزد هذا الفصل شيئًا جديدًا لمعلوماتي .

(ب) يوجد h c f لكل زوج من كثيرات الحدود .

(ج) الدالّة $\partial : R[t] \rightarrow \mathbb{Z}$ المعرّفة كالتالي : $\partial(f) = \partial f$ تشاكل .

(د) يوجد حقل كسور لكل حلقة .

(هـ) كل حقل يجب أن يكون مماثلاً لحقل كسوره .

(و) يكون $\mathbb{Z}_n$ مجالاً كاملاً إذا وفقط إذا كان حقلاً .

(ر) كل مجال كامل يجب أن يكون حقلاً .

(ز) كل حقل يجب أن يكون مجالاً كاملاً .

(ح) كل كثيرة حدود على K يجب أن تكون دالّة من K إلى K .

(ط) إذا كان K حقلاً فإن $K[t]$ حقلاً .

(١٦ ,١) ليكن D مجالاً كاملاً و F حقل كسوره . وليكن K حقلاً . وليكن $\varphi : D \rightarrow K$ تشاكل متباين .

اثبت أنه يمكن توسيع φ لتشاكل متباين وحيد $\psi : F \rightarrow K$ معرفاً كالتالي :

$\psi(a/b) = \varphi(a) / \varphi(b)$ لكل $a, b \in D$.

وإذا اعتبرنا K حقل كسورٍ آخر للمجال الكامل D واعتبرنا φ دالة احتواء فبرهن أن جميع حقول الكسور يجب أن تكون متماثلة .

(١٧ ,١) يمكن تعريف $R[t]$ بلغة المجموعات كالتالي :

لتكن S مجموعة جميع المتتاليات اللانهائية

$$(r_n)_{n \in N} = (r_0, r_1, \ldots, r_n, \ldots)$$

حيث $r_n \in R$ لكل $n \in \mathbb{N}$ و $r_n = 0$ لكل n ما عدا مجموعة منتهية من $\mathbb{N}$. لنعرف عمليتي الجمع والضرب على S كالتالي :

$(r_n) + (s_n) = (t_n)$ حيث $t_n = r_n + s_n$

حيث $(r_n)(s_n) = (u_n)$ حيث $u_n = r_n s_0 + \ldots + r_0 s_n$.

إذاكانت R حلقة ابدالية فأثبت أن S حلقة ابدالية . أثبت أن الدالة

$$\theta : R \to S$$

حيث $\theta(r) = (r,0,0,0,\ldots)$

تطمر R في S . أثبت أن S يماثل $R[t]$.

لاحظ أنّه باستطاعتنا تعريف S دون الرجوع إلى العبارة $r_0 + \ldots + r_n t^n$.

وإذا ساوينا $r \in R$ بـ $\theta(r) \in S$ و t بـ $(0,1,0,0,0,\ldots) \in S$ فإنّ $(r_n) = r_0 + \ldots + r_N t^N$ حيث يمكن اختيار N بحيث $r_n = 0$ لكل $n > N$.

الفصل الثاني

تحليل كثيرات الحدود

Factorization of Ploynomials

تلعب معادلات كثيرات الحدود $(f(\alpha)=0)$ دورًا مهمّا في الرياضيات . حيث إنّ ايجاد أحد حلول معادلة كثيرة حدود أو جميع الحلول لهذه المعادلة يتطلب معالجة دقيقة . ولقد لوحظ أنه إذا كـــانـت $f=g\,h$ حيث درجة كل من g و h أصغر من درجة f فإنّ جـمـيـع حـلـول المـعـادلـة $(f(\alpha)=0)$ هـي مـجـمـوعـة حـلـول $g(\alpha)=0$ مـع حلول $h(\alpha)=0$ ومن هذه الملاحظة البسيطة نشأ حساب كثيرات الحدود ودراسة منظمة لقابلية القسمة لكثيرات الحدود قياسًا على نظيراتها للأعداد الصحيحة ، ولقد تطرقنا إلى أحد هذه الخواص في الفصل الأول وهي خوارزمية إقليدس .

وسندرس في هذا الفصل قابليّة القسمة وسنبرهن على وجود كثيرات حدود «لا مختزلة» تلعب دورًا مشابهًا لدور الأعداد الأولية في حلقة الأعداد الصحيحة . وسنبرهن كذلك أنّه يمكن كتابة أي كثيرة حدود معرفة على حقل ما كحاصل ضرب عدد منته من كثيرات الحدود اللا مختزلة بطريقة وحيدة ، و سنعرّف أيضًا ماذا نعني بأصفار كثيرة الحدود ونربط هذا المفهوم بنظرية التحليل ، وفي البند الأخير سنرى كيفية بناء كثيرة حدود بمعرفة أصفارها .

(٢,١) اللا اختزالية

Irreducibility

التعريف التالي يناظر العدد الأوّلي في كثيرات الحدود .

تعريف

نقول إنّ كثيرة حدود معرّفة على حلقة إبداليّة بأنّها قابلة للاختزال إذا استطعنا كتابتها كحاصل ضرب كثيرتي حدود درجة كل منهما أصغر من درجة كثيرة الحدود المعطاة . وإذا كانت غير قابلة للاختزال فإنّنا نسميها لا مختزلة .

أمثلـة

(١) جميع كثيرات الحدود مـن الدرجة 0 أو 1 لا مختزلـة ، لأنـه لا يمكـن كتابـة أي منها كحاصل ضرب كثيرتي حدود بدرجة أصغر .

(٢) كثيرة الحدود $t^2 - 2$ لا مختزلة على $\mathbb{Q}$. لنرى ذلك نفرض أنها قابلة للاختزال . عندئذ

$$t^2 - 2 = (at + b)(ct + d)$$

حيـث $a, b, c, d \in \mathbb{Q}$ ، وبـالقسمـة عنـد الضـرورة مـن الممكـن أن نفـرض أنّ $a = c = 1$. ومنه $b + d = 0$ و $bd = -2$ ، وعليه فإن $b^2 = 2$. وهذا مستحيل لأنه لا يوجد عدد كسري مُرَبّعه يساوي 2 .

(٣) كثيرة الحدود $t^2 - 2$ قابلة للاختزال على $\mathbb{R}$ وذلك لأن :

$$t^2 - 2 = (t - \sqrt{2})(t + \sqrt{2})$$

من الواضح وجود كثيرات حدود لا مختزلة على حقل ما ولكنّها تصبح قابلة للاختزال على حقل أكبر .

إنّ أيّة كثيرة حدود قابلة للاختزال يمكن كتابتها كحاصل ضرب كثيرتي حدود بدرجة أصغر . إذا كانت إحداهما لا زالت قابلة للاختزال فإننا نستطيع كتابتها أيضًا كحاصل ضرب كثيرتي حدود بدرجة أصغر وهلم جرا . إن هذه العملية يجب أن تتوقف لأن درجات كثيرات الحدود لا يمكن أن تتناقص إلى ما لا نهاية ، وهذه هي الفكرة وراء برهان النظرية التالية :

نظرية (١,٢)

إذا كانت g كثيرة حدود غير صفرية على حقل K فإنّه من الممكن كتابة g كحاصل ضرب عدد منته من كثيرات الحدود اللا مختزلــة على K .

البرهان

نستخدم الاستنتاج الرياضي على درجة g .

إذا كانت $\partial g = 0$ أو $\partial g = 1$ فإنّ g لا مختزلة .

إذا كانت $\partial g > 1$ فــإنّــه إمّــا أن تكــون g لا مخــتزلــة أو أن $g = hj$ بــحيــث $\partial h , \partial j < \partial g$.

وباستخدام فرضيّة الاستنتاج نستطيع كتابة كل من j , h كحاصل ضرب كثيرات حدود لا مختزلة ، وبالتالي فإننا نستطيع كتابة g كحاصل ضرب كثيرات حدود لا مختزلة . Δ

إن أهمية الأعداد الأولية في $\mathbb{Z}$ لم تنشأ من امكانية تحليل أي عدد صحيح إلى عوامل أولية ولكن من كون هذا التحليل وحيد (باستثناء الترتيب) . وبالمثل فإن أهمية كثيرات الحدود اللا مختزلة تعتمد على نظرية الوحدانية ، و إنّ هذه الوحدانية ليست واضحة [انظر : Hardy And Wright, 1962, p. 211) . في حلقات معينة نستطيع أن نكتب أي عنصر كحاصل ضرب عدة عناصر لا مختزلة وبدون أن تكون هذه الطريقة وحيدة .

سنبرهن هنا على وحدانية تحليل كثيرات الحدود على حقل .

تعريف

إذا كانت f و g كثيرتي حدود على حقل K وكان $h\,c\,f = 1$ فإنّنا نقول إن f و g أوليتان نسبيًا .

الآن نبرهن التمهيدية التالية :

تمهيدية (٢،٢)

ليكن K حقلاً ، و f كثيرة حدود لا مختزلة على K ، g و h كثيرتي حدود على K . إذا كانت f تقسم $g\,h$ فإنّه إمّا أن تكون f تقسم g أو f تقسم h .

البرهان:

نفرض أنّ f لا تقسم g . ليكن d هو $h\,c\,f$ لكثيرتي الحدود f، g . وبما أنّ f لا مختزلة و $d \mid f$ فإنّ $d = k\,f$ $(k \in K)$ أو $d = k$ $(k \in K)$. وإذا كان $d = k\,f$ فإنّ $f \mid g$ وهذا يناقض الفرض . إذن $d = k$ وبالتالي فإن 1 أيضا يكون $h\,c\,f$ لـ f و g ومنه فإنّ g و f أوليتان نسبيًا . وباستخدام نظرية (١٢ , ١) نستطيع ايجاد كثيرتي حدود a و b على K بحيث :

$$1 = a\,f + b\,g .$$

إذن

$$h = h\,a\,f + h\,b\,g .$$

الآن $f \mid haf$ و $f \mid hbg$ (لأن $f \mid gh$). إذن $f \mid h$. وبهذا يتم البرهان . Δ

نستطيع الآن برهان الوحدانية .

نظرية (٢،٣)

لكل حقل K ، يكون تحليل كثيرات الحدود على K إلى كثيرات حدود لا مختزلة وحيدًا (باستثناء ترتيب العوامل وباستثناء العوامل الثابتة) .

البرهان

لنفرض أنّ $f = f_1 f_2 \dots f_r = g_1 g_2 \dots g_s$

حيث f كثيرة حدود على K و $f_1, f_2, \dots, f_1, g_1, g_2, \dots g_s$ كثيرات حدود لا مختزلة على K . وإذا كانت جميع كثيرات الحدود f_i ثابتة فإن $f \in K$ وبالتالي فإنّ جميع g_j ثابتة . وبالتالي فإننا نستطيع أن نفرض أن f_i كثيرة حدود غير ثابتة لكل $i = 1, \dots, r$. إذن $f_1 \mid g_1 g_2 \dots g_s$ وباستخدام الاستنتاج الرياضي وتمهيدية (٢ , ٢)

نجد أن $f_1 \mid g_i$ لعدد ما i . نستطيع أن نفترض أنّ $i=1$. ومنه $f_1 \mid g_1$. بما أن f_1 و g_1 لا مختزلتان و f_1 غير ثابتة فإننا نجد $f_1 = k_1 g_1$ حيث $k_1 \in K$. وبالمثل فإن $f_2 = k_2 g_2$ ، . . . ، $f_r = k_r g_r$ حيث $k_2, \ldots, k_r \in K$. وكذلك فإن جميع g_j $(j > r)$ يجب أن تكون ثوابت لأنه ما عدا ذلك فإنّنا سوف نجد أن درجة الطرف الأيمن أكبر من درجة الطرف الأيسر. وبهذا يتم البرهان. Δ

(٢,٢) اختبارات اللااختزالية

Tests for Irreducibility

إنّه لمن الصعب جدّا بصورة عامة أن نقدّر فيما إذا كانت كثيرة حدود معطاة لا مختزلة. فعلى سبيل المثال فكّر في كثيرة الحدود :

$$t^{16}+t^{15}+t^{14}+t^{13}+t^{12}+t^{11}+t^{10}+t^{9}+t^{8}+t^{7}+t^{6}+t^{5}+t^{4}$$

$$+t^{3}+t^{2}+t+1$$

(إن هذا ليس مجرد مثالاً سخيفاً لأنّنا سندرس كثيرة الحدود هذه بالتحديد في الفصل السابع عشر).

ليس من المجدي أن نحاول إيجاد جميع العوامل الممكنة لأنّه من الممكن أن يكون هناك عدد لا نهائي من هذه المحاولات ، ولكن باستثناء عدد كاف من هذه المحاولات فإنه من الممكن استخدام هذه الطريقة إذا فشلت جميع الطرق الأخرى. ولكن الذي نريده هنا هو إيجاد حيل بسيطة نحتفظ بها لحين الحاجة إلى استخدامها، ومن أهمها ميزان أيزنستاين(Eisenstein's criterion) . وهذه تطبق على كثيرات الحدود على $\mathbb{Z}$ ، ولكن من المعروف أن اللا اختزالية على $\mathbb{Z}$ تكافيء اللا اختزالية على Q وهذا ما قام ببرهانه جاوس وسنبدأ به.

قضية (٢,٤)

إذا كانت f كثيرة حدود لا مختزلة على $\mathbb{Z}$ فإنها أيضًا تكون لا مختزلة على Q.

البرهان

إنّ الغرض من هذه القضية أنّه عندما نتوسع إلى Q يمكن أن تظهر كثيرات حدود جديدة تكون عوامل لـ f . وسنرى أنّ هذا لا يمكن حدوثه، ولذلك نفترض أن f لا مختزلة على $\mathbb{Z}$ ولكنها قابلة للاختزال على Q . إذن يوجد كثيرتا حدود g و h على Q بحيث $f = gh$، و $\partial h, \partial g < \partial f$. وبالضرب في حاصل ضرب مقامات معاملات h و g نستطيع أن نكتب:

$$n f = g' h'$$

حيث $n \in \mathbb{Z}$ و g', h' كثيرتا حدود على $\mathbb{Z}$.

سنبرهن الآن امكانية اختصار عوامل n الأولية واحدًا واحدًا دون أن نخرج عن $\mathbb{Z}[t]$.

لنفرض أن p عامل أولي للعدد n . ندعي أنه إذا كان

$$g' = g_0 + g_1 t + ... + g_r t^r$$

$$h' = h_0 + h_1 t + ... + h_s t^s$$

فإنه إما أن يكون p يقسم جميع معاملات g_i أو p يقسم جميع معاملات h_j . إذا لم يكن هذا صحيحًا فإننا نستطيع إيجاد أصغر عددين i و j بحيث p لا يقسم g_i و p لا يقسم h_j ولكن p يقسم معامل t^{i+j} في $g' h'$ وهذا المعامل هو:

$$h_0 g_{i+j} + h_1 g_{i+j-1} + ... + h_j g_i + ... + h_{i+j} g_0$$

ولكن من طريقة اختيار i و j نجد أن p يقسم جميع الحدود في العبارة السابقة ما عدا (ربما) $h_j g_i$. ولكن p يقسم جميع العبارة. إذن $p \mid h_j g_i$. وبما أنّ p لا يقسم h_j و p لا يقسم g_i فإنّ هذا يناقض اختيار i و j. وبهذا يتم برهان الادعاء.

وبدون التأثير على الحالة العامة نستطيع أنّ نفرض أن p يقسم جميع معاملات g_i . إذن $g' = p g''$ حيث g'' كثيرة حدود على $\mathbb{Z}$ درجتها مساوية لدرجة g' (أو g) .

لنفرض أن $n = p n_1$. عندئذ:

$$p n_1 f = p g'' h'$$

ومنه

$$n_1 f = g'' h' .$$

وبالاستمرار على هذا المنوال نستطيع أن نختصر جميع عوامل n الأولية ونصل في النهاية للمساواة :

$$f = \overline{g}\ \overline{h}$$

حيث $\overline{g}$ و $\overline{h}$ كثيرتا حدود على $\mathbb{Z}$ والتي تكوّن مضاعفات كسرية لكثيرتي الحدود الأصليتين g و h. ولكن هذا يناقض لا اختزالية f على $\mathbb{Z}$. وبالتالي فإن f يجب أن تكون لا مختزلة على Q . Δ

بعد هذه الحقيقة نستطيع برهان :

نظرية (٢,٥) (ميزان أيزنستاين للاختزالية)

لتكن

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n$$

كثيرة حدود على Z . وليكن q عدد أوّلي بحيث :

١ - q لا يقسم a_n

٢ - $q \mid a_i$ ، $i = 0,1,\ldots,n-1$

٣ - q^2 لا يقسم a_0

عندئذ f لا مختزلة على Q .

البرهان

باستخدام القضية (٢ , ٤) يكفي أن نبرهن أن f لا مختزلة على $\mathbb{Z}$. لنفرض لغرض التناقض أن $f = gh$ حيث

$$g = b_0 + b_1 t + \ldots + b_r t^r$$

$$h = c_0 + c_1 t + \ldots + c_s t^s$$

كثيرتا حدود على $\mathbb{Z}$ و $\partial h, \partial g < \partial f$.

عندئذ $r + s = n$ ، $b_0 c_0 = a_0$ ، باستخدام (٢) نجد أنّ $q \mid b_0$ أو $q \mid c_0$.

وباستخدام (٣) q لا يمكن أن يقسم كلاهما ، ولذلك نستطيع أنّ نفرض أنّ $q \mid b_0$ و q لا يقسم c_0 . إذا كانت جميع المعاملات b_i قابلة للقسمة على q فإنه عندئذ نجد أن a_n يقبل القسمة على q وهذا يناقض (١) . ليكن b_i أول معامل لـ g غير قابل للقسمة على q. إذن

$$a_i = b_i c_0 + \ldots + b_0 c_i$$

حيث $i < n$. وهذا يؤدي إلى أنّ $q \mid c_0$ ، لأنّ q يقسم $a_i, b_0, \ldots, b_{i-1}$ ولا يقسم b_i . وهذا تناقض . وبالتالي فإنّ f لا مختزلة . Δ

أمثلـــة

(١) لتكن

$$f(t) = \frac{2}{9} t^5 + \frac{5}{3} t^4 + t^3 + \frac{1}{3}$$ على Q .

كثيرة الحدود هذه لا مختزلة إذا وفقط إذا كانت

$$9\, g(t) = 2 t^5 + 15 t^4 + 9 t^3 + 3$$

لا مختزلة على Q .

وبتطبيق ميزان أيزنستاين حيث $q = 3$ نجد أن f لا مختزلة .

(٢) لتكن

$$f(t) = t^{16} + t^{15} + \ldots + 1$$

المذكورة سابقًا . لاحظ أنّ f غير قابلة للمعالجة ولكن من الواضح أن $f(t)$ لا مختزلة إذا وفقط إذا كانت $f(t+1)$ لا مختزلة . وإذا أوجدنـــا $f(t+1)$ فإننا نستطيع تطبيق ميزان أيزنستاين بأخذ $q = 17$ ، وبالتالي فإن f لا مختزلة على Q. (هناك سبب وجيه لاتباع هذه الطريقة دون اللجوء إلى الحسابات المباشرة . انظر تمهيدية (١٧ , ٩).

هناك واحد من أهم اختبارات اللا اختزالية وأسهل طريقة لتوضيح هذا الاختبار يكون بواسطة مثال ، والفكرة وراء الاختبار هي : أنّ التشاكل الطبيعي $\mathbb{Z} \to \mathbb{Z}_n$ يتوسع بشكل بديهي إلى تشاكل $\mathbb{Z}[t] \to \mathbb{Z}_n[t]$. عندئذ تكون كثيرة حدود قابلة للاختزال على $\mathbb{Z}$ ، وهي حاصل ضرب $g\,h$ والتشاكل يحافظ على هذا التحليل . وإذا كان n لا

يقسم أكبر معامل في كثيرة الحدود تحت الدراسة فإن صورة كثيرة الحدود هذه يجب أن تكون لا مختزلة على $\mathbb{Z}_n$ ، وعليه إذا كانت صورة كثيرة حدود لا مختزلة على $\mathbb{Z}_n$ فإنّ كثيرة الحدود الأصلية يجب أن تكون لا مختزلة على $\mathbb{Z}$. وبما أن $\mathbb{Z}_n$ مجموعة منتهية، فإنّه يكون هناك عدد منته من الحالات التي يجب دراستها.

عند التطبيق يكون مفتاح الّحل هو اختيار القيمة المناسبة للعدد n .

مثال

لتكن

$$f(t) = t^4 + 15\,t^3 + 7 \text{ على } \mathbb{Z} .$$

على $\mathbb{Z}_5$ تكون كثيرة الحدود هذه $t^4 + 2$. وإذا كانت كثيرة الحدود هذه قابلة للاختزال على $\mathbb{Z}_5$ فإنّه إمّا أن يكون لها عامل درجته 1 أو أنّها حاصل ضرب عاملين درجة كل منهما 2 .

في الحالة الأولى يجب أن يوجد عدد $x \in \mathbb{Z}_5$ بحيث $x^4 + 2 = 0$ ، ومثل هذا العنصر مستحيل الوجود (هناك خمس قيم فقط لمثل هذا العدد x)

في الحالة الثانية يكون لدينا (دون التأثير على الحالة العامة)

$$t^4 + 2 = (t^2 + a\,t + b)\,(t^2 + c\,t + d) .$$

ومنه نجد أن $a + c = 0$ ، $a\,c + b + d = 0$ ، $b\,d = 2$.

ومنه $b + d = a^2$ وهذه تأخذ القيم 0,1,4 لأنها هي جميع القيم المربعة في $\mathbb{Z}_5$.

وعليه إمّا $b\,(1 - b) = 2$ أو $- b^2 = 2$ أو $b\,(4 - b) = 2$. وبالتعويض عن كل القيم الممكنة للعدد b وهي 0,1,2,3,4 نجد جميع هذه المعادلات خاطئة، وعليه فإنّ $t^4 + 2$ لا مختزلة على $\mathbb{Z}_5$. إذن كثيرة الحدود الأصلية $f(t)$ لا مختزلة على $\mathbb{Z}$ وبالتالي على Q.

لاحظ لو أنّنا اخترنا $\mathbb{Z}_3$ فإن $f(t)$ تكون :

$$t^4 + 1 = (t^2 + t - 1)\,(t^2 - t - 1)$$

وهذه قابلة للاختزال. وبالتالي فإن قياس 3 يفشل في إعطائنا برهان اللا اختزالية.

إنّ محاولات التجريب هذه ليست مرضية ومن الأفضل أن تكون هناك طريقة

نستطيع تطبيقها دائمًا حتى لو كانت حساباتها طويلة وعديمة الفائدة عند التطبيق . وإذا كان الحقل هو Q فإنّ مثل هذه الخوارزمية موجودة وما عدا ذلك فإن الحل غير معروف حتى الآن .

(٢,٣) أصفار كثيرات الحدود

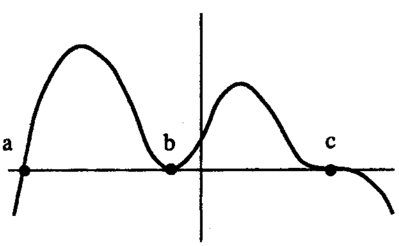
Zeros of Polynomials

سنبدأ بتقديم تعريف عام .

تعريف

لتكن R حلقة ابدالية و f كثيرة حدود على R . أي عنصر $\alpha \in R$ *بحيث* $f(\alpha) = 0$ *يسمى صفرًا لـ f في R .*

دعنا نأخذ كثيرة حدود على الأعداد الحقيقية . نستطيع هنا أن نرسم الشكل $y = f(x)$ والـذي من الممكـن أن يشبـه المنحنى في الشكل ١١ .



شكل (١١). أصفار مضاعفة لكثيرة حدود . عند (a) صفر بسيط، عند (b) صفر مضاعف مرتين . عند (c) صفر مضاعف ٣ مرات .

إن أصفار كثيرة الحدود $f(t)$ هي النقاط التي يتقاطع عندها المنحنى مع محور السينات . لتكن الأصفار a ، b، c المبينة في الشكل ١١ . عند a يظهر المنحنى على

شكل مستقيم عند المحور ، عند b يرتد المحور ، أما عند c فإنّه ينسحب بصورة أفقية . وإن تعميم هذه الظاهرة يتم بأن نقول إن b و c أصفار مضاعفة لكثيرة الحدود $f(t)$. يعتبر الصفر b صفرين متساويين ، أما الصفر c فيعتبر ثلاثة أصفار متساوية . ولكن إذا كانت متساوية فكيف يكون هناك إثنان منهما ؟ لتوضيح فكرة هذا السؤال يجب أن ندرس العوامل الخطّية (العوامل من الدرجة 1) لكثيرة الحدود f .

تمهيدية (٦ ,٢)

لتكن f كثيرة حدود على حقل K . يكون العنصر $\alpha \in K$ صفرًا لـ f إذا وفقط إذا كان $(t - \alpha) \mid f(t)$.

البرهان

إذاكان $(t - \alpha) \mid f(t)$ فإن

$$f(t) = (t - \alpha)\ g(t)$$

حيث g كثيرة حدود على K ، إذن

$$f(\alpha) = (\alpha - \alpha)\, g(\alpha) = 0 .$$

ولبرهان العكس ، لنفرض أن $f(\alpha) = 0$. باستخدام خوارزمية القسمة نستطيع إيجاد كثيرتي حدود q ، r على K بحيث :

$$f(t) = (t - \alpha)\, q(t) + r(t)$$

حيث $\partial r < 1$. إذن $r(t) = r \in K$. وبتعويض α عن t نجد أن :

$$0 = f(\alpha) = (\alpha - \alpha)\, q(\alpha) + r$$

ومنه $r = 0$. وبالتالي $(t - \alpha) \mid f(t)$. Δ

سنعرف الآن ما نعني بصفر مضاعف .

تعريف

لتكن f كثيرة حدود على حقل K . نقول إن $\alpha \in K$ صفر بسيط لـ f إذا كان $(t - \alpha) \mid f(t)$ ولكن $(t - \alpha)^2$ لا يقسم $f(t)$. ونقول إنّ α صفر مضاعف m من المرات إذا كان $(t - \alpha)^m \mid f(t)$ ولكن $(t - \alpha)^{m+1}$ لا يقسم $f(t)$. وتسمى الأصفار المضاعفة

أكثر من مرة بالأصفار المكررة (أو المضاعفة) .

فعلى سبيل المثال ، $t^3 - 3t + 2$ على Q لها الأصفار 2 − و 1 . وتحليل كثيرة الحدود هذه : $(t-1)^2 (t+2)$. إذن 2− صفر بسيط بينما 1 هو صفر مضاعف مرّتين .

عندما $K=\mathbb{R}$ وعندما نرسم منحنى كالذي في الشكل (١١) ، تكون النقاط a وشبيهاتها أصفارًا بسيطةً، والنقاط b وشبيهاتها أصفارًا مكررةً عدد زوجي من المرات أما c وشبيهاتها فإنها أصفارًا مكررةً عدد فردي أكبر من 1 من المرّات . أمّا الحقول العامة غير $\mathbb{R}$ (ما عدا Q أو حقول جزئية أخرى من $\mathbb{R}$) فإنّه لا يوجد معنى للمنحنى، ولكن الرسم الهندسي البسيط للحقل الحقيقي غالبًا ما يساعدنا على تخيّل الحالة العامة، وبالطبع الرسم وحده لا يعتبر برهانًا .

تمهيدية (٢,٧)

لتكن f كثيرة حدود غير صفرية على حقل K، ولتكن $\alpha_1, \dots, \alpha_r$ *أصفارها بتكرار* $m_1, \dots, m_r$ *على الترتيب . عندئذ .*

$$f(t) = (t-\alpha_1)^{m_1} \cdots (t-\alpha_r)^{m_r} g(t) \qquad (٢,١)$$

حيث g ليس لها أصفار في K. وبالعكس إذا تحققت المساواة (١ , ٢) وكانت g ليس لها أصفار في K فإن أصفار f في K هي $\alpha_1, \dots, \alpha_r$ بتكرار $m_1, \dots, m_r$ على الترتيب .

البرهان

لكل $\alpha \in K$ كثيرة الحدود $t - \alpha$ لا مختزلة، وعليه إذا كانت $\alpha \neq \beta$ فإنّ $t-\alpha$ و $t-\beta$ أوّليتان نسبيًا . ومن وحدانية التحليل (نظرية ٣ , ٢) نجد أن المعادلة (١ , ٢) محققة وأنه يستحيل أن يكون لـ g أصفار في K لأنه لو كان لـ g صفرًا في K فإنه يجب أن يكون لـ f أصفار أخرى أو أصفار بتكرار أكبر .

إن برهان العكس يتبع من وحدانية التحليل . Δ

من التمهيدية السابقة تستطيع برهان النظرية المشهورة التالية :

نظرية (٢,٨)

عدد أصفار كثيرة حدود على حقل (مع احتساب التكرار) أصغر أو يساوي درجة كثيرة الحدود .

البرهان

من المساواة (١ , ٢) نستنتج أن

$$m_1 + m_2 + \ldots + m_r \leq \partial f . \qquad \Delta$$

(٢,٤) كثيرات الحدود المتناظرة

Symmetric Polynomials

في العادة يكون لدينا كثيرة حدود، ويكون المطلوب منا ايجاد أصفارها . ولكن من الجائز أن يكون لدينا العكس، أي أن أصفار كثيرة حدود ما (مع التكرار) معطاة والمطلوب هو ايجاد كثيرة الحدود هذه . وهذه مسألة سهلة جداً ولدينا طريقة عامة لحلها، ومع سهولتها ، فإنّها مهمة من الناحية النظرية .

ليكن لدينا كثيرة حدود من الدرجة n أصفارها $\alpha_1, \alpha_2, \ldots, \alpha_n$. عندئذ فإنّ كثيرة الحدود هذه هي حاصل ضرب n من العوامل الخطية :

$$f(t) = k(t - \alpha_1) \ldots (t - \alpha_n)$$

حيث $k \in K$. لنفرض أنّ:

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n .$$

فلو وجدنا حواصل الضرب في المعادلة الأولى وقارنا المعاملات مع المعادلة الثانية نجد أن :

$$a_n = k$$

$$a_{n-1} = -k(\alpha_1 + \ldots + \alpha_n)$$

$$a_{n-2} = k(\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \ldots + \alpha_{n-1} \alpha_n)$$

$$\vdots$$

$$a_0 = k(-1)^n \alpha_1 \alpha_2 \ldots \alpha_n$$

المقادير في $\alpha_1, ..., \alpha_n$ في الطرف الأيمن (مع اهمال العوامل $\pm k$) لها تسمية خاصة.

تعريف

كثيرة الحدود المتناظرة الابتدائية من الرتبة r في المجاهيل $t_1, ..., t_n$ يرمز لها بالرمز $s_r(t_1, ..., t_n)$ وتعرف بأنها مجموع حواصل الضرب المختلفة الممكنة مأخوذة r في كل مرّة للعناصر $t_1, ..., t_n$. وإذا أسأنا استخدام اللغة وعوّضنا العناصر $\alpha_1, ..., \alpha_n$ بدلاً من $t_1, ..., t_n$ فإن الناتج هو كثيرة حدود متناظرة ابتدائية من الرتبة r في $\alpha_1, ..., \alpha_n$.

والمعادلات أعلاه يمكن كتابتها على الصورة:

$$a_{n-r} = k(-1)^r s_r(\alpha_1, ..., \alpha_n).$$

كثيرات الحدود هذه متناظرة لأنها لا تتغير بتبديل المجاهيل t_i. من الجدير بالذكر أن هنالك كثيرات حدود متناظرة غير ابتدائية، على سبيل المثال $t_1^2 + t_2^2 + ... + t_n^2$، إلا أنه يمكن التعبير عنها بدلالة كثيرات الحدود المتناظرة الابتدائية، ولبرهان ذلك انظر تمرين (١٣ , ٢).

نظرية (٢,٩)

أي كثيرة حدود متناظرة في $t_1, ..., t_n$ على حقل K يمكن كتابتها على شكل كثيرات حدود ابتدائية متناظرة $s_r(t_1, ..., t_n)$، $r = 0, ..., n$ درجاتها أقل أو تساوي درجة كثيرة الحدود الأصلية.

سنبرهن على نص معدل للنظرية (٩ , ٢) في النتيجة (١٥ , ٤). وسنحتاج نظرية (٩ , ٢) للبرهان على أن العدد π غير متسام (الفصل السادس). أحد براهين نظرية (٩ , ٢) يتم بواسطة الاستنتاج الرياضي ويمكن إيجاده في كتب الجبر (انظر: Salmon, 1885, p. 57). وكمثال تطبيقي على النظرية:

$$t_1^2 + t_2^2 = (t_1 + t_2)^2 - 2t_1 t_2 = s_1^2 - 2s_2.$$

تمـــارين

(١ , ٢) بيّن فيما إذا كانت كل من كثيرات الحدود التالية لا مختزلة أو قابلة للاختزال :

(أ) $t^4 + 1$ على $\mathbb{R}$،

(ب) $t^4 + 1$ على Q،

(ج) $t^7 + 11t^3 - 33t + 22$ على Q،

(د) $t^4 + t^3 + t^2 + t + 1$ على Q.

(هـ) $t^3 - 7t^2 + 3t + 3$ على Q،

(و) $t^4 + 7$ على $\mathbb{Z}_{17}$،

(ز) $t^3 - 5$ على $\mathbb{Z}_{11}$،

(ح) $t^2 - \alpha t + \beta$ على الحقل الحقل في تمرين (٦ , ١).

(٢ , ٢) في كل حالة من الحالات أعلاه حلل كثيرة الحدود إلى كثيرات حدود لا مختزلة.

(٣ , ٢) ليكن K حقلاً غير منته و f ، g كثيرتي حدود على K بحيث $f(\alpha) = g(\alpha)$ لكل $\alpha \in K$. اثبت أن $f = g$ ، هل تستطيع أن تضعف الفرض قليلاً ؟

(٤ , ٢) ليكن K حقلاً ولتكن f كثيرة حدود على K. نقول إن f أولية إذا تحقق الشرط التالي :

إذا كانت $f \mid gh$ فإن $f \mid g$ أو $f \mid h$.

أثبت أن $f \neq 0$ أولية إذا وفقط إذا كانت f لا مختزلة . (هذه النتيجة غير صحيحة إذا كان لدينا حلقة بدلاً من حقل).

(٥ , ٢) جد جميع أصفار كثيرات الحدود التالية ، على Q ، على $\mathbb{R}$ ، وعلى $\mathbb{C}$.

(ا) t^3+1 ،
(ب) $t^3-6t^2+11t-6$ ،
(ج) t^5+t+1 ،
(د) t^2+1 ،
(هـ) $t^4+t^3+t^2+t+1$ ،
(و) t^4-6t^2+11 .

(٢ , ٦) جد جميع كثيرات الحدود التي على الشكل t^2+at+b على $\mathbb{Z}_5$. في كل حالة جد a^2-4b .
ماذا تلاحظ ؟ هل تستطيع البرهان على ملاحظتك ؟

(٢ , ٧) جد ميزانًا لاختبار لا اختزالية كثيرة الحدود من الدرجة الثانية على حقل مميزه لايساوي 2 .

(٢ , ٨) برهن على أنّ مميّز الحقل $\mathbb{Z}_p(t)$ هو p حيث p عدد أوّلي .
هل $\mathbb{Z}_p(t)$ و $\mathbb{Z}_p$ متماثلان ؟

(٢ , ٩) اكتب كلاً مما يأتى بدلالة كثيرات حدود متناظرة ابتدائية في α, β, γ .
(ا) $\alpha^2+\beta^2+\gamma^2$ ،
(ب) $\alpha^3+\beta^3+\gamma^3$ ،
(ج) $\alpha^2\beta+\alpha^2\gamma+\beta^2\alpha+\beta^2\gamma+\gamma^2\alpha+\gamma^2\beta$ ،
(د) $\alpha^2\beta^2\gamma^2$ ،
(هـ) $(\alpha-\beta)^2+(\beta-\gamma)^2+(\gamma-\alpha)^2$ ،
(و) $(\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$ ،
(ز) $\alpha^2+\beta\gamma$.

(٢ ، ١٠) ما عدم الجدوى في حل معادلة كثيرة حدود بمحاولة حل معادلات كثيرات الحدود المتناظرة في الأصفار؟ (إذا كنت تشك في عدم الجدوى حاول حل كثيرة الحدود من الدرجة الثالثة) .

(٢ ، ١١) ضع علامة صح أو خطأ أمام كل من العبارات التالية :

(أ) كل كثيرة حدود على حقل K لها صفرًا في K .

(ب) إذا كانت كثيرة حدود لا مختزلة على Q فإنها لا مختزلة على $\mathbb{R}$.

(ج) إذا كانت كثيرة حدود لا مختزلة على $\mathbb{Z}$ فإنها لا مختزلة على Q .

(د) كثيرات الحدود من الدرجة الأولى لا مختزلة .

(هـ) جميع كثيرات الحدود المتناظرة ابتدائية .

(و) أي كثيرة حدود بدلالة كثيرات حدود متناظرة ابتدائية يجب أن تكون متناظرة .

(ز) يوجد عدد غير منته من كثيرات الحدود الا مختزلة على Q .

(ح) كثيرات الحدود الأولية نسبياً تكون درجاتها مختلفة .

(ط) كثيرة الحدود التي درجتها عدد أولي يجب أن تكون لا مختزلة

(ي) كثيرة الحدود التي درجتها عدد مؤلف يجب أن تكون قابلة للاختزال .

(٢ ، ١٢) لتكن $p(x,y) \in Q\,[x,y]$ كثيرة حدود متناظرة . برهن على أن $p(x,y)$ يجب أن تكون كثيرة حدود في $x\,y$ و $x+y$ كما يلي : إذا كانت p تحتوي على حد $a\,x^i\,y^j$ ، $i \neq j \in N$ و $a \in Q$ فبرهن على أن p يجب أن تحتوي على حد $a\,x^j\,y^i$. استخدم هذه الحقيقة لتعبّر عن p كمجموع حدود من الشكل $a(x^i\,y^j + x^j\,y^i)$ أو الشكل $a\,x^i\,y^j$. لاحظ أن :

$$x^i\,y^j + x^j\,y^i = x^i\,y^i(x^{j-i} + y^{j-i}) \text{ ، } i<j$$

$$x^i\,y^i = (x\,y)^i$$

$$(x^i + y^i) = (x+y)(x^{i-1} + y^{i-1}) - x\,y(x^{i-2} + y^{i-2})$$

ومن ثم أثبت أن p يمكن كتابتها كمجموع حدود كل منها كثيرة حدود في $x+y$ و xy.

(٢ , ١٣)* هـذا التمرين هـو تعميم لتمرين (٢ , ١٢) إلى n من المتغيّرات . لتكن $p(t_1,\dots,t_n)\in K[t_1,\dots,t_n]$ متناظرة ولتكن s_i هي كثيرات الحدود المتناظرة الابتدائية في t_j . يُعرّف ارتفاع وحيدة الحد $t_1^{a_1}t_2^{a_2}\dots t_n^{a_n}$ بأنه $a_1+2a_2+\dots+na_n$. يُعرّف ارتفاع p بأنه أكبر ارتفاع وحيدات الحد الموجودة في p ، وأفرض أن الجزء الأعلى لـ p هو مجموع الحدود التي ارتفاعها أعظمي . جد كثيرة حدود q على الصورة :

$$k s_1^{b_1} s_2^{b_2}\dots s_n^{b_n} \text{ ، } k\in K$$

والتي حدها الأعلى يساوي الحد الأعلى لكثيرة الحدود p . لاحظ أن ارتفاع p - q أصغر من ارتفاع p ، ثم استخدم الاستنتاج الرياضي على الارتفاع لتبرهن على أن p هي كثيرة حدود في s_i .

(٢ , ١٤)* لتكن $f(t)=a_n t^n+\dots+a_0\in K[t]$ ولنفرض أننا نستطيع أن نحلل f على حقل $K\subset L$ كالتالي:

$$f(t)=a_n(t-\alpha_1)\dots(t-\alpha_n) .$$

ضع $\sigma_j=\alpha_1^j+\dots+\alpha_n^j$

برهن معادلات نيوتن :

$$a_{n-1}+a_n\sigma_1=0$$

$$2a_{n-2}+a_{n-1}\sigma_1+a_n\sigma_2=0$$

$$\vdots$$

$$na_0+a_1\sigma_1+\dots+a_{n-1}\sigma_{n-1}+a_n\sigma_n=0$$

$$\vdots$$

$$a_0\sigma_k+a_1\sigma_{k+1}+\dots+a_{n-1}\sigma_{k+n-1}+a_n\sigma_{k+n}=0 \text{ ، } k\geq 1$$

بيّن كيفيّة استخدام هذه المعادلات استنتاجيًا لإيجاد صيغ لكل من $\sigma_1,\sigma_2,\sigma_3,\cdots$.

الفصل الثالث

امـتدادات الحقـول
Field Extensions

لقد صيغت نظريّة جالوا في البداية بدلالة كثيرات حدود على حقل الأعداد المركّبة . والصيغة الحديثة لهذه النظرية ما هي إلا تعميم للطرق التي اتّبعت في العقدين الثالث والرابع من هذا القرن على حقل عام . وبتبني وجهة النظر هذه فإنّ كثيرات الحدود تحت الدراسة تستبدل بامتداد الحقول . كل كثيرة حدود f على حقل K تعرف لنا حقلاً L يحتوي K . هناك فوائد جمة نجنيها من معالجة نظرية جالوا من وجهة نظر نظرية الحقول وتقديم كثيرات الحدود بمرحلة لاحقة .

في هذا الفصل سنعرّف امتدادات الحقول ونوضح العلاقة بينها وبين كثيرات الحدود. وسنعطي أيضًا تصنيفًا لأنماط أساسية لهذه الامتدادات ونقدم طرقًا لإنشائها .

(٣,١) امتدادات الحقول
Field Extensions

في النظرة الشاملة درسنا كثيرة حدود f (t) من الدرجة الرابعة على Q أصفارها $\pm i$ و $\pm\sqrt{5}$ ، ودرسنا العبارات الكسرية على Q لهذه الأصفار. وإن مجموعة جميع هذه العبارات الكسرية تكوّن حقلاً $Q \subseteq L$. ندّعي أن L يحتوي على جميع عناصر $\mathbb{C}$ التي على الصورة :

$$p + q\,i + r\sqrt{5} + s\,i\sqrt{5} \quad ، \quad p,q,r,s \in Q \ .$$

من الواضح أن L يجب أن يحتوي على جميع هذه العناصر ، وأنه ليس صعبًا أن نرى حاصل جمع وحاصل ضرب مثل هذه العناصر يعطينا عناصر من الشكل نفسه .
(هناك صعوبة نوعًا ما لاثبات أن مقلوب عنصر يجب أن يكون عنصرًا من الشكل

نفسه : أنظر إلى المجموعة الثالثة من الأمثلة) . وبناءً على ذلك فإنّ دراسة كثيرة حدود على Q تقودنا لدراسة حقل L يحتوي Q . وبالطريقة نفسها فإنّ دراسة كثيرة حدود على حقل عام K يقودنا لدراسة حقل L يحتوي K . سنسمي L امتدادًا للحقل K . ولأسباب تقنية إن هذا التعريف مقيد جدًا . إنّنا نريد أن نسمح لحالات يحتوي فيها L على صورة تماثلية من K وليس بالضرورة K نفسه .

تعريف

يسمى التشاكل المتباين $i : K \to L$ بامتداد حقلي، حيث K وL حقلان، K الحقل الأصغر و L الحقل الأكبر.

أمثلـة

(١) إن دوال الاحتواء $i_1 : \mathbb{Q} \to \mathbb{R}$ ، $i_2 : \mathbb{R} \to \mathbb{C}$ و $i_3 : \mathbb{Q} \to \mathbb{C}$ جميعها امتدادات حقلية .

(٢) إذا كان K حقلاً و K(t) حقل العبارات الكسرية على K و $i : K \to K(t)$ التشاكل المتباين الطبيعي (صورة كل عنصر في K هي كثيرة الحدود الثابتة المقابلة لهذا العنصر) ، فإنه من الواضح أن i امتداد حقلي .

(٣) لتكن P هي مجموعة الأعداد الحقيقية التي على الصورة $p + q\sqrt{2}$ حيث $p, q \in \mathbb{Q}$. ومن الواضح أن P حقل جزئي من $\mathbb{R}$ وذلك لأن

$$(p + q\sqrt{2})^{-1} = \frac{p}{p^2 - 2q^2} - \frac{q}{p^2 - 2q^2}\sqrt{2}$$

حيث $p \neq 0$ و $q \neq 0$. دالة الاحتواء $i : \mathbb{Q} \to P$ امتداد حقلي .

إذا كان $i : K \to L$ امتدادًا حقليًا فإننا عادة نطابق K مع صورته i(K) بحيث نعتبر دائمًا i بأنها دالة الاحتواء و K حقل جزئي من L . ونستخدم الترميز L : K للامتداد ونقول إن L امتداد لـ K . وفي المستقبل سوف نستخدم التطابق K مع i(K) .

المفهوم التالي هو مفهوم من الجبر المجرد :

تعريف

ليكن K حقلاً ، ولتكن X مجموعة جزئية غير خالية من K . الحقل الجزئي من K المنشأ من X هو تقاطع جميع الحقول الجزئية من K والتي تحتوي X .

على القاريء أن يقنع نفسه بأنّ هذا التعريف يكافيء كلاً مما يلي :

(١) أصغر حقل جزئي من K ويحتوي X .

(٢) مجموعة جميع عناصر K التي يمكن الحصول عليها من عناصر X بواسطة متتالية منتهية من العمليات المعرفة على الحقل مع اشتراط أن $X \neq \{0\}$.

مثـال

سنجد الحقل الجزئي من $\mathbb{C}$ المنشأ من $X = \{1,i\}$. (عندما يكون الحقل تحت الدراسة هو $\mathbb{C}$ فإن الرمز i هو كالعادة $\sqrt{-1}$. ليكن هذا الحقل L . عندئذ L يجب أن يحتوي على الحقل الجزئي الأولي Q من $\mathbb{C}$ ، وبما أنّ L مغلق تحت تأثير عمليات الحقل فإنّه يجب أن يحتوي على جميع العناصر التي على الشكل :

$$p + q\,i$$

حيث $p, q \in Q$. لتكن M هي مجموعة هذه العناصر . ندعي أن M حقل . من الواضح أن M مغلقة تحت عمليتي الجمع والضرب وكذلك :

$$(p + i\,q)^{-1} = \frac{p}{p^2 + q^2} - \frac{q}{p^2 + q^2}\,i$$

وعليه فإنّ كل عنصر غير صفري في M يجب أن يكون له نظير ضربي في M . إذن M حقل يحتوي X . وبما أنّ L هو أصغر حقل جزئي يحتوي X فإن $L \subseteq M$. ولكن من التعريف $M \subseteq L$. إذن $L = M$ ، ونكون قد وجدنا وصفًا للحقل الجزئي المنشأ من X.

في حالة امتداد الحقل $L : K$ يكون اهتمامنا منصبًا على الحقول الواقعة بين K و L. وهذا يعني أنّه باستطاعتنا أن نقصر اهتمامنا على المجموعات الجزئية X التي تحتوي على K وهذه المجموعات هي التي على الشكل $K \cup Y$ حيث $Y \subseteq L$.

تعريف

إذا كان $L : K$ امتداد و Y مجموعة جزئية من L فإنّ الحقل الجزئي من L المنشأ من $K \cup Y$ يكتب $K(Y)$ ونقول إننا حصلنا عليه من K بإقران Y .

مثال

ليكن $K = Q$ و $Y = \{i, -i, \sqrt{5}, -\sqrt{5}\}$. عندئذ $K(Y)$ يجب أن يحتوي K و Y . ويحتوي أيضًا على حاصل الضرب $i\sqrt{5}$ ، وعليه فإنه يحتوي على جميع العناصر التي على الشكل

$$\alpha = p + q\,i + r\sqrt{5} + s\,i\sqrt{5} \ ،\ p,q,r,s \in Q\ .$$

لتكن $L \subseteq \mathbb{C}$ هي مجموعة جميع هذه العناصر α . إذا برهنا على أن L حقلاً فإنّ $K(Y) = L$. لاحـظ أن L حقــل إذا وفقــط إذا كان

$$(p + q\,i + r\sqrt{5} + s\,i\sqrt{5})^{-1} \in L \ ،\ \text{لكل}\ (p,q,r,s) \neq (0,0,0,0)$$

سنبرهن هذا على مرحلتين . لتكن M هي المجموعة الجزئية من L التي تحتوي على جميع العناصر $p + q\,i$ ، $p,q \in Q$. عندئذ نكتب :

$$\alpha = x + y\sqrt{5}$$

حيث $x = p + q\,i \in M$ و $y = r + s\,i \in M$ لنضع

$$\beta = x - y\sqrt{5} \in L\ .$$

عندئذ

$$\alpha\beta = (x + y\sqrt{5})(x - y\sqrt{5}) = x^2 - 5y^2 = z \ ،$$

حيث $z \in M$. إذن $\alpha^{-1} = \beta z^{-1}$. الآن نضع . $z = u + v$ ، $u,v \in Q$ ونعتبر $w = u - v\,i$. بما أن $z\,w = u^2 + v^2 \in Q$ يكون لدينا

$$z^{-1} = (u^2 + v^2)^{-1}\, w \in M\ .$$

ومنه $\alpha^{-1} = \beta z^{-1} \in L$.

وهناك خيار آخر وهو أن نحسب المقدار :

$$(p + qi + r\sqrt{5} + si\sqrt{5})(p - qi + r\sqrt{5} - si\sqrt{5})(p + qi - r\sqrt{5} - si\sqrt{5})$$

$$\times (p - qi - r\sqrt{5} + si\sqrt{5})$$

ونثبت أنّ الناتج ينتمي إلى Q، ثم نقسم على :
$(p + q i + r\sqrt{5} + s i\sqrt{5})$.

لاحظ أن $K(Y)$ بصورة عامة أكبر بكثير من $K \cup Y$.

إذا كانت $Y = \{y\}$ فإنّنا نكتب $K(y)$ بدلاً من $K(\{y\})$ وبالطريقة نفسها نكتب $K(y_1, \ldots, y_n)$ بدلاً من $K(\{y_1, y_2, \ldots, y_n\})$.

أمثلة

(١) الحقل الجزئي $\mathbb{R}(i)$ من $\mathbb{C}$ يجب أن يحتوي جميع العناصر $x + y i$ حيث $x,y \in \mathbb{R}$. إذن $\mathbb{C} = \mathbb{R}(i)$.

(٢) ليكن K حقلاً و $K(t)$ حقل العبارات الكسرية في t على K . وهذا الحقل $K(t)$ هو أيضًا الحقل الجزئي المنشأ من $K \cup \{t\}$. وبما أنّ هذا الحقل مغلق تحت عمليات الحقل فإنّه يجب أن يحتوي على جميع العبارات الكسرية في t ، وبالتالي فإنه حقل العبارات الكسرية في t. إذن $K(t)$ يحمل نفس المعنى بغض النظر عن الطريقة التي ننظر له منها .

(٣) الحقل الجزئي من $\mathbb{R}$ الذي يحتوي على جميع العناصر $p + q\sqrt{2}$ حيث $p,q \in Q$ من السهل أن نرى أنه $Q(\sqrt{2})$.

(٤) ليس صحيحًا بصورة عامة أنّ الحقل $K(\alpha)$ يحتوي فقط على جميع العناصر $j + k\alpha$ حيث $j, k \in K$. بالطبع إن هذا الحقل يحتوي على هذه العناصر ولكن ليس من الضروري أن تكون هذه العناصر حقلاً . فعلى سبيل المثال في $\mathbb{R} : Q$ ليكن α الجذر التكعيبي الحقيقي للعدد 2 ولنأخذ $Q(\alpha)$. إن عناصر هذا الحقل ، هي العناصر التي تكون على الشكل $p + q\alpha + r\alpha^2$ حيث $p,q,r \in Q$. ولنبرهن ذلك يجب أن نثبت أن مجموعة هذه العناصر هي بالفعل حقل . الصعوبة الوحيدة هنا هو ايجاد النظير الضربي ، يجب على القارئ أن يكتب التفاصيل .

(٢,٣) الامتدادات البسيطة

Simple Extensions

إن أبسط الامتدادات هي التي نحصل عليها باقران عنصر واحد فقط .

تعريف

الامتداد البسيط هو امتداد $L : K$ بحيث يكون $L = K(\alpha)$ حيث $\alpha \in L$.

أمثلـة

(١) كما هو واضح من التعريف فإنّ الأمثلة من (١) إلى (٣) أعلاه جميعها امتدادات بسيطة .

(٢) احذر : من الممكن أن يكون الامتداد بسيطًا بدون أن يكون في الظاهر كذلك . ليكن $L = Q(i, -i, \sqrt{5}, -\sqrt{5})$. كما هو معطى فإن L يظهر كما لو أننا حصلنا عليه من Q باقتران أربعة عناصر جديدة . في الحقيقة $L = L'$ حيث $L' = Q(i + \sqrt{5})$. ولبرهان ذلك يكفي أن نثبت أن $i \in L'$ و $\sqrt{5} \in L'$ لأننا عندئذ نحصل على $L \subseteq L'$ و $L' \subseteq L$ وبالتالي $L = L'$. الآن L' يحتوي على :

$$(i + \sqrt{5})^2 = -1 + 2i\sqrt{5} + 5 = 4 + 2i\sqrt{5}$$

وعليه فإنه يحتوي أيضًا على :

$$(i + \sqrt{5})(4 + 2i\sqrt{5}) = 14i - 2\sqrt{5}$$

إذن فإنه يحتوي على :

$$14i - 2\sqrt{5} + 2(i + \sqrt{5}) = 16i$$

وبالتالي فإنّه يحتوي على i . ولكنه يحتوي أيضًا على :

$$(i + \sqrt{5}) - i = \sqrt{5} .$$

إذن $L = L'$ وعليه فإنّ الامتداد

$$Q(i, -i, \sqrt{5}, -\sqrt{5}) : Q$$

في الحقيقة بسيط .

ومن ناحية أخرى فإنّ $\mathbb{R} : Q$ ليس امتدادًا بسيطاً [انظر تمرين (٦ , ٣)].

هدفنا في البقية من هذا الفصل هو تصنيف جميع الامتدادات البسيطة، وسنعرف في البداية مفهوم تماثل الامتدادات ثم نقدم تقنية لانشاء امتدادات بسيطة وأخيرًا سنبرهن على أننّا أنشأنا جميع الامتدادات البسيطة (تحت سقف التماثل).

تعريف

التماثل بين امتدادين $i : K \to K^*$ و $j : L \to L^*$ هو زوج (λ , μ) من *التماثل الحقلي* $\lambda : K \to L$ و $\mu : K^* \to L^*$ بحيث يتحقق *التالي*:

$j(\lambda(k)) = \mu(i(k))$ لكل $k \in K$.

وبصورة أخرى نقول إنّ الشكل التالي إبدالي:

$$\begin{array}{ccc} K & \xrightarrow{i} & K^* \\ \lambda \downarrow & & \downarrow \mu \\ L & \xrightarrow[j]{} & L^* \end{array}$$

أي أنّ المسارين من K إلى L^* يعطيان الدالة نفسها.

إنّ السبب وراء تقديم التعريف بهذه الصورة هو أنّه طالما أنّ خواص الحقل مصانة بالتماثل فإن طمر الحقل الصغير في الحقل الكبير أيضًا مصان.

من الممكن استخدام مطابقات أخرى. إذا طابقنا K مع $i(K)$ و L مع $j(L)$ فإن i و j هما دالتا الاحتواء وشرط الابدالية يصبح الآن

$$\mu\,|_K = \lambda$$

حيث $\mu\,|_K$ ترمز إلى اقتصار μ على K. وإذا طابقنا K مع L فإن λ تصبح الدالة المحايدة وبالتالي فإن $\mu\,|_K$ الدالة المحايدة.

فيما يلي سوف نستخدم هذه المطابقات عندما يكون ذلك ممكنًا، ولكن في أماكن قليلة (نظرية ٨ , ٣) سنحتاج إلى الحالة العامة المقدمة في التعريف.

(٣,٣) إنشاء امتدادات بسيطة

Constructing Simple Extensions

لقد واجهنا نوعان أساسيان من الامتدادات البسيطة أعلاه . الامتداد $\mathbb{C} = \mathbb{R}(i)$ حصلنا عليه من $\mathbb{R}$ بإقران العنصر i الذي يحقق معادلة كثيرة حدود، بالتحديد $i^2 + 1 = 0$. والامتداد $\mathbb{C}:Q(t)$ الذي حصلنا عليه بإقران عنصر t والذي لا يحقق معادلة كثيرة حدود لأنه من التعريف، إذا كان $p \in K[t]$ فإن $p(t) = 0$ إذا وفقط إذا كانت p هي كثيرة الحدود الصفرية . سنبدأ بوضع هذا الاختلاف بصورة دقيقة :

تعريف

ليكن $K(\alpha):K$ امتدادًا بسيطا، و نقول إن α عنصر جبري على K إذا وجدت كثيرة حدود غير صفرية p على K بحيث $p(\alpha) = 0$ ، ويسمى الامتداد $K(\alpha) = K$ امتدادًا جبريًا بسيطا، وما عدا ذلك فإنّنا نقول إن α عنصر متسام على K و $K(\alpha):K$ امتداد متسام بسيط .

في هذا البند والبند الذي يليه سنصنّف جميع الامتدادات البسيطة ونجد طريقة لإنشائها، وفي حالة الامتداد المتسامي تكون المسألة سهلة : $K(t) : K$ وهو الامتداد المتسامي البسيط الوحيد (تحت سقف التماثل)، وأما إذا كان $K(\alpha) : K$ جبريًا فإنّنا سنبرهن على وجود كثيرة حدود واحدية لا مختزلة وحيدة m على K بحيث $m(\alpha) = 0$، وكثيرة الحدود m تعين لنا الامتداد بصورة وحيدة (تحت سقف التماثل) . وسنبدأ بانشاء الامتدادات البسيطة هنا وسنترك شرح التصنيف للبند القادم.

سنبدأ بانشاء امتداد بسيط متسامٍ على أي حقل .

نظرية (٣,١)

حقل العبارات الكسرية $K(t)$ امتداد متسام بسيط على الحقل K.

البرهان

من الواضح أنّ $K(t)$ هو امتداد بسيط . إذا كانت p كثيرة حدود على K بحيث

$p(t) = 0$ فإنه من تعريف $K(t)$ نجد أن $p = 0$. Δ

إنّ مسألة إنشاء امتداد جبري بسيط تحتاج إلى كياسة . وسنحتاج إلى التعريف التقني التالي :

تعريف

تسمى كثيرة الحدود

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n$$

على حقل K واحدية إذا كان $a_n = 1$.

من الواضح أن أي كثيرة حدود عبارة عن مضاعف ثابت لكثيرة حدود واحدية ، وكثيرة الحدود الواحدية هذه وحيدة طالما أن كثيرة الحدود المعطاة غير صفرية . وعلاوة على ذلك فإن حاصل ضرب كثيرتي حدود واحديتين هو كثيرة حدود واحدية .

لنفرض الآن أنّ $K(\alpha) : K$ امتداد جبري بسيط . إذن يوجد كثيرة حدود p على K بحيث $p(\alpha) = 0$. نستطيع أن نفرض أن p واحدية . ويوجد على الأقل كثيرة حدود واحدية واحدة بدرجة أصغرية بحيث يكون α صفرًا لها . ندّعي أن p وحيدة . إذا كانت p و q تحققان الشرط فإن $p(\alpha) - q(\alpha) = 0$ ، و إذا كانت $p \neq q$ فإنّه يوجد كثيرة حدود واحدية مضاعفًا ثابتًا لـ $p - q$ و α صفراً لها ، وهذا يناقض التعريف . وعليه فإنه يوجد كثيرة حدود واحدية وحيدة بدرجة أصغرية p بحيث $p(\alpha) = 0$.

تعريف

ليكن $L : K$ امتدادًا حقليًا و $\alpha \in L$ عنصرًا جبريًا على K . نقول إن كثيرة الحدود m على K هي كثيرة حدود α الأصغرية إذا كانت m كثيرة الحدود الواحدية الوحيدة بأصغر درجة بحيث $m(\alpha) = 0$.

على سبيل المثال ، $i \in \mathbb{C}$ جبري على $\mathbb{R}$. إذا أخذنا $m(t) = t^2 + 1$ فإنّ $m(i) = 0$. من الواضح أنّ m واحديّة . كثيرات الحدود الواحديّة على $\mathbb{R}$ بأصغر درجة هي

التي على الصورة $t+r$، $r \in \mathbb{R}$ أو 1 . ولكن i لا يمكن أن يكون صفراً لأي منها . إذن كثيرة حدود i الأصغرية على $\mathbb{R}$ هي $t^2 + 1$.

من الطبيعي أن نتساءل عن ماهيّة كثيرات الحدود التي من الممكن أن تكون كثيرات حدود أصغريّة . والتمهيدية التالية تزودنا ببعض المعلومات .

تمهيدية (٣،٢)

إذا كان α عنصرًا جبريًا على الحقل K فإن كثيرة حدود α الأصغرية على K يجب أن تكون لا مختزلة على K ، وتقسم أي كثيرة حدود أخرى يكون α صفرًا لها .

البرهان

لنفرض أنّ كثيرة حدود α الأصغرية على K هي m ولنفرض أن m قابلة للاختزال . إذن $m = fg$ ، $\partial f, \partial g < \partial m$. نستطيع أن نفرض أن كل من f و g واحدية . بما أن $m(\alpha) = 0$ فإن $f(\alpha)g(\alpha) = 0$ ومنه $f(\alpha) = 0$ أو $g(\alpha) = 0$ وهذا يناقض تعريف m . وبالتالي فإن m لا مختزلة على K .

نفرض الآن أن p كثيرة حدود على K بحيث $p(\alpha) = 0$. باستخدام خوارزمية القسمة نستطيع إيجاد كثيرتي حدود q و r على K بحيث

$$p = mq + r \quad \text{و} \quad \partial r < \partial m .$$

إذن $0 = p(\alpha) = 0 + r(\alpha)$. ومنه $0 = p(\alpha) = r(\alpha)$. وبما أن $\partial r < \partial m$ فإن $r = 0$ وبالتالي $m \mid p$. Δ

ليكن لدينا حقل K وكثيرة حدود واحدية لامختزلة m على K ، سوف ننشيء امتداداً $K : K(\alpha)$ بحيث تكون m كثيرة حدود α الأصغرية على K . لكننا سنحتاج قبل ذلك إلى تمهيديتين .

لتكن R و S حلقتين و $\varphi : R \to S$ تشاكل، ولتكن $\ker(\varphi) = \{x \in R : \varphi(x) = 0\}$ هي نواة φ . تذكر أنّ $\ker(\varphi)$ مثالية من الحلقة R وأن $R/\ker(\varphi)$ يماثل $\text{Image}(\varphi)$. نقول إنّ φ تشاكل متباينًا إذا كان φ متباينًا وهذا

يكافيء $\ker(\varphi) = 0$.

تمهيدية (٣,٣)

إذا كان φ تشاكلاً حلقيًا من الحقل K إلى الحلقة R و $\varphi \neq 0$ فإن φ تشاكل متباين .

البرهان

نواة φ مثالية من K . ولكن كون K حقلاً فمثاليات K هي 0 أو K . وبما أن $\varphi \neq 0$ فإن $\ker(\varphi) \neq K$. إذن $\ker(\varphi) = 0$ وبالتالي φ تشاكل متباين . Δ

لاحظ أن هذه التمهيدية غير صحيحة لو كان K حلقة : التطبيق الطبيعي $\mathbb{Z} \to \mathbb{Z}_2$ ليس تطبيقا صفريا ولا تشاكل متباين .

تمهيدية (٣,٤)

لتكن m كثيرة حدود لا مختزلة على حقل K و $\partial m > 0$ ولتكن I مثالية من K[t] عناصرها مضاعفات m . عندئذ تكون الحلقة K[t]/I حقلاً .

البرهان

لتكن المجموعة المشاركة $I + f$ عنصرًا غير صفري في الحلقة $S = K[t]/I$. وبما أنّ m لا مختزلة فإنّ m و f أوليتان نسبيًا . وباستخدام نظرية (١٢ , ١) يوجد كثيرتا حدود a و b على K بحيث

$$af + bm = 1 .$$

ومنه

$$(I+a)(I+f) + (I+b)(I+m) = I + 1 .$$

ولكن $I = I + m$ هو العنصر الصفري في S و $I + 1$ هو العنصر المحايد . إذن

$$(I + a)(I + f) = I + 1$$

ومنه فإنّ $I + a$ هو نظير $I + f$. Δ

لدينا الآن كل ما نحتاجه لبرهان :

نظرية (٣,٥)

ليكن K حقلاً و m كثيرة حدود واحدية لا مختزلة على K . عندئذ يوجد امتداد $K(\alpha):K$ بحيث تكون m هي كثيرة حدود α الأصغرية على K .

البرهان

ليكن $i : K \to K[t]$ التشاكل المتباين الطبيعي . ولتكن I مثالية من K[t] عناصرها مضاعفات m ، وليكن $S = K[t]/I$ و υ التشاكل الطبيعي $K[t] \to S$. باستخدام تمهيدية (٣ , ٤) نجد أن S حقلاً وباستخدام تمهيدية (٣ , ٣) نجد أن $\upsilon\, i$ تشاكل متباين . نطابق الآن K مع صورته $\upsilon(i(K))$ ونضع $\alpha = I + t$ واضح أن $S = K(\alpha)$. وبما أنّ $m \in I$ فإنّ $m(\alpha) = I$ وأنّ I هو العنصر الصفري في S . وبما أنّ m لا مختزلة وواحديّة فإنها يجب أن تكون كثيرة حدود α الأصغرية . لأنه لو كانت p كثيرة حدود أصغرية فباستخدام تمهيدية (٣ , ٢) نجد أن $p \mid m$. إذن $p = m$. Δ

من الممكن أن نرى طريقة الإنشاء بمنظار آخر . من كل مجموعة مشاركة I + f نختار كثيرة حدود وحيدة درجتها أصغر من ∂m . ومن عمليات الحقل S نستطيع تعريف عمليات على مجموعة كثيرات الحدود التي اخترناها كالتالي : عملية الجمع كالعادة، وعملية الضرب كالعادة باستثناء أنه بعد إجراء عملية الضرب نأخذ الباقي عند القسمة على m. ومن الممكن تعريف $K(\alpha)$ بهذه الطريقة ولكنه من الصعب البرهان على أنّه حقل .

(٣,٤) تصنيف الامتدادات البسيطة

Classifying Simple Extensions

سنقوم الآن باثبات أنّ الطرق التي استخدمت أعلاه كافية لانشاء جميع الامتدادات البسيطة (تحت سقف التماثل) . وكما سبق فإنه من السهل التعامل مع الامتدادات المتسامية .

نظرية (٣,٦)

إن أي امتداد بسيط متسام $K(\alpha):K$ يماثل الامتداد $K(t):K$ حيث $K(t)$ هو حقل العبارات الكسرية في t على K . ومن الممكن اختيار التناظر بحيث تكون صورة t هي α .

البرهان

عرف التطابق $\varphi : K(t) \to K(\alpha)$ كالتالي :

$$\varphi(f(t) / g(t)) = f(\alpha) / g(\alpha)$$

إذا كانت $g \neq 0$ فإنّ $g(\alpha) \neq 0$ (لأن α متسام) . من الواضح أن φ تشاكل وهو أحادي باستخدام تمهيدية (٣ , ٣) . من الواضح أيضًا أنه غامر . إذن φ تماثل . وعلاوة على ذلك فإن $\varphi|_K$ هي الدالة المحايدة . إذن φ تماثل بين امتدادين . وأخيراً $\varphi(t) = \alpha$. Δ

وللتعامل مع الامتداد الجبري سنقدم أولا صيغة معيارية لعناصر الحقل الكبير .

تمهيدية (٣,٧)

ليكن $K(\alpha):K$ امتدادًا جبريًا بسيطا و m كثيرة حدود α الأصغرية على K . عندئذ فإن عناصر $K(\alpha)$ تكتب بصورة وحيدة $p(\alpha)$ حيث p كثيرة حدود على K و $\partial p < \partial m$.

البرهان

كل عنصر في $K(\alpha)$ يمكن كتابته على الصورة $f(\alpha) / g(\alpha)$ حيث $f,g \in K[t]$ و $g(\alpha) \neq 0$ [لأن مجموعة جميع هذه العناصر تكون حقلاً يحتوي على K و α ومحتوى في $K(\alpha)$]. وبما أن $g(\alpha) \neq 0$ فإن m لا تقسم g ، وبما أن m لا مختزلة فإن m و g أوليتان نسبيًا . وباستخدام نظرية (١٢ , ١) نستطيع إيجاد كثيرتي حدود a و b على K بحيث $ag + bm = 1$. إذن $a(\alpha)\, g(\alpha) = 1$ ومنه :

$$f(\alpha) / g(\alpha) = f(\alpha)\, a(\alpha) = h(\alpha)$$

حيث h كثيرة حدود على K . ولتكن r هي الباقي عند قسمة h على m . إذن $r(\alpha) = h(\alpha)$. وبما أن $\partial r < \partial m$ فإننا نكون قد برهنا الوجودية .

ولبرهان الوحدانية نفرض أنّ $f(\alpha) = g(\alpha)$ حيث $\partial f, \partial g < \partial m$ إذا كان $e = f - g$ فإن $e(\alpha) = 0$ و $\partial e < \partial m$. ومن تعريف m يكون $e = 0$ ومنه $f = g$. وبهذا يتم برهان التمهيدية. Δ

مثال

ليكن $K = \mathbb{R}$، $m(t) = t^2 + t + 1$. إذا كانت m هي كثيرة حدود α الأصغرية على K فإنّ كل عنصر فى $K(\alpha)$ يجب أن يكون كثيرة حدود في α درجتها أصغر من 2. اعتبر العنصر $(3\alpha^2 + 2) / (\alpha + 4)$. لاحظ أن

$$(t^2 + t + 1) - (t - 3)(t + 4) = 13$$

ومنه

$$1 = \frac{1}{13}(t^2 + t + 1) - (t - 3)/13(t + 4)$$

إذن

$$1/(\alpha + 4) = -(\alpha - 3)/13 .$$

إذن

$$(3\alpha^2 + 2)/(\alpha + 4) = -\frac{1}{3}(3\alpha^2 + 2)(\alpha - 3)$$

$$= -\frac{1}{13}(3(-\alpha - 1) + 2)(\alpha - 3)$$

$$= -\frac{1}{13}(-3\alpha^2 + 8\alpha + 3)$$

$$= -\frac{1}{13}(11\alpha + 6)$$

$$= -\frac{11}{13}\alpha - \frac{6}{13}$$

نستطيع الآن تقديم برهان تمهيدي للنتيجة التي تنص على أنّنا نستطيع معرفة $K(\alpha)$ بمعرفة K و m.

نظرية (٣,٨)

لنفرض أنّ $K(\alpha):K$ و $K(\beta):K$ امتدادان جبريّان بسيطان بحيث إن α و β لهما كثيرة الحدود الأصغرية نفسها وهي m على K . عندئذ الامتدادان متماثلان ومن الممكن اختيار التماثل بين الحقلين الكبيرين بحيث تكون صورة α هي β .

البرهان

باستخدام التمهيدية (٣ , ٧) أي عنصر $x \in K(\alpha)$ يكتب بصورة وحيدة على الشكل :

$$x = x_0 + x_1 \alpha + ... + x_n \alpha^n \ ، \ x_1, ..., x_n \in K$$

حيث $n = \partial m - 1$. ليكن $\varphi : K(\alpha) \to K(\beta)$ معرف كالتالي :

$$\varphi(x) = x_0 + x_1 \beta + ... + x_n \beta^n \ .$$

باستخدام تمهيدية (٣ , ٧) نجد أن φ متباين وغامر ، وواضح أنّ

$$\varphi(x + y) = \varphi(x) + \varphi(y) \ .$$

وسنبرهن الآن على أنّ $\varphi(x\,y) = \varphi(x)\,\varphi(y)$ لكل $x,y \in K(\alpha)$. لنفرض أنّ $x = f(\alpha)$ ، $y = g(\alpha)$ ، $x\,y = h(\alpha)$ حيث f,g,h كثيرات حدود على K درجة كل منهما أصغر من ∂m . إذن

$$f(\alpha)\,g(\alpha) - h(\alpha) = x\,y - x\,y = 0 \ .$$

باستخدام تمهيدية (٣ , ٢) m تقسم $fg - h$ ، ومنه نستطيع ايجاد كثيرة حدود q على K بحيث $fg = mq + h$. بما أن $\partial h < \partial m$ فإن h هي الباقي عند قسمة fg على m . وبالطريقة نفسها نجد أن $f(\beta)\,g(\beta) = h(\beta)$. إذن

$$\varphi(xy) = h(\beta) = f(\beta)\,g(\beta) = \varphi(x)\,\varphi(y) \ ،$$

ومنه فإنّ φ تماثل . وبما أنّ φ هو التطابق المحايد على K فإنّ الامتدادين متماثلين . وواضح أنّ $\varphi(\alpha) = \beta$. Δ

سنحتاج عند دراسة بعض التطبيقات القادمة إلى صيغة أقوى قليلاً من النظرية السابقة وذلك لتغطية امتدادات حقول متماثلة (بدلاً من متساوية) . قبل أن نقدم النظرية العامة نحتاج للتالي :

تعريف

إذا كان $i:K\to L$ تشاكل حقلي متباين فإنّه يوجد تشاكل حقلي متباين $i:K[t]\to L[t]$ معرّف كالتالي:

$$\hat{i}(k_0+k_1t+\dots+k_nt^n)=i(k_0)+i(k_1)t+\dots+i(k_n)t^n$$

حيث $k_0,\dots,k_n\in K$. *وإذاكان i تماثل فإنّ $\hat{i}$ كذلك.*

لاحظ أن الرمز ^ ليس ضروريًا ومن الممكن الاستغناء عنه. في المستقبل سنستخدم الرمز i نفسه للتطابق بين الحقلين وللتطابق بين حلقتي كثيرات الحدود. وهذا لن يسبب أي غموض لأن $\hat{i}(k)=i(k)$ لكل $k\in K$.

نظرية (٣,٩)

ليكن كل من K و L حقلاً و $i:K\to L$ تماثل. وليكن كل من $K(\alpha)$ و $L(\beta)$ امتداداً جبريًا بسيطا للحقلين K و L على الترتيب بحيث $m_\alpha(t)$ و $m_\beta(t)$ هما كثيرتا حدود α و β الأصغريتين على K و L. ولنفرض كذلك أنّ $m_\beta(t)=i(m_\alpha(t))$. عندئذ يوجد تماثل $j:K(\alpha)\to L(\beta)$ بحيث $j|_K=i$ و $j(\alpha)=\beta$.

البرهان

لدينا الشكل

$$\begin{tikzcd} K \arrow[r] \arrow[d, "i"'] & K(\alpha) \arrow[d, dotted, "j"] \\ L \arrow[r] & L(\beta) \end{tikzcd}$$

(حيث النقاط تعني أننا لم نعرف j بعد).

وباستخدام برهان نظرية (٣,٨) كمؤشر ، نعرف j كالتالي:

أي عنصر في $K(\alpha)$ يكتب على الشكل $p(\alpha)$ حيث p كثيرة حدود على K درجتها أصغر من ∂m_α . ولنضع $j(p(\alpha))=(i(p))(\beta)$ حيث $i(p)$ كما هي معرفة أعلاه.

ويكون البرهان الآن على شاكلة برهان نظرية (٣,٨) ويترك للقاريء.

إنّ أهمية هذه النظرية تكمن في إمكانية تحديد التطابق i إلى تطابق j بين حقلين أكبر . إنّ نظريات تمدد مثل هذه والتي تنص على أنه تحت ظروف مناسبة نستطيع تمديد تطبيقات من بُنى رياضية جزئية إلى البُنى نفسها ، وتعتبر مثل هذه النظريات سلاحًا مهمًا جدًا للرياضيين . وباستخدامها نستطيع أن نوسع معرفتنا من بُنى صغيرة إلى بُنى كبيرة في متتالية من الخطوات البسيطة .

إن النظرية (٩ , ٣) تنص (تحت ظروف معينة) على أن الامتدادين $K(\alpha) : K$ و $L(\beta) : L$ متماثلان وهذا يسمح لنا أن نطابق K مع L و $K(\alpha)$ مع $L(\beta)$ باستخدام التطابقين i و j .

والنظريتان (٥ , ٣) و (٨ , ٣) معًا تزوّدنا بتصنيف كامل للامتدادات الجبرية البسيطة بواسطة كثيرات الحدود . كل امتداد يقابله كثيرة حدود واحدية لا مختزلة ، وإذا كان لدينا الحقل الصغير وكثيرة الحدود هذه نستطيع إعادة إنشاء الامتداد .

لاحظ أنّ التقابل هذا ليس متباينًا : من الممكن أن تؤدّي الامتدادات المتماثلة إلى كثيرات حدود مختلفة ، لأنه يوجد حرية في اختيار α ، ولا تنشأ أي صعوبة من ذلك .

تمارين

(١ , ٣) برهن على أنّ تماثل امتدادات الحقول علاقة تكافؤ .

(٢ , ٣) جد حقلاً جزئيًا من $\mathbb{C}$ منشأ من :

(أ) $\{0, 1\}$

(ب) $\{0\}$

(ج) $\{0, 1, i\}$

(د) $\{i, \sqrt{2}\}$

(هـ) $\{\sqrt{2}, \sqrt{3}\}$

(و) $\mathbb{R}$

(ز) $\mathbb{R} \cup \{i\}$

(٣,٣) صف الحقول الجزئية التالية من $\mathbb{C}$:

(أ) $Q(\sqrt{2})$

(ب) $Q(i)$

(ج) $Q(\alpha)$ حيث α هو الجذر التكعيبي الحقيقي للعدد 2

(د) $Q(\sqrt{5}, \sqrt{7})$

(هـ) $Q(i\sqrt{11})$

(٣,٤) ليكن $K = \mathbb{Z}_2$. صف الحقول الجزئية التالية من $K(t)$:

(أ) $K(t^2)$

(ب) $K(t+1)$

(ج) $K(t^5)$

(د) $K(t^2+1)$

(٣,٥) أي منَ الامتدادات في التمرينين (٣,٣) و (٣,٤) جبري بسيط؟ وأي منها متسام بسيط ؟

(٣,٦) برهن على أن $\mathbb{R}$ امتداد ليس بسيطاً لـ Q كالتالي :

(أ) Q مجموعة قابلة للعد .

(ب) أي امتداد بسيط لحقل قابل للعد يجب أن يكون قابلاً للعد .

(ج) $\mathbb{R}$ مجموعة غير قابلة للعد.

(٣,٧) برهـن صيغة الامتداد المتسامي للنظرية (٣,٩) على غرار النظريتين (٣,٩) و (٣,١).

(٣,٨) جد كثيرات حدود أصغرية على الحقل الصغير للعناصر التالية في كل من الامتدادات التالية :

(أ) i في $\mathbb{C} : Q$

(ب) i في $\mathbb{C} : \mathbb{R}$

(ج) $\sqrt{2}$ في $\mathbb{R} : Q$

(د) $(\sqrt{5}+1)/2$ في $\mathbb{C} : Q$

(هـ) $(i\sqrt{3} - 1)/2$ في $\mathbb{C} : Q$

(و) α في $K : P$ حيث K الحقل المعطى في تمرين (٦ , ١) ، و P الحقل الجزئي الأولي له .

(ي) α في $\mathbb{Z}_3(t)(\alpha):\mathbb{Z}_3(t)$ حيث t مجهول و $\alpha^2 = t + 1$.

(٩ , ٣) برهن على إذا كانت $t^2 - 2$ هي كثيرة حدود α الأصغرية على Q و $t^2 - 4t + 2$ هي كثيرة حدود β الأصغرية على Q فإن الامتدادين $Q(\alpha) : Q$ و $Q(\beta) : Q$ متماثلان .

(١٠ , ٣) لكل مما يأتي بين فيما إذا كانت $m(t)$ تصلح لأن تكون كثيرة حدود α الأصغرية بحيث يوجد امتداد $K(\alpha)$ لـ K .

(أ) $m(t) = t^2 - 4,\ K = \mathbb{R}$

(ب) $m(t) = t^2 + 1,\ K = \mathbb{Z}_3$

(ج) $m(t) = t^2 + 1,\ K = \mathbb{Z}_5$

(د) $m(t) = t^7 - 3t^6 + 4t^3 - t - 1,\ K = \mathbb{R}$

(١١ , ٣) ليكن K حقلاً مميزه لا يساوي 2 و $m(t)$ كثيرة حدود من الدرجة الثانية على K . برهن على أن صفري $m(t)$ يجب أن يكونا عنصران في حقل الامتداد $K(\alpha)$ لـ K حيث $\alpha^2 = k \in K$. وعليه إذا سمحنا بأخذ $\sqrt{k}$ نستطيع أن نجد حلولاً لجميع معادلات كثيرات الحدود من الدرجة الثانية على K .

(١٢ , ٣) في الحقول ذات المميّز 2 برهن على وجود معادلات من الدرجة الثانية التي لا نستطيع حلّها بإقران الجذر التربيعي لعناصر في الحقل . **(إرشاد:** حاول $\mathbb{Z}_2$) .

(١٣ , ٣) برهن على أنّنا نستطيع حل معادلات الدرجة الثانية على حقل مميزه 2 إذا سمحنا بالإضافة إلى الجذور التربيعية إقران عناصر على الشكل $\sqrt[*]{k}$ التي هي حلول للمعادلة : $(\sqrt[*]{k})^2 + \sqrt[*]{k} = k$.

(١٤ , ٣) أثبت أن الصفرين في التمرين (١٣ , ٣) للمعادلة :

$t^2+t-k=0$ هما $\sqrt[*]{k}$ و $1+\sqrt[*]{k}$.

(٣, ١٥) ليكن $K=\mathbb{Z}_3$. جد جميع كثيرات الحدود اللامختزلة من الدرجة الثانية على K ثم انشيء جميع امتدادات K بعنصر كثيرة حدوده الأصغرية من الدرجة الثانية . كم عدد فصول التماثل لهذه الامتدادات ؟ كم عدد عناصر هذه الامتدادات؟

(٣, ١٦) أنشئ امتدادات $Q : Q(\alpha)$ حيث كثيرة حدود α الأصغرية على Q هي :

(أ) t^2-5

(ب) $t^4+t^3+t^2+t+1$

(ج) t^3+2

(٣, ١٧) جد حقلاً يحتوي على ثمان عناصر .

(٣, ١٨) هل $Q(\sqrt{2}, \sqrt{3}, \sqrt{5}) : Q$ امتداد بسيط ؟

(٣, ١٩) لتكن $m(t)$ كثيرة حدود مختزلة أصغرية للعنصر α على K . هل من الضروري أن تكون $m(t)$ حاصل ضرب كثيرات حدود خطّية على $K(\alpha)$ ؟ (**إرشاد** : حاول $K=Q$ ، α الجذر التكعيبي الحقيقي للعدد 2) .

(٣, ٢٠) ضع علامة صح أو خطأ أمام كل مما يأتي :

(أ) أي حقل له امتداد غير تافه .

(ب) أي حقل له امتداد جبري غير تافه .

(ج) أي امتداد بسيط هو جبري .

(د) أي امتداد هو بسيط .

(هـ) جميع الامتدادات الجبرية البسيطة متماثلة .

(و) جميع الامتدادات المتسامية البسيطة على حقل معطى متماثلة .

(ز) أي كثيرة حدود أصغرية يجب أن تكون واحديّة .

(ح) كثيرات الحدود الواحدية دائمًا لا مختزلة .

(ط) أي كثيرة حدود هي مضاعف ثابت لكثيرة حدود لا مختزلة .

(ي) لا يوجد خطر من مطابقة الحقول المتماثلة .

الفصل الرابع

درجـــــة الامتـــــداد
The Degree of an Extension

إنّ عملية ربط بناء رياضي تحت الدراسة ببناء آخر سهل الفهم هو أسلوب مفيد جدّا في الرياضيات . ولقد أصبحت هذه العملية شائعة الاستعمال في الطوبولوجيا الجبرية مما أجبر المتخصصين في هذا الفرع إلى اعداد صياغة عامة لهذه الطرق ومن ثم أصبح من الواضح أنّ هذا الأسلوب يُبَطّن كثيرًا من المعارف الرياضية .

وفي هذا الفصل سنتبّع هذا الأسلوب بربط أي امتداد حقلي بفضاء متجهات ، وهذا يضع تحت تصرفنا طرائق الجبر الخطّي (وهي من أكثر نظريات الجبر نجاحًا) وبمساعدة الجبر الخطي نستطيع أن نحرز تقدمًا ملموسًا . وهذه الطرائق كانت من الفاعلية للدرجة التي كانت كافية لحل ثلاث من المسائل المشهورة التي بقيت بدون حل لأكثر من ألفي عام . سنناقش هذه المسائل في الفصل القادم وسنكرس جهدنا في هذا الفصل لتوضيح هذه النظرية .

(٤,١) قانون البرج
The Tower Law

إنّه ليس من الصعب أن نحصل على فضاء خطي من امتداد حقلي ، لأنه بالفعل يكون ذلك! وبصورة أدق :

نظرية (٤,١)

إذا كان $L : K$ امتداداً حقلياً فإن العمليتين :

$$\lambda \in K,\ \ u \in L,\ (\lambda,u) \to \lambda u$$

$$u, v \in L, \quad (u, v) \to u + v$$

تجعل L فضاء متّجهات على K .

البرهان

إنّ كل خاصية من خواص الفضاء الخطّي إمّا أن تكون خاصية حقل أو خاصية مقتصرة من خاصية حقل . Δ

إنّ العملية التي تحوّل لنا $L : K$ إلى فضاء متجهات ما هي إلا مثال لما يسمى «الدلال المنسى» . لأنها بكل بساطة تنسى جزءاً من البناء ، و إن هذا يسمح لنا بغض النظر عن تفاصيل كثيرة لا تفيد الموضوع الذي نحن بصدد دراسته .

وإنّ أيّ فضاء خطّي على حقل يتحدد تمامًا (تحت سقف التماثل) ببعده .

والتعريف التالي هو المصطلح الفني التقليدي في سياق الكلام عن امتدادات الحقول .

تعريف

تعرف درجة الامتداد الحقلي $L : K$ بأنها بعد فضاء المتجهات L على الحقل K ونرمز لذلك بالرمز $[L : K]$.

أمثلـة

(١) بُعد الفضاء الخطّي $\mathbb{C}$ على $\mathbb{R}$ هو 2 لأن $\{1, i\}$ أساس له . إذن $[\mathbb{C} : \mathbb{R}] = 2$.

(٢) بما أنّ $1, t, t^2 \cdots$ مستقلة خطياً على $\mathbb{C}$ فإن $[\mathbb{C}(t) : \mathbb{C}]$ عدد غير منته .

(٣) ليكن K هو الحقل المعرف في تمرين (٦ , ١)، وP هو حقله الجزئي الأولي (لاحظ $P \cong \mathbb{Z}_2$) . والمجموعة $\{1 , \alpha\}$ أساس للحقل K على P . إذن $[K : P] = 2$.

من الواضح أن الامتدادات الحقلية المتماثلة لها الدرجة نفسها .

النظريّة التالية تعرف بقانون البرج وهي تساعدنا على حساب درجات امتدادات معقدة بمعرفتنا درجات امتدادات بسيطة .

نظرية (٢.٤)

إذا كانت K, L, M حقول بحيث $K \subseteq L \subseteq M$ فإن $[M : K] = [M : L]\,[L : K]$.

ملاحظة

هذه الصيغة لا تحتاج إلى تفسير للقاريء الذي تعامل من قبل مع الأعداد الرئيسة لأنّ حاصل الضرب في الطرف الأيمن ما هو إلا حاصل ضرب عددين رئيسين . ولكن الصيغة تحتاج لبعض التفسير للقاريء الذي لم يتعامل مع الأعداد الرئيسة. وإذا كانت أي من هذه الدرجات عدد غير منته فإنّ تفسير الصيغة يتم كالتالي :

إذا كان

$[L : K] = \infty$ أو $[M : L] = \infty$ فإنّ $[M : K] = \infty$

وإذا كان $[M : K] = \infty$ فإنّ $[M : L] = \infty$ أو $[L : K] = \infty$.

البرهان

ليكن $(x_i)_{i\in I}$ أساسًا لفضاء المتّجهات L على K ، و $(y_j)_{j\in J}$ أساسًا لفضاء المتجهات M على L . لدينا $x_i \in L$ و $y_j \in M$ لكل $i \in I$ و $j \in J$.

وسنبرهن على أن $(x_i y_j)_{i\in I, j\in J}$ أساس لفضاء المتّجهات M على K ($x_i y_j$ هو حاصل الضرب في الحقل M) . وبما أنّ الأبعاد هي الأعداد الرئيسة للأساسات فإنّ هذا ينهي البرهان .

وسنبرهن على الاستقلال الخطّي أولا .

لنفرض أنّ $\sum_{i,j} k_{ij}\, x_i\, y_j = 0$ ، $k_{ij} \in K$.

باستطاعتنا أن نعيد الترتيب لنحصل على :

$$\sum_{i}\left(\sum_{i} k_{ij} x_i\right) y_i = 0$$

وبما أنّ المعاملات $\sum_i k_{ij} x_i$ تنتمي للحقل L و $(y_j)_{j\in J}$ مستقلة خطيّا على L فإنّ

$$\sum_i k_{ij} x_i = 0 .$$

وبتكرار ذلك في L نحصل على $k_{ij} = 0$ لكل $i \in I$ و $j \in J$. إذن العناصر $x_i y_j$ مستقلة خطيًا.

وأخيرًا سنبرهن على أن $x_i y_j$ تنشيء M على K . إن أي عنصر $x \in M$ يكتب على الصورة:

$$x = \sum_j \lambda_j y_j$$

حيث $\lambda_j \in L$ ، لأن y_j تنشيء M على L.

كذلك لكل $j \in J$

$$\lambda_j = \sum_i \lambda_{ij} x_i$$

حيث $\lambda_{ij} \in K$ وبضم الأجزاء نحصل على :

$$x = \sum_{i,j} \lambda_{ij} x_i y_j$$

كما هو مطلوب . Δ

مثـال

لنحاول إيجاد$[Q(\sqrt{2}, \sqrt{3}) : Q]$. ومن السهل إثبات أنّ $\{1, \sqrt{2}\}$ أساس لـ $Q(\sqrt{2})$ عـلـى Q . ولأجـل ذلـك لـنـفـرض أن $\alpha \in Q(\sqrt{2})$ ، عـنـدئـذ $\alpha = p + q\sqrt{2}$ حيث $p, q \in Q$ ومنه فإنّ $\{1, \sqrt{2}\}$ تنشيء $Q(\sqrt{2})$ على Q. يبقى أن نثبت أنّ 1 ، $\sqrt{2}$ مستقلين خطيًا على Q، ، و لنفرض أنّ $p + q\sqrt{2} = 0$ حيث $p, q \in Q$. إذا كان $q \neq 0$ فإن $\sqrt{2} = \frac{p}{q}$ عـــدد كســري وهـذا مستحيـــل . إذن $q = 0$ وبالتالي فإنّ$p = 0$.

وبالطريقة نفسها نستطيع أن نثبت أنّ $\{1, \sqrt{3}\}$ أساس لـ $Q(\sqrt{2}, \sqrt{3})$ على $(Q\sqrt{2})$. وإن أي عنصر في $Q(\sqrt{2}, \sqrt{3})$ يكتب على الصورة

$p + q\sqrt{2} + r\sqrt{3} + s\sqrt{6}$ حيث $p,q,r,s \in Q$

وبإعادة كتابة هذا العنصر كالتالي

$$(p + q\sqrt{2}) + (r + s\sqrt{2})\sqrt{3}$$

نرى أن $\{1, \sqrt{3}\}$ تنشيء $Q(\sqrt{2}, \sqrt{3})$ على $Q(\sqrt{2})$.

ولبرهان الاستقلال الخطّي نفرض أن

$$(p + q\sqrt{2}) + (r + s\sqrt{2})\sqrt{3} = 0 \; .$$

إذن إمّا أن $r + s\sqrt{2} = 0$ ومنه $p + q\sqrt{2} = 0$ أو

$$\sqrt{3} = (p + q\sqrt{2}) / (r + s\sqrt{2}) \in Q(\sqrt{2}) \; .$$

إذن $\sqrt{3} = a + b\sqrt{2}$ حيث $a,b \in Q$. وبالتربيع نجد أنّ $a\,b\sqrt{2}$ عدد كسري وهذا مستحيل إلا إذا كان $a = 0$ أو $b = 0$. ولكن في هذه الحالة $a = \sqrt{3}$ أو $b\sqrt{2} = \sqrt{3}$ وهذا مستحيل إلا إذا كان $a = b = 0$.

إذن $p + q\sqrt{2} = r + s\sqrt{2} = 0$ وبهذا نكون قد برهنا أن $\{1, \sqrt{3}\}$ أساس . الآن

$$[Q(\sqrt{2}, \sqrt{3}) : Q] = [Q(\sqrt{2}, \sqrt{3}) : Q\sqrt{2}][Q(\sqrt{2}) : Q]$$
$$= 2 \times 2 = 4$$

لاحظ أننا أيضًا نستطيع إيجاد أساس لـ $Q(\sqrt{2}, \sqrt{3})$ على Q : جد جميع حواصل ضرب الأزواج من أعداد الأساسين $\{1, \sqrt{2}\}$ و $\{1, \sqrt{3}\}$ لنحصل على $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

من أجل تطبيق قانون البرج يجب أن يكون لدينا شيء في البداية، ودرجة الامتداد البسيط سهلة الايجاد :

قضية (٣,٤)

ليكن $K(\alpha):K$ امتدادًا بسيطًا ، إذا كان هذا الامتداد متساميًا فإن $[K(\alpha) : K] = \infty$. وإذا كان جبريًا فإن $[K(\alpha):K] = \partial m$ حيث m هي كثيرة حدود α الأصغرية على K .

البرهان

في حالة الامتداد المتسامي يكفي أن نلاحظ أنّ العناصر $1, \alpha, \alpha^2, \cdots$ مستقلة خطيًا على K، وفي حالة الامتداد الجبري سنقوم بإيجاد أساس . ليكن $\partial m = n$

ولندرس العناصر $1, \alpha, ..., \alpha^{n-1}$. باستخدام تمهيدية (٣ , ٧) نجد أنّها تنشئ $K(\alpha)$ على K ، ومن فقرة الوحدانية لتمهيدية (٣ , ٧) نجد أنها مستقلة خطيًا ، وبالتالي فإنها أساس ، وأنّ :

$$[K(\alpha) : K] = n = \partial m \quad . \qquad \Delta$$

على سبيل المثال نعلم أنّ $\mathbb{C} = \mathbb{R}(i)$ حيث $t^2 + 1$ هي كثيرة حدود i الأصغريّة وهي من الدرجة الثانية . إذن $[\mathbb{C} : \mathbb{R}]=2$ وهذا يتفق مع ما رأيناه سابقًا .

إنّ فاعلية الجبر الخطّي أفضل ما يمكن عندما تكون أبعاد الفضاءات الخطّية منتهية . وعلى هذا الأساس سنركز اهتمامنا على الامتدادات التي تحدث لنا مثل هذه الفضاءات الخطّية .

تعريف

الامتداد المنتهي هو الامتداد الذي تكون درجته منتهية .

من نظرية (٣ , ٤) نستنتج أنّ جميع الامتدادات الجبرية البسيطة منتهية ، والعكس غير صحيح ، ولكن هناك بعض النتائج الجزئية : انظر تمرين (١٩ , ٤) . ولكي نستطيع أن نرى ما هو صحيح سنحتاج إلى :

تعريف

الامتداد $L : K$ امتداد جبري إذا كان كل عنصر في L جبريًا على K .

وليس بالضرورة أن تكون الامتدادات الجبرية هي امتدادات منتهية [على سبيل المثال انظر الأعداد الجبرية في البند (٢ , ٤)] . ولكن أي امتداد منته يجب أن يكون جبريًا :

تمهيدية (٤ , ٤)

$L : K$ امتداد منته إذا وفقط إذا كان L جبرياً على K ووجد عدد منته من العناصر $\alpha_1, ..., \alpha_s \in L$ بحيث يكون

$$L = K(\alpha_1, ..., \alpha_s) .$$

باستخدام الاستنتاج الرياضي والنظريتين (٢ , ٤) و (٣ , ٤) نستطيع بسهولة أن نرى أنّ أي امتداد جبري $K(\alpha_1, ..., \alpha_s) : K$ يجب أن يكون منتهيًا . وللبرهان العكس، نفرض أنّ $L : K$ امتداد منته، إذن يوجد أساس $\{\alpha_1, ..., \alpha_s\}$ لـ L على K وبالتالي $L = K(\alpha_1, ..., \alpha_s)$. يبقى أن نثبت أن $L : K$ جبري، و لنفرض أن x عنصر في L، وأن $n = [L : K]$. والمجموعة $\{1, x, ..., x^n\}$ تحتوي على $n + 1$ من العناصر ومنه فإنّها غير مستقلة خطياً على K . وإذن يوجد عناصر $k_0, k_1, ..., k_n \in K$ بحيث $k_0 + k_1 x + ... + k_n x^n = 0$ وبالتالي فإنّ x جبري على K . Δ

(٢ , ٤) الأعداد الجبرية

Algebraic Numbers

لتكن A هي مجموعة الأعداد المركّبة والجبرية على Q . وتسمى عناصر A بالأعداد الجبرية . وسنستخدم تقنية هذا الفصل لنبرهن على أن A حقلٌ .

باستخدام تمهيدية (٤ , ٤) العدد المركّب α ينتمي إلى A إذا وفقط إذا كان $[Q(\alpha) : Q] < \infty$. لتكن $\alpha, \beta \in A$. عندئذ

$$[Q(\alpha,\beta) : Q] = [Q(\alpha,\beta) : Q(\alpha)]\, [Q(\alpha) : Q] < \infty \, .$$

إذن $[Q(\alpha+\beta) : Q] < \infty$ ، $[Q(-\alpha) : Q] < \infty$ ، $[Q(\alpha\beta) : Q] < \infty$ ، وإذا كان $\alpha \neq 0$ فإن $[Q(\alpha^{-1}) : Q] < \infty$ ، وبالتالي فإن $\alpha + \beta$ ، $-\alpha$ ، $\alpha\beta$ ، α^{-1} جميعها عناصر في A ، وعليه فإن A حقلاً .

ومن الواضح أنّ A امتداد جبري على Q . ولكن من الممكن أن نثبت (انظر تمرين ٨ , ٤) أن درجة A على Q عدد غير منته، و إذن ليس بالضرورة أن يكون كل امتداد جبري منتهيًا .

تمارين

(١ , ٤) جد درجة كل من الامتدادات التالية :

(١) $Q : \mathbb{C}$

(ب) $\mathbb{Z}_5(t):\mathbb{Z}_5$

(ج) $\mathbb{R}(\sqrt{5}):\mathbb{R}$

(د) $Q(\alpha):Q$ حيث α الجذر التكعيبي للعدد 2 .

(هـ) $Q(3,\sqrt{5},\sqrt{11}):Q$

(و) $Q(\sqrt{6}):Q$

(ز) $Q(\alpha):Q$ حيث $\alpha^7=3$.

(٤ , ٢) أثبت أن أي عنصر في $Q(\sqrt{5},\sqrt{7})$ يمكن كتابته على الصورة :

$$p+q\sqrt{5}+r\sqrt{7}+s\sqrt{35}$$

حيث $p,q,r,s\in Q$. ثم جد النظير لهذا العنصر .

(٤ , ٣) إذاكان $[L:K]$ عدداً أولياً وكان $K\subseteq M\subseteq L$ فاثبت أنّ $M=L$ أو $M=K$.

(٤ , ٤) إذا كان $[L:K]=1$ فاثبت أنّ $L=K$.

(٤ , ٥) إذا كانت $K=K_0\subseteq K_1\subseteq\cdots\subseteq K_r=L$ حقولاً فأثبت أن :

$$[L:K]=[K_r:K_{r-1}]\ldots[K_2:K_1]\,[K_1:K_0] .$$

(٤ , ٦) برهن على أنّ $[L:K]$ عدد منته إذا وفقط إذا كان $L=K(\alpha_1,\ldots,\alpha_r)$ حيث r عدد منته وكل α_i جبري على K .

(٤ , ٧) باستخدام الحقيقة أن $\mathbb{R}$ فضاء متجهات على Q برهن وجود دوال $f:\mathbb{R}\longrightarrow\mathbb{R}$ بحيث $f(x+y)=f(x)+f(y)$ لكل $x,y\in\mathbb{R}$ ، و $f(x)$ ليست مضاعف ثابت للعنصر x . هل توجد مثل هذه الدوال لو اشترطنا أن تكون متصلة؟

(٤ , ٨) ليكن A حقلَ الأعداد الجبرية . برهن على أن $[A:Q]=\infty$ مستخدمًا ميزان ايزنستاين لإثبات وجود كثيرات حدود على Q بدرجات كبيرة جدًا .

(٤ , ٩) لنفرض أنّ كل كثيرة حدود على $\mathbb{C}$ يجب أن يكون لها صفرافي $\mathbb{C}$. برهن على أنّ كل كثيرة حدود على A يجب أن يكون لها صفرًا في A .

(٤ , ١٠) استخدم تمرين (٩ , ٤) للبرهان على أنّ أيّ امتداد جبري للحقل A يجب أن يكون A نفسه .

(٤ , ١١) ليكن $L:K$ امتدادًا حقليًا . أثبت أن الضرب بعدد ثابت في L تحويل خطي على L على اعتبار أنّ L هو فضاء متجهات على K . متى يكون هذا التحويل غير شاذ؟

(٤ , ١٢) ليكن $L:K$ امتدادًا منتهيًا و p كثيرة حدود لا مختزلة على K، إذا كان ∂p و $[L:K]$ أولين نسبيًا فاثبت عدم وجود أصفار لـ p في L .

(٤ , ١٣) لنفرض أنّ كلاً من $L:K$ و $M:L$ امتداد جبري . هل $M:K$ امتداد جبري؟ لاحظ أن الامتدادات ليس بالضرورة أن تكون منتهية .

(٤ , ١٤) برهن على أنّ $Q(\sqrt{3},\sqrt{5}) = Q(\sqrt{3}+\sqrt{5})$. حاول أن تعمم هذه النتيجة .

(٤ , ١٥) برهن على أن مجموعة الجذور التربيعية لجميع الأعداد الأولية يجب أن تكون مستقلة خطياً على Q .

(٤ , ١٦) جد أساس لـ $Q(\sqrt{1+\sqrt{3}})$ على Q . ثم جد $[Q(\sqrt{1+\sqrt{3}}):Q]$. جد هذه الدرجة بطريقة مختلفة .

(٤ , ١٧) إذا كان $[L:K]$ عددا أوليًا فأثبت أن L امتداد بسيط لـ K .

(٤ , ١٨) ضع علامة صح أو خطأ أمام كل من العبارات التالية :

(ا) الامتدادات التي درجاتها متساوية يجب أن تكون متماثلة .

(ب) الامتدادات المتماثلة تكون درجاتها متساوية .

(ج) جميع الامتدادات الجبرية منتهية .

(د) جميع الامتدادات المتسامية غير منتهية .

(هـ) كل عنصر في $\mathbb{C}$ جبري على $\mathbb{R}$.

(و) كل امتداد للحقل $\mathbb{R}$ يجب أن يكون منتهيًا .

(ز) كل امتداد جبري على Q يجب أن يكون منتهيًا .

(ح) A هو أكبر حقل جزئي من $\mathbb{C}$ وجبريًا على Q .

(ط) كل فضاء متجهات يجب أن يماثل فضاء متّجهات مرتبطًا مع امتداد حقلي .

(ي) امتداد حقل منته يجب أن يكون منتهيًا .

(١٩ , ٤)* ليكن $L : K$ امتدادًا جبرًا حيث K حقل غير منته . برهن على أن $L : K$ امتداد بسيط إذًا وفقط إذا وجد عدد غير منته من الحقول M بحيث $K \subseteq M \subseteq L$ باتباع ما يلي :

(ا) افرض وجود عدد منته من الحقول M واستخدم تمهيدية (٤ , ٤) لإثبات أنّ $L : K$ منته .

(ب) افـــرض $L = K(\alpha_1, \alpha_2)$ لكل $\beta \in K$ ضع $J_\beta = K(\alpha_1 + \beta\alpha_2)$ اثبت وجود عدد منته من J_β المختلفة ومن ثم $L = J_\beta$ لعدد ما β.

(ج) استخدم الاستنتاج الرياضي لبرهان الحالة العامة .

(د) ولإثبات العكس افرض أنّ $L = K(\alpha)$ امتداد جبري بسيط حيث $K \subseteq M \subseteq L$. افرض أن m هي كثيرة حدود α الأصغرية على K وافرض أن m_M هي كثيرة حدود α الأصغرية على M، و برهن على أن $m_M \mid m$ في $L[t]$، و برهن على أن m_M تُعيّن M بطريقة وحيدة وأنّ عدد مثل هذه الـ m_M منته .

الفصل الخامس

المسطرة والفرجار

Ruler and Compass

إنّ الخط المستقيم والدائرة هما الشكلان الهندسيان الوحيدان المستوفيان جميع الشروط المطلوبة في شكل هندسي وذلك وفقًا لاعتقاد افلاطون (Plato)، ولذلك نجد أنّ قدماء الإغريق تأثروا بهذه المقولة للدرجة التي حصروا فيها الأدوات المستخدمة لإنشاء أشكال هندسية إلى أداتين : المسطرة والفرجار ، وكانت المسطرة عندهم عبارة عن حافة مستقيمة بدون علامات تقسيم . وباستخدام هاتين الاداتين وحدهما نستطيع انشاء عدد كبير من الأشكال الهندسية . الخطوط المستقيمة يمكن تقسيمها إلى أي عدد من القطع المستقيمة المتساوية الطول، والزوايا يمكن تنصيفها ، ويمكن رسم خطوط متوازية . وإذا كان لدينا أي مضلع فإنه من الممكن إنشاء مربع مساحته مساوية لمساحة المضلع أو نصف مساحة المربع ، وهلم جرّا . ومن ناحية ثانية فإن هناك كثيرًا من المسائل الهندسية التي من السهل حلها ولكن نحتاج إلى أكثر من مسطرة وفرجار، وهناك ثلاث مسائل مشهورة لم يستطع قدماء الإغريق حلها بواسطة المسطرة والفرجار : مضاعفة المكعب، وتثليث الزاوية، وتربيع الدائرة . وبكلام آخر إيجاد مكعب حجمه ضعف حجم مكعب معطى، وإيجاد زاوية قياسها ثلث قياس زاوية معطاة ، ودائرة مساحتها مربّع مساحة دائرة معطاة .

وإنّ عدم قدرة قدماء الإغريق على حل هذه المسائل ليس غريبًا لأن هذه المسائل غير قابلة للحل فعلاً، ولكن لم يكن لدى الإغريق الطرق التي بواسطتها يستطيعون البرهان على استحالة الحل، وكما يظهر لم يكن لديهم حتى الشك في أن هذه المسائل مستحيلة الحل؛ وبناء على ذلك فلقد استهلكوا كثيرًا من الوقت والتفكير في البحث عن حلول لهذه المسائل .

ومن الجدير بالذكر هنا أنّ هذه المسائل قابلة للحل إذا لم نتقيد بأداتي افلاطون، ولقد استطاع الإغريق ايجاد عدد من الانشاءات تستخدم قطاعات مخروطية أو منحنيات أصعب مثل صدفية نيكومادس (Nichomedes) أو المنحنى التربيعي (انظر Klein, 1962 و Codidge, 1963). ولقد عالج أرخميدس (Archimedes) مسألة تربيع الدائرة بطريقة متميزة وحاذقة حيث برهن على نتيجة يمكن كتابتها حاليًا على الصورة

$$3\frac{10}{71} < \pi < 3\frac{1}{7}$$

وهذا إنجاز رائع بالمقارنة مع التقنية المحدودة المتاحة في ذلك الزمان. وبالطرائق المتاحة لدينا الآن يصبح من السهل أن نجيب على هذه الأسئلة. وسنستخدم الهندسة الإحداثية لنضعهما بصورة جبرية ونطبق نظرية امتدادات الحقول على تلك الصورة الجبرية الناتجة.

(٥,١) صياغة جبرية

Algebraic Formulation

الخطوة الأولى هي إعطاء فكرة حدسية للإنشاء بواسطة المسطرة والفرجار. ولنفرض أن لدينا مجموعة من النقط في المستوى الاقليدي $\mathbb{R}^2$ ولتكن P_0، ونعتبر عمليات من النوعين التاليين:

(ا) عملية ١ (مسطرة): كل نقطتين في P_0 نرسم خلالهما خطًا مستقيمًا.

(ب) عملية ٢ (فرجار): ارسم دائرة مركزها نقطة في P_0 ونصف قطرها يساوي المسافة بين نقطتين في P_0.

ويفضل الإغريق صيغة أكثر تقيدًا من عملية ٢، وبالتحديد: ارسم دائرة مركزها نقطة في P_0، وتمر بنقطة أخرى من P_0. (نستطيع الحصول على العملية ٢ بمتتالية من العمليات المقيدة هذه، أنظر تمرين (٥,١١)، وبالتالي فإنّ أي صورة نأخذها تؤدي لنا الغرض. والعملية ٢ مناسبة أكثر لنا).

تعريف

تسمى نقاط تقاطع أي مستقيمين مختلفين أو أي دائرتين مختلفتين مرسومتين باستخدام العمليتين ١ أو ٢ بأنّها النقاط القابلة للإنشاء بخطوة واحدة من P_0 ، ونقول إنّ النقطة $r \in \mathbb{R}^2$ قابلة للإنشاء من P_0 إذا وجدت متتالية منتهية :

$$r_1, r_2, \cdots, r_n = r$$

من النقاط في $\mathbb{R}^2$ بحيث لكل $i = 1,...,n$ تكون النقطة r_i قابلة للإنشاء بخطوة واحدة من المجموعة

$$P_0 \cup \{r_1, r_2, \cdots, r_{i-1}\}$$

مثال

سنبرهن على أنّ الطريقة المعتادة المتبعة لتنصيف قطعة مستقيمة يمكن أن تستنبط باستخدام عملياتنا الموضحة أعلاه. لنفرض أن لدينا نقطتين $p_1, p_2, \in \mathbb{R}^2$ (شكل ١٢) ولتكن $P_0 = \{p_1, p_2\}$.

(١) ارسم الخط $p_1 p_2$ (عملية ١)

(٢) ارسم الدائرة التي مركزها p_1 ونصف قطرها $p_1 p_2$ (عملية ٢)

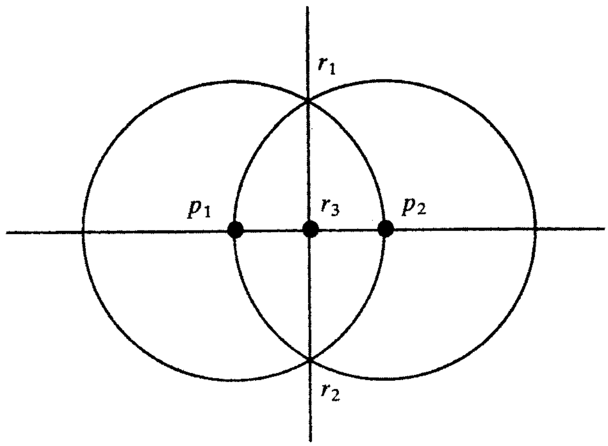
(٣) ارسم الدائرة التي مركزها p_2 ونصف قطرها $p_1 p_2$ (عملية ٢)

(٤) لتكن r_1 و r_2 هما نقطتي تقاطع هاتين الدائرتين .

(٥) ارسم الخط $r_1 r_2$ (عملية ١)

(٦) لتكن r_3 هي نقطة تقاطع الخطّين $p_1 p_2$ و $r_1 r_2$. إذن المتتالية r_1, r_2, r_3 تعرف لنا إنشاء لنقطة منتصف $p_1 p_2$.

بما أن الخط المستقيم يمكن تحديده بنقطتين عليه ، والدائرة تحدد بمركزها ، ونقطة على محيطها فإنّ جميع الأشكال الهندسية التقليدية التي يمكن إنشاؤها في الهندسة الإقليدية تقع ضمن حدي تعريفنا السابق .



شكل (١٢) . تنصيف قطعة مستقيمة باستخدام المسطرة والفرجار.

تدخل نظرية الحقول بصورة طبيعية، عند كل محطة من محطات الإنشاء نأخذ الحقل الجزئي من $\mathbb{R}$ المنشأ من النقاط التي تم إنشاؤها. ونأخذ K_0 الحقل الجزئي من $\mathbb{R}$ المنشأ من الاحداثي السيني والصادي لنقاط P_0 . إذا كان إحداثيًا r_i هما (x_i, y_i) فإننا نعرف استنتاجيًا K_i بأنه الحقل الذي نحصل عليه من K_{i-1} بإقران x_i و y_i، وبكلام آخر

$$K_i = K_{i-1}(x_i , y_i)$$

من الواضح أن:

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$$

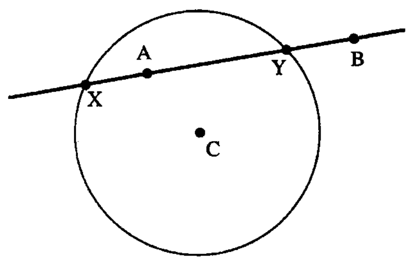
النتيجة المهمة هنا سهلة نوعًا ما :

تمهيدية (٥,١)

باستخدام الترميز أعلاه فإنّ x_i و y_i يكونا صفرين في K_i لكثيرة حدود من الدرجة الثانية على K_{i-1} .

البرهان

هناك ثلاث حالات : مستقيم يقطع مستقيمًا، ومستقيم يقطع دائرة ، ودائرة تقطع دائرة، وكل من هذه الحالات الثلاث نستطيع التعامل معها باستخدام الهندسة الاحداثية، وعلى سبيل المثال سنأخذ الحالة «مستقيم يقطع دائرة .



شكل (١٣) . مستقيم يقطع دائرة.

لنفرض أن A, B, C ثلاث نقاط احداثياتها (p,q), (r,s), (t,u) تقع في K_{i-1} .

ارسم المستقيم AB والدائرة التي مركزها C ونصف قطرها w حيث $w^2 \in K_{i-1}$ كما في الشكل ١٣ . (لاحظ أنّ $w^2 \in K_{i-1}$ لأن w هي المسافة بين نقطتين إحداثياتها واقعة في K_{i-1}. استخدم نظرية فيثاغورس). معادلة المستقيم AB هي :

$$\frac{x-p}{r-p} = \frac{y-q}{s-q} \tag{٥ , ١}$$

ومعادلة الدائرة هي :

$$(x-t)^2 + (y-u)^2 = w^2 \tag{٥ , ٢}$$

وبحل المعادلتين (١ , ٥) مع (٢ , ٥) نحصل على :

$$(x-t)^2 + \left(\frac{s-q}{r-p}(x-p) + q - u\right)^2 = w^2$$

إذن الإحداثيان السينيان لنقطتي التقاطع X و Y هما صفران لكثيرة حدود من الدرجة الثانية على K_{i-1} . وبالمثل الإحداثيان الصاديّان . Δ

إذا حددنا حقلاً بإقران صفريْ كثيرة حدود من الدرجة الثانية فإنّنا نحصل على امتداد درجته 2 . الإنشاء الهندسي يكرّر هذا عدة مرات . إذن لدينا صيغة جبرية لوجود إنشاء لنقطة معلومة :

نظرية (٥,٢)

إذا كانت $r = (x,y)$ قابلة للانشاء من مجموعة جزئية P_0 من $\mathbb{R}^2$ وكان K_0 هو الحقل الجزئي من $\mathbb{R}$ المنشأ من احداثيات نقاط P_0 فإن كلاً من الدرجتين $[K_0(x) : K_0]$ و $[K_0(y) : K_0]$ *قوة للعدد 2* .

البرهان

باستخدام تمهيدية (١ , ٥) وقضية (٣ , ٤) لدينا :

$[K_{i-1}(x_i) : K_{i-1}] = 1$ أو 2 .

(نحصل على 2 إذا كانت كثيرة الحدود على K_{i-1} التي لها الصفر x_i لامختزلة، وما عدا ذلك نحصل على 1) .

بالمثل :

$[K_{i-1}(y_i) : K_{i-1}] = 1$ أو 2 .

وباستخدام قانون البرج :

$$[K_{i-1}(x_i, y_i) : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)]\,[K_{i-1}(x_i) : K_{i-1}]$$

= 1 ، 2 أو 4

(القيمة 4 لا يمكن أن تظهر، أنظر تمرين (١٢ , ٥). وهذه الملاحظة لا نحتاجها في البرهان). إذن $[K_i : K_{i-1}]$ هو قوة للعدد 2.

باستخدام الاستنتاج الرياضي (انظر تمرين ٥ , ٤) نحصل على أنّ $[K_n : K_0]$ هو قوة للعدد 2 . ولكن

$$[K_n : K_0(x)]\,[K_0(x) : K_0] = [K_n : K_0]$$

ومنه فإنّ $[K_0(x) : K_0]$ قوة للعدد 2 . بالمثل $[K_0(y) : K_0]$ قوة للعدد 2 . Δ

(٥,٢) براهين الاستحالة

Impossibility Proofs

سنستخدم الآن النظرية أعلاه للبرهان على استحالة وجود طريقة إنشاء باستخدام المسطرة والفرجار للمسائل الثلاث التي ذكرناها في مقدمة الفصل (ننبه خبراء الرسم هنا بأننا نناقش إنشاءات دقيقة. فعلى سبيل المثال هناك طرق كثيرة لتقسيم الزاوية إلى ثلاث زوايا متساوية تقريبًا ولكن ليس هناك طريقة لتقسيمها إلى ثلاث زوايامتساوية تمامًا).

نظرية (٥,٣)

لا يمكن مضاعفة المكعّب باستخدام المسطرة والفرجار.

البرهان

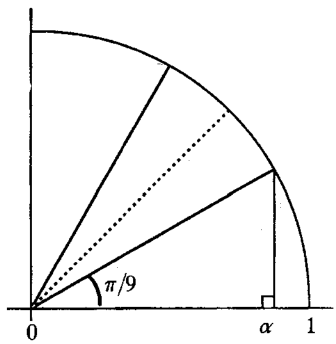
نستطيع أن نفرض أنّ طول ضلع المكعب هو 1 وأن أحد أضلاعه ينطبق على محور السينات أي أنّنا نستطيع افتراض أنّ $P_0 = \{(0,0), (1,0)\}$ ومنه $K_0 = Q$. إذا كان بإمكانا مضاعفة المكعب فإنّنا نستطيع إنشاء نقطة $(\alpha, 0)$ بحيث $\alpha^3 = 2$. وباستخدام نظرية (٥-٢) نجد أن $[Q(\alpha) : Q]$ قوة للعدد 2. لكن α صفر لكثيرة الحدود $t^3 - 2$ على Q وكثيرة الحدود هذه لا مختزلة على Q (بتطبيق ميزان أيزنستاين). إذن $t^3 - 2$ هي كثيرة حدود α الأصغرية على Q. وباستخدام نظرية (٣, ٤) نجد أن $[Q(\alpha) : Q] = 3$. وهذا تناقض. وبالتالي فإننا لا نستطيع مضاعفة المكعّب. Δ

نظرية (٥,٤)

لا يمكن تثليث الزاوية $\frac{\pi}{3}$ باستخدام المسطرة والفرجار.

البرهان

إنّ إنشاء زاوية قياسها $\frac{\pi}{3}$ يكافيء إنشاء النقطة $(\alpha, 0)$ مبتدئين بالنقطتين $(0,0)$ و$(1,0)$ حيث $\alpha = \cos(\pi/9)$. (انظر: شكل ١٤).



شكل (١٤) . تثليث $\frac{\pi}{3}$

وبناءً على ذلك فإنّنا نستطيع إنشاء $(\beta, 0)$ حيث $\beta = 2\cos(\pi/9)$. ومن حساب المثلثات لدينا :

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta).$$

فإذا كانت $\theta = \frac{\pi}{9}$ فإننا نجد أن $\cos(3\theta) = \frac{1}{2}$ وأنّ :

$$\beta^3 - 3\beta - 1 = 0 .$$

الآن $f(t) = t^3 - 3t - 1$ لا مختزلة على Q لأن $f(t+1) = t^3 + 3t^2 - 3$ لا مختزلة بتطبيق ميزان أيزنستاين . وكما هو في النظرية السابقة يكون لدينا $[Q(\beta) : Q] = 3$ وهذا تناقض . Δ

نظرية (٥,٥)

لا يمكن تربيع الدائرة باستخدام المسطرة والفرجار .

البرهان

هذا الإنشاء يكافيء إنشاء النقطة $(0, \sqrt{\pi})$ من $\{(0,0), (1,0)\}$. وبذلك نستطيع بسهولة إنشاء $(0, \pi)$. إذا كان تربيع الدائرة ممكنًا فإنّ $[Q(\pi) : Q]$ قوة للعدد

2 وبصورة خاصة فإنّ π جبري على Q ، ومن ناحية أخرى فإنّ نظرية لندمان (Lindemann) المشهورة تنص على أن π ليس جبريًا على Q . وبذلك يتم البرهان . Δ

سنبرهن على نظرية لندمان (Lindemann) في الفصل السادس . والبرهان يستخدم أفكارًا تخرج عن مسار هذا الكتاب ، لذلك قمنا بوضعها في فصل مستقل . والقارىء الذي يحب أن يسلم بصحتها يستطيع أن يغفل البرهان في الفصل السادس ، فلن تستخدم أي نتائج من النظرية في أي مكان من هذا الكتاب .

من الممكن استخدام طرق أخرى للإنشاء عوضًا على طريقة المسطرة والفرجار التقليدية . ففي عام ١٦٧٢م استطاع مور (Mohr) أن يبرهن أنه من الممكن باستخدام الفرجار فقط إنشاء أي شكل منشأ باستخدام الفرجار والمسطرة معًا (مع افتراض أننا نستطيع إنشاء مستقيم إذا علمنا نقطتين عليه) . وتنسب هذه النتيجة عادة إلى ماستشروني (Mascheroni) . ولقد درس بريانشون (Brianchon) عام ١٨١٨م الإنشاءات التي تستخدم فيها المسطرة فقط . ولقد اقترح بونسليه (Poncelet) أنّه يمكن الاستعاضة عن الفرجار بدائرة مركزها معلوم ، ولقد استخدمت هذه الطريقة من قبل ستاينر (Steiner) (١٨٣٣م) . وإذا لم يكن مركز الدائرة معلومًا فإن عدد الإنشاءات الممكنة يكون صغيرًا . ولقد سئل هلبرت (Hilbert) عن عدد الدوائر التي يجب أن تكون معلومة حتى يتسنى لنا إنشاء مركز احدها باستخدام المسطرة فقط . ولقد برهن كور (Cauer) عام ١٩١٢م على أنّ هذا مستحيل بمعرفة دائرتين فقط ، ولكن إذا كانت الدائرتان متقاطعتين ، متماستان ، أو متمركزتان فإن هذا يصبح ممكنًا . وفي الوقت نفسه استطاع كروسمان (Grossmann) أن يبرهن على أن معرفة ثلاث دوائر مستقلة تكفي لإنشاء أشكال هندسية باستخدام المسطرة فقط . ومن المعروف أيضًا أن جميع الإنشاءات التي تستخدم المسطرة والفرجار يمكن إنشاؤها بواسطة مسطرة ذات حافتين متوازتين أو متقاطعتين في نقطة . (يمكن الحصول على هذه النتائج من كتاب Klein 1962) .

وباستخدام أدوات إضافية نستطيع إنشاء أشكال أكثر ، فباستخدام مسطرة مقسمة نستطيع تقسيم الزاوية إلى ثلاث زوايا متساوية [انظر تمرين (٣ , ٥)] . وبالاطلاع على (Cundy, Rollett 1961) يمكن إيجاد أداة نستطيع بواسطتها تقسيم الزاوية إلى أي عدد من الزوايا المتساوية القياس .

تمــارين

(١ , ٥) استخدم لغة هذا الفصل لإنشاء كل مما يأتي باستخدام المسطرة والفرجار:

(ا) المنصف العمودي لخط مستقيم.

(ب) النقاط التي تقسم المستقيم إلى ثلاثة أقسام متساوية.

(ج) تقسيم مستقيم إلى n أجزاء متساوية.

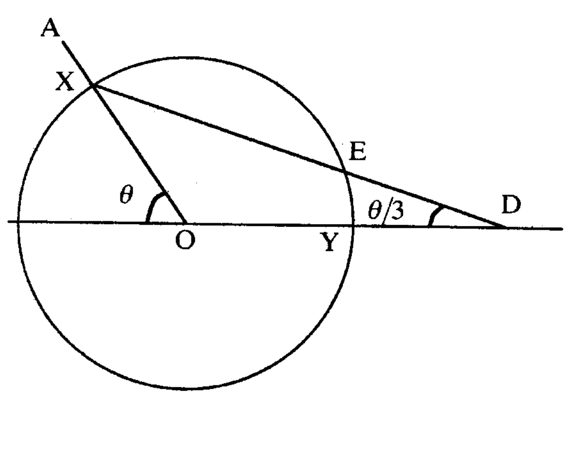
(د) مماس دائرة عند نقطة معلومة.

(هـ) المماسات المشتركة لدائرتين.

(٢ , ٥) قدّر درجات الامتدادات الحقلية التي تحصل عليها من التمرين السابق بإعطاء حد أعلى مقبول نوعًا ما.

(٣ , ٥) تحقق من أنّ الإنشاء التالي يثلث لنا الزاوية باستخدام مسطرة مُعَلَّمة (شكل ١٥). ضع على المسطرة علامتين، المسافة بينهما r . لتكن $A\hat{O}B = \theta$، ارسم دائرة مركزها O ونصف قطرها r وتقطع OA عند X ، OB عند Y . ضع المسطرة بحيث تمر حافتها في X وتكون احدى العلامتين على المستقيم OY عند D . حركها بحيث تكون العلامة الأخرى تقع على الدائرة عند E .

عندئذ تكون $E\hat{D}O = \frac{\theta}{3}$.



شكل(١٥). كيفية تثليث الزاوية باستخدام مسطرة معلمة.

(٥ , ٤) هل نستطيع تثليث الزاوية $2\pi/5$ باستخدام المسطرة والفرجار.

(٥ , ٥) برهن على استحالة إنشاء مضلّع منتظم ذو تسعة أضلاع باستخدام المسطرة والفرجار.

(٥ , ٦) بإيجاد صيغة مناسبة لـ $\cos(5\theta)$ جد طريقة لإنشاء خماسي منتظم.

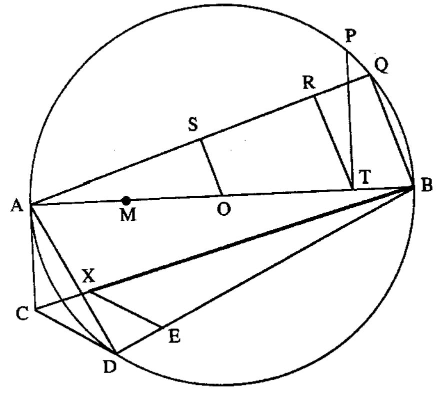
(٥ , ٧) برهن على إمكانيّة تثليث الزاوية θ باستخدام المسطرة والفرجار إذا وفقط إذا كانت كثيرة الحدود:

$$4t^2 - 3t - \cos(\theta)$$

قابلة للاختزال على $Q(\cos(\theta))$.

(٥ , ٨) اشرح تخميس الزوايا (قسمة الزاوية إلى خمس زوايا متساوية).

(٥ , ٩) تحقق من إنشاء π التقريبي (Ramanujan, 1962) (انظر شكل ١٦). افرض أنّ AB هو قطر دائرة مركزها O. نصف AO عند M، ثلث OB عند T. ارسم TP بحيث يكون عمودياً على AB ويقطع الدائرة في P. ارسم BQ = PT، ثم صل AQ. ارسم OS و TR موازيين لـ BQ. ارسم AD = AS و AC = RS مماسين للدائرة عند A. صل BC، BD و CD. اجعل BE = BM. ارسم EX موازيًا لـ CD. عندئذ طول مربع BX يكون مقاربًا لمساحة الدائرة. (سنحتاج إلى أن π تساوي تقريبًا 355/113. إنّ أول من اكتشف هذا التقريب هو العالم الفلكي الصيني ســو تشانك تشنــغ Tsu Chang Ching عام ٤٥٠ قبل الميلاد).



شكل (١٦). تربيع تقريبي للدائرة في كتاب راماناجان (Ramanujan).

(٥ , ١٠) ضع علامة صح أو خطأ أمام كل مما يلي :

(ا) يوجد إنشاءات لتثليث الزاوية إلى درجة كبيرة من التقريب .

(ب) هذه الإنشاءات مقبولة من الناحية التقريبية ولكنها غير مقبولة رياضيًا .

(ج) إحداثيات النقاط القابلة للإنشاء تنتمي للحقل الجزئي من $\mathbb{R}$ الذي درجته على الحقل الجزئي المنشأ من هذه الإحداثيات قوة للعدد 2 .

(د) لا يمكن تثليث الزاوية π باستخدام المسطرة والفرجار .

(هـ) لا يمكن إنشاء مستقيم طوله π من $\{(0,1),(1,0)\}$ باستخدام المسطرة والفرجار .

(و) لا يمكن إنشاء ثلاثة أمثال مكعب باستخدام المسطرة والفرجار .

(ز) العدد π متسام على Q .

(ح) العدد π متسام على $\mathbb{R}$.

(ط) إذاكانت $(0, \alpha)$ غير قابلة للإنشاء من $\{(0,0), (1,0)\}$ باستخدام المسطرة والفرجار فإنّ α متسام على Q .

(ي) المسائل الهندسية ليس بالضرورة أن تحل دائمًا هندسيًا .

(٥ , ١١) أثبت أنّه من الممكن الاستعاضة عن عملية ٢ بـ «ارسم دائرة مركزها P_0 وتمر بنقطة اخرى من P_0» دون التأثير على مجموعة النقاط القابلة للإنشاء .

(٥ , ١٢) في برهان نظرية (٥ , ٢) برهن على أنّه بالفعل $[K_{i-1}(x_i, y_i) : K_{i-1}] = 2$ أو 1 . **(إرشاد** : برهن على أن x_i و y_i تنتمي إلى الامتداد نفسه من الدرجة الثانية على K_{i-1}) .

الفصل السادس

الأعـداد المتسامية

Transcendental Numbers

سوف لا نحتاج إلى مادة هذا الفصل في مكان آخر فلذلك يمكن للقاريء- إن أراد - أن يستغني عنها .

لإتمام برهان استحالة تربيع الدائرة (وبذلك نتوّج ثلاثة آلاف سنة من المحاولات الرياضية) يجب أن نبرهن على أن π عدد متسام على Q . (في هذا الفصل كلمة متسام دائمًا تعني متسام على Q). البرهان المعطى هنا له صبغة تحليلية وهذا ليس غريباً حيث إنّ أفضل تعريف للعدد π هو تعريف تحليلي . والتقنية المتبعة تستخدم تكامل ، تفاضل ، وبعض المعالجة للمتراجحات ، مع التجاهل المعقول للعبارات المعقدة .

إنّ وجود أعداد متسامية في حقل الأعداد المركّبة يكتنفه شيء من الغموض ، وإن أول من برهن على وجودها هو العالم ليوفايل (Liouville) عام ١٨٤٤م باستخدام الأعداد الكسرية لتقريب الأعداد الحقيقية . ومن المعلوم أنه لا يمكن تجاوز سرعة معينة لتقريب الأعداد الجبرية باستخدام الأعداد الكسرية (انظر تمارين (٦ , ٦ - ٨ , ٦))، و إن ايجاد عدد متسام يقتصر على إيجاد عدد يمكن تقريبه بسرعة أكبر من الحد الأعلى المعلوم للأعداد الجبرية . ولقد وجد ليوفايل (Liouville) أنّ هذا صحيح للعدد الحقيقي :

$$\xi = \sum_{n=1}^{\infty} 10^{-n!}$$

ولكن لم يستطع أحد البرهان على وجود عدد متسام «بشكل مألوف» إلى أن جاء العالم هيرمايت (Hermite) عام ١٨٧٣م وبرهن على أنّ العدد e متسام . وبعد ذلك استخدم العالم ليندمان (Lindemann) طريقة متشابهة لبرهان أن π متسام وذلك عام ١٨٨٢م .

ولقد استطاع العالم كانتور (Cantor) عام ١٨٧٤م أن يقدم برهانًا على وجود الأعداد المتسامية دون أن يزودنا بأي منها، واستخدم في برهانه هذا طرقًا من نظرية المجموعات وكان هذا أول نجاح تحقق في نظرية كانتور للأعداد الرئيسة غير المنتهية، ولقد واجهها الرياضيون بحماس غير كبير [انظر تمارين (١,٦ - ٤,٦)].

وسنقدم في هذا الفصل أربعة براهين، نتبع طريقة البرهان بالتناقض في كل منها وهذا التناقض يعتمد على النتيجة السهلة التالية:

تمهيدية (٦,١)

لتكن $f:\mathbb{Z} \longrightarrow \mathbb{Z}$ دالّة بحيث $f(n)$ تؤول إلى الصفر عندما $n \to \infty$. عندئذ يوجد عدد N بحيث يكون $f(n) = 0$ لكل $n \geq N$.

البرهان

بما أنّ $f(n) \to 0$ عندما $n \to \infty$ فيكون لدينا $|f(n) - 0| < \frac{1}{2}$ عندما يكون $n \geq N$ حيث إن N عدد صحيح ما، وبما أنّ $f(n)$ عدد صحيح فإنّ هذا يؤدّي إلى أنّ $f(n) = 0$ لكل $n \geq N$.

(٦,١) اللاكسرية

Irrationality

يعتبر البرهان الذي قدمه ليندمان برهانًا فيه إبداع ولكنه معقد، وللتحضير لهذا البرهان سنبرهن أولا على نظريّات أسهل ولكنها تحمل الطابع العام نفسه، و لسنا بحاجة لهذه النتائج للبرهان على نظريّة ليندمان ولكن معرفة الأفكار التي يحتويها البرهان ستساعدنا كثيرًا. والعالم لامبارت (Lambert) هو أول من برهن على هذه النظريات عام ١٧٧٠م مستخدمًا في ذلك الكسور المتّصلة إلا أنّها غالبًا تنسب للعالم ليجندر (Legendre).

نظرية (٦,٢)

العدد الحقيقي π عدد غير كسري.

البرهان

اعتبر التكامل

$$I_n = \int_{-1}^{1} \left(1-x^2\right)^2 \cos(\alpha x)dx$$

باستخدام التكامل بالأجزاء نحصل على :

$$\alpha^2 I_n = 2n(2n-1)I_{n-1} - 4n(n-1) I_{n-2} \qquad (٦,١)$$

عندما يكون $n \geq 2$. وباستخدام الاستنتاج الرياضي على n نحصل على

$$\alpha^{2n+1} I_n = n!(P \sin(\alpha) + Q \cos(\alpha)) \qquad (٦,٢)$$

حيث أن P و Q كثيرتا حدود في α ذات معاملات صحيحة ودرجة كل منهما أصغر من $2n+1$. يظهر الحد $n!$ من العامل $2n(2n-1)$ ، وفي المعادلة (٦,١) .

ولغرض التناقض نفرض أنّ π عدد كسري . إذن $\pi = \frac{a}{b}$ حيث $a,b \in Z$ و $b \neq 0$.

ضع $\alpha = \frac{\pi}{2}$ في المعادلة (٦,٢) . إذن

$$J_n = a^{2n+1} I_n/n!$$

عدد صحيح . الآن :

$$J_n = \frac{a^{2n+1}}{n!}\int_{-1}^{1} \left(1-x^2\right)^n \cos\left(\frac{\pi}{2}x\right)dx$$

المكامل > 0 عندما $-1 < x < 1$ ، ومنه فإنّ $J_n > 0$. إذن $J_n \neq 0$ لكل n . ولكن

$$|J_n| \leq \frac{|a|^{2n+1}}{n!}\int_{-1}^{1} \cos\left(\frac{\pi}{2}x\right)dx$$

$$\leq C\,|a|^{2n+1} / n!$$

حيث إن C عدد ثابت . إذن $J_n \to 0$ عندما $n \to \infty$ وهذا يناقض **تمهيدية (٦,١)** وبالتالي فإن π غير كسري . Δ

قدّم برهان النتيجة التالية العالم ليجندر عام ١٧٩٤م في كتابه **عناصر الهندسة** (والذي تأثر به جالوا كما ذكرنا في المقدمة) .

نظرية (٦,٣)

العدد الحقيقي π^2 عدد غير كسري.

البرهان

لنفرض أنّ $\pi^2 = \frac{a}{b}$ حيث إن $a, b \in \mathbb{Z}$ و $b \neq 0$.

عرّف الدالتين:

$$f(x) = x^n(1-x)^n / n!$$

و

$$G(x) = b^n\left\{\pi^{2n}f(x) - \pi^{2n-2}f''(x) + \cdots + (-1)^n\pi^0 f^{(2n)}(X)\right\}.$$

وسنبرهن على أنّ أية مشتقة للدالة f تكون قيمتها عددًا صحيحًا عند 0 و 1. تذكر قاعدة لايبنز (Leibniz) لتفاضل حاصل الضرب:

$$\frac{d^m}{dx^m}(uv) = \sum\binom{m}{r}\frac{d^r u}{dx^r}\cdot\frac{d^{m-r}v}{dx^{m-r}}$$

إذا فاضلنا كلاً من x^n و $(1-x)^n$ أقل من n من المرات نجد أنّ قيمة كل من هذه المشتقات صفر عندما يكون $x = 0$ أو 1. وإذا فاضلنا أحدهما n أو أكثر من المّرات فإن المقام $n!$ يختصر. إذن $G(0)$ و $G(1)$ عددان صحيحان. الآن

$$\frac{d}{dx}\{G'(x)\sin(\pi X) - \pi G(x)\cos(\pi X)\} = \left\{G''(x) + \pi^2 G(x)\right\}\sin(\pi X)$$

$$= b^n \pi^{2n+2} f(x) \sin(\pi x)$$

وبما أن $f(x)$ كثيرة حدود في x درجتها 2n فإنّ $f^{(2n+2)}(x) = 0$. والعبارة الأخيرة تساوي:

$$\pi^2 a^n \sin(\pi x) f(x).$$

إذن

$$\pi\int_0^1 a^n \sin(\pi x)f(x)dx = \left[\frac{G'(x)\sin(\pi x)}{\pi} - G(x)\cos(\pi x)\right]_0^1 = G(0) + G(1)$$

وهذا عدد صحيح. كما في السابق فإنّ التكامل لا يساوي صفرًا. ولكن

$$\left|\int_0^1 a^n \sin(\pi x) f(x)dx\right| \le |a|^n \int_0^1 |\sin(\pi x)||f(x)|dx$$

$$\le |a|^n \int_0^1 \frac{\left|x^n(1-x)^n\right|}{n!}dx$$

$$\le \frac{1}{n!}\int_0^1 \left|(ax)^n(1-x)^n\right|dx$$

وهذا يؤول إلى الصفر عندما تؤول n إلى ∞ . وهذا التناقض يكمل البرهان . Δ

(٦,٢) تسامي العدد e

Transcendence of e

ننتقل الآن من اللا كسرية إلى وضع أكثر تحييرًا وهو التسامية . وإنّ العالم هيرمايت هو الذي قدم برهانًا لتسامي العدد e ولقد تمّ إعطاء صورة مبسطة لهذا البرهان من قبل كل من العلماء فارستراس ، (Weierstrass) ، هيلبرت (Hilbert)، هيروتز (Hurwitz)، وجوردان (Gordan)، وسنقدم هنا الصيغة المبسطة للبرهان (وهذا ينطبق أيضاً على برهان نظرية ليندمان) .

نظريّة (٦,٤) (هيرمايت)

العدد الحقيقي e متسام .

البرهان

نفرض أنّ e عدد ليس متساميًا . إذن

$$a_m e^m + \ldots + a_1 e + a_0 = 0$$

وبدون أن تتأثر الحالة العامة من الممكن أن نفرض أنّ $a_i \in Z$ لكل i وأن $a_0 \neq 0$.

ضع

$$f(x) = \frac{x^{p-1}(x-1)^p (x-2)^p \ldots (x-m)^p}{(p-1)!}$$

حيث إنّ p عدد أوّلي . لاحظ أن f كثيرة حدود في x درجتها تساوي $mp + p - 1$ ، ضع

$$F(x) = f(x) + f'(x) + ... + f^{(mp+p-1)}(x)$$

ولاحظ أن $f^{(mp+p)}(x) = 0$. احسب الآن :

$$\frac{d}{dx}\left\{e^{-x} F(x)\right\} = e^{-x}\left\{F'(x) - F(x)\right\}$$

$$= - e^{-x} f(x)$$

إذن لكل j

$$a_j \int_0^j e^{-x} f(x)dx = a_j \left[-e^{-x} F(x)\right]_0^j$$

$$= a_j F(0) - a_j e^{-j} F(j)$$

بالضرب في e^j والجمع من $j = 0$ إلى $j = m$ نحصل على :

$$\sum_{j=0}^{m}\left(a_j e^j \int_0^j e^{-x} f(x)dx\right) = F(0)\sum_{j=0}^{m} a_j e^j - \sum_{j=0}^{m} a_j F(j)$$

$$= -\sum_{j=0}^{m}\sum_{i=0}^{mp+p-1} a_j f^{(i)}(j) \qquad (٦,٣)$$

وذلك باستخدام المعادلة التي افترضنا أنّ e تحققها .

وسنبرهن الآن على أنّ كلاً من $f^{(i)}(j)$ عدد صحيح ، وهذا العدد الصحيح يقبل القسمة على p إلا إذا كان $j = 0$ أو $i = p-1$ ، و نستخدم قاعدة لايبنز مرّة أخرى . عندما تكون $j \neq 0$ فإن الحدود غير الصفرية نحصل عليها من العامل $(x - j)^p$ بعد اشتقاقه p من المرات . وبما أنّ $p!/(p-1)! = p$ فإنّ هذه الحدود أعداد صحيحة تقبل القسمة على p . وإذا كان $j = 0$ فإنّ أول حد غير صفري نحصل عليه عندما تكون $i = p-1$ وفي هذه الحالة :

$$f^{(p-1)}(0) = (-1)^p ... (-m)^p .$$

والحدود غير الصفرية اللاحقة هي مضاعفات p .

وعليه فإنّ قيمة المعادلة (٣ , ٦) هي :

$$kp + a_0(-1)^p \cdots (-m)^p$$

حيث $k \in Z$. الآن إذا كان $p > \max(m, |a_0|)$ فإنّ العدد الصحيح $a_0(-1)^p \cdots (-m)^p$ لا يقبل القسمة على p . ومنه إذا كان p عدداً أوليًا كبيرًا ما فيه الكفاية فإنّ قيمة المعادلة (٣ , ٦) عدد صحيح لا يقبل القسمة على p وبالتالي ليس صفرًا .

نقدّر الآن التكامل . إذا كان $0 \le x \le m$ فإنّ

$$|f(x)| \le m^{mp+p-1} / (p-1)!$$

إذن

$$\left|\sum_{j=0}^{m} a_j e^j \int_0^j e^{-x} f(x)dx\right| \le \sum_{j=0}^{m} \left|a_j e^j\right| \int_0^j \frac{m^{mp+p-1}}{(p-1)!} dx$$

$$\le \sum_{j=0}^{m} \left|a_j e^j\right| j \frac{m^{mp+p-1}}{(p-1)!}$$

وهذا يؤول إلى 0 عندما يؤول p إلى ∞ . وهذا تناقض وبالتالي فإن e متسام . Δ

(٦,٣) تسامي العدد π

Transcendence of π

إن برهان تسام π يستخدم أفكارا شبيهة بالتي استخدمت في البراهين السابقة ولكنها أعقد نوعًا ما . سنستخدم كذلك خواص كثيرات الحدود المتناظرة في أماكن عدة من البرهان (الفصل الثاني) .

نظرية (٦,٥) (ليندمان)

العدد الحقيقي π عدد متسام .

البرهان

لنفرض لغرض التناقض أنّ π صفر لكثيرة حدود غير صفرية على Q، ومنه فإنّ $i\pi$ كذلك حيث $i = \sqrt{-1}$. لتكن $\theta_1(x) \in Q[x]$ كثيرة حدود أصفارها $\alpha_1 = i\pi, \alpha_2, ..., \alpha_n$. وباستخدام نظريّة مشهورة للعالم أويلر (Euler) لدينا

$$e^{i\pi} + 1 = 0$$

إذن

$$(e^{\alpha_1}+1)(e^{\alpha_2}+1)\dots(e^{\alpha_n}+1) = 0 \qquad (٦,٤)$$

سوف ننشيء الآن كثيرة حدود بمعاملات صحيحة أصفارها هي الأسس $\alpha_{i1} + ... + \alpha_{ir}$ للعدد e التي تظهر عند فك المعادلة (٦,٤). وعلى سبيل المثال حدود على الصورة:

$$e^{\alpha_s} \times e^{\alpha_t} \times 1 \times 1 \times ... \times 1$$

تزودنا بأس $\alpha_s + \alpha_t$ وبأخذ جميع احتمالات القيم s، t نحصل على $\alpha_1 + \alpha_2, ..., \alpha_{n-1} + \alpha_n$. إنّ كثيرات الحدود الابتدائية المتناظرة لهذه القيم يجب أن تكون متناظرة في $\alpha_1, \alpha_2, ..., \alpha_n$ ، وباستخدام نظرية (٩ , ٢) نستطيع كتابتها ككثيرات حدود بدلالة كثيرات الحدود المتناظرة في $\alpha_1, ..., \alpha_n$. وهذه بدورها تكتب بدلالة معاملات θ_1 التي أصفارها $\alpha_1, ..., \alpha_n$. إذن الأزواج $\alpha_s + \alpha_t$ تحقق المعادلة $\theta_2(x) = 0$ حيث أن θ_2 كثيرة حدود بمعاملات كسرية. وبالمثل فإنّ مجاميع k من هذه الـ α يجب أن تكون أصفارًا لكثيرة حدود $\theta_k(x)$ على Q . إذن

$$\theta_1(x)\, \theta_2(x) \dots \theta_n(x)$$

هي كثيرة حدود على Q أصفارها أسس e بمفكوك المعادلة (٦,٤). وبالقسمة على قمة ملائمة لقوى الصفر x وبالضرب بعدد صحيح ملائم نحصل على $\theta(x) \in \mathbb{Z}[x]$ بحيث يكون أصفارها الأسس غير الصفرية $\beta_1, \beta_2, ..., \beta_r$ للعدد e بمفكوك

المعادلة (٤ ,٦). الآن تصبح المعادلة (٤ ,٦) كالتالي :

$$e^{\beta_1} + \ldots + e^{\beta_r} + e^0 + \ldots + e^0 = 0$$

أي

$$e^{\beta_1} + \ldots + e^{\beta_r} + k = 0 \qquad (٦ , ٥)$$

حيث $k \in \mathbb{Z}$. وبما أنّ الحد $1 \times 1 \times \ldots \times 1$ يظهر في المفكوك فإنّ $k > 0$. لنفرض أن

$$\theta(x) = c\, x^r + c_1\, x^{r-1} + \ldots + c_r$$

لاحظ أنّ $c_r \neq 0$ لأنّ 0 ليس صفراً لـ θ .

اعتبر

$$f(x) = \frac{c^s\, x^{p-1}\, \{\theta(x)\}^p}{(p-1)\,!}$$

حيث إنّ $s = rp - 1$ و p عدد أولي . واعتبر أيضًا أنّ

$$F(x) = f(x) + f'(x) + \ldots + f^{(s+p+r-1)}(x)$$

ولاحظ أنّ $f^{(s+p+r)}(x) = 0$. كما في السابق

$$\frac{d}{dx}\{e^{-x} F(x)\} = -\, e^{-x} f(x)$$

إذن

$$e^{-x}F(x) - F(0) = -\int_0^x e^{-y} f(y)\, dy$$

وبوضع $y = \lambda x$ نحصل على :

$$F(x) - e^x F(0) = -\, x \int_0^1 e^{(1-\lambda)x} f(\lambda x)\, d\lambda$$

وبفرض أنّ x تأخذ القيم $\beta_1, \ldots, \beta_r$ واستخدام المعادلة (٥ ,٦) نحصل على :

$$\sum_{j=1}^{r} F(\beta_j) + k\, F(0) = -\sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-\lambda)\beta_j} f(\lambda \beta_j)\, d\lambda \qquad (٦ , ٦)$$

سنبرهن على أن الطرف الأيسر من المعادلة (٦ ,٦) يجب أن يكون عددًا صحيحًا غير صفري عندما يكون p كبيرًا ما فيه الكفاية . الآن

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = 0$$

عندما يكون $0 < t < p$. لاحظ أنّ كل مشتقة $f^{(t)}(\beta_j)$ حيث إن $t \geq p$ يجب أن يكون p أحد عواملها لأنّنا يجب أن نفاضل $\{\theta(x)\}^p$ p مرة على الأقل لنحصل على حد غير صفري . ولكل $t \geq p$ لدينا.

$$\sum_{j=1}^{r} f^{(t)}(\beta_j)$$

كثيرة حدود متناظرة في β_j ودرجتها أصغر أو تساوي s . إذن هي كثيرة حدود درجتها أصغر أو تساوي s ومعاملاتها c_i / c وذلك باستخدام نظرية (٩ , ٢). إنّ العامل c^s في تعريف $f(x)$ يجعل هذا عددًا صحيحًا. إذن عند $t \geq p$

$$\sum_{j=1}^{r} f^{(t)}(\beta_j) = p\,k_t$$

حيث $k_t \in \mathbb{Z}$. لنركز اهتمامنا الآن على $F(0)$.

لدينـا :

$$f^{(t)}(0) = \begin{cases} 0 & (t \leq p-2) \\ c^s c_r^p & (t = p-1) \\ \ell_t p & (t \geq p) \end{cases}$$

حيث $\ell_t \in \mathbb{Z}$. إذن الطرف الأيسر من المعادلة (٦ , ٦) هو

$$K p + k c^s c_r^p$$

حيث $K \in \mathbb{Z}$. لاحظ أن $k \neq 0$ ، $c \neq 0$ و $c_r \neq 0$ وإذا خذنا

$$p > \max(k, |c|, |c_r|)$$

يصبح الطرف الأيسر من المعادلة (٦ , ٦) عددًا صحيحًا غير قابل للقسمة على p ومن ثم لا يساوي صفرًا .

والجزء الأخير من البرهان عمل روتيني حيث نقدّر الطرف الأيمن من المعادلة (٦ , ٦).

الآن

$$\left|f(\lambda\beta_j)\right| \le \frac{|c|^s\,|\beta_j|^{p-1}\,(m(j))^p}{(p-1)\,!}$$

حيث إنّ $m(j) = \sup\limits_{0\le\lambda\le1} \left|\theta(\lambda\beta_j)\right|$

إذن

$$\left| - \sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-\lambda)\beta_j} f(\lambda\beta_j)\, d\lambda \right| \le \sum_{j=1}^{r} \frac{\left|\beta_j\right|^p \left|c^s\right| \left|m(j)\right|^p\ B}{(p-1)\,!}$$

حيث

$$B = \left| \max_j \int_0^1 e^{(1-\lambda)\beta_j}\, d\lambda \right| .$$

وهذا يؤول إلى 0 عندما يؤول p إلى ∞.

وهذا تناقض وبالتالي فإن π متسام. Δ

تمــارين

التمارين الأربعة الأولى تعطينا الخطوط العريضة لبرهان كانتور على وجود أعداد متسامية.

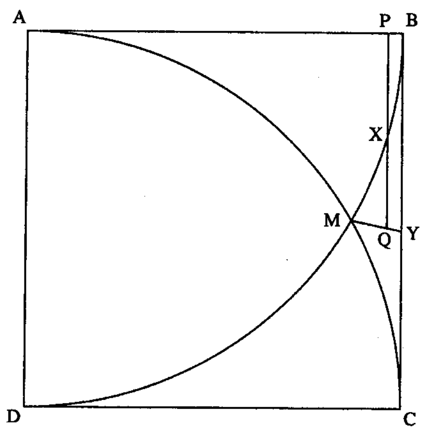
(٦,١) أثبت أنّ $\mathbb{R}$ غير قابلة للعدد.

(٦,٢) نعرف ارتفاع كثيرة الحدود $f(t) = a_0 + a_1t + \cdots + a_nt^n \in \mathbb{Z}[t]$ كالتالي: $h(f) = n + |a_0| + \ldots + |a_n|$. برهن على أنّ عدد كثيرات الحدود على $\mathbb{Z}$ التي ارتفاعها عدد معين h يجب أن يكون منتهيًا.

(٦, ٣) أثبت أنّ أيّ عدد جبري يجب أن يحقق كثيرة حدود على $\mathbb{Z}$. استخدم تمرين (٦, ٢) لإثبات أنّ عدد الأعداد الجبرية منته.

(٦, ٤) استخدم تمرين (١, ٦) وتمرين (٢و٦) لإثبات وجود الأعداد المتسامية.

(٦, ٥) لقد اقترح ثوماس هوبيز (Thomas Hobbes) (فيلسوف) الإنشاء في الشكل (٧) لتربيع الدائرة. ارسم ربعي دائرتين داخل مربّع الوحدة ABCD بحيث تتقاطع في M، ونصف القوس BM في X، وارسم PQ مارًا في X وموازيًا BC بحيث PX = XQ، صل MQ ومده ليلاقي BC في Y، عندئذ BY يساوي تمامًا القوس BM. جد الخطأ.



شكل(١٧). محاولة هوبيز لتربيع الدائرة.

التمارين الثلاثة التالية تعطينا برهان ليوفيل على وجود الأعداد المتسامية.

(٦, ٦) لنفرض أنّ x عدد غير كسري وأنّ

$$f(x) = a_n x^n + \dots + a_0 = 0$$

حيث إنّ $a_0 + \cdots + a_n \in \mathbb{Z}$. إذا كان $p,q \in \mathbb{Z}$، $q \neq 0$ و $f(p/q) \neq 0$ فأثبت أنّ $|f(p/q)| \geq 1 / q^n$.

(٦, ٧) لنفرض أنّ $x - 1 < p/q < x + 1$ وأنّ p/q أقرب إلى x من أي صفر آخر لـ f. إذا

كان $x - 1 < y < x + 1$ فاثبت وجود M بحيث $|f'(y)| < M$. استخدم نظرية القيمة المتوسطة لاثبات أن $|p/q - x| \geq M^{-1} q^{-n}$. ثم اثبت أنّه إذا كـــان $r > n$ و $k > 0$ فإنّه يوجد عدد منته من الأعداد p و q بحيث $|p/q - x| < k q^{-r}$.

(٦,٨) استخدم هذه النتيجة لبرهان أنّ العدد $\sum_{n=1}^{\infty} 10^{-n!}$ متسام .

(٦,٩) ضع علامة صح أو خطأ أمام كل مما يأتي :

(ا) π عدد غير كسري .

(ب) جميع الأعداد غير الكسرية يجب أن تكون متسامية .

(ج) أي مضاعف كسري للعدد π يجب أن يكون متساميًا .

(د) أحيانا تكون الطريقة الوحيدة لبرهان نظرية هي أن نسحب أرنبًا من قبعة .

(هـ) e عدد غير كسري .

(و) إذا كان كل من α و β متساميًا فإنّ $\alpha + \beta$ كذلك .

(ز) الأعداد المتسامية حلقة جزئية من $\mathbb{C}$.

(ح) الحقل $Q(\pi)$ يماثل $Q(t)$ حيث t غير معين .

(ط) $Q(\pi)$ و $Q(e)$ حقلان غير متماثلين .

(ي) $Q(\pi)$ يماثل $Q(\pi^2)$.

الفصل السابع

الفكرة وراء نظرية جالوا
The Idea Behind Galois Theory

سنحتاج إلى بعض الوقت قبل أن نكون جاهزين لبرهان نظريّة جالوا الرئيسة. ولتجنب احتمال الضياع عن الخط الأساسي بين الكميّة الكبيرة من الوسائل المتبعة في البرهان، سنقدم خطوطًا عريضة للنظريّة التي سنعرضها والخطوات اللازمة لبرهانها.

لقد سبق أن ربطنا فضاء متجهات مع كل امتداد خطي. وهذا الربط أداة ليست كافية لبعض المسائل، لأنها بمحض القول تقيس لنا الحجم وليس الشكل. ولقد تعمق جالوا أكثر من ذلك كما رأينا في الفكرة الشاملة أنّه ربط مع كل كثيرة حدود $p \in K[t]$ زمرة تبديلات والتي تسمى الآن بزمرة جالوا اعترافًا بفضله. ومن أهم الأسباب التي تجعل عمل جالوا مذهلاً هو أن الزمر لم تكن معروفة في تلك الأيام إلا بصورة بدائية. وكان جالوا هو أول من اكتشف أهميتها.

وفي الوقت الحاضر يستخدم أسلوب آخر للحصول على زمرة جالوا، وهذا الأسلوب يعتمد على الامتداد الحقلي $L : K$ المرتبط مع p. وسنبدأ بتقديم التعريف التالي.

تعريف

ليكن K حقل جزئيًا من الحقل L. نقول إن التماثل الذاتي α على L هو تماثل ذاتي بالنسبة إلى K إذا كان

$$\alpha(k) = k \quad \text{لكل} \quad k \in K.$$

وتأثير ذلك هو أن تكون α تماثلاً ذاتيًا للامتداد بدلاً من كون L الحقل الكبير فقط. والفكرة من اعتبار تماثلات ذاتية لكائن رياضي بالنسبة إلى كائن رياضي جزئي أسلوب

عام مفيد ، وهذا يقع في نطاق عمل مشهور قام به العالم فيلكس كلاين (Felix Klein) ، وكانت فكرة كلاين اعتبار أي هندسة كنظريّة من اللامتغيرات لزمرة تحويلات معيّنة ، وعليه فإن الهندسة الاقليدية هي دراسة اللامتغيرات لزمرة التحويلات التي تحافظ على المسافة في المستوى ، والهندسة الإسقاطية تنشأ من سماحنا لتحويلات إسقاطية ، والطوبولوجيا تنشأ من زمرة جميع الدوال المتصلة التي تكون نظائرها متصلة (تسمى تماثلات مستمرة أو تحويلات طوبولوجية) . وبهذا التفسير يكون أي امتداد حقلي عبارة عن هندسة ونقوم ببساطة بدراسة أشكال هندسية .

والمرتكز الذي تقوم عليه النظرية ما هو إلا نتيجة برهانها ليس صعبًا . وكما قال لويس كارول (Lewis Carroll) في كتابه «صيد السنارك» إنها قاعدة ضخمة ولكنها مبتذلة حيث ما يترتب عليها أكثر من محتواها .

نظرية (٧,١)

إذا كان $L:K$ امتدادًا حقليًا فإنّ مجموعة جميع تماثلات L الذاتية بالنسبة إلى K تكون زمرة تحت عملية تحصيل الدوال .

البرهان

لنفرض أنّ α و β تماثلان ذاتيان للحقل L بالنسبة إلى K ، ومن الواضح أنّ $\alpha\beta$ تماثل ذاتي للحقل L ، وكذلك إذا كان $k \in K$ فإنّ $\alpha\beta(k) = \alpha(k) = k$. إذن $\alpha\beta$ تماثل ذاتي للحقل L بالنسبة إلى K ، ومن الواضح أن الدالة المحايدة على L تماثل ذاتي بالنسبة إلى K ، وأخيرًا α^{-1} تماثل ذاتي على L ولدينا لكل $k \in K$:

$$k = \alpha^{-1}\alpha(k) = \alpha^{-1}(k) .$$

إذن α^{-1} تماثل ذاتي بالنسبة إلى K . إن تحصيل الدوال تجميعي وبالتالي فإن مجموعة جميع التماثلات الذاتية على L بالنسبة إلى K زمرة . Δ

تعريف

زمرة جالوا $\Gamma(L:K)$ للامتداد الحقلي $L:K$ هي زمرة جميع التماثلات الذاتية على L بالنسبة إلى K تحت عملية تحصيل الدوال .

أمثلـة

(١) اعتبر الامتداد $\mathbb{C} : \mathbb{R}$. لنفرض أنّ α تماثل ذاتي على $\mathbb{C}$ بالنسبة إلى $\mathbb{R}$.
ولتكن $j = \alpha(i)$ حيث $i = \sqrt{-1}$. عندئذ

$$j^2 = (\alpha(i))^2 = \alpha(i^2) = \alpha(-1) = -1$$

لأنّ $\alpha(r) = r$ لكل $r \in \mathbb{R}$. إذن إما $j = i$ أو $j = -i$. الآن لكل $x, y \in \mathbb{R}$ لدينا :

$$\alpha(x + iy) = \alpha(x) + \alpha(i)\,\alpha(y) = x + iy \ .$$

إذن لدينا الاحتمالان التاليان للتماثلات الذاتية على $\mathbb{C}$ بالنسبة إلى $\mathbb{R}$:

$$\alpha_1 : x + iy \to x + iy$$

$$\alpha_2 : x + iy \to x - iy$$

وبما أنّ α_1 هي الدالّة المحايدة فإنّها تماثل ذاتي على $\mathbb{C}$ بالنسبة إلى $\mathbb{R}$. الدالّة α_2 تعرّف بأنّها المرافق المركّب ومن الممكن أن نبرهن على أنّها تماثل ذاتي على $\mathbb{C}$ بالنسبة إلى $\mathbb{R}$ كالتالي :

$$\alpha_2((x+iy) + (u+iv)) = (x+u) - (y+v)i$$

$$= \alpha_2(x+iy) + \alpha_2(u + iv)$$

$$\alpha_2((x+iy)(u+iv)) = \alpha_2(xu-yv + i(xv+yu))$$

$$= xu - yv - i(xv+yu)$$

$$= (x-iu)\,(u-iv)$$

$$= \alpha_2(x+iy)\,\alpha_2(u+iv)$$

إذن α_2 تماثل ذاتى بالنسبة إلى $\mathbb{R}$.

وواضح أنّ $\alpha_2^2 = \alpha_1$ ، وبالتالي فإنّ زمرة جالوا Γ $(\mathbb{C} : \mathbb{R})$ زمرة دورية من الرتبة 2

(٢) ليكن c الجذر التكعيبي الحقيقي للعدد 2 واعتبر$[\mathbb{C} : Q(c)]$. إذا كانت α تماثلاً ذاتيًا على $Q(c)$ بالنسبة إلى Q فإنّ

$$(\alpha(c))^3 = \alpha(c^3) = \alpha(2) = 2 \ .$$

وبما أنّ $Q \subseteq Q(c)$ فإن $\alpha(c) = c$. إذن α هي الدالّة المحايدة وبالتالي رتبة $\Gamma(Q(c) : Q)$ تساوي 1 .

وبالرغم من سهولة برهاننا على أن مجموعة جميع التماثلات الذاتية للحقل L بالنسبة إلى K تكون زمرة ، فإنّ هذه الحقيقة وحدها لا تكفي للتقدم في موضوعنا. ولكي يكون لزمرة جالوا استخدام فإنها يجب أن تعكس شيئًا عن خواص $L : K$. ولقد اكتشف جالوا (وبعد ذلك عُبِّر عنه بدلالة كثيرات الحدود) أنّه تحت شروط إضافية يوجد تناظر أحادي بين :

(١) الزمر الجزئية لزمرة جالوا $\Gamma(L : K)$

(٢) الحقول الجزئية M من L بحيث $K \subseteq M$.

وكذلك فإنّ هذا التقابل يعكس علاقة الاحتواء، وسنعود إلى هذه النقطة بعد لحظات ولكننا سنوضح أولاً ماهية هذا التقابل.

إذا كان $L : K$ امتدادًا حقليًا فإننا نسمي الحقل M بحيث $K \subseteq M \subseteq L$ بالحقل الوسطي. لكل حقل وسطي M نشرك الزمرة $M^* = \Gamma(L : M)$. إذن K^* هو زمرة جالوا كلها وأنّ $L^* = 1$ (الدالة المحايدة على L). ومن الواضح أنّه إذا كان $M \subseteq N$ فإن $M^* \supseteq N^*$ ، لأنّ أيّ دالّة تثبت عناصر N فإنّها بالتأكيد تثبت عناصر M. وبالعكس لكل زمرة جزئية H من $\Gamma(L : K)$ نشرك المجموعة $H^\dagger$ المكونة من جميع العناصر $x \in L$ حيث $\alpha(x) = x$ لكل $\alpha \in H$. $H^\dagger$ حقل وسطي يُستنتج من :

تمهيدية (٧,٢)

إذا كانت H زمرة جزئية من $\Gamma(L : K)$ فإنّ $H^\dagger$ حقل جزئي من L يحتوي K .

البرهان

لنفرض أن $x, y \in H^\dagger$ و $\alpha \in H$. عندئذ

$$\alpha(x + y) = \alpha(x) + \alpha(y) = x + y \ .$$

وبالمثل فإنّ $H^\dagger$ مغلقة تحت عمليات الحقل الأخرى، وبالتالي فإنّها حقل جزئي من L. و بما أنّ $\alpha \in \Gamma(L : K)$ لدينا $\alpha(k) = k$ لكل $k \in K$ إذن $K \subseteq H^\dagger$. Δ

تعريف

باستخدام الترميز أعلاه يسمى $H^\dagger$ بحقل H الثابت .

من الواضح أنّه إذا كان $H \subseteq G$ فإنّ $G^{\dagger} \supseteq H^{\dagger}$. لاحظ أنّ الاحتواء معكوس هنا، ومن السهل أيضًا أن نبرهن على أنه إذا كان M حقلاً وسطيّا، و H زمرة جزئية من زمرة جالوا فإنّ

$$M \subseteq M^{*\dagger} \qquad (١ ,٧)$$

$$H \subseteq H^{\dagger *}$$

وذلك لأنّ كل عنصر في M يُثَبَّت بواسطة كل تماثل ذاتي الذي يُثَبِّت كل M ، وأنّ كل عنصر في H يُثَبِّت جميع العناصر التي يثبتها جميع H . لاحظ أنّ كلا الاحتواءين ليس بالضرورة أن يكون متساويًا. في المثال (٢) أعلاه لدينا

(c) $Q^{*\dagger} = Q$.

إذا كانت $\mathfrak{I}$ هي مجموعة جميع الحقول الوسطية و $\mathcal{G}$ مجموعة جميع الزمر الجزئية من زمرة جالوا فيكون لدينا الدالتان

$$*: \mathfrak{I} \to \mathcal{G}$$

$$\dagger: \mathcal{G} \to \mathfrak{I}$$

اللتان تحققان (١ ,٧) وتعكسان الاحتواء. نستطيع الآن تفسير فكرة جالوا كالتالي: ما هي الشروط اللازمة لجعل * و † دالتين نظيرتين لبعضهما، بحيث نحصل على تقابل بين $\mathfrak{I}$ و $\mathcal{G}$. هذه الشروط تعرف بقابلية الفصل والناظمية، وسندرسهما في الفصل الثامن.

مثال

لتكن لدينا معادلة كثيرة الحدود

$$f(t) = t^4 - 4t^2 - 5 = 0$$

التي ناقشناها في الفكرة الشاملة. وكما رأينا فإنّ تحليل هذه المعادلة هو

$(t^2 + 1)(t^2 - 5) = 0$.

وأصفارها هي $\alpha = i$ ، $\beta = -i$ ، $\gamma = \sqrt{5}$ ، $\delta = -\sqrt{5}$.

والامتداد المشترك هو $Q : L$ حيث $L = Q(i, \sqrt{5})$.

هناك أربع تماثلات ذاتية على L بالنسبة إلى Q وهم I ، R ، S و T حيث I هو التطابق

المحايد ، وباستخدام الترميز الدوري $R = (\alpha\,\beta)$ ، $S = (\gamma\,\delta)$ و $T = (\alpha\,\beta)\,(\gamma\,\delta)$.
إذن زمرة جالوا هي :

$$G = \{\, I, R, S, T \,\}.$$

والزمر الجزئية الفعليّة لها هي :

$$\{ I \}, \{ I,R \}, \{I,S \}, \{ I,T \}.$$

والحقول الثابتة المقابلة لها هي على الترتيب :

$$L, Q\left(\sqrt{5}\right), \; Q(i), \; Q\left(i\sqrt{5}\right).$$

وليس صعبًا أن تتحقق من أنّ هذه الحقول مع الحقل K هي جميع الحقول الجزئية للحقل L . وفي هذه الحالة يكون تقابل جالوا غامرًا ومتباينًا .

تمــارين

(٧ , ١) جد التماثلات الذاتية على L بالنسبة إلى K لكل من الامتدادات L : K التالية :

(أ) $Q\left(\sqrt{2}\right) : Q$

(ب) $Q(\alpha) : Q$ حيث α هو الجذر الخامس الحقيقي للعدد 7

(ج) $Q\left(\sqrt{2}, \sqrt{3}\right) : Q$

(٧ , ٢) احسب زمرة جالوا لكل من هذه الامتدادات .

(٧ , ٣) في أي من هذه الحالات يكون تقابل جالوا بين $\mathfrak{F}$ و $\mathcal{G}$ غامرًا ومتباينًا؟

(٧ , ٤) ليكن K هو الحقل المعرف في تمرين (٦ , ١) وليكن P هو حقله الجزئي الأولي . ما هي زمرة جالوا للامتداد K : P ؟ هل تقابل جالوا متباين وغامر؟

(٧ , ٥) ليكن $K(\alpha) : K$ امتدادًا جبريًا بسيطًا ، وليكن γ عنصرًا في زمرة جالـوا ، أثبت أنّ $\gamma(\alpha)$ و α لهما كثيرة الحدود الأصغرية نفسها على K ، ومن ثم أثبت أن زمرة جالوا هي زمرة تبديلات أصفار كثيرة الحدود هذه .

(٧ , ٦) جد جميع الحقول الوسطية للامتداد $Q\left(\sqrt{2}, \; \sqrt{3}, \; \sqrt{5}\right) : Q$. جد زمرة جالوا . قارن .

(٧ , ٧) ضع علامة صح أو خطأ أمام كل مما يلي :

(ا) أي تماثل ذاتي على L بالنسبة إلى K هو تماثل ذاتي على L

(ب) أي تماثل ذاتي على L بالنسبة إلى L هو التطبيق المحايد

(ج) زمرة جالوا للامتداد K : L زمرة دوريّة .

(د) زمرة جالوا للامتداد $\mathbb{R}$:$\mathbb{C}$ زمرة ابيلية .

(هـ) الدالتان * و † نظيرتا بعض في جميع الحالات .

(و) الدالتان * و † تحافظان على الاحتواء .

(ز) إذا كان $\Gamma(L : K)=1$ فإن $L = K$.

(ح) إذا كان $L = K$ فإنّ $\Gamma(L : K)=1$

(ط) يوجد تماثل ذاتي وحيد على $K(t)$ بالنسبة إلى K .

(ي) إنّ تعريف زمرة جالوا أسهل من حسابها .

الفصل الثامن

الناظمية وقابلية الفصل

Normality and Separability

في هذا الفصل سنعرف مفهومين مهمين هما الناظمية وقابلية الفصل، وسنبرهن على بعض النتائج الأساسية المتعلقة بهما.

في حالات كثيرة نجد أنّ كثيرة الحدود $p(t) \in K[t]$ ليس لها أصفار في الحقل K ولكن من الممكن أن يوجد لها أصفار في امتداد L للحقل K، وعلى سبيل المثال $t^2+1 \in \mathbb{R}[t]$ ليس لها أصفار في الحقل $\mathbb{R}$ ولكن $\pm i \in \mathbb{C}$ صفران لكثيرة الحدود هذه في الحقل $\mathbb{C}$. وسندرس هذه الظاهرة ونبرهن على أنّ أي كثيرة حدود يمكن كتابتها كحاصل ضرب كثيرات حدود من الدرجة الأولى إذا كان بالإمكان تمديد الحقل الأصلي إلى حقل انشطار مناسب، وسندرس حقول الانشطار هذه ونجد العلاقة بينها وبين مفهوم الناظميّة. ولكي نستطيع تزويد القارىء بأمثلة سنعتمد على خاصية للحقل $\mathbb{C}$ غالبًا ما تسمى بالنظرية الأساسية في الجبر وتنص على أن أي كثيرة حدود على $\mathbb{C}$ يمكن كتابتها كحاصل ضرب عوامل خطّية، سنبرهن على هذه النتيجة في الفصل التاسع عشر.

(٨,١) حقول الانشطار

Splitting Fields

سنبدأ بتعريف الانشطار.

تعريف

ليكن K حقلاً و f كثيرة حدود على K. نقول إن f منشطرة على K إذا استطعنا

كتابتها على الصورة :

$$f(t) = k(t - \alpha_1) \ldots (t - \alpha_n)$$

حيث $k, \alpha_1, \ldots, \alpha_n \in K$. وبهذه الحالة تكون جميع أصفار f في K هي $\alpha_1, \ldots, \alpha_n$.

أمثلـــة

(١) كثيرة الحدود $t^3 - 1 \in Q[t]$ منشطرة على $\mathbb{C}$ ، لأنّ

$$t^3 - 1 = (t - 1)(t - \omega)(t - \omega^2)$$

حيث $\omega = e^{2\pi i/3}$.

(٢) كثيرة الحدود $t^4 - 4t^2 - 5 \in Q[t]$ منشطرة على $Q(i, \sqrt{5})$ لأنّ:

$$t^4 - 4t^2 - 5 = (t - i)(t + i)(t - \sqrt{5})(t + \sqrt{5}) .$$

ولكنّها غير منشطرة على $Q(i)$ لأنّ أكثر ما نستطيع عمله هنا هو كتابتها على الصورة :

$$t^4 - 4t^2 - 5 = (t - i)(t + i)(t^2 - 5)$$

حيث $t^2 - 5$ لا مختزلة . وهذا يبين لنا أنه على الرغم من وجود عوامل خطية لكثيرة الحدود $p(t)$ في امتداد حقلي L فإن $p(t)$ ليس بالضرورة أن تكون منشطرة على L .

وإذا كانت f كثيرة حدود على K وكان L امتدادًا للحقل K فإن f كثيرة حدود على L . ومن ثم فإنّ انشطار f على L يعني أنّ f حاصل ضرب عدد منته من العوامل الخطية بمعاملات في L . وسنبرهن على أنه إذا كان لدينا K و f فإننا نستطيع دائمًا أن ننشيء امتدادًا Σ للحقل K بحيث تكون f منشطرة على Σ . ومن المناسب أيضًا أن نشترط عدم انشطار f على أي حقل أصغر من Σ وبذلك يكون Σ هو أصغر حقل يحقق ذلك .

تعريف

نقول إن الحقل Σ هو حقل انشطار لكثيرة الحدود f على الحقل K إذا كان $K \subseteq \Sigma$ بحيث يتحقق ما يلي:

(١) f منشطرة على Σ ،

(٢) إذا كان $K \subset \Sigma' \subset \Sigma$ *وكانت f منشطرة على* Σ' فإن $\Sigma = \Sigma'$.

ومن الواضح أنّ الشرط (٢) يكافيء (٢)* التالي :

(٢)* $\Sigma = K(\sigma_1, \ldots, \sigma_n)$ حيث $\sigma_1, \ldots, \sigma_n$ هي جميع أصفار f في Σ .

إن طريقة إنشاء حقل انشطار يتم باقران عناصر للحقل K. بحيث تكون هذه العناصر أصفارًا لكثيرة حدود f . ولكننا نعرف كيفية انشاء هذا الحقل لكثيرة حدود لا مختزلة (نظرية ٥ , ٣) ، وبالتالي فإنّنا نشطر f إلى عوامل لا مختزلة ونعالج كل عامل من هذه العوامل على حدة .

نظرية (٨,١)

ليكن K حقلاً و f كثيرة حدود على K . عندئذ يوجد حقل انشطار لـ f على K .

البرهان

باستخدام الاستنتاج الرياضي على ∂f . إذا كان $\partial f = 1$ فليس لدينا شئ نبرهن عليه لأنّ f منشطرة على K . إذا كانت f غير منشطرة على K فإنّه يجب أن يكون لها عامل غير مختزل f_1 حيث $\partial f_1 > 1$، وباستخدام نظرية (٥ , ٣) نقرن σ_1 مع K حيث $f_1(\sigma_1) = 0$ ، إذن في الحقل $K(\sigma_1)[t]$ لدينا : $f = (t - \sigma_1)g$ حيث $\partial g = \partial f - 1$ ، وباستخدام فرضية الاستنتاج يوجد حقل انشطار Σ لـ g على $K(\sigma_1)$. ولكن هذا الحقل Σ هو حقل انشطار لـ f على K . Δ

من النظرة الأولى على طريقة الإنشاء هذه نستطيع أن نرى إمكانية إنشاء حقول انشطار مختلفة لكثيرة الحدود f وذلك باختيار عوامل لا مختزلة مختلفة، وبالحقيقة فإنّ هذا لا يعطينا حقول إنشطار مختلفة (تحت سقف التماثل) ، وسنبرهن على أنّ حقول الانشطار (لكثيرة حدود f وحقل K) جميعها متماثلة . وهذه الحقيقة ليست مستغربة ولكن برهانها أكثر تعقيدًا مما نتمنى، وفكرة البرهان سهلة ومباشرة حيث نستخدم نظرية (٨ , ٣) والاستنتاج الرياضي. ولأسباب تقنية سنستخدم النظرية

(٩ , ٣). والنقطة الرئيسة في البرهان مجسدة في :

تمهيدية (٨,٢)

ليكن $i: K \to K'$ تماثل حقلي، ولتكن f كثيرة حدود على K حقلها الانشطاري على K هو Σ ، و ليكن L امتداد للحقل K' بحيث تكون $i(f)$ منشطرة على L . عندئذ يوجد تشاكل متباين $j: \Sigma \to L$ بحيث $j|_k = i$.

البرهان

لدينا الشكل التالي :

$$\begin{tikzcd} K \arrow[r] \arrow[d, "i"'] & \Sigma \arrow[d, dotted, "j"] \\ K' \arrow[r] & L \end{tikzcd}$$

حيث j سنعرفها فيما بعد .

سنستخدم الاستنتاج الرياضي على ∂f . وباعتبار

$$f(t) = k(t - \sigma_1) \dots (t - \sigma_n)$$

كثيرة حدود على Σ فإنّ كثيرة حدود σ_1 الأصغرية على K هي عامل m لا مختزل من عوامل f . الآن $i(m) \mid i(f)$ حيث $i(f)$ منشطرة على L . ومنه فإنّ

$$i(m) = (t - \alpha_1) \dots (t - \alpha_r)$$

حيث $\alpha_1 , \dots, \alpha_r \in L$. وبما أنّ $i(m)$ لا مختزلة على K' فإنّها يجب أن تكون كثيرة حدود α_1 الأصغرية على K'، وباستخدام نظرية (٩ , ٣) نستطيع إيجاد تماثل

$$j_1 : K(\sigma_1) \to K'(\alpha_1)$$

بحيث $j_1|_K = i$ و $j_1(\sigma_1) = \alpha_1$. الآن Σ حقل انشطار كثيرة الحدود $g = f/(t - \sigma_1)$ على $K(\sigma_1)$. باستخدام فرضية الاستنتاج نستطيع ايجاد تشاكل متباين $j : \Sigma \to L$ بحيث $j|_{K(\sigma_1)} = j_1$. وبالتالي فإنّ $j|_K = i$ وبهذا ينتهي البرهان . Δ

باستخدام التمهيدية أعلاه نستطيع البرهان على الوحدانية :

نظرية (٨،٣)

ليكن $i : K \to K'$ *تماثلاً حقليًا ،* T *حقل انشطار لكثيرة الحدود* f *على* K *و* T' *حقل انشطار* $i(f)$ *على* K' *. عندئذ يوجد تماثل* $j : T \to T'$ *بحيث* $j|_k = i$ *. وبمعنى آخر الامتدادان* $T : K$ *و* $T' : K'$ *متماثلان .*

البرهان

نعتبر الشكل التالي :

$$\begin{tikzcd} K \arrow[r] \arrow[d, "i"'] & T \arrow[d, dotted, "j"] \\ K' \arrow[r] & T' \end{tikzcd}$$

والمطلوب إيجاد j بحيث يكون الشكل إبداليًا ، و باستخدام تمهيدية (٢ ، ٨) نستطيع إيجاد تشاكل متباين $j : T \to T'$ بحيث $j|_k = i$. ولكن $j(T)$ حقل انشطار $i(f)$ على K' وهو محتوى في T' . وبما أن T' هو أيضًا حقل انشطار $i(f)$ على K' فإن $j(T) = T'$. ومنه فإن j شامل . إذن j تماثل وهذا ينهي برهان النظرية . Δ

أمثلـة

(١) لتكن $f(t) = (t^2 - 3)(t^3 + 1)$ على Q . نستطيع إنشاء حقل انشطار f كالتالي : في الحقل $\mathbb{C}$ نستطيع تحليل f إلى عوامل خطية

$$f(t) = (t + \sqrt{3})(t - \sqrt{3})(t + 1)\left(t - \frac{1 + i\sqrt{3}}{2}\right)\left(t - \frac{1 - i\sqrt{3}}{2}\right)$$

إذن حقل انشطار f هو حقل جزئي من $\mathbb{C}$ وبالتحديد $Q\left(\sqrt{3}\ ,\ \frac{1 + i\sqrt{3}}{2}\right)$ ، ومن

الواضح أن هذا الحقل هو $Q(\sqrt{3}, i)$.

(٢) لتكن $f(t) = (t^2 - 2t - 2)(t^2 + 1)$ على Q . وأصفار f في $\mathbb{C}$ هي : $\pm i$ ، $1 \pm \sqrt{3}$ ، إذن حقل انشطار f هو $Q(1 + \sqrt{3}, i)$ وهذا أيضًا $Q(\sqrt{3}, i)$. لاحظ أن هذا هو الحقل الذي وجدناه في المثال (١) بالرغم أن كثيرتي الحدود مختلفتان .

(٣) من الممكن أيضًا أن نجد حقل انشطار واحدًا لكثيرتي حدود لا مختزلتين ومختلفتين . فمثلاً حقل انشطار كل من $t^2 - 3$ و $t^2 - 2t - 2$ على Q هو $Q(\sqrt{3})$.

(٤) لتكن $f(t) = t^2 + t + 1$ على $\mathbb{Z}_2$. لا نستطيع هنا أن نستخدم الحقل $\mathbb{C}$ ولذلك يجب أن نستخدم الطريقة الأساسية لانشاء حقل انشطار ، و الحقل الأصلي $\mathbb{Z}_2$ يحتوي على عنصرين هما 1 و 0 . لاحظ أن f لا مختزلة ، إذن نستطيع إقران عنصر ξ بحيث تكون f هى كثيرة حدود ξ الأصغرية على $\mathbb{Z}_2$. عندئذ $\xi^2 + \xi + 1 = 0$ ومنه $\xi^2 = \xi + 1$ (لاحظ أن مميز $\mathbb{Z}_2$ هو 2) والعناصر التالية تكون حقلاً .

$$0, 1, \xi, 1 + \xi \quad .$$

وللبرهان على ذلك نكوّن جدولي الجمع والضرب :

+	0	1	ξ	$1+\xi$
0	0	1	ξ	$1+\xi$
1	1	0	$1+\xi$	ξ
ξ	ξ	$1+\xi$	0	1
$1+\xi$	$1+\xi$	ξ	1	0

.	0	1	ξ	$1+\xi$
0	0	0	0	0
1	0	1	ξ	$1+\xi$
ξ	0	ξ	$1+\xi$	1
$1+\xi$	0	$1+\xi$	1	ξ

(على سبيل المثال حساب $\xi(1+\xi)$ في جدول الضرب يكون كالتالي :
$\xi(1+\xi) = \xi + \xi^2 = \xi + \xi + 1 = 1$) .

من الجدولين نجد أن $\mathbb{Z}_2(\xi)$ حقلاً يحتوي على أربعة عناصر . الآن نجد أن :

$$t^2 + t + 1 = (t - \xi)(t - 1 - \xi)$$

على $\mathbb{Z}_2(\xi)$ ولكن ليس على حقل أصغر . إذن $\mathbb{Z}_2(\xi)$ هو حقل انشطار f على $\mathbb{Z}_2$.

(٨,٢) الناظميّة

Normality

إنّ فكرة الامتدادات الناظميّة كانت واضحة تمامًا لدى جالوا (ولكن كالعادة بدلالة كثيرات حدود على $\mathbb{C}$) . وبالدراسة الحديثة هذه الامتدادات تأخذ الشكل التالي :

تعريف

يكون الامتداد $L : K$ ناظميًا إذا كانت أي كثيرة حدود f لا مختزلة على K ولها على الاقل صفرًا واحدًا في L تكون منشطرة في L .

وعلى سبيل المثال $\mathbb{C} : \mathbb{R}$ امتداد ناظمي لأنّ أي كثيرة حدود (مختزلة أم لا) تنشطر في $\mathbb{C}$. ومن جهة أخرى نستطيع ايجاد امتدادات ليست ناظميّة . ليكن α الجذر التكعيبي الحقيقي للعدد 2 ولنعتبر $Q(\alpha) : Q$. كثيرة الحدود $t^3 - 2$ اللا مختزلة لها صفراً بالتحديد α في $Q(\alpha)$ ولكنها لا تنشطر في $Q(\alpha)$. لأنها لو انشطرت

لوجد ثلاثة جذور حقيقية مختلفة للعدد 2 وهذا مستحيل .

وإذا قارنّا هذه الأمثلة بأمثلة زمرة جالوا في الفصل السابع وجدنا أنّ للامتداد الناظمي $\mathbb{C} : \mathbb{R}$ ميزة مهمة في زمرة جالوا . وبالتحديد فإن تقابل جالوا متباين وغامر ، ولكن هذا ليس صحيحًا في حالة الامتداد غير الناظمي . وهذه ليست الميزة الوحيدة ولكنها توضح لنا أهمية الامتدادات الناظمية . وهناك علاقة وثيقة بين الامتدادات الناظمية وحقول الانشطار ، وهذه العلاقة تمدنا بمدى واسع من الامتدادات الناظمية :

نظريّة (٤,٨)

يكون الامتداد $L : K$ ناظميًا ومنتهيًا إذا وفقط إذا كان L حقل انشطار لكثيرة حدود على K.

البرهان

لنفرض أنّ $L : K$ ناظمي ومنته، وباستخدام تمهيدية (٤ , ٤) $L = K(\alpha_1 ,..., \alpha_s)$ حيث α_i جبري على K . لتكن m_i كثيرة حدود α_i الأصغرية على K ولتكن $f = m_1 \dots m_s$. إنّ كل m_i لا مختزلة على K ولها صفر $\alpha_i \in L$. إذن باستخدام الناظمية كل من m_i تنشطر على L . وبالتالي فإنّ f تنشطر على L ، وبما أنّ L منشأ من K وأصفار f فإنه يجب أن يكون حقل انشطار f على K .

وللبرهان على العكس ، نفرض أنّ L حقل انشطار كثيرة حدود g على K . ومن الواضح أن $L : K$ امتداد منته . وللبرهان على ناظميّة الامتداد نأخذ كثيرة حدود لا مختزلة f على K ولها صفر في L ونبرهن أنّها تنشطر في L . لنفرض أن $M \supseteq L$ حقل انشطار fg على K . ولنفرض أن θ_1 و θ_2 صفرى لـ f في M . سنبرهن على أن

$$[L(\theta_1) : L] = [L(\theta_2) : L] .$$

يتم البرهان على ذلك بالنظر إلى حقول جزئية من M ترتبط مع بعض كما في الشكل :

$$\begin{tikzcd}
 & M & \\
L(\theta_1) \arrow[ur] & & L(\theta_2) \arrow[ul] \\
 & L \arrow[uu] \arrow[ul] \arrow[ur] & \\
K(\theta_1) \arrow[uu] & & K(\theta_2) \arrow[uu] \\
 & K \arrow[uu] \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

حيث الأسهم تدل على الاحتواء .

الآن إذا كان 2 أو $j = 1$:

$$[L(\theta_j) : L][L:K] = [L(\theta_j) : K] = [L(\theta_j) : K(\theta_j)][K(\theta_j) : K] \qquad (٨ , ١)$$

وباستخدام قضية (٣ , ٤) ، $[K(\theta_1) : K] = [K(\theta_2) : K]$. من الواضح أن $L(\theta_j)$ حقل انشطار g على $K(\theta_j)$ وباستخدام نظرية (٨ , ٣) $K(\theta_1)$ يماثل $K(\theta_2)$. إذن باستخدام نظرية (٨ , ٣) الامتدادات $L(\theta_j):K(\theta_j)$ متماثلة حيث $j = 1,2$ وبالتالي لهما الدرجة نفسها. بالتعويض في (١ , ٨) والاختصار نجد أن

$$[L(\theta_1) : L] = [L(\theta_2) : L]$$

كما وعدنا سابقًا .

الآن إذا كان $\theta_1 \in L$ فإنّ $[L(\theta_1) : L] = 1$ ومنه $[L(\theta_2) : L] = 1$ وبالتالي $\theta_2 \in L$. إذن $L : K$ ناظمي . Δ

(٨,٣) قابلية الفصل

Separability

لم يميز جالوا مفهوم قابلية الفصل بوضوح وذلك لأنّه كان يشتغل في حقل الأعداد المركّبة $\mathbb{C}$ (حيث كما سنرى قابلية الفصل هنا محققة تلقائيًا) ، و هناك العديد من براهين جالوا التي احتوت على هذا المفهوم ولكن بشكل ضمني ، و إن هذا المفهوم يجب أن يكون واضحًا وبالأخص عند دراسة الحقول ذات المميز غير الصفري .

تعريف

نقول إنّ كثيرة الحدود اللامختزلة f على K قابلة للفصل على K إذا كانت جميع أصفارها بسيطة في حقل انشطار. أي أنّ f تكون على الصورة التالية في أي حقل انشطار :

$$k(t - \sigma_1) \dots (t - \sigma_n)$$

حيث جميع σ_i مختلفة.

تعريف

نقول أن كثيرة الحدود اللامختزلة f على K لا منفصلة إذا لم تكن قابلة للفصل على K.

أمثلة

(١) كثيرة الحدود $t^4 + t^3 + t^2 + t + 1$ قابلة للفصل على $\mathbb{Q}$ لأنّ حقلها الانشطاري حقل جزئي من $\mathbb{C}$ وأصفارها في $\mathbb{C}$ هي $e^{2\pi i/5}$ ، $e^{4\pi i/5}$ ، $e^{6\pi i/5}$ ، $e^{8\pi i/5}$ وجميعها مختلفة.

(٢) ليكن $K_0 = \mathbb{Z}_p$ حيث p عدد أوّلي. وليكن $K = K_0(u)$ حيث u متسام على K_0 ولتكن

$$f(t) = t^p - u \in K[t]$$

ليكن Σ هو حقل انشطار f على K و τ صفر لـ f في Σ. إذن $u = \tau^p$. الآن باستخدام نظرية ذات الحدين لدينا :

$$(t - \tau)^p = t^p + \binom{p}{1} t^{p-1}(-\tau) + \dots + (-\tau)^p$$

ولكن $\binom{p}{r}$ يقبل القسمة على p لكل $0 < r < p$ وذلك لأنّ p يظهر في البسط ولا يظهر

في مقام المفكوك $p!/r!(p-r)!$ ، ولكن في K أي مضاعف للعدد p يجب أن يكون صفرًا. إذن

$$f(t) = (t-\tau)^p = t^p - \tau^p = t^p - u \ .$$

ومنه إذا كان $\sigma^p - u = 0$ فإنّ $(\sigma - \tau)^p = 0$ ، أي أنّ $\sigma = \tau$ وبالتالي جميع أصفار f في Σ متساوية.

يبقى أن نثبت أن f لا مختزلة على K . لنفرض أنّ $f = gh$ حيث $h,g \in K[t]$ و $\partial h, \partial g < \partial f$. إذن $g(t) = (t-\tau)^s$ حيث $0 < s < p$ وذلك من وحدانية التحليل. إذن العدد الثابت τ^s لـ g يجب أن يكون عنصراً في K . ومنه فإن $\tau \in K$ وذلك لأنه يوجد عددان صحيحان a و b بحيث $as + bp = 1$ وبما أن $\tau^{as+bp} \in K$ فإن $\tau \in K$. إذن $\tau = v(u)/w(u)$ حيث $v,w \in K_0[u]$ ومنه

$$v(u)^p - u(w(u))^p = 0 \ .$$

وبما أنّه لا يمكن اختصار الحدود الأعظمية الدرجة فإنّ f لا مختزلة. وبالتالي فإن f لا منفصلة على K.

(٤,٨) التفاضل الشكلي

Formal Differentiation

لكثيرات الحدود المعرّفة على $\mathbb{R}$ هناك وسيلة معيارية لمعرفة الأصفار المكررة وذلك بواسطة التفاضل، ومن الممكن تعميم هذه الطريقة لأي حقل عام ولكن يلزمنا أولا أن نعرّف المشتقّة بطريقة شكلية.

تعريف

لنفرض أنّ

$$f(t) = a_0 + a_1 t + \dots + a_n t^n \in K[t]$$

حيث K حقل. المشتقة الشكلية لـ f هي كثيرة الحدود

$$Df = a_1 + 2a_2 t + \dots + n a_n t^{n-1} \ .$$

إذا كان $K = \mathbb{R}$ فهذه هي المشتقّة الاعتيادية، وبصورة عامة لا يمكن أن نأمل بأن

نعتبر Df معدّل التغير لكثيرة الحدود f ولكن بعض الخواص المهمة للمشتقّة تبقى صحيحة هنا، وعلى وجه الخصوص نستطيع أن نثبت بسهولة أن :

$$D(f + g) = Df + Dg$$

$$D(fg) = Df.g + f.Dg$$

$$D(\lambda) = 0$$

$$D(\lambda f) = \lambda.Df$$

حيث f و g كثيرتا حدود على K و $\lambda \in K$.

من هذه الخواص الأساسية لـ D نستطيع أن نقدّم ميزان لوجود الأصفار المكّررة بدون معرفة هذه الأصفار .

تمهيدية (٨,٥)

لتكن $f \neq 0$ كثيرة حدود على الحقل K . عندئذ يكون لـ f صفر مكرر في حقل انشطار إذا وفقط إذا وجد قاسم مشترك لـ f و Df درجته أكبر أو تساوي 1 .

البرهان

لنفرض وجود صفر مكرر لـ f في حقل انشطار Σ. إذن على Σ

$$f(t) = (t - \alpha)^2 g(t)$$

حيث $\alpha \in \Sigma$. ومنه

$$Df = (t - \alpha) \{(t - \alpha) Dg + 2g\} .$$

إذن $(t - \alpha)$ هو قاسم مشترك لكل من f و Df في $\Sigma[t]$ ، وبالتالي فإنّ كثيرة حدود α الأصغرية على K هي قاسم مشترك لكل من f و Df في $K[t]$.

لنفرض الآن عدم وجود أصفار مكرّرة لكثيرة الحدود f، وسنبرهن باستخدام الاستنتاج الرياضي على ∂f أن f و Df أوّليان نسبيًا في $\Sigma[t]$ وبالتالي فهما أوليان نسبيًا في $K[t]$.

إذا كانت $\partial f = 1$ فالعبارة واضحة . لنفرض إذًا أن $f(t) = (t - \alpha)\, g(t)$ حيث $(t - \alpha)$ لا تقسم $g(t)$. عندئذ

$$. \ Df = (t - \alpha)\, Dg + g$$

إذا كان هناك قاسم لـ g يقسم Df أيضًا فإنّ هذا القاسم يجب أن يقسم Dg وذلك لأن $(t - \alpha)$ لا تقسم $g(t)$. وباستخدام فرضية الاستنتاج لدينا g و Dg أوّليان نسبيًا . إذن f و Df أوّليان نسبيًا وهذا هو المطلوب .

نستطيع الآن إعطاء شرط كاف ولازم لقابلية الفصل لكثيرة حدود لا مختزلة .

قضية (٨,٦)

إذا كان K حقلاً مميزه صفر فإن أي كثيرة حدود لا مختزلة على K يجب أن تكون قابلة للفصل على K . وإذا كان مميز K هو $p > 0$ وكانت f كثيرة حدود لا مختزلة على K فإن f لا منفصلة إذا وفقط إذا كانت

$$f(t) = k_0 + k_1 t^p + \cdots + k_r t^{rp}$$

حيث $k_0, \ldots, k_r \in K$.

البرهان

كثيرة الحدود f على K لا منفصلة إذا وفقط إذا وجد قاسم مشترك لـ f و Df درجته أكبر أوتساوي 1 ، وبما أنّ f لا مختزلة فإنّ $\partial Df < \partial f$ ، عندئذ $Df = 0$. وعليه إذا كانت

$$f(t) = a_0 + \ldots + a_m t^m$$

فإنّ هذا يكافيء $na_n = 0$ لكل عدد صحيح $n > 0$ ، وإذاكان المميّز صفرًا فإنّ هذا يكافيء $a_n = 0$ لكل n ، أما إذا كان المميّز هو $p > 0$ فإنّه يكافئ $a_n = 0$ حيث p لا يقسم n ، وبوضع $k_i = a_{ip}$ نحصل على المطلوب . Δ

ملاحظة

في حالة كون f لا منفصلة على حقل مميّزه p نستطيع إنّ نقول إنّ أسس t الوحيدة التي نحصل عليها هي مضاعفات p، أي أنّ $f(t) = g(t^p)$ حيث g كثيرة حدود على K .

تعريف

نقول أن كثيرة الحدود f قابلة للفصل على K إذا كانت جميع قواسمها اللا مختزلة قابلة للفصل على K . إذا كان $L : K$ امتداد حقلي و $\alpha \in L$ جبري فإننا نقول أن α قابل للفصل على K إذا كانت كثيرة حدود α الأصغرية على K قابلة للفصل على K . ونقول أن الامتداد الجبري $L : K$ امتداد قابل للفصل إذا كان كل $\alpha \in L$ قابلاً للفصل على K.

سننهي هذا البند بأن نبرهن على أن قابلية الفصل في الامتدادات الجبرية تبقى صحيحة على الحقول الوسطية .

تمهيدية (٨,٧)

إذا كان $L : K$ امتدادًا جبريًا قابلاً للفصل وكان M حقلاً وسطيًا فإن $M : K$ و $L : M$ قابلان للفصل .

البرهان

من الواضح أنّ $M : K$ قابل للفصل ، و لنفرض أنّ $\alpha \in L$ و m_K، m_M كثيرتا حدود α الاصغريّتين على K و M على الترتيب . الآن $m_M \mid m_K$ في $M[t]$. وبما أنّ α قابل للفصل على K فإنّ m_K قابلة للفصل على K وبالتالي فإنّ m_M قابلة للفصل على M . إذن $L : M$ امتداد قابل للفصل . Δ

تمارين

(٨ , ١) جد حقولاً جزئية من $\mathbb{C}$ بحيث تكون حقول انشطار على Q لكثيرات الحدود .

. $t^3 - 1 , t^4 + 5t^2 + 6, t^6 - 8$.

(٨ , ٢) جد درجة كل من هذه الحقول باعتبارها امتدادات للحقل Q .

(٨ , ٣) جد حقل انشطار لـ t^3+2t+1 على $\mathbb{Z}_3$.

(٨ , ٤) جد حقل انشطار لـ $t^3 + t^2 + t + 2$ على $\mathbb{Z}_3$. هل هذا الحقل يماثل

الحقل الذي وجدته في التمرين (٨,٣) ؟

(٨,٥) جد جميع كثيرات الحدود التربيعية الواحدية على $\mathbb{Z}_5$. أيٌ من كثيرات الحدود هذه لا مختزلة ؟ جد حقل انشطار لبعض كثيرات الحدود اللا مختزلة. هل جميع هذه الحقول متماثلة ؟ ما هو عدد عناصر كل من هذه الحقول ؟.

(٨,٦) أثبت إمكانية تعميم مفهوم المشتقّة الشكلية على $K(t)$ بتعريف
. $D(f/g) = (Df.g - f.Dg) / g^2$
أثبت الخواص المهمة لـ D .

(٨,٧) بين أيًا من كثيرات الحدود التالية قابلة للفصل باعتبارها كثيرات حدود على الحقول Q، $\mathbb{C}$، $\mathbb{Z}_2$، $\mathbb{Z}_3$، $\mathbb{Z}_5$، $\mathbb{Z}_7$، $\mathbb{Z}_{19}$:

$$7t^5 + t - 1\ ,\ t^3 + 1\ ,\ t^2 + 2t - 1\ ,\ t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$$

(٨,٨) أي من الامتدادات التالية ناظمي :

(ا) $Q(t) : Q$

(ب) $Q(\sqrt{-5}) : Q$

(ج) $Q(\alpha) : Q$ حيث α الجذر الحقيقي السابع للعدد 5 .

(د) $Q(\sqrt{5}, \alpha) : Q(\alpha)$ حيث α كما في الفرع (ج) .

(هـ) $\mathbb{R}\left(\sqrt{-7}\right) : \mathbb{R}$.

(٨,٩) أثبت أنّ أي امتداد من الدرجة الثانية يجب أن يكون ناظميًا. هل هذا صحيح إذاكانت الدرجة أكبر من 2 ؟

(٨,١٠) إذا كان Σ حقل انشطار لـ f على K وكان $K \subseteq L \subseteq \Sigma$ فأثبت أنّ Σ حقل انشطار لـ f على L.

(٨,١١) لتكن f كثيرة حدود من الدرجة n على K وليكن Σ حقلاً انشطاريًا لـ f على K . أثبت أنّ $[\Sigma : K]$ يقسم $n!$.

(٨,١٢) ضع علامة صح أو خطأ أمام كل مما يلي :

(ا) أي كثيرة حدود يجب أن تنشطر على حقل ما .

(ب) كثيرة الحدود $t^3 + 5$ قابلة للفصل على $\mathbb{Z}_7$.

(ج) حقول الانشطار جميعها متماثلة .

(د) أي امتداد منته يجب أن يكون ناظميًا .

(هـ) أي امتداد قابل للفصل يجب أن يكون ناظميًا .

(و) كل امتداد منته ناظمي يجب أن يكون حقلاً انشطاريًا لكثيرة حدود ما .

(ز) $Q(\sqrt{19}) : Q$ امتداد ناظمي وقابل للفصل .

(ح) $Q(\sqrt{21}) : Q$ امتداد ناظمي وقابل للفصل .

(ط) كثيرة الحدود القابلة للاختزال لا يمكن أن تكون قابلة للفصل .

(ي) إذا كان $Df = 0$ فإنّ $f = 0$ حيث f كثيرة حدود على حقل .

(١٣ , ٨)* أنشيء امتدادًا منتهيًا وغير بسيط .

الفصل التاسع

درجات الحقول ورتب الزمر

Field Degrees and Group Orders

للبرهان على النظرية الأساسية لجالوا في الفصل الحادي عشر سنحتاج إلى إثبات أنّه إذا كانت H زمرة جزئية من زمرة جالوا لامتداد ناظمي قابل للفصل ومنته L : K فإنّ $H^{\dagger *} = H$. والطريقة التي سنتبعها لذلك هي أن كلاً من H و $H^{\dagger *}$ زمرة منتهية و$|H| = |H^{\dagger *}|$. وإذا عرفنا أنّ $H \subseteq H^{\dagger *}$ فإنّنا نستنتج بذلك أنهما متساويتان. (إن هذا هو السبب الرئيس الذي يدفعنا على التركيز على الامتدادات المنتهية والزمر المنتهية. لاحظ أنه بحالة المجموعات غير المنتهية من الممكن أن نجد مجموعتين لهما العدد الرئيس نفسه وتحتوي إحداهما على الأخرى ولكنهما ليستا متساويتين. على سبيل المثال $\mathbb{Z} \subseteq Q$ وكلاهما قابلة للعد).

إن هدف هذا الفصل هو إنجاز جزء من حسابات رتبة $H^{\dagger *}$ ، وبالتحديد سنحسب $[H^{\dagger} : K]$ بدلالة رتبة H . وفي الفصل العاشر سنجد رتبة $H^{\dagger *}$ بدلالة هذه الدرجة، وبربط هذه النتائج مع بعض نحصل على بغيتنا.

(٩,١) الاستقلال الخطّي للتشاكلات المتباينة

Linear Independence of Monomorphisms

النظريّة الأولى التي سنبرهن عليها هنا تنسب إلى ديدكند (Dedekind) حيث كان أوّل من قدّم دراسة نظامية لتماثلات الحقول الذاتية. ولغرض تبسيط فكرة البرهان نقدم مثالاً سهلاً؛ لنفرض أنّ كلاً من L, K حقل ولنفرض أنّ كلاً من λ , μ تشاكل متباين من K إلى L . وسنبرهن على أنّه لا يمكن أن يكون λ مضاعف ثابت لـ μ إلا إذا كان $\lambda = \mu$. (نعني بكلمة ثابت هنا عنصراً L) . لنفرض أنّه يوجد عنصر $a \in L$

بحيث يكون

$$\mu(x) = a\,\lambda(x)$$

لكل $x \in K$. وباستبدال x بـ $y\,x$ حيث $y \in K$ نحصل على

$$\mu(y\,x) = a\,\lambda(y\,x).$$

وبما أنّ كلاً من μ , λ تشاكل نحصل على :

$$\mu(y)\,\mu(x) = a\,\lambda(y)\,\lambda(x).$$

ولكن لدينا أيضًا :

$$\lambda(y)\,\mu(x) = a\,\lambda(y)\,\lambda(x).$$

من المعادلتين أعلاه نحصل على :

$$\lambda(y) = \mu(y)$$

لكل $y \in K$. إذن $\lambda = \mu$.

إن تعميم ديدكند (Dedekind) لهذه النتيجة هو :

تمهيدية (٩,١) (ديدكند)

إذا كان كل من K و L حقلاً فإن أي مجموعة مختلفة من التشاكلات المتباينة من K إلى L يجب أن تكون مستقلة خطيًا على L .

البرهان

لنفرض أنّ $\lambda_1,\dots,\lambda_n$ تشاكلات متباينة من K إلى L ولنفرض أنها غير مستقلة خطيًا على L ، إذن يوجد أعداد $a_1,\dots,a_n$ ليست جميعها أصفارًا بحيث يتحقق :

$$a_1\lambda_1(x_1)+\dots+a_n\lambda_n(x)=0 \qquad (٩,١)$$

لكل $x \in K$. وبدون التأثير على الحالة العامة نستطيع أنّ نفرض أن $a_i \neq 0$ لكل $1 \le i \le n$. ولنفرض أنّ (٩,١) هي أصغر معادلة متحققة وتحتوي على أصغر عدد n من الحدود من بين جميع المعادلات المتحققة والتي تكون على تلك الصورة . وبكلام

آخر نفرض عدم وجود معادلة على الصورة (١ , ٩) وتحتوي على أقل من n من الحدود .

وبما أنّ $\lambda_1 \neq \lambda_n$ فإنّه يوجد $y \in K$ بحيث يكون $\lambda_1(y) \neq \lambda_n(y)$. إذن $y \neq 0$. وباستبدال x بـ y x في المعادلة (١ , ٩) نحصل على :

$$a_1 \lambda_1(y\, x) + \ldots + a_n \lambda_n(y\, x) = 0$$

لكل $x \in K$ ومنه :

$$a_1 \lambda_1(y)\, \lambda_1(x) + \ldots + a_n \lambda_n(y)\, \lambda_n(x) = 0 \qquad (٩ , ٢)$$

لكل $x \in K$. وبضرب المعادلة (١ , ٩) في $\lambda_1(y)$ وبطرح المعادلة (٢ , ٩) نحصل على :

$$a_2\big(\lambda_2(x)\lambda_1(y) - \lambda_2(x)\,\lambda_2(y)\big) + \ldots + a_n\big(\lambda_n(x)\,\lambda_1(y) - \lambda_n(x)\,\lambda_n(y)\big) = 0$$

معامل $\lambda_n(x)$ هو $a_n(\lambda_1(y) - \lambda_n(y)) \neq 0$. إذن نحصل على معادلة على صورة (١ , ٩) وبحدود أقل ، وهذا يناقض الفرض ، وبالتالي فإنّ وجود معادلة على شكل (١ , ٩) مستحيل ، وتكون التشاكلات المتباينة مستقلة خطيًا . Δ

للبرهان على نتيجتنا الثانية نحتاج إلى التمهيديتين التاليتين . الأولى منهما نظرية معروفة من الجبر الخطي ونقدمها دون برهان

تمهيدية (٩،٢)

ليكن

$$a_{m1} x_1 + \ldots + a_{mn} x_n = 0$$

نظامًا من المعادلات الخطية المتجانسة في n من المتغيرات و m من المعادلات حيث المعاملات a_{ij} تنتمي إلى حقل ما . عندئـذ إذا كـان $n > m$ فإنه يوجد للنظام حل غير تافه . Δ

هذه التمهيدية تبرهن عادة في المقرر الأول للجبر الخطي ويمكن الحصول عليها في أي كتاب جبر خطي (على سبيل المثال هالموس Halmos, 1958, p. 91) .

التمهيدية الثانية تزودنا بمبدأ عام ومهم .

تمهيدية (٩,٣)

لتكن G زمرة عناصرها المختلفة هي $g_1,\ldots,g_n$ وإذا كان $g \in G$ فإنّه عندما يتغير j من 1 إلى n فإنّ العناصر gg_i تُكّون جميع G بحيث يتكرر كل عنصر من عناصر G مرة واحدة فقط .

البرهان

ليكن $h \in G$ ، إذن $g^{-1}h = g_j$ ومنه $h = gg_j$ وإذا كان $gg_i = gg_j$ فإنّ $g_i = g^{-1}gg_i = g^{-1}gg_j = g_j$ ، إذن الدالة $g_i \to gg_i$ دالّة متباينة وشاملة من G إلى $\{gg_1,\ldots,gg_n\}$. Δ

سنحتاج إلى بعض الترميز

ترميز

نرمز للعدد الرئيس للمجموعة S بالرمز $|S|$. فإذا كانت G زمرة فإنّ $|G|$ يرمز لرتبة هذه الزمرة .

وسنبرهن الآن على النظرية الرئيسة في هذا الفصل التي برهانها يشبه إلى حد ما برهان التمهيدية (١ , ٩) .

نظرية (٩,٤)

لتكن G زمرة منتهية من زمرة التماثلات الذاتية للحقل K ، وليكن K_0 هو حقل G الثابت . عندئذ $[K:K_0]=|G|$.

البرهان

لنفرض أنّ $|G| = n$ وأن هذه العناصر هي $g_1,\ldots,g_n$ حيث $g_1 = 1$.

(١) نفرض أن $[K:K_0] = m < n$. ولنفرض أن $\{x_1,\ldots,x_m\}$ أساس للحقل K على K_0 . باستخدام تمهيدية (٩ , ٢) نستطيع إيجاد $y_1,\ldots,y_n \in K$ ليست جميعها أصفارًا بحيث

$$g_1(x_j)y_1+\dots+g_n(x_j)y_0=0 \qquad (٩,٣)$$

حيث $j=1,\dots,m$. ليكن $a\in K$. عندئذ

$$a=\alpha_1x_1+\dots+\alpha_mx_m$$

حيث $\alpha_1,\dots,\alpha_m\in K_0$. إذن

$$\begin{aligned}g_1(a)y_1+\cdots+g_n(a)y_n&=g_1\left(\sum_\ell\alpha_\ell x_\ell\right)y_1+\cdots+g_n\left(\sum_\ell\alpha_\ell x_\ell\right)y_n\\&=\sum_\ell\alpha_\ell\left(g_1(x_\ell)y_1+\cdots+g_n(x_\ell)y_n\right)\\&=0\end{aligned}$$

وذلك باستخدام المعادلة (٣ , ٩). إذن التشاكلات المتباينة المختلفة $g_n,\dots,g_n$ غير مستقلة خطيًا وهذا يناقض تمهيدية (١ , ٩)، إذن $m\geq n$.

(٢) لنفرض الآن أنّ $[K:K_0]>n$ ، عندئذ يوجد مجموعة مكوّنة من $n+1$ عنصرًا في K مستقلة خطيًا على K_0 ، ولتكن $\{x_1,\dots,x_{n+1}\}$ هي تلك المجموعة. باستخدام تمهيدية (٢ , ٩) يوجد $y_1,\dots,y_{n+1}\in K$ وليست جميعها أصفارًا بحيث لكل $j=1,\dots,n$ يكون:

$$g_j(x_1)\,y_1+\dots+g_j(x_{n+1})\,y_{n+1}=0 \qquad (٩,٤)$$

نختار $y_1,\dots,y_{n+1}$ بحيث يكون عدد العناصر التي لا تساوي صفرًا أقل ما يمكن، ونعيد الترقيم بحيث

$$y_1,\dots,y_r\neq0\quad,\quad y_{r+1},\dots,y_{n+1}=0\ .$$

وباستخدام المعادلة (٤ , ٩) نجد:

$$g_j(x_1)y_1+\dots+g_j(x_r)\,y_r=0 \qquad (٩,٥)$$

لنفرض أنّ $g\in G$ ، و باستخدام المعادلة (٥ , ٩) نحصل على نظام المعادلات:

$$gg_j(x_1)\,y_1+\dots+gg_j(x_r)\,y_r=0 \qquad (٩,٦)$$

وبضرب المعادلات (٥ , ٩) في $g(y_1)$ و (٦ , ٩) في y_1 والطرح نحصل على:

$$g_j(x_2)\big(y_2 g(y_1) - g(y_2) y_1\big) + \dots + g_j(x_r)\big(y_r g(y_1) - g(y_r) y_1\big) = 0$$

وهذا النظام مثل النظام (٩ , ٥) ولكن بمعادلات أقل وبذلك نحصل على تناقض ما لم لتكن المعاملات

$$y_i g(y_1) - y_1 g(y_i)$$

جميعها أصفارًا. وإذا كانت كذلك فإنّنا نحصل على :

$$y_i y_1^{-1} = g(y_i y_1^{-1})$$

لكن $g \in G$ ومنه $y_i y_1^{-1} \in K_0$ إذن يوجد $z_1, \dots, z_r \in K_0$ و $k \in K$ بحيث $y_i = k z_i$ لكل i . وبذلك تصبح المعادلـــة (٩ , ٥) عند $j = 1$ كالتالي :

$$x_1 k z_1 + \dots + x_r k z_r = 0$$

وبما أنّ $k \neq 0$ نستطيع أن نختصره وبذلك نكون قد أثبتنا أنّ x_i غير مستقلة خطيًا على K_0 . وهذا تناقض . إذن $[K : K_0] \leq n$. وباستخدام الجزء الأول من البرهان نحصل على :

$$[K : K_0] = n = |G|$$

نتيجة (٩,٥)

إذا كانت G هي زمرة جالوا للامتداد الحقلي $L : K$ المنته وكانت H زمرة جزئية منتهية من G فإنّ

$$[H^\dagger : K] = [L : K] / |H|$$

البرهان

باستخدام نظرية (٩ , ٤) نجد أن :

$$[H^\dagger : K] = [L : K] / [L : H^\dagger] = [L : K] / |H|. \qquad \Delta$$

أمثلة

سنوضح النظرية (٩ , ٤) بمثالين ، أحدهما مباشر والآخر غير مباشر .

(١) لتكن G هي زمرة تماثلات $\mathbb{C}$ الذاتية التي تتكون من التماثل المحايد والتماثل

المرافق. حقل G الثابت هو $\mathbb{R}$ ، لأنــه لو كــان $x - iy = x + iy$ و $x, y \in \mathbb{R}$ فـإنّ $y = 0$ والعكس صحيح أيضًا. إذن

$$[\mathbb{C} : \mathbb{R}] = |G| = 2$$

(٢) ليكن $K = Q(w)$ حيث $w = e^{2\pi i/5} \in \mathbb{C}$. الآن $w^5 = 1$ وعنــاصر $Q(w)$ تكتب على الصورة.

$$p + q w + r w^2 + s w^3 + t w^4 \qquad (٩,٧)$$

حيث $p,q,r,s,t \in Q$. من السهل ايجاد زمرة جالوا للامتداد $Q : Q(w)$، لأنه لو كان α تماثلاً ذاتيًا للحقل $Q(w)$ بالنسبة إلى Q فإن

$$(\alpha(w))^5 = \alpha(w^5) = \alpha(1) = 1 .$$

إذن $\alpha(w) = w, w^2, w^3, w^4$. وهذا يعطينا الاحتمالات التالية :

$$\begin{aligned}
\alpha_1 &: p + qw + rw^2 + sw^3 + tw^4 \rightarrow p + qw + rw^2 + sw^3 + tw^4 \\
\alpha_2 &: \qquad\qquad\qquad\qquad\qquad\quad \rightarrow p + sw + qw^2 + tw^3 + rw^4 \\
\alpha_3 &: \qquad\qquad\qquad\qquad\qquad\quad \rightarrow p + rw + tw^2 + qw^3 + sw^4 \\
\alpha_4 &: \qquad\qquad\qquad\qquad\qquad\quad \rightarrow p + tw + sw^2 + rw^3 + qw^4
\end{aligned}$$

ومن السهل البرهان على أن هذه جميعها تماثلات ذاتية على $Q(w)$ بالنسبة إلى Q . إذن رتبة زمرة جالوا للامتداد $Q : Q(w)$ تساوي 4، ومن السهل أنّ نجد أن Q هو الحقل الثابت لهذه الزمرة، إذن باستخدام نظرية (٩,٤) يجب أن يكون $[Q(w) : Q] = 4$.

وللوهلة الأولى يبدو أن ما حصلنا عليه الآن خطأ لأن العبارة (٩,٧) تكتب لنا كل عنصر بدلالة 5 عناصر أساسية ولذلك من الطبيعي أن نعتقد أن درجة الامتداد تساوي 5 ، ويدعم هذا الاعتقاد كون w صفرًا لكثيرة الحدود $t^5 - 1$. ولكن القاريء الذكي يكون قد خمن مصدر هذه المعضلة: $t^5 - 1$ ليست كثيرة حدود w الأصغرية على Q وذلك لأنها قابلة للاختزال. وبالحقيقة فإنّ كثيرة حدود w الأصغرية على Q هي :

$$t^4 + t^3 + t^2 + t + 1$$

ودرجتها تساوي 4 . إن المعادلة (٩ , ٧) تبقى محققة ولكن العناصر التي افترضنا أنّها أساسية غير مستقلة خطيًا لأن :

$$w^4 + w^3 + w^2 + w + 1 = 0 .$$

إذن كل عنصر في $Q(w)$ يكتب بصورة وحيدة على الشكل :

$$p + qw + rw^2 + sw^2$$

حيث $p, q, r, s \in Q$. ولكننا لم نستخدم هذا الشكل لأنّه ينقصه التناظر وبذلك يجعل حساباتنا صعبة .

تمـــارين

(٩ , ١) افحص صحة النظريّة (٩ , ٤) للامتدادات المعطاة في التمرين (٧ , ١) وزمر جالوا لها .

(٩ , ٢) جد الحقل الثابت للزمرة الجزئية $\{\alpha_1, \alpha_4\}$ في المثال الثاني أعلاه . افحص صحة النظرية (٩ , ٤) .

(٩ , ٣) حل المثال الثاني أعلاه إذا كان $w = e^{2\pi i/7}$.

(٩ , ٤) جد جميع التشاكلات المتباينة من Q إلى $\mathbb{C}$.

(٩ , ٥) جد جميع التشاكلات المتباينة من الحلقة $\mathbb{Z}$ إلى Q .

(٩ , ٦) أثبت أن أيّ تشاكل متباين من الحلقة $\mathbb{Z}$ إلى الحقل K يمكن توسيعه إلى تشاكل متباين وحيد من الحقل Q إلى الحقل K . هل يبقى ذلك ممكنًا لو لم يكن K حقلاً ؟

(٩ , ٧) ضع علامة صح أو خطأ أمام كل مما يأتي :

(ا) إذا كان S مجموعة جزئية منتهية من T وكان $|S| = |T|$ فـإن $S = T$.

(ب) العبارة (ا) صحيحة في حالة المجموعات غير المنتهية .

(ج) يوجد تشاكل متباين وحيد من Q إلى Q .

(د) يوجد p من التماثلات الذاتية على $\mathbb{Z}_p$.

(هـ) إذا كان كل من K و L حقلاً فإنه يوجد على الأقل تشاكل متباين من K إلى L .

(و) إذا كان كل من K و L حقلاً ووجد تشاكل متباين من K إلى L فإنّ مميز K = مميز L .

(ز) إذا كان كل من K و L حقلا بحيث مميز K = مميز L فإنّه يجب أن يوجد تشاكل متباين من K إلى L .

(ح) إذا كان مميز K = p فإنّه يجب أن يوجد تشاكل متباين وحيد من $\mathbb{Z}_p$ إلى K .

(ط) التماثلات الذاتية المختلفة على الحقل K مستقلة خطيًا على K .

(ي) التشاكلات المتباينة المستقلة خطيًا يجب أن تكون مختلفة .

الفصل العاشر

التشاكلات المتباينة، التماثلات الذاتية والانغلاقات الناظمية

Monomorphisms, Automorphisms and Normal Closures

إنّ موضوع هذا الفصل هو إنشاء تماثلات ذاتية بمواصفات معينة . وسنبدأ بتعميم التماثل الذاتي بالنسبة إلى K ويعرف بالتشاكل المتباين بالنسبة إلى K، وسنستخدم هذه التشاكلات المتباينة بالنسبة إلى K لبناء تماثلات ذاتية بالنسبة إلى K وذلك في حالة الامتدادات الناظمية ، وباستخدام ذلك نستطيع إيجاد رتبة زمرة جالوا لأي امتداد ناظمي ، قابل للفصل ومنته ، وبالاستعانة بنتائج الفصل التاسع نحصل على جزء مهم من النظرية الأساسية في الفصل الحادي عشر .

سنقدم أيضًا مفهوم الانغلاق الناظمي لامتداد منته . وهذا المفهوم يستخدم كوسيلة للالتفاف حول بعض العوائق التقنية المتسببة من الامتدادات غير الناظمية .

(١٠,١) التشاكلات المتباينة بالنسبة إلى K

K - Monomorphisms

نبدأ بتعميم التماثلات الذاتية على الحقل L بالنسبة إلى K .

تعريف

لنفرض أن K حقل جزئي من كل من الحقلين M و L . عندئذ التشاكل المتباين من M إلى L بالنسبة إلى K هو تشاكل حقلي متباين $\varphi : M \to L$ بحيث يحقق : $\varphi(k) = k$ *لكل* $k \in K$.

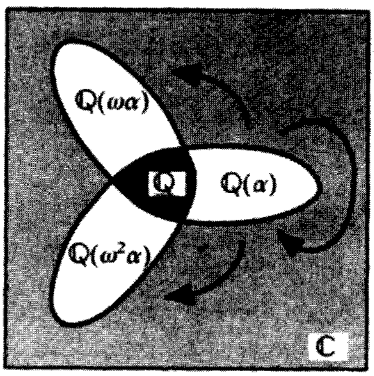
مثال

لنفرض أنّ $K = Q$ و $M = Q(\alpha)$ حيث α هو الجذر التكعيبي الحقيقي للعدد 2 و $L = \mathbb{C}$. وبإمكاننا أن نعرف تشاكل متباين $\varphi : M \to L$ بالنسبة إلى K بأن نجعل $\varphi(\alpha) = w\alpha$ حيث $\alpha = e^{2\pi i/3}$، وبصورة أدقّ إن كل عنصر في M يكتب على الشكل $p + q\alpha + r\alpha^2$ حيث $p, q, r \in Q$. نعرف

$$\varphi(p + q\alpha + r\alpha^2) = p + qw\alpha + rw^2\alpha^2 .$$

وبما أنّ α و $w\alpha$ لهما كثيرة الحدود الأصفرية نفسها وبالتحديد $t^3 - 2$ ، وباستخدام نظرية (٨ , ٣) نجد أن φ تشاكل متباين بالنسبة إلى K .

في حالتنا هذه يوجد تشاكلان متباينان آخران بالنسبة إلى K ؛ أحدهما التطبيق المحايد ، والآخر يجعل صورة α هي $w\alpha^2$ (انظر الشكل ١٨) .



شكل (١٨). التشاكلات المتباينة بالنسبة إلى Q للامتداد $Q : Q\left(\sqrt[3]{2}\right)$

وبصورة عامة إذا كان $K \subseteq M \subseteq L$ فإنّ أي تماثل ذاتي على L بالنسبة إلى K يعطينا تشاكلاً متبايناً $M \to L$ بالنسبة إلى K، وإن اهتمامنا يكمن في الحالة التي نستطيع عندها أن نحصل على العكس .

نظرية (١٠,١)

لنفرض أن $L : K$ امتداد ناظمي ومنته ولنفرض أن $K \subseteq M \subseteq L$ ليكن $\tau : M \to L$ تشاكلاً متباينًا بالنسبة إلى K . عندئذ يوجد تماثل ذاتي $\sigma : L \to L$ بحيث يكون $\sigma|_M = \pi$.

البرهان

باستخدام نظرية (٨,٤) نستطيع إيجاد كثيرة حدود f على K بحيث يكون L حقل انشطار f على K . إذن L هو حقل انشطار f على M وعلى $\tau(M)$ ولكن $\tau|_K$ هو التطبيق المحايد . إذن $\tau(f) = f$.

نعتبر الشكل التالي :

$$\begin{tikzcd} M \arrow[r] \arrow[d, "\tau"'] & L \arrow[d, dotted, "\sigma"] \\ \tau(M) \arrow[r] & L \end{tikzcd}$$

باستخدام نظرية (٨,٣) نستطيع إيجاد تماثل ذاتي $\sigma : L \to L$ بحيث $\sigma|_M = \tau$ وبما أن $\sigma|_K = \tau|_K$ هو التطبيق المحايد فإن σ تماثل ذاتي على L بالنسبة إلى K . Δ

تستخدم هذه النتيجة لإنشاء تماثلات ذاتية بالنسبة إلى K كالتالي :

قضية (١٠,٢)

إذا كان $L : K$ امتدادًا ناظميًا ومنتهيًا وكان α , β صفرين في L لكثيرة حدود لا مختزلة p على K فإنه يجب أن يوجد تماثل ذاتي σ على L بالنسبة إلى K بحيث $\sigma(\alpha) = \beta$.

البرهان

باستخدام نظرية (٨,٣) نستطيع ايجاد تماثل $\tau : K(\alpha) \to K(\beta)$ بحيث يكون $\tau|_K$ تطبيقًا محايدًا و $\tau(\alpha) = \beta$. ونستطيع أن نستخدم نظرية (١٠,١) لتوسيع τ إلى تماثل ذاتي σ على L بالنسبة إلى K . Δ

(٢, ١٠) الانغلاقات الناظميّة

Normal Closures

عندما تكون الامتدادات غير ناظمية فإننا نوسع هذه الامتدادات لنحصل بالتالي على امتدادات ناظمية .

تعريف

ليكن L امتدادًا جبريًا للحقل K . الانغلاق الناظمي للامتداد $L : K$ هو امتداد N للحقل L بحيث :

(١) $N : K$ امتداد ناظمي .

(٢) إذا كان $L \subseteq M \subseteq N$ و $M : K$ ناظمي فإنّ $M = N$.

من الواضح أنّ N هو أصغر امتداد ناظمي على K للحقل L .

النظرية التالية تؤمن لنا ما نحتاجه من الانغلاقات الناظمية وتبرهن لنا على وحدانيّة هذه الانغلاقات .

نظرية (٣, ١٠)

إذا كان $L : K$ امتدادًا منتهيًا فإنّه يوجد انغلاق ناظمي N للامتداد $L : K$ وهذا الانغلاق امتدادًا منته للحقل K، وإذا كان M انغلاقًا ناظميًا آخر فإنّ الامتدادين $M : K$ و $N : K$ متماثلان .

البرهان

لتكن العناصر $x_1, ..., x_r$ أساسًا للحقل L على K ولتكن m_i كثيرة حدود x_i الأصغرية على K . لنفرض أنّ N هو حقل انشطار $f = m_1 m_2 .... m_r$ على L . إذن N هو أيضًا حقل انشطار f على K ، وباستخدام نظرية (٤ , ٨) يكون N : K امتدادا ناظميا منتهيًا . لنفرض أنّ $N \supseteq P \supseteq L$ حيث P : K ناظمي ، لكل كثيرة حدود m_i صفر x_i في P ، وباستخدام الناظمية نجد أنّ f تنشطر في P . وبما أن N حقل

انشطار f فإن $P = N$. إذن N انغلاق ناظمي .

لنفرض الآن أن M و N انغلاقان ناظميّان . كثيرة الحدود f أعلاه تنشطر في M و N ومنه فإنّ كلاً من M و N يحوي حقل انشطار لـ f على K . حقلا الانشطار هذان يحتويان L وناظميين على K ، وعليه فإنّهما يجب أن يكونا M و N . وباستخدام وحدانية حقل الانشطار (نظرية ٣ , ٨) نستنتج أنّ $M : K$ و $N : K$ متماثلان . Δ

مثال

اعتبر $Q(c) : Q$ حيث c هو الجذر التكعيبي الحقيقي للعدد 2 . لقد رأينا سابقاً أن هذا الامتداد غير ناظمي، و إذا فرضنا أنّ K هو حقل انشطار $t^3 - 2$ على Q ومحتوى في $\mathbb{C}$ فإنّ $K = Q(c, cw, cw^2)$ حيث $w = (-1 + i\sqrt{3})/2$ هو جذر تكعيبي مركب للعدد 1 . الآن K هو انغلاق ناظمي للامتداد $Q(c) : Q$ ، نجد انغلاقًا ناظميًا بإقران جميع الاصفار المفقودة .

الانغلاقات الناظميّة تساعدنا على وضع قيود على مدى التشاكل المتباين .

تمهيدية (٤ , ١٠)

لنفرض $K \subseteq L \subseteq N \subseteq M$ حيث $L : K$ منته و N انغلاق ناظمي للامتداد $L : K$. ولنفرض أن $\tau : L \to N$ تشاكل متباين بالنسبة إلى K . عندئذ $\tau(L) \subseteq N$.

البرهان

لنفرض أنّ $\alpha \in L$ و m كثيرة حدود α الأصغرية على K، إذن

$$0 = m(\alpha) = \tau(m(\alpha)) = m(\tau(\alpha)) .$$

ومنه فإنّ $\tau(\alpha)$ صفر لـ m ، وبما أنّ $N : K$ ناظمي فإنّ $\tau(\alpha) \in N$. إذن $\tau(L) \subseteq N$. Δ

إنّ النتيجة التي حصلنا عليها من التمهيدية (٤ , ١٠) تسمح لنا بأن نركّز اهتمامنا عند مناقشتنا للتشاكلات المتباينة على الانغلاقات الناظمية للامتدادات تحت الدراسة . والنظريّة التالية تزودنا بعكس ما للتمهيدية أعلاه .

نظرية (٥,١٠)

إذا كان $L : K$ امتدادًا منتهيًا فإنّ العبارات التالية متكافئة :

(١) *$L : K$ ناظمي .*

(٢) *يوجد امتداد ناظمي N للحقل K يحتوي L بحيث يكون كل تشاكل متباين $\tau : L \to N$ بالنسبة إلى K تماثلا ذاتيًا على L بالنسبة إلى K .*

(٣) *لكل امتداد M للحقل K ويحتوي L يكون كل تشاكل متباين $\tau : L \to N$ بالنسبة إلى K تماثلاً ذاتيًا على L بالنسبة إلى K .*

البرهان

سنبرهن (١) ⟸ (٣) ⟸ (٢) ⟸ (١) .

(١) ⟸ (٣): إذا كان $L : K$ امتدادًا ناظميًا فإن L انغلاق ناظمي للامتداد $L : K$ وباستخدام تمهيدية (٤ , ١٠) نجد أنّ $\tau(L) \subseteq L$. وبما أن τ تحويل خطّي بالنسبة إلى K معرّف على فضاء متجهات ذو بعد منته L على K وهو متباين فإنّ بعد $\tau(L)$ = بعد L .
إذن $\tau(L) = L$ و τ تماثل ذاتي على L بالنسبة إلى K .

(٣) ⟸ (٢): ليكن N انغلاقًا ناظميًا للامتداد $L : K$. نظرية (٣ , ١٠) تضمن لنا وجود N الذي يحقق الشروط المعطاة في (٣) .

(٢) ⟸ (١): لنفرض أنّ f كثيرة حدود لا مختزلة على K ولها صفر $\alpha \in L$ ، وباستخدام ناظميّة N نجد أنّ f تنشطر على N . وإذا كان $\beta \in N$ صفرًا لـ f فإنه يوجد تماثل ذاتي σ على N بحيث يكون $\sigma(\alpha) = \beta$ وذلك باستخدام نظرية (٢ , ١٠) .
وباستخدام الفرض نجد أن σ تماثل ذاتي على L بالنسبة إلى K وأنّ

$$\beta = \sigma(\alpha) \in \sigma(L) = L \ .$$

إذن f تنشطر على L وأنّ $L : K$ ناظمي . Δ

النظرية التالية لها طابع حسابي .

نظرية (٦،١٠)

ليكن $L : K$ امتدادًا قابلاً للفصل ومنته درجته n . عندئذ يوجد بالضبط n من التشاكلات المتباينة من L إلى انغلاق ناظمي N (ومن ثم إلى اي امتداد ناظمي M للحقل K ويحتوي L) بالنسبة إلى K .

البرهان

باستخدام الاستنتاج الرياضي على $[L : K]$.

إذا كان $[L : K] = 1$ فالنتيجة واضحة .

لنفرض أنّ $[L : K] = k > 1$. ولنفرض أنّ $\alpha \in L \setminus K$ وله كثيرة الحدود الأصغرية m على K . إذن

$$\partial m = [K(\alpha) : K] = r > 1 .$$

وبما أنّ m كثيرة حدود لا مختزلة وقابلة للفصل ولها صفر واحد في الامتداد الناظمي N فإنّ m تنشطر في N وتكون أصفارها $\alpha_1, ..., \alpha_r$ جميعها مختلفة، و باستخدام الاستنتاج الرياضي نجد أنّ هناك بالضبط s من التشاكلات المتباينة $\rho_1, ..., \rho_s : L \to N$ بالنسبة إلى $K(\alpha)$ حيث $s = [L : K(\alpha)] = k / r$. وباستخدام نظرية (٢ , ١٠) يوجد r من التماثلات الذاتية المختلفة $\tau_1, ..., \tau_r$ على N بالنسبة إلى K بحيث $\tau_i(\alpha) = \alpha_i$. التطبيقات

$$\psi_{ij} = \tau_i \rho_j$$

تعطينا $k = rs$ من التشاكلات المتباينة المختلفة من L إلى N بالنسبة إلى K . ونبرهن الآن على أنّ هذه هي جميع التشاكلات المتباينة المختلفة من L إلى N بالنسبة إلى K . لنفرض أنّ $\tau : L \to N$ تشاكل متباين بالنسبة إلى K. إذن $\tau(\alpha)$ صفر لـ m في N ، ومنه فإنه يوجد i بحيث $\tau(\alpha) = \alpha_i$. التطبيق $\psi = \tau_i^{-1} \tau$ تشاكل متباين من L إلى N بالنسبة إلى K . إذن باستخدام الاستنتاج الرياضي يوجد j بحيث يكون $\psi = \rho_j$. ومنه فإنّ $\tau = \tau_i \rho_j = \psi_{ij}$ وبهذا يتم البرهان . Δ

نستطيع الآن أن نحسب رتبة زمرة جالوا لامتداد ناظمي ، قابل للفصل ومنته .

نتيجة (١٠,٧)

إذا كان $L:K$ امتدادًا ناظميًا وقابلاً للفصل ومنتهيا ودرجته n فإنه يوجد بالضبط n من التماثلات الذاتية المختلفة علَى L بالنسبة إلى K ومن ثم $|\Gamma(L:K)| = n$.

البرهان

استخدم النظريّتين (٥ , ١٠) و (٦ , ١٠) . Δ

نستطيع الآن بسهولة أن نحصل على النظرية المهمة التالية :

نظرية (١٠,٨)

ليكن $L:K$ امتدادًا منتهيًا و G زمرة جالوا لهذا الامتداد . إذا كان $L:K$ ناظميًا قابلاً للفصل فإن K هو الحقل الثابت للزمرة G .

البرهان

لنفرض أنّ K_0 هو حقل G الثابت ولنفرض أنّ $[L:K]=n$، و باستخدام النتيجة (١٠ , ٧) نجد أنّ $|G|=n$ ، وباستخدام نظريّة (٤ , ٩) نجد أن $[L:K_0]=n$ وبما أن $K \subseteq K_0$ فإن $K = K_0$. Δ

هناك عكس لهذه النظريّة يرينا لماذا يجب أن نفترض امتدادات ناظميّة وقابلة للفصل لكي يكون تقابل جالوا متباينًا وغامرًا. ولكن قبل ذلك نحتاج النظرية التالية التي تشبه إلى حد كبير نظرية (٦ , ١٠) نصًا وبرهانًا .

نظرية (١٠,٩)

لنفرض أن $K \subseteq L \subseteq M$ حيث $M:K$ منته و $[L:K]=n$. عندئذ يوجد على الأكثر n من التشاكلات المتباينة من L إلى M بالنسبة إلى K .

البرهان

لنفرض أنّ N هو انغلاق ناظمي للامتداد $M:K$ ، إذن باستخدام نظرية (٣ , ١٠) نجد أنّ $N:K$ منته وأنّ كل تشاكل متباين من L إلى M بالنسبة إلى K يجب أن يكون

تشاكلا متباينا من L إلى N بالنسبة إلى K، إذن من الممكن أن نفرض أنّ M امتداد ناظمي للحقل K بأخذ N بدلاً من M . والآن نستطيع أن نستخدم الاستنتاج الرياضي على $[L:K]$ كما في برهان النظرية (٦ , ١٠) ما عدا إنّنا فقط نستطيع البرهان على وجود s' من التشاكلات المتباينة من L إلى N بالنسبة إلى $K(\alpha)$ حيث $s' \le s$ (بالاستنتاج) وكذلك يوجد r' من التماثلات الذاتية المختلفة على N بالنسبة إلى K حيث $r' \le r$ (لأن أصفار m في N ليست بالضرورة مختلفة). أما باقي البرهان فإنّه يبقى كما هو.

لاحظ كذلك لو لم يكن $L:K$ قابلاً للفصل فإنّه يوجد أقل من n من التشاكلات المتباينة من L إلى M بالنسبة إلى K لأنّه يوجد α بحيث $r' < r$. Δ

نظرية (١٠,١٠)

إذا كان $L:K$ منته و G زمرة جالوا لهذا الامتداد و K هو حقل G الثابت فإن $L:K$ ناظمي وقابل للفصل .

البرهان

باستخدام نظرية (٤ , ٩) نجد أنّ $[L:K] = |G| = n$ ، ويوجد بالضبط n من التشاكلات المتباينة من L إلى L بالنسبة إلى K وبالتحديد عناصر G . ولكن كما لاحظنا في برهان نظرية (٩ , ١٠) ، إذا كان $L:K$ غير قابل للانفصال فإنّه يوجد أقل من n من التشاكلات المتباينة من L إلى L بالنسبة إلى K . إذن $L:K$ قابل للفصل.

وسنستخدم نظرية (٥ , ١٠) لبرهان الناظمية، ولنفرض أنّ N امتداد للحقل K ويحتوي L ولنفرض أنّ $\tau : L \to N$ تشاكل متباين بالنسبة إلى K . وبما أن كل عنصر في زمرة جالوا للامتداد $L:K$ يعرف لنا تشاكلاً متبايناً من L إلى N بالنسبة إلى K فإنّه يوجد n من التشاكلات المتباينة من L إلى N بالنسبة إلى K وهذه تماثلات ذاتية على L ، ولكن باستخدام نظرية (٩ , ١٠) نجد أن τ يأخذ على الأكثر n من القيم، ومنه فإنّ τ هو أحد هذه التشاكلات. إذن τ تماثل ذاتي على L . وباستخدام نظرية (٥ , ١٠) نجد أنّ $L:K$ ناظمي. Δ

إذا كان تقابل جالوا متباينًا وغامرًا فإنّ K يجب أن يكون الحقل الثابت لزمرة

جالوا للامتداد $L : K$، ومنه كما رأينا أعلاه فإنّ $L : K$ يجب أن يكون ناظميًا قابلاً للفصل. وفي الفصل الحادي عشر سنبرهن أن هذا الشرط كاف لجعل تقابل جالوا متباينًا وغامرًا.

تمارين

(١٠ , ١) إذاكان $L : K$ منته فاثبت أن كل تشاكل متباين من L إلى L بالنسبة إلى K يجب أن يكون تماثلاً ذاتيًا، هل تبقى النتيجة صحيحة إذا كان الامتداد غير منته؟

(١٠ , ٢) أنشيء انغلاقًا ناظميًا N لكل من الامتدادات التالية:

(ا) $Q(\alpha) : Q$ حيث α الجذر الحقيقي الخامس للعدد 3.

(ب) $Q(\beta) : Q$ حيث α الجذر الحقيقي السابع للعدد 2.

(ج) $Q(\sqrt{2}, \sqrt{3}) : Q$.

(د) $Q(\alpha, \sqrt{2}) : Q$ حيث α الجذر التكعيبي الحقيقي للعدد 2.

(هـ) $Q(\gamma) : Q$ حيث γ صفر لكثيرة الحدود $t^3 - 3t^2 + 3$.

(١٠ , ٣) جد زمرة جالوا لكل من الامتدادات (ا)، (ب)، (ج) و(د) في التمرين (١٠ , ٢).

(١٠ , ٤) جد زمرة جالوا للامتداد $N : Q$ حيث N هو الانغلاق الناظمي.

(١٠ , ٥) أثبت عدم صحة تمهيدية (١٠ , ٤) إذا لم نشترط أن يكون الامتداد $N : K$ ناظميًا ولكنها صحيحة لأي امتداد ناظمي $N : K$ وليس فقط للانغلاق الناظمي.

(١٠ , ٦) استخدم نتيجة (١٠ , ٧) لإيجاد رتبة زمرة جالوا للامتداد $Q(\sqrt{2}, \sqrt{3}, \sqrt{5}) : Q$.

(١٠ , ٧) ضع علامة صح أو خطأ أمام كل مما يلي:

(ا) كل تشاكل متباين بالنسبة إلى K هو تماثل ذاتي بالنسبة إلى K.

(ب) يوجد انغلاق ناظمي لكل امتداد منته.

(ج) إذا كان $K \subseteq L$ و σ تماثلاً ذاتياً على L بالنسبة إلى K فإن $\sigma|_K$ تماثل ذاتي على K بالنسبة إلى K .

(د) كل امتداد لحقل مميزه صفر يجب أن يكون ناظميًا .

(هـ) الامتداد الذي زمرة جالوا له رتبتها 1 ناظمي .

(و) الامتداد الناظمي والقابل للفصل والمنته تكون زمرة جالوا له منتهية .

(ز) زمرة جالوا دائمًا أبيلية .

(ح) لا يوجد تقابل جالوا للامتدادات غير الناظمية .

(ط) الامتداد الناظمي والقابل للفصل والمنته ذو الدرجة n تكون رتبة زمرة جالوا له تساوي n .

(ي) زمرة جالوا للامتدادات الناظمية دورية .

الفصل الحادي عشر

تقابـــل جالـــوا
The Galois Correspondence

لقد وصلنا أخيرًا إلى ما كنّا نصبو إليه وهو برهان الخواص الأساسية لتقابل جالوا بين الامتداد الحقلي وزمرة جالوا. ولقد قمنا بالبرهان على معظم ما هو مطلوب في الفصول السابقة ولم يبق علينا إلا أن نربط هذه البراهين ببعضها البعض.

(١١,١) النظرية الأساسيّـة
The Fundamental Theorem

لنبدأ بتذكير القاريء ببعض الاصطلاحات التي قدمناها في الفصل السابع. ليكن $L : K$ امتدادًا حقليًا ولتكن G زمرة جالوا لهذا الامتداد التي عناصرها جميع التماثلات الذاتية على L بالنسبة إلى K، ولتكن $\mathfrak{I}$ مجموعة الحقول الوسطية M و $\mathbf{G}$ مجموعة جميع الزمر الجزئية H من G. وقد قمنا بتعريف التطبيقين:

$$*: \mathfrak{I} \to \mathbf{G}$$

$$\dagger: \mathbf{G} \to \mathfrak{I}$$

كالتالي: إذا كان $M \in \mathfrak{I}$ فإنّ M^* هي زمرة التماثلات الذاتية على L بالنسبة إلى M. وإذا كانت $H \in \mathbf{G}$ فإنّ $H^\dagger$ هو حقل H الثابت. ولقد لاحظنا أن كلاً من $*$ و $\dagger$ تعكس الاحتواء وأن $M \subseteq M^{*\dagger}$ و $H \subseteq H^{\dagger *}$.

نظرية (١١,١) (النظرية الأساسية لجالوا)

ليكن $L : K$ ناظميًا قابلاً للفصل ومنتهيًا درجته n، ولتكن G زمرة جالوا لهذا الامتداد، $\mathfrak{I}$، $\mathbf{G}$، $*$، $\dagger$ كما هي معرفة أعلاه، عندئذ:

(١) رتبة زمرة جالوا G تساوي n .

(٢) التطبيقان * و † نظيرا بعضهما البعض ويعرفان لنا تقابلاً متباينًا بين $\mathfrak{I}$ و G يعكس الاحتواء .

(٣) إذا كان M حقلاً وسطيًا فإن :

$$[L : M] = |M^*|$$

$$. [M : K] = |G| / |M^*|$$

(٤) الحقل الوسطي M يكون امتدادًا ناظميًا للحقل K إذ وفقط إذا كانت M^* زمرة جزئية ناظمية من G (بالمفهوم الاعتيادي لنظرية الزمر) .

(٥) إذا كان الحقل الوسطي M امتدادًا ناظميًا للحقل K فإنّ زمرة جالـــوا للامتداد $M : K$ تماثل زمرة الخارج G/M^* .

البرهـان

الفقرة الأولى هي النتيجة (٧ , ١٠) . ولبرهان الفقرة الثانية لدينا من تمهيدية (٨ , ٧) أن $L : M$ قابل للفصل وباستخدام نظرية (٤ , ٨) يكون من الواضح أن $L : M$ ناظمي . إذن باستخدام نظرية (٨ , ١٠) يكون M هو حقل M^* الثابت . وبالتالي :

$$M^{*\dagger} = M \tag{١ , ١١}$$

الآن نأخذ $H \in \mathbf{G}$. نعلم أنّ $H \subseteq H^{\dagger *}$ وباستخدام المعادلة (١ , ١١) يكون $H^{\dagger *\dagger} = (H^{\dagger})^{*\dagger} = H^{\dagger}$. باستخدام نظرية (٤ , ٩) لدينا :

$$. |H| = [L : H^{\dagger}]$$

إذن

$$|H| = [L : H^{\dagger *\dagger}]$$

وباستخدام نظرية (٤ , ٩) مرّة أخرى نحصل على :

$$. [L : H^{\dagger *\dagger}] = |H^{\dagger *}|$$

إذن $|H^{\dagger *}| = |H|$. وبمـا أنّ H و $H^{\dagger *}$ زمرتـان منتهيتان و $H \subseteq H^{\dagger *}$ فإن $H = H^{\dagger *}$ وبهذا نكون قد برهنا على الفقرة الثانية .

وللبرهان على الفقـرة الثـالثة لاحظ أيـضًا أنّ $L : M$ ناظمي وقابل للفصل .

وباستخدام النتيجة (٧ , ١٠) نحصل على $[L : M] = |M^*|$، والمساواة الثانية يمكن الحصول عليها بسهولة.

لاحظ أنّ $|G|/|M^*|$ هو دليل M^* في G في المفهوم الاعتيادي لنظرية الزمر.

وللبرهان على الفقرتين الأخيرتين من النظرية (١ , ١١) نحتاج إلى تمهيدية :

تمهيدية (٢, ١١)

إذا كان $L : K$ امتدادا و M حقل وسطي و τ تماثل ذاتي على L بالنسبة إلى K فإنّ :

$$\left(\tau(M)\right)^* = \tau M^* \tau^{-1}$$

البرهان

لنفرض أنّ $M' = \tau(M)$، ولنفرض أنّ $\gamma \in M^*$ و $x_1 \in M'$ عندئذ يوجد $x \in M$، بحيث يكون $x_1 = \tau(x)$، ومنه

$$(\tau \gamma \tau^{-1})(x_1) = \tau \gamma(x) = \tau(x) = x_1$$

إذن

$$\tau M^* \tau^{-1} \subseteq M'^*$$

وبالطريقة نفسها

$$\tau^{-1} M'^* \tau \subseteq M^*$$

إذن

$$M'^* \subseteq \tau M^* \tau^{-1}$$

وبهذا يتم برهان التمهيدية. Δ

ونبرهن الآن على الفقرة الرابعة من النظرية (١ , ١١). لنفرض أنّ $M : K$ ناظمي و $\tau \in G$. إذن $\tau|_M : M \to L$ تشاكل متباين بالنسبة إلى K وباستخدام نظرية (٥ , ١٠) يكون تماثلاً ذاتياً على M بالنسبة إلى K . وباستخدام تمهيدية (٢ , ١١) لدينا $M^* = \tau M^* \tau^{-1}$ ومنه M^* زمرة جزئية ناظمية من G .

وللبرهان على العكس لنفرض أنّ $\sigma : M \to L$ تشاكل متباين بالنسبة إلى K .
باستخدام نظرية (١ , ١٠) يوجد تماثل ذاتي τ على L بالنسبة إلى K بحيث $\sigma = \tau|_M$. والآن بما أنّ M^* زمرة جزئيّة ناظميّة من G فإن $\tau M^* \tau^{-1} = M^*$ ، وباستخدام تمهيدية (٢ , ١١) نجد أنّ $(\tau(M))^* = M^*$. وباستخدام الفقرة الثانية من النظرية (١ , ١١) نجد أنّ $\tau(M) = M$. إذن $\sigma(M) = M$ وبذلك يكون σ تماثلاً ذاتيًا على M بالنسبة إلى K . وباستخدام نظرية (٥ , ١٠) يكون M : K ناظميًا .

نبرهن الآن على الفقرة الخامسة. لنفرض أنّ G' هي زمرة جالوا للامتداد M : K . نعرف التطبيق $\varphi : G \to G'$ كالتالي :

$\varphi(\tau) = \tau|_M$ لكل $\tau \in G$.

من الواضح أنّ φ تشاكل من الزمرة G إلى الزمرة G' . وباستخدام نظرية (١ , ١٠) نجد أن φ غامر ، ومن الواضح أن $\ker(\varphi) = M^*$. إذن باستخدام نظريّة الزمر نجد أن :

$$G' = \mathrm{Im}(\varphi) \cong G / \ker(\varphi) = G / M^* . \qquad \Delta$$

لاحظ كيف استخدمنا نظريّة (٤ , ٩) في برهان الجزء الثاني من نظرية (١ , ١١) .
لقد كان هذا الاستخدام مهمًا جدًا ، ومن هذا يأتي جمال الرياضيات . إذ تعتمد نظرياتها الشيّقة على نتائج سبقتها ولا تقل عنها تشويقًا وجمالاً .

ومن الممكن تعميم الفقرتين (٤) و (٥) من النظرية (١ , ١١) (انظر تمرين ٢ , ١١).

إنّ أهمية النظريّة الأساسية تكمن في اعتبارها أداة قوية وليست في قيمتها الجوهرية ؛ إنّها تساعدنا على تطبيق نظرية الزمر على مسائل صعبة المعالجة في نظرية الحقول (كثيرات الحدود) ، وسنسخر معظم الفصول الباقية من هذا الكتاب لاستثمار مثل هذه التطبيقات ، ولكن قبل الاستمرار في ذلك سنعزز موقفنا بتوضيح النظريّة بدراسة امتداد حقلي معين مع زمرة جالوا له . وسنخصص الفصل الثاني عشر لذلك .

تمارين

(١ , ١١) اكتب التفاصيل لتقابل جالوا للامتداد $Q(i, \sqrt{5}) : Q$ حيث

$G = \{ I,R,S,T\}$ هي زمرة جالوا لهذا الامتداد المعطاة في الفكرة الشاملة .

(٢ , ١١) ليكن $L : K$ امتداداً منتهيًا قابلاً للفصل ناظميًا وزمرة جالوا له هي G، وليكن M , N حقلين وسطيين بحيث $M \subseteq N$ ، برهن على أنّ $N : M$ ناظمي إذا وفقط إذا كانت N^* زمرة جزئية ناظمية من M^*، وفي هذه الحالة برهن على أنّ زمرة جالوا للامتداد $N : M$ تماثل M^* / N^* .

(٣ , ١١) اختبر النتيجة في التمرين (٢ , ١١) على المثال المعطى في التمرين (١ , ١١) .

(٤ , ١١)* ليكن K حقلاً مميزه لا يساوي 2 أو 3 ويحتوي على عنصر بحيث $i^2 = -1$. اعتبر التماثل الذاتي على $K(t)$ بحيث يثبت K ويأخذ t إلى أي من العناصر

$$\pm t, \pm 1/t, \pm i(t+1)/(t-1), \pm i(t-1)/(t+1), \pm i(t+i)/(t-1), \pm (t-i)/(t+i)$$

أثبت أنّ هذه العناصر تكون زمرة تماثل زمرة الدوران لرباعي الوجوه المنتظم، جد حقل هذه الزمرة الثابت . (**ارشاد** : اعتبر كرة قطرها 1 مثبته بحيث يكون قطبها الجنوبي هو نقطة الأصل في المستوى المركب $\mathbb{C}$، والاسقاطات من القطب الشمالي تعرف تطبيقاً من $\mathbb{C}$ إلى هذه الكرة بحيث تمثل دائرة الوحدة في $\mathbb{C}$ خط الاستواء، وارمز للقطب الشمالي بالرمز ∞ وسمّ نقاط الكرة الأخرى بنقاط $\mathbb{C}$ المقابلة لها، وهذه هي كرة ريمان، وادرس تأثير التطبيق أعلاه على هذه الكرة وبصفة خاصة على ثماني الوجوه الذي رؤوسه هي $0, \infty, \pm 1, \pm i$ (Klein, 1913) .

(٥ , ١١)* ليكن $\gamma = \sqrt{2+\sqrt{2}}$. أثبت أن $Q(\gamma) : Q$ ناظمي وزمرة جالوا له دورية . برهن أيضًا على أنّ $Q(\gamma, i) = Q(\delta)$ حيث $\delta^4 = i = \sqrt{-1}$.

الفصل الثاني عشر

مثال مُحدّد
A Specific Example

إنّ الامتداد الذي سنناقشه في هذا الفصل هو من الامتدادات المفضّلة لكُتّاب نظريّة الحقول وذلك لأنّه انموذج قياسي . إنّ مناقشة مثال أبسط سوف لا يكفي لتوضيح النظريّة على نحو كاف ، وأي مثال أصعب سوف يكون غير عملي ، وهذا المثال هو زمرة جالوا لحقل انشطار $t^4 - 2$ على Q .

سنجزيء المناقشة إلى أجزاء صغيرة وذلك ليسهل على القاريء فهمها .

(١) لتكن $f(t) = t^4 - 2$ على Q وليكن K حقل انشطار لـ f حيث $K \subseteq \mathbb{C}$. يمكن تحليل f في $\mathbb{C}$ كالتالي :

$$f(t) = (t - \varepsilon)(t + \varepsilon)(t - i\,\varepsilon)(t + i\,\varepsilon)$$

حيث ε هو الجذر الرابع الحقيقي الموجب للعدد 2 .

من الواضح أن $K = Q(\varepsilon, i)$ ، و بما أن مميز $K = 0$ و K حقل انشطار فإن $K : Q$ منته ، قابل للفصل وناظمي .

(٢) لنجد $[K : Q]$. لدينا :

$$[K : Q] = [Q(\varepsilon, i) : Q(\varepsilon)]\,[Q(\varepsilon) : Q] .$$

وبما أنّ $i^2 + 1 = 0$ و $Q(\varepsilon) \subseteq \mathbb{R} \not\ni i$ فإنّ $t^2 + 1$ هي كثيرة حدود i الأصغرية على $Q(\varepsilon)$. إذن $[Q(\varepsilon, i) : Q(\varepsilon)] = 2$.

وبما أنّ ε صفر لـ f على Q ، وبما أنّ f لا مختزلة باستخدام ميزان أيزنستاين (نظرية ٥ , ٢) فإنّ f هي كثيرة حدود ε الأصغرية على Q ومنه فإنّ

$[Q(\varepsilon) : Q] = 4$. إذن

$$[K : Q] = (2)(4) = 8$$

(٣) نجد عناصر زمرة جالوا للامتداد $K : Q$، إما بطريقة مباشرة، أو بتطبيق نظرية (٩ , ٣) عدّة مرّات، ونستطيع أن نجد تماثلاً ذاتيًا σ على K بالنسبة إلى Q بحيث يكون:

$\sigma(i) = i$ و $\sigma(\varepsilon) = i\,\varepsilon$.

وكذلك τ بحيث يكون

$\tau(i) = -i$ و $\tau(\varepsilon) = \varepsilon$

الجدول التالي يوضّح لنا حواصل ضرب هذه التماثلات المختلفة على K بالنسبة إلى Q:

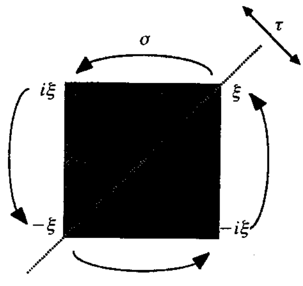
التماثل الذاتي	تأثيره على ε	تأثيره على i
1	ε	i
σ	$i\varepsilon$	i
σ^2	$-\varepsilon$	i
σ^3	$-i\varepsilon$	i
τ	ε	$-i$
$\sigma\tau$	$i\varepsilon$	$-i$
$\sigma^2\tau$	$-\varepsilon$	$-i$
$\sigma^3\tau$	$-i\varepsilon$	$-i$

حواصل الضرب الأخرى لا تنتج لنا تماثلات ذاتية جديدة لأنّ $\tau^2 = 1$ ، $\sigma^4 = 1$ ، $\tau\sigma = \sigma^3\tau$ ، $\tau\sigma^2 = \sigma^2\tau$ ، $\tau\sigma^3 = \sigma\tau$.

الآن إنّ صورة i تحت تأثير أي تماثل ذاتي على K بالنسبة إلى Q يجب أن تكون صفراً لكثيرة الحدود $t^2 + 1$، إذن $i \to \pm i$. بالمثل $\varepsilon \to \pm\varepsilon$ أو $\varepsilon \to \pm i\,\varepsilon$. وجميع الاحتمالات الممكنة (عددها 8) ظهرت في الجدول أعلاه وبالتالي فهذه هي جميع التماثلات الذاتية على K بالنسبة إلى Q

(٤) نستطيع أن نجد زمرة جالوا G بشكل مجرد. لاحظ أن
. $G = \langle \sigma,\tau : \sigma^4 = \tau^2 = 1 ,\ \tau\sigma = \sigma^3\tau \rangle$

إذن G هي الزمرة الزوجية من الرتبة 8. سنرمز لهذه الزمرة بالرمز D_8 . الزمرة D_8 لها تفسير هندسي حيث هي زمرة تناظرات المربّع. في الحقيقة من الممكن أن نربط رؤوس المربع بأصفار كثيرة الحدود $t^4 - 2$ بطريقة تجعل التناظرات الهندسية هي بالضبط تبديلات الأصفار التي تظهر في زمرة جالوا (انظر شكل ١٩).



شكل (١٩). زمرة جالوا D_8 بالنظر اليها كزمرة تناظرات مربع.

(٥) من السهل إيجاد جميع الزمر الجزئية من G. إذا فرضنا أن C_n ترمز للزمرة الدوروية التي رتبتها n و x يرمز للضرب المباشر فإن الزمر الجزئية هي :

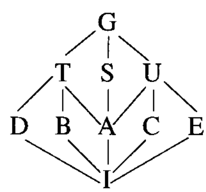
رتبه 8:	G	$G \cong D_8$
رتبه 4:	$\{1,\sigma,\sigma^2,\sigma^3\}$	$S \cong C_4$
	$\{1,\sigma^2,\tau,\sigma^2\tau\}$	$T \cong C_2 \times C_2$
	$\{1,\sigma^2,\sigma\tau,\sigma^3\tau\}$	$U \cong C_2 \times C_2$

رتبة 2:

$$\begin{array}{ll} A \cong C_2 & \{1,\sigma^2\} \\ B \cong C_2 & \{1,\tau\} \\ C \cong C_2 & \{1,\sigma\tau\} \\ D \cong C_2 & \{1,\sigma^2\tau\} \\ E \cong C_2 & \{1,\sigma^3\tau\} \end{array}$$

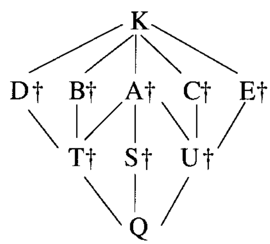
رتبه 1: $I \cong C_1 \qquad \{1\}$

(٦) علاة الاحتواء بين هذه الزمر الجزئيّة يبيّنها الشكل الشبكي التالي :



(تكون $X \subseteq Y$ إذا وجدت متتالية من الخطوط المائلة إلى أعلى من X إلى Y) .

(٧) من تقابل جالوا نستطيع ايجاد الحقول الوسطية . وبما أن هذا التقابل يعكس الاحتواء فإننا نحصل على الشكل الشبكي التالي للحقول :



(٨) نصف الآن عناصر هذه الحقول الوسطية .

هناك ثلاثة حقول من K ، درجة كل منها على Q تساوي 2، وهذه الحقول هي

. $Q(i\sqrt{2})$ ، $Q(\sqrt{2})$ ، $Q(i)$

من الواضح أنّ هذه الحقول هي $S^{\dagger}$ ، $T^{\dagger}$ ، $U^{\dagger}$ على الترتيب. إنّ ايجاد الحقول الثابتة الأخرى ليس بهذه السهولة، و لتوضيح كيفية ايجادها نجد $C^{\dagger}$ كمثال لذلك. يمكن كتابة كل عنصر في K على الصورة :

$$x = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4 i + a_5 i\varepsilon + a_6 i\varepsilon^2 + a_7 i\varepsilon^3$$

حيث $a_0, a_1, \ldots, a_7 \in Q$. إذن

$$\sigma\tau(x) = a_0 + a_1 i\varepsilon - a_2\varepsilon^2 - a_3 i\varepsilon^3 - a_4 i + a_5(-i)i\varepsilon - a_6 i(i\varepsilon)^2 - a_7 i(i\varepsilon)^3$$
$$= a_0 + a_5\varepsilon - a_2\varepsilon^2 - a_7\varepsilon^3 - a_4 i + a_1 i\varepsilon + a_6 i\varepsilon^2 - a_3 i\varepsilon^3$$

إذن يبقى العنصر x ثابتًا تحت تأثير $\sigma\tau$ (وبالتالي تحت تأثير C) إذا وفقط إذا كان

$$a_0 = a_0,\ a_1 = a_5,\ a_2 = -a_2,\ a_3 = -a_7$$
$$a_4 = -a_4,\ a_5 = a_1,\ a_6 = a_6,\ a_7 = -a_3$$

ومنه نجد أنّ a_0 و a_6 يمكن اختيارها اعتباطيًا وأنّ

. $a_3 = -a_7$ وأن $a_1 = a_5$ ، $a_2 = 0 = a_4$

ومنه نجد أنّ:

$$x = a_0 + a_1(1+i)\varepsilon + a_6 i\varepsilon^2 + a_3(1-i)\varepsilon^3$$

$$= a_0 + a_1\{(1+i)\varepsilon\} + \frac{a_6}{2}\{(1+i)\varepsilon\}^2 - \frac{a_3}{2}\{(1+i)\varepsilon\}^3$$

وهذا يعني أنّ

$$C^{\dagger} = Q\big((1+i)\varepsilon\big) .$$

بالمثل نستطيع أن نبيّن أنّ:

$$A^{\dagger} = Q(i, \sqrt{2})$$

$$B^{\dagger} = Q(\varepsilon)$$

$$D^{\dagger} = Q(i\varepsilon)$$

$$E^{\dagger} = Q((1-i)\varepsilon)$$

من السهل الآن أن نتحقق من علاقة الاحتواء في الشكل الشبكي الذي وجدناه في الفقرة (٧).

(٩) إنّ إثبات كون هذه الحقول هي جميع الحقول الوسطية يعتبر تمرينًا مزعجًا ولكنّه مباشر.

(١٠) الزمر الجزئيّة الناظميّة من G هي I ، A ، U ، T ، S ، G. إذن الامتدادات $I^{\dagger}$ ، $A^{\dagger}$ ، $U^{\dagger}$ ، $T^{\dagger}$ ، $S^{\dagger}$ ، $G^{\dagger}$ يجب أن تكون ناظمية على Q ومحتواه في K.

لاحظ أيضاً أن هذه الحقول هي حقول انشطار على Q لكثيرات الحدود:

$$t ، t^2+1 ، t^2-2 ، t^2+2 ، t^4-t^2-2 ، t^4-2$$

على الترتيب ولذلك فيجب أن تكون امتدادات ناظميّة على Q. ومن ناحية أخرى $Q : B^{\dagger}$ ليس ناظميًا على Q لأن $t^4 - 2$ لها صفر ε في $B^{\dagger}$ ولكنها غير منشطرة في $B^{\dagger}$. بالمثل الامتدادات $E^{\dagger}$ ، $D^{\dagger}$ ، $C^{\dagger}$ ليست ناظمية على Q.

(١١) بالاستناد إلى نظريّة جالوا فإن زمرة جالوا للامتداد $Q : A^{\dagger}$ تماثل G/A. ولكن $G/A \cong C_2 \times C_2$ ، و دعنا نحسب زمرة جالوا للامتداد $Q : A^{\dagger}$ مباشرةً. بما أنّ $A^{\dagger} = Q(i, \sqrt{2})$ فإنّه يوجد أربعة تماثلات ذاتية على Q:

التماثل	تأثيره على i	تأثيره على $\sqrt{2}$
1	i	$\sqrt{2}$
α	i	$-\sqrt{2}$
β	- i	$\sqrt{2}$
αβ	- i	$-\sqrt{2}$

وبما أنّ $\alpha^2 = \beta^2 = 1$ و $\alpha\beta = \beta\alpha$ فإنّ هذه الزمرة هي $C_2 \times C_2$ كما هو متوقع.

(١٢) لاحظ أن الشكلين الشبكيين لكل من $\mathfrak{I}$ و G ليسا متماثلين إلاّ إذا قلبنا

أحدهما. إذن لا يوجد تقابل مثل تقابل جالوا ويحافظ على علاقة الاحتواء، وإن عكس الاحتواء في تقابل جالوا يمكن أن يكون غريبًا من الوهلة الأولى ولكنه بالحقيقة طبيعي تمامًا وله الأهمية نفسها التي تتمتع بها التقابلات المحافظة على الاحتواء.

(١٣) إنّ من الصعب بصورة عامة حساب زمرة جالوا لامتداد حقلي معطى وعلى وجه الخصوص عندما لا يكون هنا صيغة واضحة لكتابة عناصر الحقل الكبير (انظر الفصل الثامن عشر).

تمـــارين

(١٢,١) جد زمرة جالوا للامتدادات التالية:

(أ) $Q(\sqrt{2}, \sqrt{5}) : Q$.

(ب) $Q(\alpha) : Q$ حيث $\alpha = e^{2\pi i/3}$

(ج) $K : Q$ حيث K هو حقل انشطار $t^4 - 3t^2 + 4$ على Q.

(١٢,٢) جد الزمر الجزئيّة لكل زمرة جالوا التي وجدتها في التمرين السابق.

(١٢,٣) جد الحقول الثابتة لهذه الزمر.

(١٢,٤) جد الزمر الناظميّة الجزئيّة لكل زمرة جالوا أعلاه.

(١٢,٥) اثبت أنّ الامتدادات المقابلة للزمر الناظمية هي بالفعل امتدادات ناظمية.

(١٢,٦) تحقق من أنّ زمرة جالوا لكل من هذه الامتدادات الناظمية هي بالفعل زمرة الخارج المناسبة.

الفصل الثالث عشر

الزمر البسيطة والقابلة للحل
Soluble and Simple Groups

لتطبيق تقابل جالوا يجب أن يكون لدينا الإلمام بعدد من مفاهيم نظرية الزمر. وسنفترض أن القاريء على دراية بالمباديء الأساسية لنظرية الزمر: الزمر الجزئية، والزمر الجزئية الناظمية، وزمر الخارج، والمرافقات، والتبديلات، ونظريات التماثل الأساسية. يمكن ايجاد أي مفهوم نحتاجه (بالإضافة إلى مادة هذا الفصل) في أي كتاب في نظرية الزمر، على سبيل المثال [Ledermann, 1961] أو [MacDonald, 1989]. البند (١ , ١٣) مكرس لتعريف الزمر القابلة للحل وشرح بعض الخواص الأساسية لها. هذه الزمر لها أهمية كبيرة عند دراسة نظريّة حل المعادلات باستخلاص الجذور. البند (٢ , ١٢) يناقش الزمر البسيطة. والهدف الرئيس هو البرهان على أن الزمرة المتناوبة من الدرجة أكبر من 4 زمرة بسيطة، والبند (٣ , ١٣) يزوّدنا بمقدمة لنظريّة الزمر من نوع p ونظرية سايلو التي سنستخدمها للبرهان على وجود زمر منتهية بحيث تكون بعض زمرها الجزئية حسنة السلوك.

(١٣,١) الزمر القابلة للحل
Soluble Groups

إنّ أوّل من قدّم الزمر القابلة للحل هو جالوا وذلك عند دراسة حل المعادلات باستخلاص الجذور، ولقد أصبح واضحًا بعد ذلك أنّ هذه الزمر لها أهمية كبيرة في كثير من مجالات الرياضيات.

في التعريف التالي وما يلي بعد ذلك الرمز $H \lhd G$ يعني أن H زمرة ناظمية جزئية من الزمرة G.

تعريف

نقول إنّ الزمرة G قابلة للحل إذا وجدت متسلسلة منتهية من الزمر الجزئية

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G \qquad (١٣,١)$$

بحيث:

(١) $G_i \lhd G_{i+1}$ لكل $i = 0, 1, \ldots, n-1$ ،

(٢) G_{i+1} / G_i أبيلية لكل $i = 0,1,\ldots,n-1$.

لاحظ أن الشرط (١٣,١) لا يؤدي إلى أن $G_i \lhd G$ وذلك لأنّ $G_i \lhd G_{i+1} \lhd G_{i+2}$ ليس بالضرورة أنْ يؤدّي إلى أنّ $G_i \lhd G_{i+2}$ (انظر تمرين ١٣,٥).

أمثلة

(١) أي زمرة أبيلية قابلة للحل وذلك بمتسلسلة $1 \subseteq G$.

(٢) زمرة التباديل S_3 قابلة للحل لأنه يوجد لها زمرة جزئية ناظمية مولّدة بالدور(123) وخارجها زمرة دوريّة رتبتها 2 .

(٣) الزمرة الزوجية D_8 التي رتبتها 8 قابلة للحل. وباستخدام ترميز الفصل الثاني عشر S زمرة جزئية ناظميّة من D_8 رتبتها 4 خارجها زمرة رتبتها 2 وكذلك S أبيلية.

(٤) زمرة التبديلات S_4 قابلة للحل، لها المتسلسلة

$$1 \lhd V \lhd A_4 \lhd S_4$$

حيث A_4 الزمرة المتناوبة رتبتها 12 و V عناصرها التبديلات 1، (12)(34)، (13)(24)، (14)(23)، وهي حاصل الضرب المباشر لزمرتين دورويتين رتبة كل منها 2. (الرمز V مأخوذ من الكلمة الذي قدمها كلاين، Vieregruppe، والتي تعني زمرة رباعية).

الزمر الخارجة هي:

$V / 1 \cong V$ أبيلية رتبتها 4.

$A_4 / V \cong C_3$ أبيلية رتبتها 3 .

$S_4 / A_4 \cong C_2$ أبيلية رتبتها 2 .

(٥) زمرة التبديلات S_5 غير قابلة للحل ولكننا سنرجيء البرهان على ذلك إلى النتيجة (٥ , ١٣).

نذكر القارئ بنظريات التماثل التالية :

تمهيدية (١ , ١٣)

لتكن G، H ، A زمرًا.

(١) *إذا كان* $H \lhd G$ *و* $A \subseteq G$ *فإن* $H \cap A \lhd A$ *وأن*

$$\frac{HA}{H} \cong \frac{A}{H \cap A}.$$

(٢) *إذاكانت* $H \lhd G$ *و* $H \subseteq A \lhd G$ *فإن* $H \lhd A$ ، $A/H \lhd G/H$ *وأن:*

$$\frac{G}{A} \cong \frac{G/H}{A/H}$$

(تعرّف الفقرتين (١) و (٢) بالنظريّة الأولى والنظريّة الثانية للتماثل ، على الترتيب).

الاستخدام الحكيم لنظريتي التماثل أعلاه يثبت لنا أنّنا نستطيع المحافظة على خاصية قابلية الحل للزمر تحت تأثيرات عدِة منها ما هو مذكور في النظريّة التالية :

نظرية (٢ , ١٣)

لتكن G زمرة ، H زمرة جزئية من G و N زمرة جزئية ناظمية من G. عندئذ:

(١) *إذا كانت G قابلة للحل فإنّ H قابلة للحل.*

(٢) *إذا كانت G قابلة للحل فإنّ G/N قابلة للحل.*

(٣) *إذا كانت كل من N و G/N قابلة للحل فإنّ G قابلة للحل.*

البرهان

(١) لتكن :

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = G$$

متسلسلة للزمرة G حيث الخوارج G_{i+1} / G_i أبيلية.

ولنفرض أنّ $H_i = G_i \cap H$. إذن يكون للزمرة H المتسلسلة:

$$1 = H_0 \triangleleft \cdots \triangleleft H_r = H$$

سنبرهن أنّ الخوارج أبيلية. الآن

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_{i+1} \cap H)}{G_i}$$

وذلك باستخدام النظريّة الأولى للتماثل، و لكن الزمرة الأخيرة هذه هي زمرة جزئيّة من G_{i+1} / G_i وهي أبيلية، إذن H_{i+1} / H_i أبيلية وبذلك تكون H قابلة للحل.

(٢) إذا عرّفنا G_i كما في السابق فإنّ للزمرة G/N المتسلسلة:

$$N / N = G_0N / N \triangleleft G_1N / N \triangleleft \cdots \triangleleft G_rN / N = G / N.$$

والخارج النموذجي لهذه المتسلسلة هو:

$$\frac{G_{i+1}N/N}{G_iN/N}$$

وباستخدام النظرية الثانية للتماثل نجد أنّ هذا الخارج يماثل:

$$\frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap G_iN} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap G_iN)/G_i}$$

وهو خارج زمرة أبيلية G_{i+1} / G_i وبذلك يكون أبيليًا. إذن G / N قابلة للحل.

(٣) يوجد متسلسلتان:

$$1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = N$$

$$N / N = G_0 / N \triangleleft G_1 / N \triangleleft \cdots \triangleleft G_s / N = G / N$$

بخوارج أبيلية. اعتبر المتسلسلة التالية للزمرة G:

$$1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = N = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_s = G.$$

تكون خوارج هذه المتسلسلة إما N_{i+1}/N_i (وهو أبيلي) أو G_{i+1} / G_i وهذه الزمرة

تماثل

$$\frac{G_{i+1}/N}{G_i/N}$$

وهي أبيلية أيضًا. إذن G قابلة للحل. Δ

دعنا نقول إنّ الزمرة G هي امتداد للزمرة A بالنسبة إلى الزمرة B إذا وجدت زمرة جزئية ناظمية N من G تماثل A بحيث يكون $G/N \cong B$، و عندئذ من الممكن أن نختصر الخواص الثلاثة بالنظرية أعلاه بالقول إن طائفة الزمر القابلة للحل مغلقة بالنسبة إلى الزمر الجزئية، الخارج والامتداد، و إن طائفة الزمر الأبيلية مغلقة بالنسبة إلى الزمر الجزئية والخارج ولكنها ليست مغلقة بالنسبة إلى الامتداد، وهذا هو السبب الذي قادنا إلى تعريف الزمر القابلة للحل.

(١٣,٢) الزمر البسيطة

Simple Groups

ندرس الآن صنفًا من الزمر يكاد يكون العكس للزمر القابلة للحل.

تعريف

نقول إنّ الزمرة G بسيطة إذا كانت 1 و G هما الزمرتان الجزئيتين الناظميتين الوحيدتين من G.

إنّ كل زمرة دوريّة رتبتها عدد أولي هي زمرة بسيطة وذلك لأنّ 1 و G هما الزمرتان الجزئيتان الوحيدتان من G (ومن ثم لا يوجد أي زمرة جزئية ناظميّة أخرى)، إن هذه الزمر أبيلية ومن ثم قابلة للحل، وفي الحقيقة إنّ هذه هي جميع الزمر البسيطة والقابلة للحل:

نظرية (١٣,٣)

تكون الزمرة القابلة للحل بسيطة إذا وفقط إذا كانت زمرة دوريّة رتبتها عدد أولي.

البرهان

إذاكانت G زمرة بسيطة وقابلة للحل فإنّ لها المتسلسلة :

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

حيث إننا بتجاهل التكرار نستطيع أن نفرض أنّ $G_i \neq G_{i+1}$، و بما أنّ G_{n-1} زمرة جزئيّة ناظميّة فعليّة من G و G بسيطة فإنّ $G_{n-1} = 1$ ، ومنه فإنّ $G = G_n / G_{n-1}$ أبيلية . وبما أنّ كل زمرة جزئيّة من زمرة أبيلية يجب أن تكون ناظمية وأنّ كل عنصر من G يُولّد زمرة جزئية دوريّة فإنّ G يجب أن تكون دوريّة ولا تحتوي على زمر فعلية غير الزمرة التافهة ، إذن رتبة G عدد أولي .

الاتجاه المعاكس واضح تمامًا . Δ

تلعب الزمر البسيطة دورًا مهمًا عند دراسة الزمر المنتهية ، وذلك لأن هذه الزمر تعتبر أحجار البناء الأساسية التي تتكون منها جميع الزمر المنتهية . وفي الحقيقة إنّ نظرية جوردان - هولدر (Jordan - Holder) التي لن نعرضها تنص على أن كل زمرة منتهية يوجد لها متسلسلة من الزمر الجزئية تشبه (المعادلة ١ , ١٣) التي خوارجها زمر بسيطة وهذه الزمر البسيطة تعتمد اعتمادًا كليًا على الزمرة وليس على اختيار المتسلسلة .

وبالرغم من أهمية الزمر البسيطة فإنّنا لن نحتاج إلى معرفة غير النتيجة التالية عنها :

نظرية (١٣ , ٤)

إذا كان $n \geq 5$ فإن زمرة التناوب A_n زمرة بسيطة .

البرهان

لنفرض أنّ $1 \neq N \lhd A_n$. والاستراتيجة التي سنتبعها في البرهان هي : أولاً سنبرهن على أنّه إذا احتوت N على دورة رتبتها 3 فإنّها تحوي جميع الدورات ذات الرتبة 3. وبما أن الدورات ذات الرتبة 3 تُولّد A_n فإن $N = A_n$ ، ثانيًا نبرهن على أنّ

N تحتوي بالفعل على دورة رتبتها 3 (وهنا نحتاج إلى أن $n \geq 5$) .

لنفرض إذن أنّ N تحتوي على دورة رتبتها 3 وبدون أن تتأثر الحالة العامة نستطيع أن نفرض أنّ هذه الدورة هي (123)، و بما أنّ (32k) تبديل زوجي لكل $k > 3$ فإن $(32k) \in A_n$ ، ومنه فإنّ

$$(32k)^{-1} (123) (32k) = (1k2)$$

عنصر في N ، إذن N تحتوي على $(12k) = (1k2)^2$ لكل $k \geq 3$ . . الآن S_n مُولَّدة من جميع المناقلات $(1\ i)$ حيث $i = 2,...,n$. وبما أنّ A_n هي مجموعة حواصل ضرب عدد زوجي من هذه المناقلات فإنّه مُولَّدة بجميع العناصر التي على الصورة:

$$.\ (1\ i)\ (1\ j) = (1\ i\ j)$$

ولكن لكل $i \neq 2$ لدينا:

$$.\ (1ij) = (12j)(12i)(12j)^{-1}$$

إذن جميع الدورات (12k) تُولِّد A_n ، وبهذا فإنّ $N = A_n$. يبقى أن نبرهن على أن N تحتوي على دورة من الرتبة 3 على الأقل، ويتم ذلك بدراسة الحالات التالية:

(١) لنفرض أنّ N تحتوي على عنصر

$$x = abc\cdots$$

حيث ....a,b,c, دورات منفصلة وحيث

$$.\ m \geq 4 \ ، \ a = (a_1, ..., a_m)$$

لتكن $t = (a_1\ a_2\ a_3)$. إذن $t^{-1} x t \in N$.

وبما أنّ t تتبادل مع كل من ... a, b, c, (دورات منفصلة) فإنّ

$$t^{-1} x t = (t^{-1} a t) b c ...$$

ضع $t^{-1} x t = (t^{-1} a t) b c ... = z$.

إذن $zx^{-1} = (a_1\ a_3\ a_m) \in N$ ومنه فإن N تحتوي على دورة من الرتبة 3 .

(٢) لنفرض الآن أنّ N تحتوي على عنصر فيه على الأقل دورتان من الرتبة 3 . وبدون التأثير على الحالة العامة نستطيع أن نفرض أنّ N تحتوي :

$$x = (123)(456)\, y$$

حيث y تبديل يثبت العناصر 1,2,3,4,5,6 .

إذاكان $t = (234)$ فإن N تحتوي العنصر :

$$(t^{-1} x\, t)\, x^{-1} = (12436) \; .$$

وكما في الحالة (١) فإن N تحتوي دورة رتبتها 3 .

(٣) إذا احتوت N على عنصر $x = (ijk)p$ حيث p حاصل ضرب مناقلات منفصلة عن بعضها ومنفصلة عن (ijk) فإنّ N تحتوي $x^2 = (ikj)$ وهذه دورة رتبتها 3 .

(٤) تبقى الحالة التي يكون فيها كل عنصر في N هو عبارة عن حاصل ضرب مناقلات منفصلة عن بعضها (إذا كانت $n = 4$ فإنّ هذه الحالة تعطينا الزمرة V)، وبما أنّ $n \geq 5$ نستطيع أن نفرض أنّ N تحتوي على

$$x = (12)\,(34)\, p$$

حيث p تثبت 1,2,3,4 . وإذا كانت $t = (234)$ فإنّ N تحتوي على :

$$(t^{-1}\; x\, t)\, x^{-1} = (14)\,(23) \; .$$

وإذا كانت $u = (145)$ فإنّ N تحتوي على :

$$u^{-1}(t^{-1}\; x\, t\, x^{-1})\, u = (45)\,(23)$$

ومنه فإنّ N تحتوي على :

$$(45)\,(23)\,(14)\,(23) = (145)$$

وهذا يناقض الفرض بأنّ كل عنصر في N هو حاصل ضرب مناقلات منفصلة . إذن A_n بسيطة لكل $n \geq 5$. Δ

ومن الجدير بالذكر هنا أنّ A_5 هي أصغر زمرة غير أبيلية وبسيطة وكان جالوا هو أول من برهن ذلك . من النظرية السابقة نحصل على النتيجة :

نتيجة (٥ , ١٣)

الزمرة S_n غير قابلة للحل لكل $n \geq 5$.

البرهان

إذا كانت S_n قابلة للحل فإنّه باستخدام نظريّة (٢ , ١٣) تكون A_n قابلة للحل ، وبما أنّ A_n بسيطة (نظرية ٤ , ١٣) فإنّه باستخدام نظرية (٣ , ١٣) تكون رتبة A_n عددًا أوليًا . ولكن $\frac{n!}{2} = |A_n|$ عددًا مؤلفًا إذا كان $n \geq 5$. Δ

سوف نحتاج في الفصل الرابع عشر إلى معرفة الحقيقة البسيطة التالية من زمرة التبديلات :

تمهيدية (٦ , ١٣)

زمرة التبديلات S_n تُولَّد بالدورات (12) و $(12 \ldots n)$ لكل n .

البرهان

لنفرض أنّ $t = (12)$ و $c = (12 \ldots n)$ ولنفرض أن G هي الزمرة المُولَّدة بالعنصرين c و t . إذن $c^{-1} t c = (23) \in G$ ومنه فإن $c^{-1} (23) c = (34)$ عنصر في G وهكذا . إذن G تحتوي على جميع المناقلات $(m, m+1)$. ومنه فإنّ G تحتوي على :

$$(12)(23)(12) = (13)\ ,\ \ (13)(34)(13) = (14)\ ,\ldots$$

إذن G تحتوي على جميع المناقلات $(1\, m)$. ومنه فإنّ G تحتوي على جميع المناقلات $(1\, m)(1\, r)(1\, m) = (m\, r)$. وبما أن كل عنصر في S_n هو حاصل ضرب مناقلات فإن $G = S_n$. Δ

(١٣,٣) الزمر من نوع p

p - Groups

سنبدأ بتذكير القاريء ببعض المفاهيم من نظريّةالزمر .

تعريف

نقول إنّ العنصرين a و b من الزمرة G مترافقان في G إذا وجد عنصر $g \in G$ بحيث $a = g^{-1}bg$ ، و *علاقة الترافق* هي علاقة تكافؤ على G وتسمى *فصول التكافؤ* بفصول ترافق G .

إذا كانت $C_1,\cdots,C_r$ هي فصول ترافق الزمرة G فإن أحد هذه الفصول يجب أن يحتوي على العنصر المحايد فقط وليكن C_1 ، إذن $|C_1|=1$. وبما أن فصول الترافق تجزيء G فإن:

$$|C_1| = 1 + |C_2| + \cdots + |C_r| \qquad (١٣,٢)$$

وهذه المعادلة تعرف بمعادلة فصول G .

تعريف

إذا كانت G زمرة $x \in G$ فإنّ مركز x في G يرمز له بالرمز $C_G(x)$ ويعرف بأنّه مجموعة العناصر $g \in G$ بحيث يكون:

$$. x\, g = g\, x$$

$C_G(x)$ زمرة جزئيّة من G لكل $x \in G$. توجد علاقة مهمة بين المركزات وفصول الترافق.

تمهيدية (١٣,٧)

إذا كانت G زمرة و $x \in G$ فإن عدد عناصر فصل ترافق x يساوي دليل $C_G(x)$ في G.

البرهان

تتحقق المساواة:

$$g^{-1}\, x\, g = h^{-1}\, x\, h$$

إذا وفقط إذا

$$h\, g^{-1}\, x = x\, h\, g^{-1}$$

وهذا يعني أنّ

$$. h\, g^{-1} \in C_G(x)$$

وبعبارة أخرى فإنّ g و h يقعان في المجموعة المشاركة لـ $C_G(x)$ في G نفسها ، ولكن

عدد هذه المجموعات المشاركة هو دليل $C_G(x)$ في G وبهذا يتم البرهان على التمهيدية . Δ

نتيجة (١٣,٨)

عدد عناصر أي فصل ترافق لزمرة منتهية يجب أن يقسم رتبة الزمرة . Δ

نقدم الآن طائفة الزمر من نوع p .

تعريف

ليكن p عددًا أوليًا . تسمى الزمرة المنتهية G زمرة من نوع p إذا كانَ $|G| = p^n$ حيث n عدد صحيح موجب .

على سبيل المثال الزمرة الزوجيّة D_8 هي زمرة من نوع 2، وإذا كان $n \geq 3$ فإنّ S_n لا يمكن أن تكون زمرة من نوع p لأي عدد أولي p .

سنحتاج إلى التعريف التالي قبل أن نبرهن على إحدى الخواص المهمة للزمر من p.

تعريف

مركز الزمرة G يرمز له بالرمز $Z(G)$ ويعرف بأنّه جميع العناصر $x \in G$ التي تحقق :

$x g = g x$ *لكل* $g \in G$.

مركز G زمرة جزئية ناظميّة من G. كثير من الزمر يكون مركزها يحتوي على العنصر المحايد فقط ، وعلى سبيل المثال $Z(S_3) = 1$، ومن ناحية أخرى إذا كانت G زمرة أبيلية فإن $Z(G) = G$ ، وإنّ وجود مركز غير تافه غالبًا ما يكون مفيدًا في نظريّة الزمر ، والزمر من نوع p لها هذه الخاصية .

نظرية (١٣,٩)

إذا كان $G \neq 1$ زمرة من نوع p فإن $Z(G) \neq 1$.

البرهان

باستخدام المعادلة (٢ , ١٣) نجد أنّ:

$$p^n = |G| = 1 + |C_2| + \ldots + |C_r|$$

ولكن من النتيجة (٨ , ١٣) لدينا

$$|C_i| = p^{n_i}$$

حيث $n_i \geq 0$. وبما أنّ $p \mid p^{n_i}$ فإنّه يوجد على الأقل $p - 1$ من الأعداد $|C_i|$ كلٍ منها يساوي 1 . وإذا كان x عنصرًا في فصل ترافق فيه عنصر واحد فقط فإنّ

$$g^{-1} x g = x$$

لكل $g \in G$ ، أي أنّ $g x = x g$. إذن $x \in Z(G)$ وبالتالي فإنّ $Z(G) \neq 1$. Δ

تمهيدية (١٠ , ١٣)

إذا كان G زمرة من النوع p رتبتها p^n فإنّه يوجد متسلسلة من الزمر الجزئية الناظمية :

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

بحيث يكون $|G_i = P^i|$ لكل $i = 0, 1, \ldots, n$.

البرهان

باستخدام الاستنتاج الرياضي على n .

إذا كان $n = 0$ فإن النتيجة واضحة .

إذا كان $n \neq 0$ فإنّ $Z = Z(G) \neq 1$ وذلك باستخدام النظرية (٩ , ١٣) . وبما أن Z زمرة أبيلية من الرتبة p^m فإنّها تحتوي على عنصر رتبته p .

إذا كانت K هي الزمرة الجزئية الدورية المولدة بهذا العنصر فإنّ $|K| = p$. وبما أنّ $K \subseteq Z$ فإنه K ناظمية من G . الزمرة G / K زمرة من p رتبتها p^{n-1} . وباستخدام فرضية الاستنتاج نستطيع إيجاد متسلسلة من الزمر الجزئيّة الناظميّة

$$K / K = G_1 / K \subseteq \cdots \subseteq G_n / K$$

حيث $|G_i / K| = p^{i-1}$. إذن $|G_i| = p^i$ و $G_1 \lhd G$. وإذا وضعنا $G_0 = 1$ فإنّنا نحصل

على المطلوب . Δ

نتيجة (١١ , ١٣)

كل زمرة من النوع p يجب أن تكون قابلة للحل .

البرهان

زمر الخارج G_i / G_{i+1} في المتسلسلة التي وجدناها في التمهيدية (١٠ , ١٣) جميعها من الرتبة p ، ومن ثم فهي زمر دورية وبالتالي فهي أبيلية . Δ

ولقد اكتشف العالم النرويجي سايلو (Sylow) بعض النظريّات الأساسية عن وجود زمر جزئية من نوع p من زمر منتهية ، سنحتاج إلى نظرية واحدة فقط من هذه النظريات وذلك في الفصل الرابع عشر ، وعند برهان النظريّة الأساسية في الجبر ، سنبرهن على هذه النظرية الآن ولكنّنا نقدم أولاً نصًا لجميع نظريات سايلو .

نظرية (١٢ , ١٣) (سايلو)

لتكن G زمرة منتهية من الرتبة $p^\alpha r$ حيث p عدد أولي لا يقسم r. عندئذ

(١) *يوجد على الأقل زمرة جزئيّة واحدة من G رتبتها p^α ،*

(٢) *جميع الزمر الجزئية هذه مترافقة في G،*

(٣) *أي زمرة جزئية من النوع p يجب أن تكون محتواة في زمرة جزئية من الرتبة p^α ،*

(٤) *عدد الزمر الجزئية من G ذات الرتبة p^α يطابق 1 قياس p.*

النظرية (١٢ , ١٣) تقودنا للتعريف التالي :

تعريف

إذا كانت G زمرة منتهية من الرتبة $p^\alpha r$ حيث p عدد أولي لا يقسم r فإن زمرة سايلو الجزئية من نوع p هي زمرة جزئية من G رتبتها p^α .

وباستخدام هذا الاصطلاح تنص النظريّة (١٢ , ١٣) على وجود زمرة سايلو جزئية من نوع p لكل عدد أولي p ، وجميعها مترافقة ، وجميعها زمر أعظمية من G ، وعددها يطابق 1 قياس p .

سنبرهن على الفقرة (١) من النظريّة (١٢ , ١٣) ولكنّنا نحتاج قبل ذلك إلى التمهيدية التالية :

تمهيدية (١٣ , ١٣)

إذا كان A زمرة أبيلية منتهية رتبتها تقسم p فإنّ A تحتوي على عنصر رتبته p.

البرهان

نستخدم الاستنتاج الرياضي على $|A|$. إذا كان $|A|$ عددًا أوليًا فإن النتيجة واضحة . ولنفرض أنّ $|A|$ عدد مؤلف ، ولتكن M زمرة جزئيّة من A بحيث يكون $|M| = m$ أعظميًا ، وإذا كان $p \mid m$ فإننا نحصل على النتيجة بواسطة الاستنتاج . ولنفرض إذاً أن p لا يقسم m . ليكن $t \in A$ و $t \notin M$ ، ولتكن T الزمرة الجزئية الدورية المولّدة من t ، إذن MT زمرة جزئيّة من A و $M \subseteq MT$ وبما أن $|M|$ أعظمي فإنّنا نستنتج أنّ $A = MT$. ومن النظرية الأولى للتماثل نجد أنّ :

$$|MT| = |M|\,|T| / |M \cap T|$$

ومنه فإنّ p يقسم r حيث r رتبة T ، وبما أن T دورية فإنّ رتبة العنصر $t^{r/p}$ يجب أن تكون p . وبهذا يتم البرهان . Δ

برهان الفقرة (١) من النظرية (١٢ , ١٣)

باستخدام الاستنتاج الرياضي على $|G|$.

من الواضح أنّ النظريّة صحيحة عندما $|G| = 1$ أو $|G| = 2$. لتكن $C_1, \cdots, C_s$ فصول ترافق G و $c_i = |C_i|$. من المعادلة (٢ , ١٣) نحصل على :

$$p^{\alpha} r = c_1 + c_2 + \ldots + c_r \qquad (١٣ , ٣)$$

ليكن Z_i هو مركز العنصر $x_i \in C_i$ في G وليكن $|Z_i| = n_i$. باستخدام التمهيدية (٧ , ١٣) نجد أن :

$$n_i = p^{\alpha} r / c_i \qquad (١٣ , ٤)$$

لنفرض أولاً أنّ أحد الأعداد c_i عدد صحيح أكبر من 1 ولا يقبل القسمة على p. باستخدام المعادلة (٤ , ١٣) نجد في هذه الحالة أنّ $n_i < p^{\alpha} r$ ، وأنّ n_i يقبل القسمة على p^{α} . وباستخدام فرضية الاستنتاج نجد أنّ Z_i تحتوي على زمرة جزئية رتبتها p^{α} .

لنفرض الآن أنّ $c_i = 1$ أو p يقسم c_i لكل $i = 1,...,s$ وليكن $z = |Z(G)|$. كما في النظرية (٩ , ١٣) z هو جميع الأعداد i حيث $c_i = 1$ إذن

$$p^{\alpha} r = z + k p$$

حيث k عدد صحيح ، ومنه فإنّ p يقسم z وأن مركز G غير تافه وليكن Z وأنّ p يقسم $|Z|$. وباستخدام التمهيدية (١٣ , ١٣) نستطيع إيجاد عنصر في Z رتبته p ، وبالتالي زمرة جزئيّة P من G رتبتها p. بما أنّ $P \subseteq Z$ فإن $P \triangleleft Z$. وباستخدام فرضية الاستنتاج نجد أنّ G/P تحتوي على زمرة جزئيّة S/P رتبتها $p^{\alpha-1}$. إذن S زمرة جزئيّة من G رتبتها p^{α} وبهذا يتم البرهان . Δ

من النظرية السابقة نستطيع أن نبرهن نظريّة تنسب إلى كوشي (Cauchy) (عادةً برهانها يسبق نظرية سايلو) .

نظرية (١٤ , ١٣) (كوشي)

إذا كان p عددًا أوليًا يقسم رتبة الزمرة المنتهية G فإنّ G تحتوي على عنصر رتبته p.

البرهان

لتكن S زمرة سايلو من النوع p من الزمرة G . إذن $S \neq 1$ ، وباستخدام تمهيدية (١٠ , ١٣) يكون للزمرة زمرة جزئيّة ناظميّة رتبتها p ، وبالتالي فإن رتبة أي عنصر (غير المحايد) في هذه الزمرة هو p. Δ

مثـال

لتكن $G = S_4$ ، إذن $|G| = 24$. واستنادًا إلى نظريّة سايلو يكون للزمرة G زمر جزئيّة من الرتب 3 و 8 . ومن السهل إيجاد الزمر الجزئية ذات الرتبة 3 : أي دورة رتبتها 3 مثل (123) أو (134) أو (234) تُولّد زمرة جزئية رتبتها 3 ، ولإيجاد زمرة جزئية رتبتها 8 نفرض أن V هي زمرة كلاين (Klein) من الرتبة 4 ، وهذه ناظميّة في G . لتكن t مناقلة و T هي الزمرة من الرتبة 2 المولّدة بالمناقلة t . إذن $V \cap T = 1$ و $V\,T$ زمرة جزئية من الرتبة 8 .

إنّ التمرين (٨ , ١٣) يوضّح لنا استحالة الحصول على نظريّات مماثلة لنظرية سايلو إذا تعدينا أسس الأعداد الأولية .

تمـارين

(١ , ١٣) أثبت أنّ الزمرة ذات الوجهين العامة
$D_{2n} = \langle a,b : a^n = b^2 = 1, b^{-1}ab = a^{-1} \rangle$ قابلة للحل .

(٢ , ١٣) استخدم فقط الحقيقة أنّ A_5 زمرة بسيطة لإثبات أنّ S_n غير قابلة للحل لكل $n \geq 5$.

(٣ , ١٣) برهن على أنّ أيّ الزمرة جزئيّة ناظميّة من زمرة ما يجب أن تكون اتّحاد فصول ترافق . جد فصول ترافق A_5 ، ومن ثم برهن على أنّ A_5 بسيطة .

(٤ , ١٣) اثبت أنّ المناقلات (1n) ,.... ,(12) تُولّد S_n .

(٥ , ١٣) جد زمر سايلو من النوع 2 ، 3، 5 للزمرة S_5 .

(٦ , ١٣) اثبت أنّ الزمرة المنتهية G تكون زمرة من النوع p إذا وفقط إذا كانت رتبة كل عنصر في G هي p^k حيث $k \in \mathbb{Z}$.

(٧ , ١٣) إذا كان من الممكن إنشاء النقطة (α,β) من (0,0) و (1,0) باستخدام المسطرة والفرجار فاثبت أنّ زمرة جالوا لكل من الامتدادين $Q(\alpha) : Q$ و $Q(\beta) : Q$ هي زمرة من نوع 2 .

(١٣ , ٨) اثبت عدم وجود زمرة جزئيّة من A_5 رتبتها 15 .

(١٣ , ٩) اثبت أنّ الزمرة الجزئيّة وزمرة الخارج لزمرة من نوع p هي زمرة من نـوع p، واثبت أنّ امتداد زمرة من نوع p بالنسبة إلى زمرة من نوع p يجب أن تكون زمرة من نوع p .

(١٣ , ١٠) اثبت أنّ مركز S_n يحتوي على العنصر المحايد فقـط لكـل $n \geq 3$.

(١٣ , ١١) اثبت أنّ الزمرة التي رتبتها p^2 (pعدد أوّلي) يجب أن تكون أبيلية ، ومن ثم اثبت أنّ هناك زمرتين غير متماثلتين فقط من الرتبـة p^2 لأي عدد أوّلي p .

(١٣ , ١٢) جد فصول ترافق D_{2n} ، اختر عنصراً من كل فصل ترافق وجد مركزه، ثم اختبر صحة التمهيدية (١٣ , ٧) .

(١٣ , ١٣) إذا كان $x, g \in G$ فاثبت أنّ

$$C_G(g^{-1} x g) = g^{-1} C_G(x) g \; .$$

(١٣ , ١٤) ضع علامة صح أو خطأ أمام كل من العبارات التالية :

(ا) كل زمرة قابلة للحل يجب أن تكون زمرة من نوع p .

(ب) جميع زمر سايلو الجزئية من زمرة منتهية يجب أن تكون قابلة للحل .

(ج) الضرب المباشر لزمر قابلة للحل يجب أن يكون زمرة قابلة للحل .

(د) كل زمرة بسيطة وقابلة للحل هي زمرة دورية .

(هـ) كل زمرة دورية هي زمرة بسيطة .

(و) S_n زمرة بسيطة لكل $n \geq 5$.

(ز) كل فصل ترافق لزمرة G يجب أن يكون زمرة جزئية من G

(ح) كل زمرة منتهية تحتوي على زمرة سايلو من نوع p لكل عدد أولي p .

(ط) كل زمرة منتهية غير تافهة من نوع p يجب أن يكون مركزها غير تافه .

(ي) كل زمرة بسيطة من نوع p يجب أن تكون أبيلية .

(١٣ , ١٥) أثبت أن علاقة الناظمية غير متعدية .

(إرشاد: اعتبر $G \subseteq V \subseteq S_4$ حيث G مولدة بالعنصر (34)(12)) .

(١٦ , ١٣) هناك طريقتان للحصول على تشاكل بين الزمر : الطريقة الأولى هي تعريف التشاكل كدالة تتمتع بخواص معيّنة ، والطريقة الأخرى هي الحصول على تشاكل بدلالة زمرة الخارج ، والعلاقة بين هاتين الطريقتين كالتالي : إذا كان $\varphi : G \to H$ تشاكلاً فإن $\ker(\varphi) \lhd G$ و $G / \ker(\varphi) \cong \mathrm{Im}(\varphi)$ ، وإذا كانت $N \lhd G$ فإنّنا نستطيع إيجاد تشاكل غامر $\varphi : G \to G/N$ بحيث $\ker(\varphi) = N$. اثبت أنّ نظريتي التماثل الأولى والثانية هما عبارة عن الحقيقتين التاليتين بدلالة خارج الزمر :

(ا) اقتصار التشاكل على الزمر الجزئيّة تشاكل أيضًا .

(ب) تركيب أي تشاكلين هو تشاكل أيضًا .

(١٧ , ١٣)* استخدم عدد عناصر فصول الترافق لإثبات أنّ زمرة التناظرات الدورانية لذى الاثني عشر وجهًا المنتظم يجب أن تكون بسيطة ، واثبت أن هذه الزمرة تماثل الزمرة A_5 .

الفصل الرابع عشر

حل المعادلات باستخلاص الجذور
Solution of Equations by Radicals

(١٤,١) مقدمة تاريخية
Historical Introduction

لقد تحدثنا عن تاريخ حل معادلات كثيرات الحدود باستخلاص الجذور في مقدمة هذا الكتاب . و هدف هذا الفصل هو استخدام تقابل جالوا للحصول على الشرط الذي يجب أن يتحقق في المعادلة القابلة للحل باستخلاص الجذور ، وبالتحديد : يجب أن تكون زمرة جالوا المقابلة للمعادلة قابلة للحل . ومن ثم فإنّنا سننشيء كثيرة حدود من الدرجة الخامسة بحيث تكون زمرة جالوا لها غير قابلة للحل ، وبهذا نبرهن على استحالة حل معادلات كثيرات الحدود من الدرجة الخامسة باستخلاص الجذور . إنّ قابلية حل زمرة جالوا هي أيضا شرط كاف لقابلية حل معادلة كثيرة الحدود باستخلاص الجذور ، ولكننا سنؤخّر ذلك إلى الفصل الخامس عشر .

شكل (٢٠). لقد اعتقد جالوا أنه وجد حلاً لمعادلة كثيرة الحدود من الدرجة الخامسة ثم غير رأيه.

(١٤,٢) امتدادات جذريّة

Radical Extensions

تحتاج صياغة فكرة «الحل باستخلاص الجذور» إلى كثير من الحذر. وسنبدأ هذه الصياغة من وجهة نظر امتدادات الحقول.

إنّ الحصول على امتداد جذري يتم باقران جذور نونية لقيم n مختلفة. على سبيل المثال العبارة التالية جذر:

$$\sqrt[3]{11}\,\sqrt[5]{\frac{7+\sqrt{3}}{2}} + \sqrt[4]{1+\sqrt[3]{4}}$$

ولإيجاد امتداد للحقل Q يحوي هذا العنصر فإننّا يجب أن نقرن كلاً من العناصر التالية على الترتيب:

$$\alpha = \sqrt[3]{11} \text{ ، } \beta = \sqrt{3} \text{ ، } \gamma = \sqrt[5]{\frac{7+\beta}{2}} \text{ ، } \delta = \sqrt[3]{4} \text{ ، } \varepsilon = \sqrt[4]{1+\delta}\ .$$

المثال أعلاه يقترح التعريف التالي:

تعريف

يسمى الامتداد $L:K$ جذريًا إذا كان $L = K(\alpha_1,\dots,\alpha_m)$ حيث لكل $i = 1,\dots,m$ فإنّه يوجد عدد صحيح $n(i)$ بحيث يكون:

$$i \ge 2\ ,\ \ \alpha_i^{n(i)} \in K(\alpha_i,\cdots,\alpha_{i-1})$$

ونقول إنّ العناصر α_i تكون متتالية جذرية للامتداد $L:K$.

وعلى سبيل المثال: العبارة أعلاه محتواة في الامتداد الجذري $Q(\alpha,\beta,\gamma,\delta,\varepsilon)$ للحقل Q حيث $\alpha^3 = 11$ ، $\beta^2 = 3$ ، $\gamma^5 = \dfrac{7+\beta}{2}$ ، $\delta^3 = 4$ ، $\varepsilon^4 = 1+\delta$

من الواضح أنّ أي عبارة جذريّة يجب أن تكون محتواة في امتداد جذري ما. وتكون كثيرة الحدود قابلة للحل باستخلاص الجذور إذا كانت جميع أصفارها عبارات جذرية على الحقل الأصلي.

تعريف

لتكن f كثيرة حدود على حقل K مميّزه صفر وليكن Σ حقل انشطار f على K.

نقول إن f قابلة للحل باستخلاص الجذور إذا وجد حقل $\Sigma \subseteq M$ بحيث يكون $M : K$ *امتداداً جذريًا .*

يجب أن نوضّح بعض الأمور المتعلقة بهذا التعريف :

أولاً: سنقصر هذا الفصل على حقول مميّزها صفر لأنّنا ولأسباب تقنية نحتاج إلى تعريف أعمّ للحل باستخلاص الجذور لو كـان مميّز الحقـل $p > 0$، ولذلك فإنّنا نستخدم في هذا الفصل حقولاً مميّزاتها أصفار وعند استخدامنا حقولاً مميزاتها ليست أصفارًا سنذكر كيفية معالجتها .

ثانيًا: يجب أن نلاحظ أنّ الامتداد $\Sigma : K$ ليس بالضرورة جذريًا ، ونحن نريد أن نعبّر عن كل شيء داخل حقل الانشطار باستخدام الجذور ، ولكننا لا نتوقع أن نعبر عن جميع هذه الأشياء باستخدام الجذر نفسه ، وإذا كـان $M : K$ جذريًا وكـان L حقلاً وسطيًا فإنّه ليس بالضرورة أن يكون $L : K$ جذريًا (انظر تمرين ٧ , ١٤) .

ثالثا: نريد التعبير عن جميع أصفار f باستخدام الجذور ، ولكن من الجائز أن تكون هناك أصفار لـ f غير قابلة للتعبير عنها باستخدام الجذور ، بكل بساطة خذ حاصل ضرب كثيرتي حدود أحدهما قابلة للحل باستخلاص الجذور والأخرى غير قابلة للحل باستخلاص الجذور . ولكن لو كـانت f لا مختزلة وكان باستطاعتنا التعبير عن أحد أصفارها باستخدام الجذور فإنّنا نستطيع أن نستنتج باستخدام نظرية (٨ , ٣) أنّه من الممكن التعبير عن جميع أصفار f باستخدام الجذور .

النظريّة الرئيسة التي سنبرهن عليها هي :

نظرية (١٤,١)

إذا كان K حقلاً مميزه صفر ، وكان $K \subseteq L \subseteq M$ *حيث* $M : K$ *امتداد جذري فإن زمرة جالوا للامتداد* $L : K$ *يجب أن تكون قابلة للحل .*

إنّ كلمة قابلة للحل المثيرة للفضول تعني : كثيرة الحدود القابلة للحل (باستخلاص الجذور) يجب أن تكون زمرة جالوا لها قابلة للحل .

إنّ برهان هذه النظرية يحتاج إلى بعض التمهيديّات .

تمهيدية (١٤,٢)

إذا كان $L:K$ امتدادًا جذريًا ، و M إغلاقًا ناظميًا للامتداد $L:K$ فإن $M:K$ امتداد جذري .

البرهان

لنفرض أنّ $L = K(\alpha_1, ..., \alpha_r)$ حيث $\alpha_i^{n(i)} \in K(\alpha_1, ..., \alpha_{i-1})$ ، ولنفرض أنّ f_i هي كثيرة حدود α_i الأصغرية على K. من الواضح أن $L \subseteq M$ هو حقل انشطار $\prod_{i=1}^{r} f_i$. لكل صفر β_{ij} لـ f_i في M يوجد تماثل $\sigma : K(\alpha_i) \to K(\beta_{ij})$ وذلك باستخدام نظرية (٣,٨) . وباستخدام قضية (٢,١٠) يوجد تماثل ذاتي $\tau : M \to M$ بالنسبة إلى K بحيث يكون τ امتداداً لـ σ . وبما أن α_i جذري على K فإن β_{ij} جذري على K ، وبالتالي فإنّ $M:K$ جذري . Δ

التمهيديتان التاليتان تبيّنان أنّ بعض زمر جالوا زمر أبيلية .

تمهيدية (١٤,٣)

ليكن K حقلاً مميزه صفر، و L حقل انشطار $t^p - 1$ ، وعلى K حيث p عدد أولي. عندئذ تكون زمرة جالوا للامتداد $L:K$ أبيلية .

البرهان

مشتقة $t^p - 1$ هي $p\,t^{p-1}$ ومنه فإنّ جميع أصفار $t^p - 1$ في L يجب أن تكون أصفارًا بسيطة، ومن الواضح أن هذه الأصفار تحت عملية الضرب تكوّن زمرة، وبما أنّ هذه الأصفار مختلفة فإنّ رتبة الزمرة هي p ، ومنه فإنّها دورية ، و لنفرض أن ε مولّد لهذه الزمرة، إذن $L = K(\varepsilon)$ ومن ثم فإنّ أي تماثل ذاتي على L بالنسبة إلى K يتحدد تماماً إذا علمنا تأثيره على ε . وكذلك فإن التماثلات الذاتية على K تبدل أصفار $t^p - 1$.
إذن إنّ أي تماثل ذاتي على L بالنسبة إلى K يجب أن يكون على الصورة:

$. \; \alpha_j : \varepsilon \to \varepsilon^j$

ومنه فإنّ $\alpha_i \alpha_j(\varepsilon) = \alpha_j \alpha_i(\varepsilon) = \varepsilon^{ij}$ وبالتالي فإن زمـرة جالوا أبيليـة . Δ

تمهيدية (١٤,٤)

لتكـن $t^n - 1$ كثيرة حدود تنشطر في حقـل K مميزه صفر . وليكـن $a \in K$ و L حقل انشطار لـ $t^n - a$ على K . عندئذ تكون زمرة جالوا للامتداد $L : K$ أبيلية .

البرهان

لنفرض أنّ α صفر لكثيرة الحدود $t^n - a$ ، وبما أنّ $t^n - 1$ تنشطر في K فإنّ أي صفر لكثيرة الحـدود $t^n - a$ يجب أن يكـون على الصورة $\varepsilon\alpha$ حيث ε صفر لكثيرة الحدود $t^n - 1$ في K ، وبما أن $L = K(\alpha)$ فإنّ أي تماثل ذاتي على L بالنسبة إلى K يتحدد تمامًا عند معرفة تأثيره على α . ليكن كل من

$$\varphi : \alpha \to \varepsilon\alpha$$

$$\psi : \alpha \to \eta\alpha$$

تماثلاً ذاتيًا بالنسبة إلى K حيث $\varepsilon, \eta \in K$. إذن

$$\varphi\psi(\alpha) = \varepsilon\eta\alpha = \eta\varepsilon\alpha = \psi\varphi(\alpha)$$

وبالتالي فإنّ زمرة جالوا أبيلية . Δ

التمهيدية التالية تزودنا بالجزء الرئيس من برهان النظريّة (١٤,١) .

تمهيدية (١٤,٥)

إذا كان K حقلاً مميّزه صفر ، وكان $L : K$ امتدادًا ناظميًا وجذريًا فإنّ $\Gamma(L:K)$ قابلة للحل .

البرهان

لنفـرض أنّ $L = K(\alpha_1, ..., \alpha_n)$ حيـث $\alpha_i^{n(i)} \in K(\alpha_1, ..., \alpha_{i-1})$.

وبإدخال عناصر α_j عند الضرورة نستطيع أن نفرض أنّ $n(i)$ عدد أولي لكل i . وبصورة خاصة نستطيع ايجاد عدد أولي p بحيث يكون $\alpha_1^p \in K$.

سنستخدم الاستنتاج الرياضي على n والفرض أن n(i) عدد أولي لكل i ، ومن الواضح أنّ التمهيدية محققة عند $n = 0$ ، وإذا كان $\alpha_1 \in K$ فإن $L = K(\alpha_2, ..., \alpha_n)$ ومنه $\Gamma(L : K)$ قابلة للحل بالاستنتاج الرياضي، لنفرض إذن أنّ $\alpha_1 \notin K$ ، ولتكن f هي كثيرة حدود α_1 الأصغرية على K، وبما أنّ $L : K$ ناظمي فإنّ f تنشطر في L . وبما أنّ مميز K صفر فإنّ $L : K$ قابل للفصل ومنه فإنّ جميع أصفار f بسيطة. وبما أنّ $\alpha_1 \notin K$ فإنّ درجة f أكبر أو تساوي 2 ، ولنفرض أنّ β صفر لـ f و $\alpha_1 \neq \beta$. وليكن $\varepsilon = \alpha_1 / \beta$. إذن $\varepsilon^p = 1$ و $\varepsilon \neq 1$ ، ومنه فإنّ رتبة ε هي p في زمرة L الضربية ، ومنه فإنّ $1, \varepsilon, \varepsilon^2, ..., \varepsilon^{p-1}$ هي $\sqrt[p]{1}$ المختلفة في L . إذن $t^p - 1$ تنشطر في L .

لنفرض أنّ M حقل جزئي من L بحيث يكون حقل انشطار $t^p - 1$ على K ، أي أنّ $M = K(\varepsilon)$. اعتبر سلسلة الحقول الجزئية $K \subseteq M \subseteq M(\alpha_1) \subseteq L$.

الشكل التالي يوضح لنا الاستراتيجية التي سنتبّعها في ما تبقى من البرهان

L
$|$ $\longrightarrow$ $\Gamma(L : M(\alpha_1))$ قابلة للحل بفرضية الاستنتاج
$M(\alpha_1)$
$|$ $\longrightarrow$ $\Gamma(M(\alpha_1) : M)$ أبيلية باستخدام تمهيدية (٤ , ١٤)
M
$|$ $\longrightarrow$ $\Gamma(M : K)$ أبيلية باستخدام تمهيدية (٣ , ١٤)
K

لاحظ أنّ $L : K$ منته ، ناظمي وقابل للفصل وبالتالي فإنّ $L : M$ كذلك ، ومن ثم فإنّه يمكن استخدام نظرية (١ , ١١) على كل من $L : K$ و $L : M$.

بما أنّ $t^p - 1$ تنشطر في M و $\alpha_1^p \in M$ فإنّ برهان التمهيدية (٤ , ١٤) يضمن لنا أنّ $M(\alpha_1)$ حقل انشطار $t^p - \alpha_1^p$ على M . إذن $M(\alpha_1) : M$ ناظمي ، وباستخدام تمهيدية (٤ , ١٤) نجد أنّ $\Gamma(M(\alpha_1) : M)$ أبيلية . وبتطبيق نظرية (١ , ١١) على $L : M$ نحصل على :

$$\Gamma(M(\alpha_1) : M) \cong \Gamma(L : M) / \Gamma(L : M(\alpha_1)) .$$

بما أنّ $L = M(\alpha_1)(\alpha_2, ..., \alpha_n)$ فإن $L : M(\alpha_1)$ امتداد جذري وناظمي. وباستخدام فرضية الاستنتاج نجد أنّ $\Gamma(L : M(\alpha_1))$ قابلة للحل. ومن ثم باستخدام نظرية (٢، ١٣) (٣) نجد أن $\Gamma(L : M)$ قابلة للحل، و بما أنّ M حقل انشطار $t^p - 1$ على K فإن $M : K$ امتداد ناظمي. وباستخدام تمهيدية (٣، ١٤) نجد أنّ $\Gamma(M : K)$ أبيلية. وبتطبيق نظرية (١، ١١) على الامتداد $L : K$ نحصل على:

$$\Gamma(M : K) \cong \Gamma(L : K) / \Gamma(L : M) .$$

وباستخدام نظرية (٢، ١٣) (٣) نجد أنّ $\Gamma(L : K)$ قابلة للحل وبهذا تتم خطوة الاستنتاج. Δ

نستطيع الآن أن نبرهن النظريّة الرئيسة.

برهان النظرية (١، ١٤)

ليكن K_0 هو الحقل الثابت لزمرة جالوا $\Gamma(L : K)$ و $N : M$ إغلاق ناظمي للامتداد $M : K_0$. إذن

$$K \subseteq K_0 \subseteq L \subseteq M \subseteq N .$$

وبما أنّ $M : K_0$ امتداد جذري فإنّ $N : K_0$ امتداد جذري ناظمي وذلك باستخدام التمهيدية (٢، ١٤)، وباستخدام التمهيدية (٥، ١٤) نجد أنّ $\Gamma(N : K_0)$ قابلة للحل.

الامتداد $L : K_0$ ناظمي وذلك باستخدام نظريّة (١٠، ١٠)، وباستخدام نظريّة (١، ١١) نجد أنّ:

$$\Gamma(L : K_0) \cong \Gamma(N : K_0) / \Gamma(N : L)$$

وباستخدام نظرية (٢، ١٣) (٢) نجد أنّ $\Gamma(L : K_0)$ قابلة للحل. ولكن $\Gamma(L : K) = \Gamma(L : K_0)$. إذن $\Gamma(L : K)$ قابلة للحل. Δ

الفكرة وراء هذا البرهان فكرة بسيطة: الامتداد الجذري هو عبارة عن سلسلة من الامتدادات باقران جذور نونية، وزمرة جالوا لهذه الامتدادات أبيلية. إذن زمرة جالوا للامتدادات الجذرية تتكون من متتالية من الزمر الأبيلية، ولكن لسوء الحظ هناك مشكلة تقنية في البرهان وذلك لأنّنا نحتاج لأن نقرن جذور الوحدة ونجعل بعض

الامتدادات ناظمية قبل أن نستطيع استخدام تقابل جالوا.

والآن ندرس عملية الانتقال من الحقول إلى كثيرات الحدود وبعمل هذه الدراسة نكون قد تبنينا وجهة نظر جالوا الأصلية.

تعريف

لتكن f كثيرة حدود على الحقل K وليكن Σ حقل انشطار f على K. تعرف زمرة جالوا لـ f على K بأنها الزمرة $\Gamma(\Sigma : K)$.

لتكن G هي زمرة جالوا لكثيرة الحدود f على الحقل K. إذا كان $\alpha \in \Sigma$ صفرًا لـ f فإنّ $f(\alpha) = 0$. إذن لكل $g \in G$ لدينا:

$$f(g(\alpha)) = g(f(\alpha)) = 0.$$

إذن نستنتج أنّ كل عنصر $g \in G$ يعطينا تبديلاً g' لأصفار f في Σ، وبما أنّ Σ مُوَلَّد من أصفار f فإنّ كل عنصرين مختلفين من G يؤديان إلى تبديلين مختلفين. ونستنتج الآن بسهولة أنّ الدالة $g \to g'$ تشاكل متباين من G إلى زمرة تبديلات أصفار f. وبكلام آخر فإنّنا نستطيع اعتبار G على أنها زمرة تبديلات أصفار f. وبهذه الطريقة عرّف جالوا زمرة جالوا، ولسنوات كثيرة بعد ذلك لم يدرس الرياضيون زمرًا غير زمر التبديلات، إلى أن جاء كيلي (Cayley) وقدّم الزمرة بصورتها المجرّدة، على الرغم من أنّ العالم كرونكر (Kronecker) كان قدم في العام ١٨٧٠م نظام مسلمات للزمر [انظر Hutingdon, 1905].

ونستطيع الآن أن نعيد نص النظريّة (١٤,١) كالتالي:

نظرية (١٤,٦)

لتكن f كثيرة حدود على حقل K مميزه صفرًا، و إذا كانت f قابلة للحل باستخلاص الجذور فإنّ زمرة جالوا لها على K قابلة للحل.

[إنّ عكس هذه النظرية صحيح أيضًا: أنظر نظريّة (١٥,١١)].

بناءً على ما تقدم: لايجاد كثيرة حدود غير قابلة للحل باستخلاص الجذور فإنّه يكفي أن نجد واحدة بحيث تكون زمرة جالوا لها غير قابلة للحل . وهناك طريقتان رئيستان لإيجاد ذلك. **الأولى:** هي النظر إلى ما يسمى كثيرة الحدود العامة من الدرجة n (ندرسها في الفصل الخامس عشر) ، و أحد عيوب هذه الطريقة أنّها لا تبرهن لنا على وجود كثيرات حدود بمعاملات كسرية بحيث تكون غير قابلة للحل باستخلاص الجذور. **والطريقة الثانية:** والتي ستتبنّاها هنا هي أن نجد كثيرة حدود بمعاملات كسرية معينة بحيث تكون زمرة جالوا لها غير قابلة للحل. وبما أنّ زمر جالوا صعبة الإيجاد فإنّنا نحتاج إلى شيء من البراعة مع المعرفة التامة بزمر التبديلات، وكذلك يجب علينا الاستعانة بالنظريّة الأساسيّة للجبر.

(١٤,٣) كثيرة حدود خماسية الدرجة غير قابلة للحل

An Insoluble Quintic

لاحظ جيدًا: لا يوجد شيء تحت كم قميصي . . .

تمهيدية (١٤,٧)

ليكن p عددًا أوليًا ، و f كثيرة حدود لا مختزلة درجتها p على Q. إذا كان عدد أصفار f غير الحقيقية في $\mathbb{C}$ هو 2 بالضبط فإنّ زمرة جالوا لـ f على Q هي زمرة التبديلات S_p.

البرهان

باستخدام النظرية الأساسية للجبر فإنّ $\mathbb{C}$ يحتوي على حقل انشطار Σ لـ f . لتكن G هي زمرة جالوا لـ f على Q باعتبارها زمرة تبديلات أصفار f. إنّ جميع هذه الأصفار مختلفة وذلك لأنّ مميز Q صفر. إذن G زمرة جزئية من S_p . ولكن عند

إنشاء حقل انشطار لـ f فإننا نقرن أولاً عنصرًا درجته p ، أي أن $[\Sigma : Q]$ يقسم على p . وباستخدام نظريّة (١ , ١١) (١) نجد أن p يقسم $|G|$ ، وباستخدام نظريّة (١٤ , ١٣) نجد أنّ G تحتوي على عنصر من الرتبة p . ولكن العناصر التي رتبتها p في S_p هي فقط الدورات التي رتبتها p .

بما أنّ أخذ المرافق في $\mathbb{C}$ يعطينا تماثلاً ذاتيًا على $\mathbb{C}$ بالنسبة إلى Q فإنّنا نجد أنّ هذا يعطينا أيضًا تماثلاً ذاتيًا على Σ بالنسبة إلى Q . وهذا التماثل يبقي الأصفار الحقيقية لـ f وعددها $p - 2$ ثابتة وينقل أحد الأصفار غير الحقيقية إلى الصفر الآخر . إذن G تحتوي على مناقلة . وبدون التأثير على الحالة العامة فإننا نستطيع أن نفرض أن G تحتوي (12) و $(123 \dots p)$. وباستخدام تمهيدية (٦ , ١٣) نجد أنّ هذين العنصرين يولّدان S_p . إذن $G = S_p$. Δ

ونستطيع الآن تقديم كثيرة حدود من الدرجة الخامسة غير قابلة للحل باستخلاص الجذور .

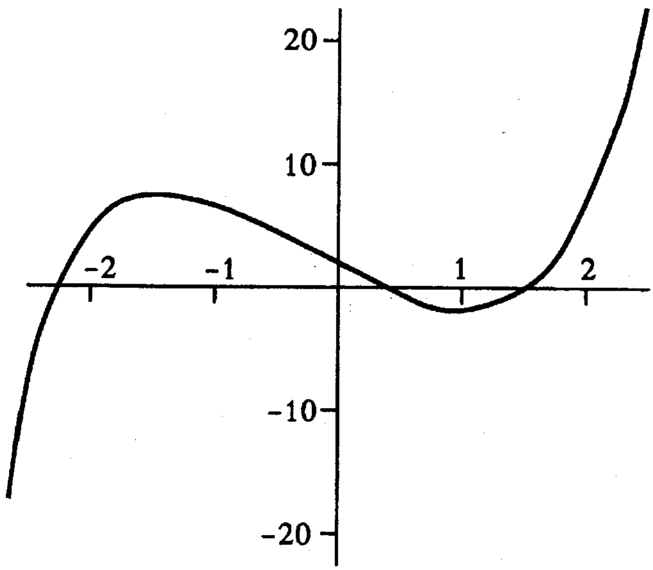
نظرية (١٤,٨)

كثيرة الحدود $t^5 - 6t + 3$ على Q غير قابلة للحل باستخلاص الجذور .

البرهان

لتكن $f(t) = t^5 - 6t + 3$. باستخدام ميزان ايزنستاين نجد أنّ f لا مختزلة على Q ، وسنبرهن أنّ عدد أصفار f الحقيقية هو 3 وهذه الأصفار جميعها بسيطة وبالتالي فإن هناك صفرين غير حقيقين لـ f ، وبما أنّ 5 عدد أولي فإنّه ينتج من تمهيدية (١٤ , ٧) أنّ زمرة جالوا لـ f على Q هي S_5 ، وباستخدام نتيجة (١٣ , ٥) S_5 غير قابلة للحل . وباستخدام نظرية (١٤ , ٦) نجد أنّ f غير قابلة للحل باستخلاص الجذور .

يبقى أن نبرهن على أنّ عدد أصفار f الحقيقية هي 3 ، وجميعها بسيطة . الآن $f(-2) = -17$ ، $f(-1) = 8$ ، $f(0) = 3$ ، $f(1) = -2$ و $f(2) = 23$. الشكل (٢١) هو منحنى المعادلة $y = f(x)$.



شكل (٢١). كثيرة حدود من الدرجة الخامسة لها ثلاثة أصفار حقيقية.

من الشكل يظهر أنّ عدد أصفار f الحقيقية هو 3 ، ولكنّنا يجب أن نكون دقيقين ، وباستخدام نظريّة رول نجد أنّ أصفار f يجب أن تكون مفصولة بأصفار Df، ولكنّ $Df = 5t^4 - 6$ لها الصفران $\pm\sqrt[4]{6/5}$. وبما أنّ f و Df أوليتان نسبياً فإنّ جميع أصفار f يجب أن تكون بسيطة (وذلك لأن f لا مختزلة ومميز Q صفر). إذن عدد أصفار f الحقيقية على الأكثر 3، وبما أنّ الدالة المتّصلة المعرّفة على الأعداد الحقيقية لا يمكن أن تتغير إشارتها إلاّ إذا قطعت محور السينات فإنّنا نجد أن عدد أصفار f على الأقل 3 . بل عدد أصفار f الحقيقية هو بالضبط 3 ، وبهذا نكون قد أنهينا البرهان . Δ

من المؤكد أن هذا ليس هو نهاية القصة، وأنّ طرق قتل كثيرة حدود من الدرجة الخامسة أكثر من طرق خنقها باستخلاص الجذور . ولإثباتنا لعدم صلاحية استخلاص الجذور لحل المسألة فمن الطبيعي أن نحاول ايجاد طرق أعم لحل هذه المسألة .

وعلى المستوى الدنيوي فإنّ طرق التحليل العددي ملائمة لايجاد أصفار كثيرة الحدود (في $\mathbb{R}$ أو $\mathbb{C}$) لأيّ درجة تقريبية نحتاجها ، وهذه طريقة عملية مفيدة (بالحقيقة هي الطريقة العملية الوحيدة). وإنّ النظريّة الرياضيّة التي تكمن وراء هذه الطرق العددية أبعد من أن تكون مجرد نظريّة دنيويّة ، ولكنها لا تعطي الاستنارة العقلية من وجهة النظر الجبرية.

وطريقة أخرى لحل هذه المسألة تكمن في السؤال :

ما هي الخاصيّة المهمة التي تتمتع بها عمليّة استخلاص الجذور ؟

لنفرض أنّنا عرّفنا أي عدد حقيقي a فوق الجذر $\sqrt[*]{a}$ بأنّه الصفر الحقيقي لكثيرة الحدود $t^5 + t - a$. لقد برهن جيرارد (Jerrard) [انظر : Kollros, 1949] على أنّ معادلة كثيرة الحدود من الدرجة الخامسة قابلة للحل باستخدام الجذور وفوق الجذور ، وبدلاً من اكتشاف طرق وقواعد جديدة فإن باستطاعتنا أن نعدّل القواعد المعروفة لدينا .

وقد اكتشف العالم هيرمايت (Hermite) أنّه من الممكن حل معادلة كثيرة الحدود من الدرجة الخامسة باستخدام الدوال القياسيّة الناقصية ، وهذه عبارة عن دوال خاصة في الرياضيات التقليدية تظهر في مجال من الرياضيات مختلف تمامًا (تكامل الدوال الجبريّة) ، وهذه الطريقة تحاكي طريقة حل معادلة الدرجة الثالثة باستخدام حساب المثلثات المعروفة . وللتأكيد على وحدة أفرع الرياضيات حقق العالم كلاين (Klein) نجاحًا في ربط معادلات الدرجة الخامسة ، والدوال الناقصية ، وزمرة دورانات عشروني الوجوه المنتظم مع بعضها . والزمرة الأخيرة هذه تماثل الزمرة A_5 والتي في رأينا تلعب دورًا رئيسًا في مسألة معادلة الدرجة الخامسة . ولقد ساعد اكتشاف كلاين هذا على توضيح العلاقة غير المتوقعة بين الدوال الناقصية ونظرية معادلات كثيرات الحدود . و استطاع بعد ذلك العالم بوينكار (Boincare') تعميم هذه الأفكار لتشمل كثيرات الحدود بأية درجة . ودور عشروني الوجوه موضّح في [Klein, 1913] .

ولزمرة جالوا الكثيرة حدود لا مختزلة خاصيّة مهمة سنسجلها هنا ولكنّنا نحتاج قبل ذلك إلى :

تعريف

لتكن G زمرة التبديلات على $\{1, ..., n\}$. نقول إن G متعدية إذا وجد $\gamma \in G$ بحيث يكون $\gamma(i) = j$ لكل $i, j \le n$.

ومكافيء لذلك يكفي أن نثبت إنه لكلّ $i \le n$ ، فإنّه يوجد $\gamma \in G$ بحيث أنّ $\gamma(1) = i$ وذلك لأنه عندئذ نستطيع ايجاد $\delta \in G$ بحيث يكون $\delta(1) = j$ وبالتالي فإنّ $(\delta\gamma^{-1})(i) = j$.

أمثلة

(١) زمرة كلاين الرباعية V متعدية على $\{1,2,3,4\}$. لأنّ

$$(1)[1] = 1$$

$$(12)(34)[1] = 2$$

$$(13)(24)[1] = 3$$

$$(14)(23)[1] = 4$$

(٢) الزمرة الدورية المولّدة بالعنصر $\alpha = (1234)$ متعدية على $\{1,2,3,4\}$. في الحقيقة $\alpha^{i}(1) = i$ لكل $i = 1,2,3,4$.

(٣) الزمرة الدورية المولّدة بالعنصر $\beta = (123)$ ليست متعدية على $\{1,2,3,4\}$ لأنّه لا يوجد i بحيث يكون $\beta^{i}(1) = 4$.

قضية (٩,١٤)

زمرة جالوا لكثيرة حدود لا مختزلة p متعدية على مجموعة أصفار p .

البرهان

لنفرض أن كلاً من α و β صفرًا لكثيرة الحدود p . لاحظ أنّ p هي كثيرة حدود

كل من α و β الأصغرية، و باستخدام نظرية (٨ , ٣) ونظرية (٢ , ١٠) نستطيع إيجاد عنصر γ في زمرة جالوا بحيث يكون $\gamma(\alpha) = \beta$. Δ

تمـارين

(١٤ , ١) إذا لم يسبق (أونسيت) حل معادلات الدرجة الثالثة والرابعة باستخلاص الجذور فحاول أن تحلهما (سنقدم طريقة حل في الفصل الخامس عشر).

(١٤ , ٢) جد امتدادًا جذريًا للحقل Q يحتوي على العناصر التالية في $\mathbb{C}$:

(أ) $\left(\sqrt{11} - \sqrt[7]{23}\right) / \sqrt[4]{5}$

(ب) $\left(\sqrt{6} + 2\sqrt[3]{5}\right)^4$

(ج) $\left(2\sqrt[5]{5} - 4\right) / \sqrt{1 + \sqrt{99}}$

(١٤ , ٣) ما هي زمرة جالوا لكثيرة الحـدود $t^p - 1$ على Q للعـدد الأولي p ؟

(١٤ , ٤) اثبت أنّ كلاً من كثيرات الحدود التالية على Q غير قابلة للحل باستخلاص الجذور :

$$t^5 - 4t + 2$$

$$t^5 - 4t^2 + 2$$

$$t^5 - 6t^2 + 3$$

$$t^7 - 10t^5 + 15t + 5$$

(١٤ , ٥) حل معادلة الدرجة السادسة

$$t^6 + 2t^5 - 5t^4 + 9t^3 - 5t^2 + 2t + 1 = 0$$

باستخلاص الجذور (**إرشاد** : ضع $u = t + 1/t$).

(١٤ , ٦) إذا كان $L : K$ امتدادًا جذريًا وكان M حقلاً وسطيًا فاثبت أنّه ليس بالضرورة

أن يكون $M : K$ امتدادًا جذريًا .

(١٤ , ٧) إذا كانت p كثيرة حدود على K وكان من الممكن التعبير عن أحد أصفارها بدلالة جذور فأثبت أنه يمكن التعبير عن كل صفر من أصفارها بدلالة جذور .

(١٤ , ٨) ضع علامة صح أو خطأ أمام كل مما يأتي :

(ا) جميع معادلات الدرجة الرابعة على حقل مميزه صفر قابلة للحل باستخلاص الجذور .

(ب) جميع الامتدادات الجذرية منتهية .

(ج) جميع الامتدادات المنتهية جذرية .

(د) رتبة زمرة جالوا لكثيرة حدود من الدرجة n تقسم $n!$.

(هـ) جميع كثيرات الحدود من الدرجة الخامسة القابلة للاختزال يمكن حلها باستخلاص الجذور .

(و) يوجد كثيرة حدود من الدرجة الرابعة بحيث تكون زمرة جالوا لها هي S_4.

(ز) زمرة جالوا لكثيرة حدود لا مختزلة من الدرجة 11 والتي لها صفران غير حقيقين فقط هي S_{11} .

(ح) الاغلاق الناظمي للامتداد الجذري يجب أن يكون جذرياً .

(ط) $|A_5| = 60$.

(١٤ , ٩)* ليكن K حقلاً مميّزه صفر ، و t متساميًا على K . اعتبر المعادلات (في x,y,z) :

$$x^2 = y + t$$
$$y^2 = z + t \qquad (١٤ , ١)$$
$$z^2 = x + t \, .$$

برهن على أنّ أيّ حل x في امتداد ما إمّا أن يحقق $x^2 = x + t$ أو يحقق معادلة من الدرجة السادسة على $K(t)$. وبرهن على أن مجموعة أصفار

المعادلة من الدرجة السادسة التي وجدتها يمكن تجزئتها إلى مجموعتين كل منهما تحتوي على ثلاثة عناصر ، وهذه الأصفار إما أن تبقى ثابتة أو تتبدل فيما بينها تحت تأثير التماثلات الذاتية لحقل الانشطار ، ومن ثم حل المعادلات (١٤ , ١) باستخلاص الجذور . [انظر : Ramanujan, 1962] .

(١٤ , ١٠)* إذا كانت C_2 هي زمرة جالوا للامتداد $L : K$ فاثبت أنّها ناظميّة ، وإذا كان مميّز K لا يساوي 2 فاثبت أنّ $L = K(\alpha)$ حيث $\alpha^2 \in K$.

(١٤ , ١١)* لنفرض أنّ $L : K$ نا ظمي وقابل للفصل ودرجته 4 وزمرة جالوا له هي $C_2 \times C_2$ و مميّز K لا يساوي 2 ؛ أثبت أنّ $L = K(\alpha,\beta)$ حيث $\alpha^2, \beta^2 \in K$.

(١٤ , ١٢)* وبالعكس إذا كان مميّز K لا يساوي 2 ، $\alpha^2 = a \in K$ و $\beta^2 = b \in K$ وجميع العناصر a,b,ab ليست مربّعات في K فاثبت أنّ زمرة جالوا للامتداد $K : K(\alpha,\beta)$ هي $C_2 \times C_2$.

(١٤ , ١٣)* إذا كان N عددًا صحيحًا كبيرًا لدرجة مقبولة و p عددًا أوليًا فاثبت استحالة حل كثيرة الحدود $x(x - Np^2)(x + Np^2)(x^2 + N^2p^4) + p$ باستخلاص الجذور .

(١٤ , ١٤)* ليكن p عددًا أوليًا فرديًا وليكن $\varepsilon = \sqrt[p]{1}$ عددًا غير حقيقي ، أثبت أنّ زمرة جالوا للامتداد $Q : Q(\varepsilon)$ تماثل الزمرة الضربية $\mathbb{Z}_p \setminus \{0\}$ ، ومن ثم فهي دورية . وأثبت أنّه يوجد حقل جزئي وحيد K من $Q(\varepsilon)$ بحيث يكون $[K : Q] = 2$. إفرض أنّ Γ هي زمرة جالوا للامتداد $Q : Q(\varepsilon)$ و χ هو

التشاكل الوحيد $\Gamma \rightarrow \{\pm 1\}$. ضع $\alpha = \sum_{s=1}^{p-1} \chi(s)\varepsilon^{s}$. أثبت أن

$\alpha \notin Q$ ، $\alpha^2 \in Q$ و $\alpha^2 = (-1)^{\frac{p-1}{2}} p$ ومن ثم برهن على أنّ

$K = Q(\alpha)$.

الفصل الخامس عشر

معادلة كثيرة الحدود العامة

The General Polynomial Equation

إنّ ما نسميه «كثيرة الحدود العامة» ما هي في الحقيقة إلاّ كثيرة حدود خاصة جدًا حيث لا تحقق معاملاتها أي علاقة جبرية Q، وهذه الخاصية تجعل دراستها أسهل من دراسة كثيرة الحدود على Q، وعلى وجه الخصوص فإنّ حساب زمرة جالوا لها أسهل من حسابها لكثيرة حدود على Q، وكنتيجة لذلك نستطيع أن نبرهن على عدم وجود حل لكثيرة الحدود العامة من الدرجة الخامسة باستخلاص الجذور، وذلك دون الحاجة إلى الاستعانة بكثير من نتائج نظريّة الزمر كما فعلنا في الفصل الرابع عشر. وبهذا يكون باستطاعتنا البرهان على عدم وجود صيغة عامة لحل جميع معادلات الدرجة الخامسة باستخلاص الجذور. وبما أنّ ذلك لا يمنع مسبقًا احتمال وجود حلول باستخلاص الجذور لجميع كثيرات الحدود من الدرجة الخامسة التي لا يمكن وضعها بصيغة عامة واحدة فإنّ نتائج هذا الفصل ليست بقوة النتائج التي حصلنا عليها في الفصل الرابع عشر. ومن الظاهر أنّ زمرة جالوا لكثيرة الحدود العامة من الدرجة n هي S_n، وهذا يبرهن لنا مباشرةً استحالة حل كثيرة الحدود العامة من الدرجة الخامسة. وسنستخدم معرفتنا بخواص S_2، S_3 و S_4 لإيجاد طرق لحل معادلات الدرجة الثانية، الثالثة والرابعة العامة.

(١٥,١) درجات التسامي

Transendence Degrees

وحتى الآن لم نحتج للتعامل مع الامتدادات المتسامية كثيرًا. وفي الحقيقة إن فرضية إنّ الامتدادات منتهية لعبت دورًا مهمًا جدًا في دراستنا. وسنقدم الآن طائفة

أوسع من الامتدادات التي لا تزال تغلب عليها صفة الانتهاء.

تعريف

نقول إن الامتداد $L : K$ منتهي التوليد إذا كان $L = K(\alpha_1,...,\alpha_n)$ حيث n عدد صحيح موجب.

لاحظ أنّ α_i من الممكن أن يكون جبريًا أو متساميًا على K.

تعريف

لتكن العناصر $t_1,...,t_n$ متسامية على الحقل K وتنتمي إلى امتداد حقلي L لـ K. نقول إن هذه العناصر مستقلة إذا لم يوجد كثيرة حدود غير صفرية p على K (في n من المجاهيل) بحيث يكون

$$p(t_1,...,t_n) = 0$$

في L.

على سبيل المثال، إذا كان t متساميًا على K، وكان u متساميًا على K(t) فإنّ K(t,u) امتداد منتهي التوليد للحقل K، وأنّ t,u مستقلان. ومن ناحية أخرى t و t + 1 كلاهما متسام على K ولكنهما ليسا مستقلين.

التمهيدية التالية تزوّدنا بمعلومات عن بنية الامتدادات المنتهية التوليد.

تمهيدية (١٥,١)

إذا كان $L : K$ امتدادًا منتهي التوليد فإنه يوجد حقل وسطي M بحيث يكون:

(١) $M = K(\alpha_1,...,\alpha_1)$ حيث α_i مستقلة ومتسامية على K.

(٢) $L : M$ امتداد منته.

البرهان

بما أنّ L : K منتهي التوليد فإنّ $M = K(\beta_1,...,\beta_n)$، وإذا كان كل من β_i جبريًا على K فإنّ L : K منته وذلك باستخدام تمهيدية (٤ , ٤)، وبالتالي نأخذ

$M = K$. لنفرض إذًا أنّ أحد هذه العناصر وليكن β_j متساميًا على K . ضع $\alpha_1 = \beta_j$. إذا كان $L : K(\alpha_1)$ ليس منتهياً فإنّنا نستطيع إيجاد عنصر β_k متسامياً على $K(\alpha_1)$. ضع $\alpha_2 = \beta_k$. وبالاستمرار على هذا المنوال نحصل على $M = K(\alpha_1,...,\alpha_r)$ بحيث يكون الامتداد $L : M$ منتهيًا . من الواضح أن α_i عناصر مستقلة ومتسامية على K . Δ

التمهيدية التالية تنسب إلى ستاينز (Steinitz) وتبرهن لنا على أنّ عدد العناصر المستقلة المتسامية لا تعتمد على اختيار M .

تمهيدية (١٥,٢) (ستاينز)

باستخدام ترميز تمهيدية (١٥ , ١) إذا كان $N = K(\beta_1,...,\beta_s)$ *حقلاً وسطيًا آخر بحيث تكون* $\beta_1,...,\beta_s$ *مستقلة ومتسامية على* K *وكان* $L : N$ *منتهيًا فإنّ* $r = s$.

البرهان

بما أنّ $[L : M]$ منته، و β_1 جبري على M فإنّنا نستطيع الحصول على معادلة كثيرة حدود:

$$p(\beta_1, \alpha_1, ..., \alpha_r) = 0 \ .$$

يوجد i بحيث يظهر α_i في هذه المعادلة . وبدون التأثير على الحالة العامة نستطيع أن نفرض أنّ $\alpha_i = \alpha_1$. إذن α_1 جبري على $K(\beta_1, \alpha_2, ..., \alpha_r)$ و $L : K(\beta_1, \alpha_2, ..., \alpha_r)$ منته . وباستخدام الاستنتاج نستطيع أن نستبدل كلاً من α_i بـ β_i لنحصل على الامتداد المنته

$$L : K(\beta_1, ..., \beta_r) \ .$$

إذا كان $s > r$ فإنّ β_{r+1} يجب أن يكون جبريًا على $K(\beta_1, ..., \beta_r)$ ، وهذا مستحيل . إذن $s \le r$ وبالطريقة نفسها $r \le s$ وبهذا يتم البرهان . Δ

تعريف

يسمى العدد r *الذي حصلنا عليه في التمهيدية (١٥ , ١) بدرجة التسامي*

للامتداد $L : K$.

ليكن لدينا على سبيل المثال الامتداد $K(t, \alpha, u) : K$ حيث t متسام على K ، $t = \alpha^2$ و u متسام على $K(t, \alpha)$. إذن $M = K(t,u)$ حيث t ، u عنصران مستقلان ومتساميان على K والامتداد

$$K(t,\alpha,u) : M = M(\alpha) : M$$

منته . إذن درجة التسامي هي 2 .

إذا كان $K(\alpha_1, ..., \alpha_r) : K$ امتدادًا بحيث إنّ α_i عناصر مستقلة ومتسامية فإنّه من السهولة استخدام الاستنتاج الرياضي لإثبات أنّ هذا الامتداد يماثل الامتداد $K(t_1, ..., t_r) : K$ حيث $K(t_1, ..., t_r)$ هو حقل العبارات الكسرية في المجاهيل t_i .

(١٥,٢) كثيرة الحدود العامة

The General Polynomial

ليكن K حقلاً و $t_1, ..., t_n$ عناصر مستقلة ومتسامية على K ، ومن الممكن النظر إلى الزمرة S_n على أنّها زمرة تماثلات ذاتية على الحقل $K(t_1, ..., t_n)$ بالنسبة إلى K وذلك بتعريف

$$\sigma(t_i) = t_{\sigma(i)}$$

لكل $\sigma \in S_n$. على سبيل المثال إذا كان $n = 4$ و $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ فإنّ $\sigma(t_1) = t_2$ ، $\sigma(t_2) = t_4$ ، $\sigma(t_3) = t_3$ و $\sigma(t_4) = t_1$. ومن ذلك نستطيع حساب $\sigma\left(\frac{t_1^5 t_4}{t_2^4 - 7t_3}\right)$ على سبيل المثال كالتالي :

$$\sigma\left(\frac{t_1^5 t_4}{t_2^4 - 7t_3}\right) = \frac{t_2^5 t_1}{t_4^4 - 7t_3}$$

ومن الواضح أنّ العناصر المختلفة في S_n تعطينا تماثلات ذاتية مختلفة بالنسبة إلى K ، ومن الواضح أيضًا أنّ حقل S_n الثابت F يحتوي على جميع كثيرات الحدود المتناظرة في t_i ، وعلى وجه الخصوص يحتوي على كثيرات الحدود المتناظرة الابتدائية. $s_r = s_r(t_1,\ldots,t_n)$. سنبرهن أن كثيرات الحدود المتناظرة الابتدائية هذه تولد F .

تمهيدية (١٥و٣)

باستخدام الترميز أعلاه يكون $F = K(s_1,\ldots,s_n)$.

البرهان

نستخدم الاستنتاج الرياضي على n لنبرهن على أنّ

$$[K(t_1,\ldots,t_n) : K(s_1,\ldots,s_n)] \le n!\,.$$

اعتبر

$$K(t_1,\ldots,t_n) \supseteq K(s_1,\ldots,s_n,t_n) \supseteq K(s_1,\ldots,s_n)$$

بما أنّ $f(t_n) = 0$ حيث $f(t) = t^n - s_1 t^{n-1} + \ldots + (-1)^n s_n$ فإنّ

$$[K(s_1,\ldots,s_n,t_n) : K(s_1,\ldots,s_n)] \le n\,.$$

وإذا فرضنا أنّ $s'_1,\cdots,s'_{n-1}$ هي كثيرات الحدود المتناظرة الابتدائية في $t_1,\ldots,t_{n-1}$ فيكون لدينا

$$s_j = t_n s'_{j-1} + s'_j$$

إذن

$$K(s_1,\cdots,s_n,\ t_n) = K(t_n,\ s'_1,\cdots,s'_{n-1})$$

وباستخدام فرضية الاستنتاج نحصل على :

$$\begin{aligned}[K(t_1,\ldots,t_n) &: K(s_1,\ldots,s_n,t_n)]\\ &= [K(t_n)(t_1,\ldots,t_{n-1}) : K(t_n)(s'_1,\ldots,s'_{n-1})]\\ &\le (n-1)!\end{aligned}$$

وباستخدام قانون البرج نحصل على المطلوب.

ومن الواضح أنّ $K(s_1,\ldots,s_n)$ محتوى في حقل S_n الثابت F . باستخدام نظرية (٤ , ٩) نحصل على

$$[K(t_1,\ldots,t_n):F] = |S_n| = n!.$$

إذن $F = K(s_1,\ldots,s_n)$. Δ

نتيجة (١٥,٤)

من الممكن كتابة أي كثيرة حدود متناظرة في $t_1,\ldots,t_n$ على K كعبارة كسرية في $s_1,\ldots,s_n$.

البرهان

كثيرات الحدود المتناظرة تنتمي للحقل الثابت F . Δ

[يجب على القاريء أن يقارن النتيجة أعلاه مع النظرية (٩ , ٢)].

تمهيدية (١٥,٥)

باستخدام الترميز أعلاه تكون $s_1,\ldots,s_n$ عناصر مستقلة متسامية على K .

البرهان

$K(t_1,\ldots,t_n)$ امتداد منته للحقل $K(s_1,\ldots,s_n)$ وبذلك فإنّ لهما درجة التسامي نفسها على K وبالتحديد n . إذن العناصر s_i مستقلة لأنّه لو كانت غير مستقلة فإنّ درجة تسامي الامتداد: $K(s_1,\ldots,s_n)$ تكون أقل من n . Δ

تعريف

ليكن K حقلاً و $s_1,\ldots,s_n$ عناصر مستقلة ومتسامية على K. كثيرة الحدود العامة من الدرجة n «على» K هي كثيرة الحدود

$$t^n - s_1t^{n-1} + s_2t^{n-2} - \cdots + (-1)^n s_n$$

على الحقل $K(s_1,\ldots,s_n)$.

لقد استخدمنا علامتي الاقتباس لأن كثيرة الحدود هذه معرّفة على $K(s_1,\ldots,s_n)$ وليس على K .

نظرية (١٥,٦)

ليكن K حقلاً و g كثيرة الحدود العامة من الدرجة n «على» K وليكن Σ حقل انشطار g على $K(s_1,\ldots,s_n)$ و $t_1,\ldots,t_n$ هي أصفار g في Σ . عندئذ تكون هذه الأصفار مستقلة ومتسامية على K وزمرة جالوا للامتداد $\Sigma : K(s_1,\ldots,s_n)$ هي الزمرة S_n.

البرهان

باستخدام نظرية (٤ , ٨) نجد أنّ الامتداد $\Sigma : K(s_1,\ldots,s_n)$ امتدادًا منتهيًا، ومنه فإنّ درجة تسامي $\Sigma : K$ تساوي درجة تسامي $K(s_1,\ldots,s_n) : K$، وهذه الدرجة هي n. وبما أن $\Sigma = K(t_1,\ldots,t_n)$ فإنّ t_i مستقلّة ومتسامية على K، وذلك لأنّه لو كانت بينهما أي علاقة جبرية لكانت درجة التسامي أقل من n. ومن الفصل الثاني نعلم أنّ s_i هي كثيرات الحدود الابتدائية في $t_1,\ldots,t_n$. وكما بيّنا سابقًا فإنّ S_n يمكن اعتبارها زمرة التماثلات الذاتية على $\Sigma = K(t_1,\ldots,t_n)$ ، وباستخدام تمهيدية (١٥ , ٣) يكون $K(s_1,\ldots,s_n)$ هو حقلها الثابت. وباستخدام نظرية (١٠ , ١٠) نجد أنّ الامتداد $\Sigma : K(s_1,\ldots,s_n)$ قابلاً للفصل وناظمي (نحصل على الناظمية من تعريف Σ كحقل انشطار) ، وباستخدام نظرية (٤ , ٩) نجد أنّ درجة هذا الامتداد هي $|S_n| = n!$. وباستخدام نظرية (١ , ١١) (١) نجد أنّ رتبة زمرة جالوا لهذا الامتداد هي $n!$ وتحتوي S_n وبالتالي فهي S_n . Δ

ومن النظرية (٦ , ١٤) والنتيجة (٥ , ١٣) نحصل على :

نظرية (١٥,٧)

إذا كان K حقلاً مميزه صفر وكان $n \geq 5$ فإن كثيرة الحدود العامة من الدرجة n «على» K لا يمكن حلها باستخلاص الجذور. Δ

(١٥,٣) حل معادلات الدرجة الرابعة

Solving Quartic Equations

بما أنّ كثيرة الحدود العامة «على» K هي في الحقيقة على حقل الامتداد $K(s_1, ..., s_n)$ حيث s_i عناصر مستقلة ومتسامية فإنّنا لا نستطيع استنتاج استحالة حل كثيرات حدود على K من الدرجة $n \geq 5$ باستخلاص الجذور من النظرية (٧ , ١٥). وعلى سبيل المثال: هذه النظرية لا تستبعد احتمال حل جميع كثيرات الحدود من الدرجة الخامسة باستخلاص الجذور ، ولكن الصيغة المستخدمة في كل حالة تختلف اختلافًا كبيراً عن الصيغة المستخدمة في حالة أخرى وبذلك لا يمكن إيجاد صيغة عامة واحدة لحل جميع معادلات الدرجة الخامسة. ومن ناحية أخرى إذا استطعنا حل كثيرة الحدود العامة من الدرجة n «على» K باستخلاص الجذور فإنّنا نستطيع حل أيّة كثيرة حدود من الدرجة n على K باستخلاص الجذور وذلك بالتعويض عن $s_1, ..., s_n$ بعناصر من K في الحل. وهذا هو السبب بتسمية كثيرة الحدود هذه بكثيرة الحدود العامة. من النظرية (٧ , ١٥) نجد أنّ أقصى ما نستطيع عمله هو حل كثيرات الحدود من الدرجة $n \leq 4$. وسنعمل على حل كثيرات الحدود هذه بدراسة خواص S_n حيث $n \leq 4$ واستخدام عكس النظرية (٦ , ١٤) .

تعريف

ليكن $L : K$ امتدادًا ناظميًا منتهيًا وزمرة جالوا له هي G . نعرّف معيار $a \in L$ ونرمز له بالرمز $N(a)$ كالتالي:

$$N(a) = \tau_1(a)\tau_2(a)\cdots\tau_n(a)$$

حيث $\tau_1, ..., \tau_n$ هي عناصر G.

ومن الواضح أنّ $N(a)$ ينتمي إلى حقل G الثابت (استخدم تمهيدية ٣ , ٩) وإذا كان الامتداد قابلاً للفصل أيضًا فإن $N(a) \in K$.

النظريّة التالية تعرف بنظريّـــة هيلبرت رقـــم ٩٠ (Hilbert's Theorem 90) وذلك لظهورها تحمل هذا الرقم في تقريره من الأعداد الجبرية في العام ١٨٩٣م.

نظرية (١٥,٨)

ليكن $L:K$ امتدادًا ناظميًا منتهيًا حيث زمرة جالوا G له زمرة دورية مولّدة بالعنصر τ، وليكن $a \in L$. عندئذ $N(a)=1$ إذا وفقط إذا وجد عنصر $b \in L$ ، $b \neq 0$ بحيث يكون $a = b/\tau(b)$.

البرهان

إذا كان $a = b/\tau(b)$ و $b \neq 0$ ، $|G| = n$ فإنّ

$$N(a) = a \times \tau(a) \times \tau^2(a) \times \ldots \times \tau^{n-1}(a)$$

$$= \frac{b}{\tau(b)} \times \frac{\tau(b)}{\tau^2(b)} \times \frac{\tau^2(b)}{\tau^3(b)} \times \ldots \times \frac{\tau^{n-1}(b)}{\tau^n(b)}$$

$$= 1$$

وذلك لأنّ $\tau^n = 1$.

وللبرهان على العكس نفرض أنّ $N(a) = 1$. لنأخذ $c \in L$ ونعرّف

$$d_0 = a\,c$$

$$d_1 = (a \times \tau(a))\,\tau(c)$$

$$\vdots$$

$$d_i = (a \times \tau(a) \times \ldots \times \tau^i(a))\,\tau^i(c)$$

حيث $0 \le i \le n-1$. إذن

$$d_{n-1} = N(a)\,\tau^{n-1}(c) = \tau^{n-1}(c) \ .$$

وكذلك

$$d_{i+1} = a \times \tau(d_i) \ ، \ 0 \le i \le n-2 \ .$$

ضع

$$b = d_0 + d_1 + \ldots + d_{n-1} \ .$$

سوف نختار c بحيث يكون $b \neq 0$، ولنفرض أنّ $b = 0$ لكل اختيار للعنصر c. إذن لكل $c \in L$ يكون لدينا :

$$\lambda_0 \tau^0(c) + \lambda_1 \tau(c) + \ldots + \lambda_{n-1} \tau^{n-1}(c) = 0$$

حيث $\lambda_i = a \times \tau(a) \times \ldots \times \tau^i(a) \in L$.

ومن ثم فإنّ التماثلات الذاتية المختلفة τ^i غير مستقلة على L وهذا يناقض تمهيدية (٩ , ١). إذن نستطيع اختيار c بحيث يكون $b \neq 0$. الآن

$$\tau(b) = \tau(d_0) + \ldots + \tau(d_{n-1})$$

$$= \frac{1}{a}(d_1 + \ldots + d_{n-1}) + \tau^n(c)$$

$$= \frac{1}{a}(d_1 + \ldots + d_{n-1})$$

$$= b / a$$

إذن $a = b / \tau(b)$. Δ

نظرية (١٥,٩)

لنفرض أنّ $L : K$ امتدادًا ناظميًا قابلاً للفصل ومنتهيًا حيث زمرة جالوا G زمرة دورية رتبتها عدد أوّلي p ومولّدة بالعنصر τ . ولنفرض أنّ K حقل مميّزه صفر أو أوّلي نسبيًا مع p وأنّ $t^p - 1$ تنشطر على K، عندئذ $L = K(\alpha)$ حيث α صفر لكثيرة حدود لا مختزلة $t^p - 1$ على K ، $a \in K$.

البرهان

إنّ أصفار $t^p - 1$ عددها p وتكون زمرة رتبتها p ومن ثم فهي دورية. إذن أصفار $t^p - 1$ يجب أن تكون على الصورة ε^i ، $1 \leq i \leq p$ حيث $\varepsilon \in K$ و $\varepsilon^p = 1$

وبما أنّ $\varepsilon \in K$ فإنّ $\tau^i(\varepsilon) = \varepsilon$ لكل i ومن ثمّ

$N(\varepsilon) = \varepsilon \times \varepsilon \times \ldots \times \varepsilon = 1$.

وباستخدام نظرية (١٥ , ٨) نستطيع ايجاد $\alpha \in L$ بحيث يكون

$\varepsilon = \alpha / \tau(\alpha)$.

ومنه فإنّ

$$\tau(\alpha) = \varepsilon^{-1}\alpha, \tau^2(\alpha) = \varepsilon^{-2}\alpha, \cdots$$

وإنّ $a = \alpha^p$ يبقى ثابتًا تحت تأثير G ، ومن ثمّ فإنّ $a \in K$. الآن $K(\alpha)$ هو حقل انشطار $t^p - a$ على K . إنّ جميع صور α تحت تأثير التماثلات الذاتية $1, \tau, ..., \tau^{p-1}$ بالنسبة إلى K مختلفة وبالتالي فإنّ لدينا p من التماثلات الذاتية المختلفة على $K(\alpha)$ بالنسبة إلى K . وباستخدام نظرية (١ , ١١) نجد أنّ $[K(\alpha) : K] \geq p$. ولكن $[L:K]=|G|=p$. إذن $L = K(\alpha)$ ، $t^p - a$ كثيرة حدود α الأصغرية على K (لأنّها لو لم تكن كذلك لكان لدينا $[K(\alpha) :K] < p$)، وبالتالي فإن $t^p - a$ لا مختزلـــة على K . Δ

باستطاعتنا الآن البرهان على عكس النظرية (٦ , ١٤) كما وعدنا سابقًا .

نظرية (١٠,١٥)

ليكن K حقلاً مميزه صفر ، و $L : K$ امتدادًا ناظميًا منتهيًا ، و G زمرة جالوا لهـذا الامتداد . إذا كانت G قابلة للحل فإنه يوجد امتداد R للحقل L بحيث يكون $R : K$ جذريًا .

البرهان

بما أنّ المميّز صفر فإنّ جميع الامتدادات قابلة للفصل ، سنستخدم الاستنتاج الرياضي على $|G|$. ومـن الواضح أنّ النظريّة صحيحة عند $|G| = 1$. إذا كانت $|G| \neq 1$ فإنّنا نختار زمرة جزئيّة ناظميّة فعليّة عظمى H من G (نستطيع ذلك لأنّ G منتهية) . وبما أن H عظمى فإن G/H بسيطة وباستخدام نظرية (٢ , ١٣) نجد أن G/H قابلة للحل . باستخدام نظريـة (٣ , ١٣) نجد أنّ G/H دورية رتبتها عدد أولي p . ليكن N هو حقل انشطار $t^p - 1$ على L . ومن نظرية (٤ , ٨) نجد أن L حقل انشطار كثيرة حدود ولتكن f على K ومنه فإن N هو حقل انشطار $f \times (t^p - 1)$ على L . وباستخدام نظرية (٤ , ٨) مرة أخرى نجد أن الامتداد $N : K$ ناظمي . إن زمرة جالوا للامتداد $N : L$ أبيلية وذلك باستخدام تمهيدية (٤ , ١٤) وباستخدام نظرية (١ , ١١)

نجد أن $\Gamma(L : K)$ تماثل $\Gamma(N : K) / \Gamma(N : L)$. ومن نظرية (٢ , ١٣) نجد أن $\Gamma(N : K)$ قابلة للحل. ولنفرض أن M حقل جزئي من N مولّد من K وأصفار $t^p - 1$. إذن $N : M$ ناظمي. ومن الواضح أنّ $M : K$ جذري، وبما أنّ $L \subseteq N$ فإنّنا نحصل على ما نريد إذا استطعنا إيجاد امتداد R للحقل N بحيث يكون $R : M$ جذريًا.

وسنبرهن الآن على أنّ زمرة جالوا للامتداد $N : M$ تماثل زمرة جزئية من G.

لنفرض أن τ تماثل ذاتي على N بالنسبة إلى M وأنّ $\tau |_L$ هو اقتصار τ على L. بما أنّ $L : K$ ناظمي فإنّ $\tau |_L$ تماثل ذاتي على L بالنسبة إلى K وبالتالي فإنّ $\varphi : \Gamma(N : M) \to \Gamma(L : K)$ المعرف كالتالي:

$$\varphi(\tau) = \tau |_L$$

تشاكل بين الزمرتين $\Gamma(N : M)$ و $\Gamma(L : K)$. إذا كان $\tau \in \ker \varphi$ فإنّ τ يُثبّت جميع عناصر M و L وهذه تُولّد N. إذن $\tau = 1$ ومنه فإنّ φ متباين. إذن $\Gamma(N : M)$ تماثل زمرة جزئية J من $\Gamma(L : K)$.

إذا كانت $J = \varphi(\Gamma(N : M))$ زمرة جزئيّة فعلية من G فإنّه باستخدام فرضية الاستنتاج نستطيع إيجاد امتداد R للحقل N بحيث يكون $R : M$ جذريًا.

أما إذا كانت $J = G$ فإنّنا نستطيع إيجاد زمرة جزئية $I \lhd \Gamma(N:M)$ دليلها p، بالتحديد $I = \varphi^{-1}(H)$. ولنفرض أنّ P هو حقل $I^{\dagger}$ الثابت. إذن $[P : M] = p$ وذلك باستخدام نظرية (١ , ١١)، وباستخدام النظرية نفسها نجد أنّ $P : M$ ناظمي، وأنّ $t^p - 1$ تنشطر في M. وباستخدام نظرية (٩ , ١٥) نجد أن $P = M(\alpha)$ حيث $\alpha^p = a \in M$، ولكن $N : P$ امتداد ناظمي ورتبة زمرة جالوا له أقل من $|G|$. وباستخدام فرضية الاستنتاج نستطيع إيجاد امتداد R للحقل N بحيث يكون $R : P$ جذريًا. إذن $R : M$ جذريًا وبهذا يتم برهان النظرية. Δ

ملاحظة

لمعالجة الحقل الذي مميزه $p > 0$ يجب علينا أن نعرّف الامتداد الجذري بصورة مختلفة. وعلاوة على اقران العناصر α بحيث ينتمي العنصر α^n للحقل تحت الدراسة فإنه يجب أن نسمح كذلك بإقران العناصر α بحيث ينتمي العنصر $\alpha^p - \alpha$

للحقل تحت الدراسة . والعبارة : كثيرة الحدود قابلة للحل باستخلاص الجذور إذا وفقط إذا كانت زمرة جالوا لها قابلة للحل تبقى صحيحة هنا . وعند دراستنا للامتدادات ذات الدرجة p لحقول مميزها p فإن البرهان مختلف حيث لا نستطيع البرهان على النظرية (١٥ , ٩) . وإذا لم نغير تعريف معنى الحل باستخلاص الجذور فإنّه على الرغم من أن كل كثيرة حدود قابلة للحل يجب أن تكون زمرة جالوا لها قابلة للحل فإن العكس ليس بالضرورة أن يكون صحيحًا . وفي الحقيقة بعض كثيرات حدود الدرجة الثانية التي زمرة جالوا لها أبيلية لا يمكن حلها باستخلاص الجذور[انظر تمرين (١٢ , ٣ و ١٣ , ٣)] .

بما أنّ حقل الانشطار هو امتداد ناظمي دائمًا فإنّنا نحصل على :

نظرية (١٥,١١)

على الحقل الذي مميّزه صفر تكون كثيرة الحدود قابلة للحل إذا وفقط إذا كانت زمرة جالوا لها قابلة للحل .

البرهان

استخدم النظريتين (٦ , ١٤) و (١٠ , ١٥) . Δ

إنّ زمرة جالوا لكثيرة الحدود العامة من الدرجة n هي S_n، ولقد رأينا أنّ S_n قابلة للحل عندما $n \le 4$ وبالتالي فإنّ كثيرة الحدود العامة من الدرجة n حيث $n \le 4$ قابلة للحل باستخلاص الجذور وذلك على حقل مميزه صفر .

وسنستخدم خواص زمرة التبديلات لنجد حلولاً لكثيرات الحدود العامة من الدرجة أقل أو يساوي 4 .

(ا) الخطيـة

$t - s_1$.

ومن الواضح أنّ $t_1 = s_1$ يكون صفرًا لكثيرة الحدود الخطية .

(ب) الدرجة الثانية

$$t^2 - s_1 t + s_2 .$$

لنفرض أنّ t_1 و t_2 هما صفرا كثيرة الحدود . تتكون زمرة جالوا S_2 من عنصرين هما العنصر المحايد والتطبيق الذي تكون صورة t_1 تحت تأثيره هي t_2 . إذن

$$(t_1 - t_2)^2$$

عنصر تثبته الزمرة S_2 ومن ثم ينتمي إلى $K(s_1, s_2)$.

وبإجراء حسابات مباشرة نجد أنّ :

$$(t_1 - t_2)^2 = s_1^2 - 4 s_2$$

إذن

$$t_1 - t_2 = \pm \sqrt{s_1^2 - 4 s_2}$$

$$t_1 + t_2 = s_1$$

وبالتالي فإنّنا نحصل على الصيغة المعروفة :

$$t_1, t_2 = \frac{s_1 \pm \sqrt{s_1^2 - 4 s_2}}{2}$$

(ج) الدرجة الثالثة

$$t^3 - s_1 t^2 + s_2 t^3 - s_3$$

لنفرض أنّ t_1, t_2, t_3 هي أصفار كثيرة الحدود . إن لزمرة جالوا S_3 المتسلسلة التالية :

$$1 \lhd A_3 \lhd S_3$$

حيث زمر الخارج أبيلية .

لنقرن العنصر $w \neq 1$ حيث $w^3 = 1$. ولنعتبر

$$y = t_1 + w t_2 + w^2 t_3 .$$

إنّ عناصر A_3 تبدّل t_1 ، t_2 ، t_3 بشكل دوري ومن ثمّ فإنّها تضرب y بقوة العدد w . إذن A_3 تثبت y^3 وبالمثل إذا كان

$$z = t_1 + w^2 t_2 + w t_3$$

فإنّ A_3 تثبت z^3 .

الآن أي تبديل فردي في S_3 يبدّل y^3 و z^3 ومن ثم فإنّ S_3 تثبت $y^3 + z^3$ و $y^3 z^3$ وبالتالي ينتميان إلى $K(s_1, s_2, s_3)$. (سوف نقدّم صيغًا تفصيلية في نهاية هذا الفصل). إذن y^3 و z^3 هما صفران لكثيرة حدود من الدرجة الثانية على $K(s_1, s_2, s_3)$ والتي يمكن حلها كما في (ب). وبأخذ الجذر التكعيبي نحصل على y و z. وبما أنّ

$$s_1 = t_1 + t_2 + t_3$$

فإنّ

$$t_1 = \frac{1}{3} (s_1 + y + z)$$

$$t_2 = \frac{1}{3} (s_1 + w^2 y + w z)$$

$$t_3 = \frac{1}{3} (s_1 + w y + w^2 z) .$$

(د) الدرجة الرابعة

$$t^4 - s_1 t^3 + s_2 t^2 - s_3 t + s_4 .$$

لنفرض أنّ t_1, t_2, t_3, t_4 هي أصفار كثيرة الحدود. إنّ لزمرة جالوا S_4 المتسلسلة التالية :

$$1 \lhd V \lhd A_4 \lhd S_4$$

حيث زمر الخارج أبيلية وحيث إنّ

$$V = \{1, (12)(34), (13)(24), (14)(23)\} .$$

إنّه لمن الطبيعي أن نعتبر المعادلات التالية :

$$y_1 = (t_1 + t_2)(t_3 + t_4)$$

$$y_2 = (t_1 + t_3)(t_2 + t_4)$$

$$y_3 = (t_1 + t_4)(t_2 + t_3)$$

إنّ هذه العناصر تتبدل فيما بينها تحت تأثير أي عنصر من S_4 ، ومن ثم فإنّ جميع كثيرات الحدود المتناظرة الابتدائية في y_1, y_2, y_3 تنتمي إلى $K(s_1, s_2, s_3, s_4)$. (سنقدّم صيغًا تفصيلية في نهاية هذا الفصل). إذن y_1, y_2, y_3 أصفار لكثيرة حدود من الدرجة الثالثة على $K(s_1, s_2, s_3, s_4)$ تسمى بالتكعيبية المُفكّكة. وبما أنّ

$$t_1 + t_2 + t_3 + t_4 = s_1$$

فإنّنا نستطيع إيجاد ثلاث كثيرات حدود من الدرجة الثانية أصفارها هي :

$t_1 + t_2, \ t_3 + t_4, t_1 + t_3$ و $t_2 + t_4, t_1 + t_4, t_2 + t_3$.

ومن ثمّ فإنّنا نستطيع بسهولة إيجاد t_1, t_2, t_3, t_4 .

ولغرض التكامل في الموضوع سنقدّم صيغًا تفصيلية كما أشرنا سابقًا. ولمزيد من التفاصيل يستطيع القارىء الرجوع إلى [Van der Waerden, 1953] .

الدرجة الثالثة. باستخدام تحويل تسكرينهاوس (Tschirnhaus)

$$u = t - \frac{1}{3} s_1$$

كثيرة الحدود العامة من الدرجة الثالثة على الصورة :

$$u^3 + pu + q \ .$$

إذا استطعنا إيجاد أصفار كثيرة الحدود هذه فيصبح من السهل إيجاد أصفار كثيرة الحدود العامة من الدرجة الثالثة. وباتّباع الطرق المستخدمة أعلاه لكثيرة الحدود هذه نحصل على :

$$y^3 + z^3 = -27q$$

$$y^3 z^3 = -27p^3$$

ومنه فإنّنا نجد أنّ y^3 ، z^3 هما صفرا كثيرة الحدود

$$t^2 + 27qt - 27p^3 \ .$$

وهذا يعطينا قانون فونتانا (Fontana's formula) الذي أشرنا إليه في المقدمة التاريخية.

الدرجة الرابعة. نستخدم هنا تحويل تسكرينهاوس

$$u = t - \frac{1}{4} s_1$$

وبذلك تأخذ كثيرة الحدود العامة من الدرجة الرابعة الصورة :

$$t^4 + p t^2 = q t + r .$$

وباتباع الطرق أعلاه نجد أنّ:

$$y_1 + y_2 + y_3 = 2p$$
$$y_1 y_2 + y_1 y_3 + y_2 y_3 = p^2 - 4r$$
$$y_1 y_2 y_3 = -q^2$$

والمفككة التكعيبية هي :

$$t^3 - 2pt^2 + (p^2 - 4r)t + q^2$$

حيث y_1, y_2, y_3 أصفار هذه المفككة التكعيبية ونحصل على :

$$2t_1 = \sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3}$$
$$2t_2 = \sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3}$$
$$2t_3 = -\sqrt{-y_1} + \sqrt{-y_2} - \sqrt{-y_3}$$
$$2t_4 = -\sqrt{-y_1} - \sqrt{-y_2} + \sqrt{-y_3}$$

حيث $(\sqrt{-y_1})(\sqrt{-y_2})(\sqrt{-y_3}) = -q$.

شكل(٢٢). كاردانو (Cardano)، أول من نشر حلاً لكثيرتي الحدود من الدرجة الثالثة والرابعة.

تمارين

(١٥ , ١) إذاكان K حقلاً قابلاً للعدّ، و L : K امتدادًا منتهي التوليد فأثبت أنّ L قابل للعدّ، ومن ثم أثبت أن $\mathbb{R} : Q$ و $\mathbb{C} : Q$ غير منتهي التوليد.

(١٥ , ٢) احسب درجة التسامي لكل من الامتدادات التالية:

(أ) $Q(t,u,v,w) : Q$ حيث t,u,v,w مستقلة ومتسامية على Q.

(ب) $Q(t,u,v,w) : Q$ حيث $t^2 = 2$ ، u متسام على Q(t) ، $v^3 = t + 5$ و w متسام على Q(t,u,v).

(ج) $Q(t,u,v) : Q$ حيث $t^2 = u^3 = v^4 = 7$.

(١٥ , ٣) في التمهيدية (١ , ١٥) أثبت أنّ الدرجة [L : M] لا تعتمد على اختيار M [**إرشاد** : اعتبر $K(t^2)$ حقلاً جزئيًا من K(t)].

(١٥ , ٤) لنفرض أنّ $K \subseteq L \subseteq M$ حيث إن كلاً من الامتدادين M : K و L : M منتهي التوليد ، أثبت أنّ درجتي تسامي الامتدادين M : K و L : K متساويتان إذا وفقط إذا كان الامتداد M : L منتهيًا.

(١٥ , ٥) استخدم الحقيقة : «أي زمرة منتهية تماثل زمرة جزئية من S_n» لإثبات أنّ أيّة زمرة منتهية يجب أن تماثل زمرة جالوا لامتداد منته. (أنّه من غير المعلوم أنّ أيّة زمرة هي عبارة عن زمرة جالوا لامتداد ناظمي ومنته للحقل Q).

(١٥ , ٦) أثبت أنّ كثيرة الحدود $x^3 - 3x + 1$ إمّا أن تكون لا مختزلة، وإمّا أن تنشطر في K ، وذلك لأي حقل K . (**إرشاد** : اثبت أن أيّ صفر يمكن كتابته كعبارة كسرية في أيّ صفر آخر).

(١٥ , ٧) ليكن K حقلاً مميزه صفر، وليكن L : K امتدادًا منتهيًا وناظميًا وزمرة جالوا له هي G . لكل $a \in L$ عرف الأثر كالتالي:

$$T(a) = \tau_1(a) + \dots + \tau_n(a)$$

حيث $\tau_1, \dots, \tau_n$ عناصر G المختلفة. اثبت أن $T(a) \in K$ وأنّ $T : L \to K$ تطبيق شامل.

(١٥ , ٨) في التمرين السابق إذا كانت G دوريّة ومولّدة بالعنصر τ فاثبت أن $T(a) = 0$ إذا وفقط إذا وجد عنصر $b \in L$ بحيث $a = b - \tau(b)$.

(١٥ , ٩) حل كل من كثيرات الحدود التالية باستخلاص الجذور على Q .

(أ) $t^3 - 7t + 5$

(ب) $t^3 - 7t + 6$

(ج) $t^4 + 5t^3 - 2t - 1$

(د) $t^4 + 4t + 2$

(١٥ , ١٠) أثبت أنّ الامتداد الجبري المنتهي التوليد يجب أن يكون منتهيًا ومن ثم أوجد امتدادًا جبريًا غير منتهي التوليد .

(١٥ , ١١) ضع علامة صح أو خطأ أمام كل مما يلي :

(أ) كل امتداد منته يجب أن يكون منتهي التوليد .

(ب) كل امتداد منتهي التوليد يجب أن يكون جبريًا .

(ج) درجة التسامي للامتداد منتهي التوليد لا تتغير تحت تأثير التماثل .

(د) إذا كانت $t_1 ,..., t_n$ عناصر مستقلة ومتسامية فإنّ كثيرات الحدود المتناظرة الابتدائية لهما يجب أن تكون عناصر مستقلة ومتسامية أيضًا .

(هـ) زمرة جالوا لكثيرة الحدود العامة من الدرجة n قابلة للحل لكل n .

(و) كثيرة الحدود العامة من الدرجة الخامسة قابلة للحل باستخلاص الجذور .

(ز) تطبيق المعيار هو تشاكل حقلي .

(ح) الزمر الجزئيّة الفعليّة من S_3 هي 1 و A_3 فقط .

(ط) كثيرة الحدود العامة من الدرجة n «على» K هي كثيرة حدود في مجهول واحد على K .

(ي) درجة تسامي الامتداد $Q(t) : Q$ هي 1 .

(١٥ , ١٢)* لتكن كثيرة حدود θ الأصغرية على Q هي :

$$t^3 + at^2 + bt + c$$

جد شرطًا لازمًا وكافيًا بدلالة a ، b ، c بحيث يكون $\theta = \varphi^2$ حيث $\varphi \in Q(\theta)$. (إرشاد : اعتبر كثيرة حدود φ الأصغرية) .

اكتب $\sqrt[3]{28} - 3$ كمربع كامل في $Q(\sqrt[3]{28})$ وأكتب $\sqrt[3]{5} - \sqrt[3]{4}$ كمربع كامل في $Q(\sqrt[3]{5}, \sqrt[3]{2})$ [انظر : Ramanujan, 1962] .

(١٥ , ١٣)* لتكن Γ زمرة التماثلات الذاتية المنتهية للحقل K وليكن K_0 حقلها الثابت، وليكن t متساميًا على K . أثبت على وجود تماثل ذاتي وحيد σ' على K(t) بحيث يتحقّق :

$$\sigma'(k) = \sigma(k) \quad , \quad k \in K$$

$\sigma'(t) = t$. وذلك لكل $\sigma \in \Gamma$

وأثبت أنّ التماثلات الذاتية σ' تكون زمرتها Γ' تماثل الزمرة Γ وحقلها الثابت $K_0(t)$.

(١٥ , ١٤)* ليكن t متساميًا على K. ولتكن $a, b, c, d \in K$ حيث $ad-bc\neq 0$ أثبت أنّ التطبيق

$$\begin{Bmatrix} a & b \\ c & d \end{Bmatrix}$$

المعرف كالتالي :

$$t \to (a\,t + b) / (c\,t + d)$$

يعيّن لنا تماثلاً ذاتيًا على K(t) بالنسبة إلى K. برهن على أنّ أيّ تماثل ذاتي على K(t) بالنسبة إلى K يمكن الحصول عليه بهذه الطريقة .

(١٥ , ١٥)* لتكن Γ هي زمرة جالوا للامتداد K(t) : K، برهن على وجود تشاكل $\varphi : GL_2(K) \to \Gamma$ حيث $GL_2(K)$ هي زمرة جميع المصفوفات اللامنفردة من الشكل 2 x 2 على الحقل K وأنّ

$$\varphi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{Bmatrix} a & b \\ c & d \end{Bmatrix}$$

برهن على أنّ $\ker(\varphi)$ هي مجموعة المصفوفات

$$\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$$

حيث $0 \neq k \in K$ ، ومن ثمّ

$$\Gamma \cong GL_2(K) / \ker(\varphi) = PGL_2(K)$$

حيث $PGL_2(K)$ هي زمرة الاسقاط الخطية العامة .

الفصل السادس عشر

الحقول المنتهية
Finite Fields

تلعب الحقول التي تحتوي على عدد منته من العناصر دورًا مهمًا في كثير من فروع الرياضيات مثل نظرية الأعداد، نظرية الزمر، الهندسة الاسقاطية وغيرها. ومن الحقول المنتهية المألوفة لدينا الحقول $\mathbb{Z}_p$ حيث p عدد أولي، ولكن هناك حقولاً منتهية غيرها. وفي هذا الفصل نقدم تصنيفًا كاملاً للحقول المنتهية، وسنرى أنّ أيّ حقل منته يمكن تعيينه بشكل وحيد (تحت سقف التماثل) بعدد عناصره وهذا العدد يجب أن يكون قوة لعدد أوّلي، ولكل عدد أوّلي p وعدد صحيح $n > 0$ يوجد حقل يحتوي على p^n من العناصر.

(١٦,١) تصنيف الحقول المنتهية
Structure of Finite Fields

سنبدأ ببرهانٍ العبارة الثانية من العبارات الثلاث أعلاه.

نظرية (١٦,١)

إذا كان F حقلاً منتهيًا فإنّ مميز F هو $p > 0$، وأنّ عدد عناصر F هو p^n، حيث n هو درجة F على حقله الجزئي الأولي.

البرهان

لنفرض أن P هو الحقل الجزئي الأولي من F، وبما أنّ Q غير منته فإنّ $P \ncong Q$ ومن ثمّ فإنّ $P \cong \mathbb{Z}_p$ حيث p عدد أوّلي. إذن مميّز F هو p. باستخدام نظريّة (١ , ٤) نجد

أنّ F فضاء متجهـــات على P ، وبما أنّه منته فإنّه يجب أن يكون ذا بعـد منته وليكـــن $[F : P] = n$. لنفرض أنّ $x_n ,..., x_1$ أساس لـ F على P، إذن أيّ عنصر في F يمكن كتابته بصورة وحيدة على الشكل :

$$\lambda_1 x_1 +...+ \lambda_n x_n$$

حيث $\lambda_1 ,..., \lambda_n \in P$. بما أنّ $|P| = p$ فإنه يوجد p من الخيارات لكل λ_i وبالتالي فإنّه يوجد p^n من هذه العناصر . إذن $|F| = p^n$. Δ

من النظريّة أعلاه نستطيع أن نستنتج استحالة وجود حقول عدد عناصرها 6، 10، 12، 14، 18، 20، . . . لاحظ الفرق مع نظرية الزمر حيث إنّه يوجد زمرة رتبتها أيّ عدد معطى، ومن الممكن أن يكون هناك أكثر من زمرة واحدة لها الرتبة نفسها . وسنثبت استحالة ذلك في الحقول المنتهية ولكنّنا سنحتاج أولاً إلى تمهيدية أشير إليها ضمنيًا في الفصل الثامن .

تمهيدية (١٦،٢)

ليكن K حقلاً مميزه $p > 0$. التطبيق $\varphi: K \to K$ المعرف كالتالي

$$\varphi(k) = k^p \text{ لكل } k \in K$$

تشاكل حقلي متباين . وإذا كان K منتهيًا فإنّ φ تماثل ذاتي .

البرهان

لنفرض أنّ $x, y \in K$. إذن

$$\varphi(xy) = (xy)^p = x^p y^p = \varphi(x) \varphi(y) .$$

أيضًا

$$\varphi(x+y) = (x+y)^p$$
$$= x^p + px^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + pxy^{p-1} + y^p$$

وكما لاحظنا في الفصل الثامن فإنّ p يقسم $\binom{p}{r}$ لكل $1 \le r \le p-1$. إذن

$$\varphi(x+y) = x^{p} + y^{p} = \varphi(x) + \varphi(y)$$

إذن φ تشاكل . وبما أنّ $\varphi(1) = 1 \neq 0$ فإنّ φ متباين وذلك باستخدام تمهيدية (٣ , ٣) .

إذا كان K منته فإنّ أيّ تشاكل متباين من K إلى K يجب أن يكون شاملاً ومن ثمّ فإن φ تماثل ذاتي . Δ

تعريف

إذا كان K حقلاً مميزه $p > 0$ فإن التطبيق المعرف في التمهيدية (٢ , ١٦) يسمى تشاكلاً فروبيناس (Frobenius) المتباين على K وإذا كان K منتهيًا فإنّه يسمّى تماثل فروبيناس الذاتي .

في الحقل $\mathbb{Z}_5$ نجد أنّ φ هو التطبيق المحايد . أما في الحقل المعطى في تمرين (١ , ٦) فإن $\varphi(0) = 0$ ، $\varphi(1) = 1$ ، $\varphi(\alpha) = \beta$ ، $\varphi(\beta) = \alpha$ ومن ثـمّ فإنّ φ ليس تطبيقًا محايدًا دائمًا .

نظرية (١٦,٣)

ليكن p عددًا أوليًا و $q = p^n$ حيث n عدد صحيح موجب، عندئذ يحتوي الحقل F على q من العناصر إذا وفقط إذا كان حقل انشطار لكثيرة الحدود $f(t) = t^q - t$ على الحقل الجزئي الأولي $P \cong \mathbb{Z}_P$ من F .

البرهان

لنفرض أولاً أنّ $|F| = q$. المجموعة $F \setminus \{0\}$ تكون زمرة مع عملية الضرب رتبتها $q - 1$ ، ومن ثمّ إذا كان $x \in F$ و $x \neq 0$ فإنّ $x^{q-1} = 1$. إذن $x^{q} - x = 0$. وبما أنّ $0^{q} - 0 = 0$ فإنّ كل عنصر في F وهو صفر لكثيرة الحدود $t^{q} - t$ ، ومن ثمّ فإنّ $f(t)$ تنشطر في F . وبما أنّ أصفار f هي جميع عناصر F فإنّ هذه العناصر بالتأكيد تُولِّد F ، وبالتالي فإنّ F هو حقل انشطار f على P .

وللبرهان على العكس ، نفرض أنّ K هو حقل انشطار f على $\mathbb{Z}_P$ ، وبمـا أنّ

$Df = -1$ أولية نسبيًا مع f فإنّ جميع أصفار f في K مختلفة ، ومن ثمّ فإنّ عدد أصفار f هو q . لنفرض أن x و y صفران لكثيرة الحدود f . إذن $x^q = \varphi^n(x)$ حيث φ هو تشاكل فروبيناس المتباين ، ومن ثمّ فإنّ φ^n تشاكل متباين أيضًا . إذن

$$(xy)^q - xy = x^q y^q - xy = xy - xy = 0$$

$$(x+y)^q - (x+y) = x^q + y^q - (x+y) = (x+y) - (x+y) = 0$$

$$(x^{-1})^q - x^{-1} = x^{-q} - x^{-1} = x^{-1} - x^{-1} = 0 .$$

إذن جميع أصفار f في K تكون حقلاً وهذا يجب أن يكـون حقل الانشطار K . إذن $|K| = q$. Δ

بما أن حقول الانشطار موجودة ووحيدة (تحت سقف التماثل) نحصل على :

نظرية (١٦,٤)

إنّ أيّ حقل منته يجب أن يحتوي على $q = p^n$ من العناصر حيث p عدد أولي و n عدد صحيح موجب ، ولكل عدد q من هذه الأعداد فإنه يوجد حقل وحيد (تحت سقف التماثل) يحتوي على q من العناصر والذي يمكن إنشاؤه كحقل انشطار $t^q - t$ على $\mathbb{Z}_p$.

ترميز

يرمز للحقل الذي يحتوي على q من العناصر بالرمز GF(q) . (الحرفان GF كل منهما أوّل حرف من الكلمتين حقل جالوا باللغة الانجليزية وذلك اعترافًا لجميل مكتشف هذا الحقل) .

(١٦,٢) الزمرة الضربيّة

The Multiplicative Group

بالرغم من أنّ التصنيف أعلاه للحقول المنتهية مهم بحد ذاته ، إلاّ أنّه لا يزوّدنا بمعلومات عن التركيب الداخلي للحقل . وإن هناك كثيرًا من الأسئلة التي تطرح نفسها : ما هي الحقول الجزئية؟ وكم عددها؟ وما هي زمرة جالوا؟ وسنكتفي هنا بالبرهان على نظرية مهمة تزوّدنا بمعلومات عن تركيب الزمرة الضربية $F \setminus \{0\}$ للحقل

المنته F، ولكننا نحتاج قبل ذلك لبعض المعلومات عن الزمر الأبيلية.

تعريف

أس الزمرة المنتهية يرمز له بالرمز $e(G)$ ، ويعرف بأنه المضاعف المشترك الأصغر لرتب عناصر G .

ومن الواضح أنّ $e(G)$ يقسم $|G|$. وليس من الضروري أن تحتوي الزمرة G على عنصر رتبته $e(G)$ فعلى سبيل المثال إذا كانت $G = S_3$ فإن $e(G) = 6$ ولكن لا يوجد عنصر في S_3 رتبته 6 ، أمّا إذا كانت الزمرة أبيلية فإنّنا نحتاج إلى :

تمهيدية (١٦,٥)

إنّ أية زمرة أبيلية منتهية تحتوي على عنصر رتبته $e(G)$.

البرهان

لنفرض أنّ $e = e(G) = p_1^{\alpha_1} \cdots P_n^{\alpha_n}$ حيث p_i أعدادًا أوّلية مختلفة و $\alpha_i \geq 1$.
ومن تعريف $e(G)$ يجب أن تحتوي G على عناصر g_i رتبتها قابلة للقسمة على $p_i^{\alpha_i}$.
إذن يوجد قوى a_i للعنصر g_i رتبته $p_i^{\alpha_i}$. ضع

$$g = a_1 a_2 \ldots\ldots a_n .$$

إذا كان $g^m = 1$ حيث $m \geq 1$ فإنّ

$$a_i^m = a_1^{-m} \ldots\ldots a_{i-1}^{-m} a_{i+1}^{-m} \ldots\ldots a_n^{-m} .$$

ومن ثمّ إذا كان

$$q = p_1^{\alpha_1} \ldots\ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots\ldots p_n^{\alpha_n}$$

فإنّ $a_i^{mq} = 1$. ولكن q أولي نسبيًا مع رتبة a_i ومن ثمّ فإنّ $p_i^{\alpha_i}$ يقسم m . إذن e يقسم m ، ومن الواضح أن $g^e = 1$ ، إذن رتبة g هي e . Δ

نتيجة (١٦,٦)

إذاكانت G زمرة أبيلية منتهية، وكان $e(G) = |G|$ فإنّ G زمرة دورية .

البرهان

العنصر g الذي وجدناه يُولِّد G . Δ

سنستخدم هذه النتيجة مباشرةً .

نظرية (١٦,٧)

إذا كانت G زمرة جزئية منتهية من الزمرة الضربية $K\setminus\{0\}$ للحقل K فإن G دورية .

البرهان

بما أنّ عملية الضرب على K ابدالية فإن G إبدالية . ولنفرض أنّ $e=e(G)$ ، إذن لكل $x \in G$ لدينا $x^e = 1$ ، ومن ثمّ فإنّ x صفر لكثيرة الحدود $t^e - 1$ على K . وكثيرة الحدود هذه لها على الأكثر e صفرًا وذلك باستخدام نظرية (٢ , ٨) . إذن $|G| \leq e$. ولكن $e \leq |G|$ ، ومنه فإنّ $|G| = e$، وباستخدام نتيجة (١٦ , ٦) نجد أنّ G دورية . Δ

نتيجة (١٦,٨)

الزمرة الضربية لأي حقل منتهي دورية . Δ

ممّا سبق نستنتج أنّه لأيّ حقل منته F يجب أن يوجد على الأقل عنصرًا واحدًا x بحيث يكون أيّ عنصر غير صفري في F هو عبارة عن x مرفوعًا لقوّة ما . وسنقدّم مثالين على ذلك .

أمثلة

(١) قوى العدد 2 في الحقل GF(11) هي على الترتيب :

. 1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1

إذن 2 يُولِّد الزمرة الضربية ، ومن ناحية أخرى فإنّ قوى العدد 4 هي

. 1, 4, 5, 9, 3, 1

إذن 4 لا يولد الزمرة الضربية .

(٢) بما أنّ $t^2 - 2$ لا مختزلة على $\mathbb{Z}_5$ ، فإنّ GF(25) هو حقل انشطار $t^2 - 2$ على $\mathbb{Z}_5$ ، إذن كل عنصر في GF(25) يمكن كتابته على الصورة $a + b\alpha$ حيث $\alpha^2 = 2$ ، ومن الممكن أن نعتبر $\alpha = \sqrt{2}$. لنأخذ العنصر $2 + \sqrt{2}$ (نحصل على هذا بالتجريب)، وقوى هذا العنصر هي على الترتيب :

$$1, 2+\sqrt{2}, 1+4\sqrt{2}, 4\sqrt{2}, 3+3\sqrt{2}, 2+4\sqrt{2},$$
$$2, 4+2\sqrt{2}, 2+3\sqrt{2}, 3\sqrt{2}, 1+\sqrt{2}, 4+3\sqrt{2},$$
$$4, 3+4\sqrt{2}, 4+\sqrt{2}, \sqrt{2}, 2+2\sqrt{2}, 3+\sqrt{2},$$
$$3, 1+3\sqrt{2}, 3+2\sqrt{2}, 2\sqrt{2}, 4+4\sqrt{2}, 1+2\sqrt{2}, 1$$

إذن $2 + \sqrt{2}$ يُولِّد الزمرة الضربية .

من الجدير بالذكر هنا هو عدم وجود طريقة معلومة لايجاد مُولِّد غير طريقة التجريب ، ولكن لحسن الحظ فإن البرهان على وجود مُولِّد عادةً يكون كافيًا .

تمـــارين

(١٦ , ١) لأيّ من قيم n التالية يوجد حقل يحتوي على n عنصرًا؟

$$1, 2, 3, 4, 5, 6, 17, 24, 312, 65536, 65537, 83521,$$
$$103823, \quad 2^{216091} - 1$$

(١٦ , ٢) هل نستطيع الاستفادة من نتائج هذا الفصل لحل تمريني (٣ , ٨) و (٤ , ٨) ؟

(١٦ , ٣) انشيءحقولاً عدد عناصر كل منها 8 ، 9 ، 16 .

(١٦ , ٤) ليكن φ تماثل فروبيناس الذاتي على $GF(p^n)$. جد أصغر عدد $m > 0$ بحيث يكون φ^m هو التطبيق المحايد .

(١٦ , ٥) برهن على أنّ الحقول الجزئية من الحقل $GF(p^n)$ تماثل $GF(p^r)$ حيث r يقسم n ، وأنّ لكل r يوجد حقل جزئي وحيد .

(١٦ , ٦) برهن على أنّ زمرة جالوا للامتداد $GF(p^n) : GF(p)$ هي زمرة دورية رتبتها n ومولَّدة بتماثل فروبيناس الذاتي φ ، أثبت أنّ تقابل جالوا في حال الحقول

المنتهية يجب أن يكون شاملاً ومتباينًا ثم جد زمرة جالوا للامتداد $GF(p^m) : GF(p^n)$ حيث m يقسم n .

(١٦ , ٧) هل يوجد أعداد مؤلفة r بحيث تقسم $\binom{r}{s}$ لكل $1 \le s \le r-1$ ؟

(١٦ , ٨) جد مُولِّدًا للزمرة الضربية للحقل $GF(n)$ حيث n هو :

8 ,9 ,13 ,17 ,19 ,23 ,29 ,31 ,37 ,41, 49 .

(١٦ , ٩) برهن على أنّ الزمرة الجمعية للحقل $GF(p^n)$ هي حاصل ضرب مباشر لعدد n من الزمر الدورية رتبة كل منها p .

(١٦ , ١٠) اعتبر $\mathbb{Z}_2(t)$ لإثبات أنّ تشاكل فروبيناس المتباين ليس بالضرورة تماثلاً ذاتيًا .

(١٦ , ١١) ما هي قيم n بحيث تحتوي الزمرة S_n على عنصر رتبته $e(S_n)$ ؟

(**إرشاد** : ضع كل عنصر في S_n وقارن ذلك بتقدير للقيمة $e(S_n)$) .

(١٦ , ١٢) ضع علامة صح أو خطأ أمام كل مما يلي :

(ا) يوجد حقل عدد عناصره 124 .

(ب) يوجد حقل عدد عناصر زمرته الضربية 124 .

(ج) يوجد حقل عدد عناصره 125 .

(د) تحتوي الزمرة الضربية للحقل $GF(19)$ على عنصر رتبته 3

(هـ) جميع الحقول التي عدد عناصر كل منها 121 متماثلة .

(و) يوجد حقل جزئي من $GF(2401)$ يماثل $GF(49)$.

(ز) كل تشاكل متباين من حقل منته إلى نفسه يجب أن يكون تماثلاً .

(ح) الزمرة الجمعية للحقل المنته دورية .

(ط) الزمرة الضربية لأي حقل دورية .

(ي) أس الزمرة هو أعلى رتبة لعناصرها .

(١٦ , ١٣)* برهن على أنّ كل عنصر في الحقل المنتهي يمكن كتابته كمجموع مربعين .

الفصل السابع عشر

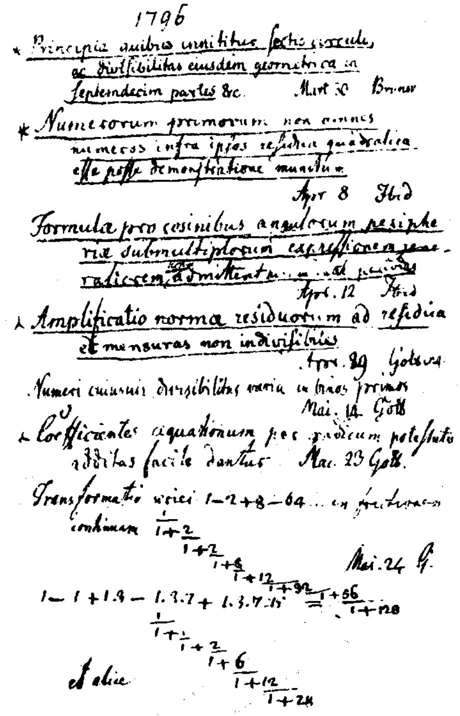
المضلعات المنتظمة
Regular Polygons

نعود الآن إلى مسألة متطوّرة من مسائل الإنشاءات باستخدام المسطرة والفرجار. وسنتطرق إلى السؤال التالي: ما هي قيم n التي يكون عندها المضلع المنتظم ذو n من الأضلاع قابل للإنشاء باستخدام المسطرة والفرجار؟

لقد تمكّن الإغريق من إنشاء مضلّعات منتظمة عدد أضلاعها 3، 5، 15، وكذلك استطاعوا إنشاء مضلع ذي 2n من الأضلاع بمعرفة مضلع ذي n من الأضلاع. ولقد مضى حوالي عشرون قرنًا على اكتشافات الإغريق دون أن يحدث تطور يذكر في هذا الاتجاه. وفي ٣٠ آذار عام ١٧٩٦م استطاع العالم جاوس (Gauss) أن يكتشف إمكانية إنشاء المضلع المنتظم ذي 17 ضلعًا (شكل ٢٣) وكان عمره في ذلك الوقت ١٩ عامًا. ولقد حسم هذا الاكتشاف اختيار جاوس للرياضيات بعد أن كان مترددًا بين التخصص بها أو باللغات. وفي كتابه (Disquisitiones Arithmeticae) الذي أعيد طبعه تحت عنوان جاوس (١٩٦٦م) ذكر شرطًا كافيًا ولازمًا لإنشاء المضلّع ذي n ضلعًا، وبرهن فقط الشرط الكافي فقط، وادّعى أنّ لديه برهانًا للشرط اللازم ولكنه لم ينشره أبدًا. وليس هناك شك في صحة ادّعاء جاوس.

(١٧,١) ما هي الانشاءات الممكنة؟
Which Constructions Are Possible?

لغرض الحصول على شرط كاف ولازم لوجود إنشاءات باستخدام المسطرة والفرجار يجب أن نبرهن على نظريّة أكثر تفصيلاً من النظرية (٢, ٥)، وهذا يتطلب منا حرصًا لمعرفة الإنشاءات المحتملة.



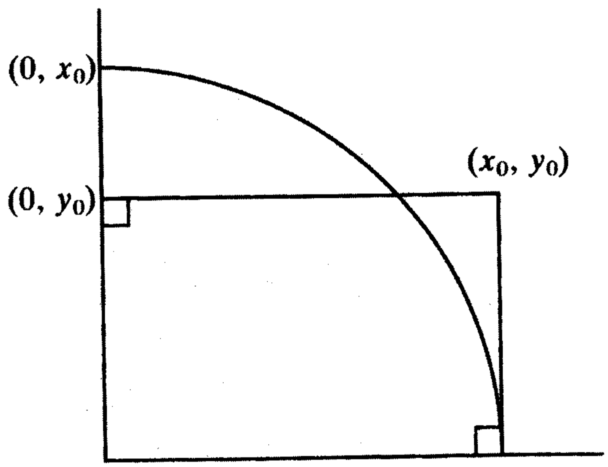
شكل (٢٣). الصفحة الأولى من دفتر ملاحظات جاوس الذي سجل فيها إنشاءه للمضلع ذي 17 ضلعًا.

تمهيدية (١٧,١)

إذا كان P مجموعة جزئية من $\mathbb{R}^2$ تحتوي على النقطتين (0,0) و (1,0) فإن النقطة (x,y) تكون قابلة للإنشاء من P عندما تنتمي x و y للحقل الجزئي من $\mathbb{R}$ المولَّد بعناصر إحداثيات نقاط P .

البرهان

من الواضح كيفيّة إنشاء $(0, x_0)$ و $(0, y_0)$ لأيّة نقطة (x_0, y_0) . من النقطتين (0,0) و (1,0) نستطيع أن ننشيء محوري الاحداثيات ومن ثم نستمر كما في الشكل (٢٤).



شكل(٢٤).إنشاء $(0, x_0)$ و $(0, y_0)$ من (x_0, y_0) .

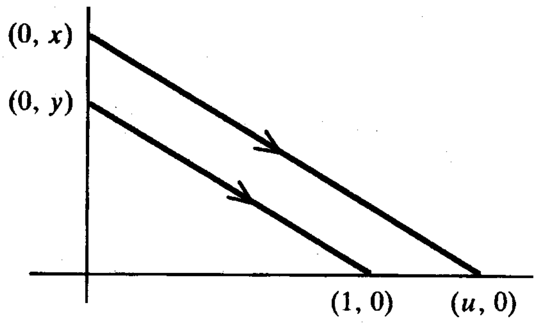
وإذا أعطينا $(0, x_0)$ و $(0, y_0)$ فإنّنا نستخدم طريقة الإنشاء نفسها ولكن بالصورة العكسية للحصول على (x_0, y_0) . إذن للبرهان على التمهيديّة يكفي أن نثبت إمكانيّة إنشاء كل من $(0, x + y)$ ، $(0, x - y)$ ، $(0, x y)$ و $(0, x/y)$ حيث $y \neq 0$ من النقطتين $(0,x)$ و $(0,y)$.

إن إنشاء النقطتين $(0, x + y)$ و $(0, x- y)$ واضح ، وذلك إذا رسمنا قطاعين نصف قطر كل منهما y ومركـــزه $(0,x)$ فإنّهما يقطعـان المحـور y في النقطتـين $(0, x + y)$ و $(0, x - y)$.

لإنشاء $(0, xy)$ و $(0, x/y)$ نتبع ما يلي :

صل النقطتين $(1,0)$ و $(0,y)$ ثم ارسم مستقيمًا موازيًا يمر بالنقطة $(0,x)$. هذا المستقيم يقطع المحور x في النقطة $(u,0)$. ومن تشابه المثلثين يكون $u/x = 1/y$ ومنه فإنّ $u = x/y$. وإذا أخذنا $x = 1$ فإنّنا نستطيع إنشاء $(1/y, 0)$ ومن ثمّ $(0,1/y)$. وبأخذ $1/y$ بدلاً من y نستطيع إنشاء $(xy, 0)$. ممّا سبق نكون قد أنشأنا كـــلاً من $(0,xy)$ و $(0, x/y)$.

(انظر الشكل ٢٥). Δ



شكل (٢٥). إنشاء $u = x / y$.

تمهيدية (١٧,٢)

ليكن $K(\alpha):K$ امتدادًا درجته 2 بحيث $K(\alpha) \subseteq \mathbb{R}$ ، وعندئذ يمكن إنشاء أية نقطة $\mathbb{R}^2 \ni (z, t)$ حيث $t \in K(\alpha)$ و z من مجموعة منتهية من النقاط التي إحداثياتها تنتمي إلى K.

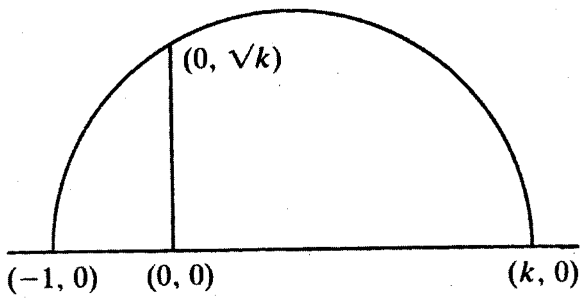
البرهان

لدينا $\alpha^2 + p\alpha + q = 0$ حيث $p, q \in K$. إذن

$$\alpha = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

وبما أنّ $K(\alpha) \subseteq \mathbb{R}$ فإنّ $p^2 - 4q > 0$ ، وإذا استطعنا إنشاء $(0, \sqrt{k})$ لكل عدد موجب $k \in K$ من عدد منته من النقاط (x_r, y_r) حيث $x_r, y_r \in K$ فإنّنا نحصل على المطلوب باستخدام تمهيدية (١٧, ١) .

أنشيء $(-1, 0)$ و $(k, 0)$، وارسم نصف دائرة بحيث تكون هاتان النقطتان هما نهايتا قطر بحيث تقطع المحور y في النقطة (v و 0) . ومن نظرية تقاطع الأوتار نجد أنّ $v^2 = 1 \times k$ ومن ثمّ فإنّ $v = \sqrt{k}$. (انظر الشكل ٢٦) . Δ



شكل(٢٦). إنشاء $\sqrt{k}$.

نظرية (١٧,٣)

لنفرض أن K حقل جزئي $\mathbb{R}$ مُولَّد باحداثيات نقاط من مجموعة جزئية $P \subseteq \mathbb{R}^2$ ولنفرض أنّ α و β ينتميان إلى امتداد L للحقل K ويحتوي $\mathbb{R}$ بحيث توجد متسلسلة منتهية من الحقول الجزئية

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L$$

تحقق $[K_{i+1} : K_i] = 2$ لكل $i = 0,\dots, r-1$. عندئذ يمكن إنشاء (α,β) من P .

البرهان

باستخدام الاستنتاج الرياضي على r.

إذا كان $r = 0$ فالعبارة صحيحة باستخدام تمهيديّة (١ , ١٧) إذا كان $r > 0$ فإن (α,β) قابلة للإنشاء من عدد منته من النقاط التي إحداثياتها تنتمي إلى K_{r-1} وذلك باستخدام تمهيدية (٢ , ١٧). وباستخدام فرضية الاستنتاج نجد أن هذه النقاط قابلة للإنشاء من P ومن ثمّ فإنّ (α,β) قابلة للإنشاء من P . Δ

من النظريّة (٢ , ٥) نجد أيضًا أنّ وجود الحقول K_i شرط لازم لإنشاء (α,β) من P .

القضية التالية أضعف من النظرية (٣ , ١٧) ولكنّها أكثر استخدامًا .

قضية (١٧,٤)

إذا كان K حقلاً جزئيًا من $\mathbb{R}$ مولدًا بإحداثيات نقاط تنتمي إلى مجموعة جزئية $P \subseteq \mathbb{R}^2$ ، وإذا كان α و β ينتميان إلى امتداد ناظمي L للحقل K بحيث أن $L \subseteq \mathbb{R}$ و $[L:K] = 2^r$ حيث $r \in \mathbb{Z}$ فإنّ (α,β) قابلة للانشاء من P .

البرهان

بما أنّ المميّز صفرًا فإنّ $L : K$ قابل للفصل .

لتكن G هي زمرة جالوا للامتداد $L : K$. باستخدام نظرية (١ , ١١) نجد أنّ $|G| = 2^r$ ومن ثمّ فإنّ G زمرة من النوع 2 . وباستخدام تمهيدية (١٠ , ١٣) يوجد متسلسلة من الزمر الجزئية الناظمية

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_r = G$$

بحيث يكون $|G_i| = 2^i$. ليكن K_i هو الحقل الثابت $G^{\dagger}_{r-i}$. وباستخدام نظرية (١ , ١١) نجد أن $[K_{j+1} : K_j] = 2$ لكل j . وباستخدام نظرية (١٧ , ٣) نجد أنّ (α,β) قابلة للإنشاء من P .

(١٧,٢) المضلّعات المنتظم

Regular Polygons

سنستخدم أفكارًا من الجبر والهندسة لإيجاد قيم n بحيث يكون المضلّع المنتظم ذو n من الأضلاع قابلاً للإنشاء . ولتوفير الجهد نقدم التعريف التالي :

تعريف

نقول إنّ العدد الصحيح الموجب n قابل للإنشاء إذا كان المضلّع المنتظم ذو n من الأضلاع قابلاً للإنشاء باستخدام المسطرة والفرجار .

الخطوة الأولى هي اختصار قيم n لتكون قوى عدد أوّلي .

تمهيدية (١٧,٥)

إذا كان n قابل للإنشاء و m يقسم n فإنّ m قابل للإنشاء. وإذا كان m و n أوليين نسبياً وقابلين للإنشاء فإنّ $m\,n$ قابل للإنشاء.

البرهان

إذا كان m يقسم n فإنّنا نستطيع إنشاء مضلع منتظم ذي m من الأضلاع بتوصيل كل d رأس في المضلع المنتظم ذي n من الأضلاع حيث $d = n/m$. وإذا كان m و n أوليين نسبيًا فإننا نستطيع ايجاد عددين صحيحين a و b بحيث يكون $am + bn = 1$.
إذن

$$\frac{1}{mn} = a \times \frac{1}{n} + b \times \frac{1}{m} .$$

ومن ثمّ من الزاويتين $2\pi/m$ و $2\pi/n$ نستطيع إنشاء الزاوية $2\pi/mn$ ومنها نستطيع إنشاء المضلّع المنتظم ذي $m\,n$ من الآضلاع. Δ

من هذه التمهيدية نحصل مباشرة على:

نتيجة (١٧,٦)

إذا كان $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ حيث $p_1, \dots, p_r$ أعدادًا أولية مختلفة فإنّ n قابل للإنشاء إذا وفقط إذا كان كل $p_i^{\alpha_1}$ قابلاً للإنشاء. Δ

وكذلك فإنّه من السهل الحصول على:

تمهيدية (١٧,٧)

إذا كان α عددًا صحيحًا موجبًا فإن 2^α قابل للإنشاء.

البرهان

نستطيع تنصيف الزاوية باستخدام المسطرة والفرجار، وبذلك نستطيع إنشاء 2^α باستخدام الاستنتاج الرياضي على α. Δ

مما سبق نستطيع أن نختصر المسألة إلى قوى عدد أوّلي فردي. الآن نقدم الأفكار

الجبرية : في حقل الأعداد المركبة نجد أنّ مجموعة الجذور النونية للعدد 1 تمثل رؤوس مضلع منتظم ذي n من الأضلاع . وعلاوة على ذلك فإنّ هذه الجذور هي أصفار كثيرة الحدود التالية :

$$t^{n} -1 = (t-1)(t^{n-1} + t^{n-2} + ... + t + 1) .$$

سنركّز اهتمامنا على العامل الثاني من الطرف الأيمن .

تمهيديّة (١٧,٨)

ليكن p عددًا أوليًا بحيث يكون p^n قابلاً للإنشاء ، وليكن ε هو الجذر p^n البدائي للعدد 1 في $\mathbb{C}$. عندئذ درجة كثيرة حدود ε الأصغرية على Q هي قوة للعدد 2 .

البرهان

ليكن $\varepsilon = e^{2\pi i/p^n}$ ، بما أنّ p^n قابل للإنشاء فإنّنا نستطيع إنشاء النقطة (α,β) حيث $\alpha = \cos(2\pi/p^n)$ و $\beta = \sin(2\pi/p^n)$ وذلك بإسقاط رأس من رؤوس المضلع المنتظم ذي p^n ضلعًا على محوري الإحداثيات . وباستخدام نظرية (٢ , ٥) نجد أنّ :

$$[Q(\alpha,\beta) : Q] = 2^{r}$$

حيث $r \in \mathbb{Z}$. إذن

$$[Q(\alpha,\beta, i) : Q] = 2^{r+1} .$$

ولكن $\varepsilon = \alpha + i\beta$ ينتمي إلى $Q(\alpha,\beta, i)$ ومن ثم فإنّ $[Q(\varepsilon) : Q]$ قوة للعدد 2 وذلك لأنّ $Q(\varepsilon) \subseteq Q(\alpha,\beta,i)$ ، إذن درجة كثيرة حدود ε الأصغرية على Q هي قوة للعدد 2 .

الخطوة التالية هي حساب كثيرات الحدود الأصغرية لإيجاد درجة كل منها . وفي الحقيقة يكفي أن ندرس الحالتين p و p^2 فقط .

تمهيديّة (١٧,٩)

إذا كان p عددًا أوليًا وكان ε هو الجذر p البدائي للعدد 1 في $\mathbb{C}$ فإنّ كثيرة حدود

ε الأصغرية على Q هي:

$$f(t) = 1 + t + \ldots + t^{p-1}.$$

البرهان

لاحظ أنّ $f(t) = (t^p - 1) / (t - 1)$ ، وبما أنّ $\varepsilon^p - 1 = 0$ و $\varepsilon \neq 1$ فإنّ $f(\varepsilon) = 0$. ولإكمال البرهان يكفي أن نبرهن على أنّ $f(t)$ لا مختزلة. ضع $t = 1 + u$ حيث u مجهول جديد، إذن $f(t)$ لا مختزلة على Q إذا وفقط إذا كانت $f(1 + u)$ لا مختزلة. ولكن

$$f(1 + u) = \frac{(1+u)^p - 1}{u} = u^{p-1} + ph(u)$$

حيث h كثيرة حدود في u على $\mathbb{Z}$ وحدّها الثابت هو 1 . وباستخدام نظرية (٢ , ٥) نجد أنّ $f(1+u)$ لا مختزلة عل Q . Δ

تمهيدية (١٧,١٠)

إذا كان p عددًا أوليًا وكان ε الجذر p^2 البدائي للعدد 1 في $\mathbb{C}$ فإنّ كثيرة حدود ε الأصغرية على Q هي:

$$g(t) = 1 + t^p + \ldots + t^{p(p-1)}.$$

البرهان

لاحظ أنّ $g(t) = \dfrac{(t^{p^2} - 1)}{(t^p - 1)}$ ، بما أنّ $\varepsilon^{p^2} - 1 = 0$ و $\varepsilon^p - 1 \neq 0$ فإنّ $g(\varepsilon) = 0$. ويكفي أن نثبت أن $g(t)$ لا مختزلة على Q . وكما في التمهيديّة السابقة نأخذ $t = 1 + u$. إذن

$$g(1+u) = \frac{(1+u)^{p^2} - 1}{(1+u)^p - 1}$$

ولكن بأخذ قياس العدد p نجد أنّ:

$$\frac{(1+u^{p^2})-1}{(1+u^p)-1} = u^{p(p-1)} \ .$$

إذن $g(1+u) = u^{p(p-1)} + pk(u)$ حيث $k(u)$ كثيرة حدود في u على $\mathbb{Z}$. ومن

$$g(1+u) = 1 + (1+u)^p + \ldots + (1+u)^{p(p-1)}$$

نجد أنّ الحد الثابت في k هو 1 ، وباستخدام نظريّة (٥ , ٢) نجد أنّ $g(1+u)$ لا مختزلة على Q. Δ

نقدّم الآن النظريّة الرئيسة .

نظرية (١١ ,١٧) (جــاوس)

المضلّع المنتظم ذو n من الأضلاع قابل للإنشاء باستخدام المسطرة والفرجار إذا وفقط إذا كان

$$n = 2^r p_1 \ldots . p_s$$

حيث r و s عددان صحيحان غير سالبين ، و $p_1, \ldots, p_s$ أعداد أولية فردية على الصورة

$$p = 2^{2^{r_i}} + 1$$

حيث r_i أعداد صحيحة موجبة .

البرهان

لنفرض أنّ n قابل للإنشاء . من المكن كتابة n على الصورة

$$n = 2^r p_1^{\alpha_1} \ldots . p_s^{\alpha_s}$$

حيث $p_1, \ldots, p_s$ أعداد أوّلية فرديّة مختلفة . وباستخدام النتيجة (٦ , ١٧) نجد أنّ كلّ $p_i^{\alpha_i}$ قابل للإنشاء . وإذا كان $\alpha_i \geq 2$ فإن p_i^2 قابل للإنشاء وذلك باستخدام نظرية (٣ , ١٧) . وباستخدام التمهيدية (٨ , ١٧) نجد أنّ درجة كثيرة الحدود الأصغرية للجذر p_i^2 البدائية للعدد 1 على Q هي قوة للعدد 2 . وباستخدام التمهيدية (١٠ , ١٧) نجد أنّ $p_i(p_i - 1)$ هو قوّة للعدد 2 وهذا مستحيل لأنّ p_i فردي . إذن $\alpha_i = 1$ لكل i . ومنه فإنّ p_i قابل للإنشاء . وباستخدام التمهيدية (٩ , ١٧) نجد أنّ:

$$p_i - 1 = 2^{s_i}$$

حيث $s_i \in \mathbb{Z}$. لنفرض أنّ $a > 1$ هو قاسم فردي للعدد s_i ومن ثمّ فإنّ $s_i = ab$. إذن $p_i = (2^b)^a + 1$.

وبما أنّ a فردي فإنّ:

$$t^a + 1 = (t+1)(t^{a-1} - t^{a-2} + \ldots + 1)$$

ومنه فإنّ $2^b + 1$ يقسم p_i وهذا مستحيل.

إذن لا يمكن أن يكون هناك قاسم فردي للعدد s_i ، ومن ثمّ فإنّ $s_i = 2^{r_i}$ حيث $r_i \in \mathbb{Z}^+$.

وللبرهان على العكس يكفي أن نأخذ قواسم العدد n التي على شكل قوّة لعدد أوّلي وذلك باستخدام النتيجة (٦ , ١٧). وباستخدام التمهيدية (٧ , ١٧) نجد أن 2^r قابل للإنشاء. يجب أن نبرهن على أنّ كل p_i قابل للإنشاء. ولنفرض أنّ ε هو الجذر p_i البدائي للعدد 1. إذن باستخدام التمهيدية (٩ , ١٧) يوجد a بحيث يكون:

$$[Q(\varepsilon) : Q] = p_i - 1 = 2^a .$$

الآن $Q(\varepsilon)$ هو حقل انشطار لكثيرة الحدود:

$$f(t) = 1 + \ldots + t^{p-1}$$

على Q ومن ثمّ فإنّ $Q(\varepsilon) : Q$ ناظمي. ولكن هذا الامتداد قابل للفصل أيضًا (لأنّ المميّز صفر). وباستخدام التمهيديّة (٤ , ١٤) نجد أنّ زمرة جالوا $\Gamma(Q(\varepsilon) : Q)$ أبيلية. ولنفرض أنّ $K = \mathbb{R} \cap Q(\varepsilon)$. إذن

$$\cos(2\pi / p_i) = (\varepsilon + \varepsilon^{-1}) / 2 \in K .$$

الآن درجة $Q(\varepsilon) : K$ هي 2 ومن ثمّ باستخدام النظرية (١ , ١١) نجد أنّ $\Gamma(Q(\varepsilon) : K)$ هي زمرة جزئيّة من $G = \Gamma(Q(\varepsilon) : Q)$ رتبتها 2. وبما أنّ G أبيلية فإنّ $\Gamma(Q(\varepsilon) : K) \lhd G$. إذن $K : Q$ امتداد ناظمي درجته 2^{a-1} . وباستخدام النظرية (٤ , ١٧) نجد أنّ النقطة $(\cos(2\pi / p_i), 0)$ قابلة للإنشاء وبهذا يتمّ البرهان. Δ

(١٧,٣) أعداد فيرما

Fermat Numbers

المسألة الآن هي عبارة عن مسألة في نظرية الأعداد ، ولنعتبر التعريف التالي :

تعريف

عدد فيرما من الرتبة n هو العدد $F_n = 2^{2^n} + 1$.

يصبح السؤال الآن : لأي قيم n يكون العدد F_n أوّلي ؟ .

لقد لاحظ فيرما في العام ١٦٤٠م أنّ الأعداد

$F_0 = 3$ ، $F_1 = 5$ ، $F_2 = 17$ ، $F_3 = 257$ و $F_4 = 65537$

جميعها أعداد أوّلية ، ولقد أعتقد أن جميع الأعداد F_n أوّلية ، ولكن أويلر دحض هذا الاعتقاد في العام ١٧٣٢م .

إنّ أعداد فيرما الأولية المعروفة هي فقط تلك الأعداد التي اكتشفها فيرما .

قضية (١٧,١٢)

المضلّع المنتظم ذو p من الأضلاع حيث p عدد أولي بحيث $p < 10^{40000}$ *قابل للإنشاء إذا كان* $p = 2, 3, 5, 17, 257, 65537$.

(١٧,٤) الإنشـاءات

Constructions

لقد تمّ إنشاء المضلّع المنتظم ذي 17 ضلعًا من قبل عدد من العلماء ، وكان أوّل إنشاء تمّ نشره هو للعالم هوجينين (Huguenin) في العام ١٨٠٣م [انظر Klein, 1913] . ولقد تمّ برهان عدد من هذه الإنشاءات باستخدام الهندسة التركيبية (أي الهندسة الإقليدية بدون إحداثيات) . وقد نشر العالم راشيلوت (Richelot) في العام ١٨٢٢م عدّة أبحاث لإنشاء المضلّع المنتظم ذي 257 ضلعًا تحت أطول عنوان صادفته بحياتي . لقد ذكر العالم بل (Bell) عام ١٩٦٥م قصّة طالب فائق الحماس الذي كلّفه بإيجاد

إنشاء للمضلّع المنتظم ذي 65537 ضلعًا وعاد الطالب بهذا الإنشاء بعد عشرين عامًا. وبالرغم من أنّ هذه القصة يصعب تصديقها إلا أنّها ليست مبالغة من العالم بل لأنّ البروفيسور هيرمز (Hermes) استغرق عشرة أعوام في هذه المسألة وأعتقد أن بحثه لا يزال محفوظاً في جوتنجن (Gottingen).

إنّ إحدى الطرق لإنشاء مضلّع منتظم ذي 17 ضلعًا هي الاعتماد على ما قدمناه في هذا الفصل، والتي تزودنا في الحقيقة بإنشاء كامل بعد إجراء بعض الحسابات الإضافية. وسنقدم هنا إنشاء مأخوذًا من كتاب (Hardy and Wright, 1962).

إنّ أوّل أهدافنا هو ايجاد عبارات لأصفار كثيرة الحدود:

$$\frac{t^{17}-1}{t-1} = t^{16}+\dots+t+1 \qquad (١٧,١)$$

على $\mathbb{C}$. لنفرض أنّ $\theta = 2p/17$ وأنّ

$\varepsilon_k = e^{ki\theta} = \cos k\theta + i \sin k\theta$.

إذن أصفار (١٧,١) في $\mathbb{C}$ هي $\varepsilon_1, \dots, \varepsilon_{16}$.

الجدول التالي يبين قوى العدد 3 قياس 17:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^m	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

لنفرض أنّ:

$$x_1 = \varepsilon_1 + \varepsilon_9 + \varepsilon_{13} + \varepsilon_{15} + \varepsilon_{16} + \varepsilon_8 + \varepsilon_4 + \varepsilon_2$$
$$x_2 = \varepsilon_3 + \varepsilon_{10} + \varepsilon_5 + \varepsilon_{11} + \varepsilon_{14} + \varepsilon_7 + \varepsilon_{12} + \varepsilon_6$$
$$y_1 = \varepsilon_1 + \varepsilon_{13} + \varepsilon_{16} + \varepsilon_4$$
$$y_2 = \varepsilon_9 + \varepsilon_{15} + \varepsilon_8 + \varepsilon_2$$
$$y_3 = \varepsilon_3 + \varepsilon_5 + \varepsilon_{14} + \varepsilon_{12}$$
$$y_4 = \varepsilon_{10} + \varepsilon_{11} + \varepsilon_7 + \varepsilon_6$$

الآن:

$$\varepsilon_k + \varepsilon_{17-k} = 2\cos(k\theta) \qquad (١٧,٢)$$

حيث $k = 1, ..., 16$ ومن ثمّ فإنّ:

$$x_1 = 2(\cos\theta + \cos 8\theta + \cos 4\theta + \cos 2\theta)$$
$$x_2 = 2(\cos 3\theta + \cos 7\theta + \cos 5\theta + \cos 6\theta)$$

$$\begin{aligned} y_1 &= 2(\cos\theta + \cos 4\theta) \\ y_2 &= 2(\cos 8\theta + \cos 2\,\theta) \\ y_3 &= 2(\cos 3\theta + \cos 5\theta) \\ y_4 &= 2(\cos 7\theta + \cos 6\theta) \end{aligned} \qquad (١٧,٣)$$

ومن المعادلة (١ , ١٧) نجد أنّ:

$$x_1 + x_2 = -1$$

وباستخدام المعادلة (٣ , ١٧) والمعادلة:

$$2\cos m\theta \cos n\theta = \cos(m+n)\theta + \cos(m-n)\theta$$

نجد أنّ

$$\begin{aligned} x_1x_2 = 2\{&\cos 4\theta + \cos 2\theta + \cos 6\theta + \cos 4\theta + \cos 6\theta + \cos 5\theta \\ &+ \cos 7\theta + \cos 11\theta + \cos 5\theta + \cos 15\theta + \cos\theta + \cos 13\theta + \cos 3\theta \\ &+ \cos 14\theta + \cos 21\theta + \cos 7\theta + \cos\theta + \cos 3\theta + \cos 11\theta + \cos\theta \\ &+ \cos 9\theta + \cos 2\theta + \cos 10\theta + \cos 5\theta + \cos\theta + \cos 9\theta + \cos 5\theta \\ &+ \cos 7\theta + \cos 3\theta + \cos 4\theta + \cos 8\theta\} = -4 \end{aligned}$$

وذلك باستخدام المعادلة (٢ , ١٧). إذن x_1 و x_2 صفران لكثيرة الحدود:

$$t^2 + t - 4 \qquad (١٧,٤)$$

وبما أنّ $x_1 > 0$ فإنّ $x_1 > x_2$.

وباستخدام حساب المثلثات كما أعلاه نجد أنّ:

$$y_1 + y_2 = x_1 \text{ و } y_1 y_2 = -1$$

وأنّ y_1 و y_2 صفران لكثيرة الحدود:

$$t^2 - x_1 t - 1 \quad (١٧ , ٥)$$

وكذلك $y_1 > y_2$ بالمثل نجد أنّ y_3 و y_4 صفري لكثيرة الحدود:

$$t^2 - x_2 t - 1 \quad (١٧ , ٦)$$

وأنّ $y_3 > y_4$.

الآن

$$2\cos\theta + 2\cos4\theta = y_1$$

$$4\cos\theta\cos4\theta = 2(\cos5\theta + \cos3\theta) = y_3$$

ومن ثمّ فإنّ

$$z_2 = 2\cos 4\theta \text{ و } z_1 = 2\cos\theta$$

صفران لكثيرة الحدود:

$$t^2 - y_1 t + y_3 \quad (١٧ , ٧)$$

وأنّ $z_1 > z_2$.

وبحلّ المعادلات (١٧ , ٤) – (١٧ , ٧) واستخدام المتراجحات نحصل على المعادلة:

$$\cos\theta = \frac{1}{6}\left\{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}} + \sqrt{68+12\sqrt{17}-16\sqrt{34+2\sqrt{17}}-2\left(1-\sqrt{17}\right)\sqrt{34-2\sqrt{17}}}\right\}$$

ممّا سبق نستطيع الحصول على الإنشاء الهندسي للمضلع المنتظم ذي 17 ضلعًا وذلك بإنشاء الجذور التربيعية المناسبة. وباستخدام قدر أكبر من التفكير نستطيع الحصول على إنشاء أكثر جمالاً واقتناعًا.

الطريقة التالية تنسب إلى ريشموند (Richmond) عام ١٨٩٣م.

لنفرض أنّ φ هي أصغر زاوية حادة موجبة بحيث يكون $\tan4\varphi = 4$. إذن كل زاوية من الزوايا φ ، 2φ و 4φ يجب أن تكون حادة، ومن ثمّ فإنّنا نستطيع كتابة (١٧ , ٤) كالتالي:

$$t^2 + 4t\cos 4\varphi - 4$$

حيث صفراها هما:

$2\tan 2\varphi$ و $-2\cot 2\varphi$.

ومن ثمّ فإنّ:

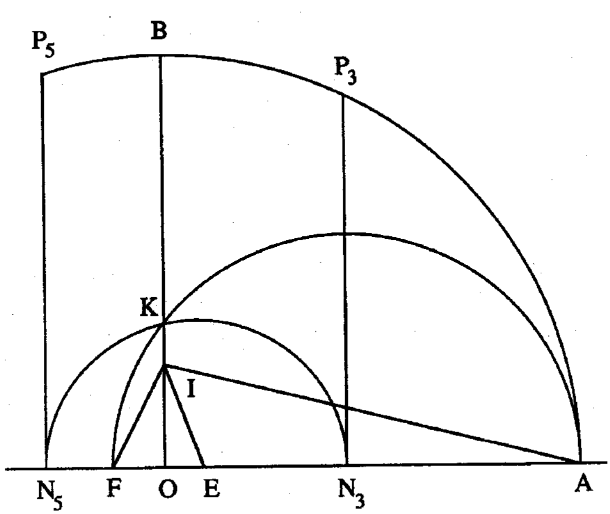
$x_1 = 2\tan 2\varphi$ و $x_2 = -2\cot 2\varphi$

ومنه فإنّ

$$y_1 = \tan(\varphi + \pi/4)$$
$$y_2 = \tan(\varphi - \pi/4)$$
$$y_3 = \tan\varphi$$
$$y_4 = -\cot\varphi$$

إذن

$$2(\cos 3\theta + \cos 5\theta) = \tan\varphi$$
$$4\cos 3\theta \cos 5\theta = \tan(\varphi - \pi/4) \qquad (١٧,٨)$$



شكل (٢٧). إنشاء مضلّع منتظم ذي 17 ضلعًا.

الآن (كما فى الشكل ٢٧) نفرض أنّ OA و OB نصفا قطرين متعامدين لدائرة . خذ $OI = \frac{1}{4} OB$ و $O\hat{I}E = \frac{1}{4} \; O\hat{I}A$ ، جد F على AO بحيث يكون $E\hat{I}F = \pi/4$، واجعل الدائرة التي قطرها AF تقطع OB في K والدائرة التي مركزها E وتمر في K تقطع OA في N_3 و N_5 كما هو موضح، وارسم $N_3 P_3$ و $N_5 P_5$ عمودين على OA . إذن $O\hat{I}A = 4\varphi$ و $O\hat{I}E = \varphi$. وكذلك

$$2(\cos A\hat{O}P_3 + \cos A\hat{O}P_5) = 2\,\frac{ON_3 - ON_5}{OA}$$

$$= 4\,\frac{OE}{OA} + \frac{OE}{OI} = \tan\varphi$$

وأيضًا

$$4\cos A\hat{O}P_3 \cos A\hat{O}P_5 = -4\,\frac{ON_3 \times ON_5}{OA \times OA}$$

$$= -4\,\frac{OK^2}{OA^2} \quad = -4\,\frac{OF}{OA} = -\,\frac{OF}{OI}$$

$$= \tan(\varphi - \pi/4)$$

وبمعادلة ذلك مع المعادلة (١٧,٨) نجد أنّ:

$$A\hat{O}P_3 = 3\,\theta$$

$$A\hat{O}P_5 = 5\,\theta$$

إذن A ، P_3 ، P_5 هي الرؤوس رقم صفر، ثلاث، خمسة للمضلّع المنتظم ذي 17 ضلعًا المرسوم داخل الدائرة المعينة . ونستطيع الآن وبسهولة أن نجد باقي الرؤوس .

تمــارين

(١٧,١) تحقق من كل من الإنشاءات التقريبية التالية للمضلّعات المنتظمة (أولدرويد ١٩٥٥).

(١) ذو سبعة أضلاع : أنشيء $\arccos[(4+\sqrt{5})/10]$ إذا علمت زاوية

قيمتها $2\pi/7$ تقريبًا.

(ب) ذو تسعة أضلاع : أنشيء $\arccos[(5\sqrt{3}-1)/10]$.

(ج) ذو أحد عشر ضلعًا : أنشيء كلاً من $\arccos(\frac{8}{9})$ و $\arccos(\frac{1}{2})$ وخذ حاصل طرحهما.

(د) ذو ثلاثة عشر ضلعًا : أنشيء كلاً من $\arctan(1)$ و$\arctan[(4+\sqrt{5})/20]$ وخذ حاصل طرحهما.

(١٧,٢) إذا كان n عددًا فرديًا فاثبت أن المضلّعات المنتظمة ذات n من الأضلاع التي يمكن إنشاؤها هي فقط المضلعات التي يكون فيها n قاسما للعدد $2^{32}-1$.

(١٧,٣) جد العدد التقريبي لمراتب F_{1945} . ثم وضّح صعوبة إيجاد قواسم لأعداد فيرما.

(١٧,٤) استخدم المعادلة

$$641 = 5^4 + 2^4 = 5 \times 2^7 + 1$$

لإثبات أنّ 641يقسم F_5 .

(١٧,٥) أثبت أنّ

$$F_{n+1} = 2 + F_n F_{n-1} \dots F_0$$

ثم استنتج أنّ F_m و F_n أوّليان نسبيًا إذا كان $m \neq n$، وبرهن على وجود عدد غير منته من الأعداد الأولية.

(١٧,٦) جد جميع قيم $n \le 100$ بحيث يكون المضلّع المنتظم ذو n ضلعًا قابلاً للإنشاء باستخدام المسطرة والفرجار.

(١٧,٧) تحقق من الانشاء التالي للخماسي المنتظم : ارسم دائرة مركزها O ونصف قطريها OP_0 و OB متعامدان، وافرض أن D هي نقطة منتصف OB ثم صل DP_0 . نصف $O\widehat{D}P_0$ ليلاقي OP_0 في N، وارسم NP_1 ليكون عموديًا على OP_0 ويقطع الدائرة في P_1. عندئذ تكون النقطتان P_0 وP_1 هما رأسًا الخماسي رقم صفر و رقم 1 المرسوم داخل الدائرة.

(١٧,٨) ضع علامة صح أو خطأ أمام كل مما يلي :

(أ) لا يمكن أن يكون العدد $2^n + 1$ أوليا إلا إذا كان n قوة للعدد 2

(ب) إذا كان n قوة لعدد فإن $2^n + 1$ أولي .

(ج) المضلع المنتظم ذو 771 ضلعًا قابل للإنشاء باستخدام المسطرة والفرجار .

(د) المضلع المنتظم ذو 768 ضلعًا قابل للإنشاء باستخدام المسطرة والفرجار .

(هـ) المضلع المنتظم ذو 25 ضلعًا قابل للإنشاء باستخدام المسطرة والفرجار .

(و) إذا كان p عددًا أوليًا فرديًا فإنّه لا يمكن إنشاء المضلع المنتظم ذي p^2 ضلعاً باستخدام المسطرة والفرجار .

(ز) إذا كان n عددًا صحيحًا موجبًا فإنّه من الممكن إنشاء مستقيم طوله $\sqrt{n}$ باستخدام المسطرة والفرجار .

(ح) إذا كانت احداثيات نقطة تنتمي إلى امتداد ناظمي للحقل Q درجته قوة 2 فإنّه باستطاعتنا إنشاء هذه النقطة باستخدام المسطرة والفرجار .

(ط) المضلع المنتظم ذو 51 ضلعًا يمكن إنشاؤه باستخدام المسطرة والفرجار .

(ي) إذا كان p عددًا أوليًا فإنّ $t^{p^2} - 1$ لا مختزلة على Q .

(٩ , ١٧)* ناقش انشاء المضلعات المنتظمة باستخدام المسطرة والفرجار وتثليثالزاوية . (على سبيل المثال كل من المضلع ذي 9 أضلاع والمضلّع ذي 13 ضلعًا قابل للإنشاء . استخدم حل المعادلة من الدرجة الثالثة بواسطة حساب المثلثات) .

الفصل الثامن عشر

حساب زمرة جالوا

Calculating Galois Groups

إنّ تطبيق نظريّة جالوا يتطلب منّا ايجاد زمرة جالوا لكثيرة الحدود تحت الدراسة ، وهذه مهمة أبعد من أن تكون سهلة المنال . والذي قمنا به إلى حد الآن هو استخدام بعض السمات المميّزة لكثيرة الحدود لحساب زمرة جالوا لها ، أو تقديم بعض النتائج التي لا تتطلب منا غير معرّفة بعض خواص زمرة جالوا ، وقد حان الوقت لنواجه هذه المهمة . وهذا الفصل يحتوي على دراسة تامة لكثيرتي الحدود من الدرجة الثالثة والدرجة الرابعة ، سنقدم أيضًا خوارزمية لحساب زمرة جالوا لأيّة كثيرة حدود والتي سيكون لها أهمية من الناحية النظرية على الرغم من كونها مزعجة جدًا من الناحية التطبيقية . ومن الجدير بالذكر وجود طرق أفضل ولكنّها تقع خارج نطاق هذا الكتاب .

(١٨,١) طريقة مباشرة لحل معادلة الدرجة الثالثة
Bare Hands on The Cubic

سنبدأ بحساب زمرة جالوا لمعادلة الدرجة الثالثة على Q حيث نستطيع إيجادها بطرق مباشرة . اعتبر كثيرة الحدود من الدرجة الثالثة :

$$f(t) = t^3 - s_1 t^2 + s_2 t - s_3 \in Q[t] .$$

حيث إنّ المعاملات s_j هي كثيرات الحدود المتناظرة الابتدائيّة في الأصفار $\alpha_1, \alpha_2, \alpha_3$. إذا كانت f قابلة للاختزال فإنّه من السهل حساب زمرة جالوا لها : فهي 1 إذا كانت جميع الأصفار كسرية و S_2 ما عدا ذلك . ولنفرض أنّ f لامختزلة على Q، ليكن $\Sigma = Q(\alpha_1, \alpha_2, \alpha_3)$ حقل انشطار f على Q . وباستخدام نظرية (١٤,٩) نجد أن زمرة جالوا هي زمرة جزئيّة متعدية من S_3 . إذن فهي إمّا أن تكون

S_3 أو A_3 ، ولنفرض أنّها A_3. ما هي المعلومات التي نحصل عليها من ذلك عن الأصفار $\alpha_1, \alpha_2, \alpha_3$ ؟ من تقابل جالوا نجد أنّ حقل A_3 الثابت $A_3^\dagger$ هو Q ، وإن عناصر A_3 هي (1) , (123) , (132). وإنّ أيّة عبارة في $\alpha_1, \alpha_2, \alpha_3$ تبقى ثابتة تحت تأثير التبديلات الدورية ويجب أن تنتمي إلى Q. هناك عبارتان واضحتان من هذا النوع هما :

$$\varphi = \alpha_1^2 \alpha_2 + \alpha_2^2 \alpha_3 + \alpha_3^2 \alpha_1$$

$$\psi = \alpha_1^2 \alpha_3 + \alpha_2^2 \alpha_1 + \alpha_3^2 \alpha_2$$

في الحقيقة وبجهد بسيط نستطيع أن نبرهن على أنّ

$$A_3^\dagger = Q(\varphi , \psi)$$

(انظر تمرين ٣ , ١٨). وبكلام آخر ؛ فإنّ زمرة جالوا لكثيرة الحدود f هي A_3 إذا وفقط إذا كان كلّ من φ و ψ كسرًا .

سنحسب الآن φ و ψ. بما أنّ S_3 مُولّدة من A_3 و (12) وأنّ (12) تبدل φ و ψ فإنّ كلاً من $\varphi+\psi$ و $\varphi\psi$ كثيرة حدود متناظرة ابتدائية في $\alpha_1, \alpha_2, \alpha_3$. وباستخدام نظرية (٩ , ٢) نجد أنّهما كثيرتي حدود في s_1, s_2, s_3 ، ويمكن حساب كثيرتي الحدود كالتالي : لدينا

$$. \ \varphi + \psi = \sum_{i \neq j} \alpha_i^2 \alpha_j$$

وبالمقارنة مع

$$s_1 s_2 = (\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1 \alpha_2 + \alpha_2 \alpha_3 + \alpha_3 \alpha_1)$$

$$= \sum_{i \neq j} \alpha_i^2 \alpha_j + 3 \alpha_1 \alpha_2 \alpha_3$$

نجد أنّ :

$$\varphi + \psi = s_1 s_2 - 3 s_3$$

حيث g_i دوال في $s_1,\cdots,s_n$ يمكن حسابها بالتفصيل، وعلى وجه الخصوص نجد أنّ $Q \in K[t,x_1,\cdots,x_n]$ ، ونكتب الآن Q كحاصل ضرب كثيرات حدود لا مختزلة في $K[t,x_1,\cdots,x_n]$:

$$Q = Q_1 Q_2 \cdots Q_k$$

وفي الحلقة $\Sigma[t,x_1,\cdots,x_n]$ نجد أنّ

$$Q_j = \prod_{\sigma \in s_j} \left(t - \sigma_x(\beta)\right)$$

حيث S_n هي اتحاد المجموعات الجزئيّة غير المتقاطعة S_j. نعيد الترقيم بحيث يكون عنصر S_n المحايد ينتمي إلى S_1 ومن ثمّ فإنّ $t - \beta$ يقسم Q_1 في $\Sigma[t,x_1,\cdots,x_n]$.

إذا كان $\sigma \in S_n$ فإنّ

$$. Q = \sigma_x Q = (\sigma_x Q_1) \ldots (\sigma_x Q_k)$$

إذن σ_x تبدّل القواسم اللامختزلة Q_j لكثيرة الحدود Q. إذا فرضنا أنّ

$$G = \{\sigma \in S_n \mid \sigma_x Q_1 = Q_1\}$$

زمرة جزئية من S_n فيكون لدينا:

نظرية (١٨،٣)

زمرة جالوا G لكثيرة الحدود f تماثل الزمرة G.

البرهان

في الحقيقة، المجموعة الجزئيّة S_1 من S_n تساوي G وذلك لأنّ:

$$S_1 = \{\sigma : \Sigma[t,x_1,\cdots,x_n] \text{ في } Q_1 \text{ تقسم } t - \sigma_x\beta\}$$

$$S_1 = \{\sigma : \Sigma[t,x_1,\cdots,x_n] \text{ في } \sigma_x^{-1} Q_1 \text{ تقسم } t - \beta$$

$$= \{\sigma : \sigma_x^{-1} Q_1 = Q_1\} = G$$

ضع

$$H=\prod_{\sigma\in G}\left(t-\sigma_{\alpha}(\beta)\right)=\prod_{\sigma\in G}\left(t-\sigma_{x}(\beta)\right).$$

ومن الواضح أنّ $H\in K[t,x_1,\cdots,x_n]$. و H تقسم Q في $\Sigma[t,x_1,\cdots,x_n]$ ، ومنه فإنّ H تقسم Q في $\Sigma(x_1,\cdots,x_n)[t]$ ، إذن H تقسم Q في $K(x_1,\cdots,x_n)[t]$ ومن ثمّ فإنّ H تقسم Q في $K[x_1,\cdots,x_n]$ ، إذن H هي حاصل ضرب عوامل لا مختزلة Q_j من Q. وبما أن $y - \beta$ تقسم H فإنّ Q_1 أحد هذه العوامل. إذن Q_1 تقسم H في $K[t, x_1,..., x_n]$ ومن ثمّ فإنّ $G\subseteq G$.

وللبرهان على العكس، إذا كان $\gamma\in G$ فإنّ

$$\gamma(Q_1)=\prod_{\sigma\in S_1}(t-\gamma_x\,\sigma_x(\beta))$$

$$=\prod_{\sigma\in S_1}(t-\gamma_x^{-1}\,\sigma_x(\beta))$$

$$=\gamma\alpha^{-1}\prod_{\sigma\in S_1}(t-\sigma_x(\beta))$$

$$=\gamma\alpha^{-1}(Q_1)$$

ولكن $Q_1\in K[t, x_1,..., x_n]$ ، ومن ثمّ فإنّ $\gamma\alpha^{-1}(Q_1)=Q_1$. إذن $\gamma\in G$ وبالتالي فإن $G\supseteq G$. Δ

مثال

لنفرض أنّ α ، β صفرًا كثيرة الحدود $t^2 - A t + B = 0$ حيث $A=\alpha+\beta$ و $B=\alpha\beta$ عندئذ تكون Q هي:

$$Q=(t-\alpha x-\beta y)(t-\alpha y-\beta x)$$

$$= t^2 - t(\alpha x + \beta y + \alpha y + \beta x) + (\alpha^2 + \beta^2)xy + \alpha\beta(x^2 + y^2)$$
$$= t^2 - t(Ax + Ay) + (A^2 - 2B)\,xy + B(x^2 + y^2)$$

وهذه إمّا أن تكون لا مختزلة أو حاصل ضرب كثيرتي حدود من الدرجة الأولى. إذا كان

$$A^2(x+y)^2 - 4[(A^2 - 2B)xy + B(x^2 + y^2)]$$

ليس مربعًا كاملاً فهي لا مختزلة. ولكن هذه العبارة هي

$$(A^2 - 4B)\,(x - y)^2$$

وهذا مربّع كامل إذا وفقط إذا كان $A^2 - 4B$ مربّعًا كاملاً. إذن زمرة جالوا هي الزمرة التافهة إذا كان $A^2 - 4B$ مربّعا كاملاً، أمّا إذا لم يكن $A^2 - 4B$ مربعًا كاملاً فإنّ زمرة جالوا هي S_2.

تمـــارين

(١٨, ١) لتكن $f \in K[t]$ حيث مميز $K \neq 2$. إذا لم يكن $\Delta(f)$ مربعًا كاملاً في K، وكانت G هي زمرة جالوا لكثيرة الحدود f، فأثبت أنّ $K(\delta)$ هو الحقل الثابت للزمرة $G \cap A_n$.

(١٨, ٢) جد صيغة لمايز كثيرة الحدود من الدرجة الثانية.

(١٨, ٣) استخدم ترميز النظرية (١٨, ١) لإثبات أنّ $A_3^{\dagger} = Q(\varphi, \psi)$.

(١٨, ٤) أثبت أنّ δ يساوي محدّد فاندرموند (Vandermonde) التالي:

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ & & \vdots & \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix}$$

جد حاصل ضرب هذه المصفوفة ومنقولها، ثـمّ جد محدّد المصفوفة الناتجة

لإثبات أنّ $\Delta(f)$ يساوي :

$$\begin{vmatrix} n & \lambda_1 & \cdots & \lambda_{n-1} \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ & & \vdots & \\ \lambda_{n-1} & \lambda_n & \cdots & \lambda_{2n-2} \end{vmatrix}$$

حيث $\lambda_k = \alpha_1^k + \ldots + \alpha_n^k$.

ومن ثمّ استخدم تمرين (١٤ , ٢) لحساب $\Delta(f)$ عندما تكون f من الدرجة 2 ، 3 أو 4 . بيّن أنّ النتيجة التي حصلت عليها تتفق مع ما سبق .

(١٨ , ٥) إذا كانت $f(t) = t^n + at + b$ فأثبت أنّ:

$$\Delta(f) = \mu_{n+1}\, n^n\, b^{n-1} - \mu_n (n-1)^{n-1}\, a^n$$

حيث μ_n يساوي 1 إذا كان n مضاعف للعدد 4 ويساوي 1- ما عدا ذلك .

(١٨ , ٦) أثبت أنّ أيّة زمرة جزئيّة متعديّة من S_4 يجب أن تكون إحدى الزمر التالية :

A_4 = الزمرة المتناوبة من الدرجة الرابعة .

$V = \{1,(12)(34), (13)(24), (14)(23)\}$

D_8 = الزمرة المولّدة من V و (12)

C_4 = الزمرة المولّدة من (1234) .

(١٨ , ٧) لتكن f كثيرة حدود لا مختزلة من الدرجة الرابعة على الحقل K الذي مميّزه ≠ 2 ، 3 وممايزُها Δ . ولتكن g هي المفككة التكعيبيّة لـ f وليكن M هو حقل انشطار g . أثبت أنّ:

(أ) $\Gamma(f) = S_4$ إذا وفقط إذا كان Δ ليس مربّعًا كاملاً في K و g لا مختزلة على K .

(ب) $\Gamma(f) = A_4$ إذا وفقط إذا كان Δ مربّعًا كاملاً في K و g لا مختزلة على K .

(ج) $\Gamma(f) = D_8$ إذا وفقط إذا لم يكن Δ مربّعًا كاملاً في K ، g لامختزلة

K و f لا مختزلة على M .

(د) $\Gamma(f) = V$ إذا وفقط إذا كان Δ مربّعًا كاملاً في K و g تنشطر على K .

(هـ) $\Gamma(f) = C_4$ إذا وفقط إذا لم يكن Δ مربّعًا كاملاً في K ، g تنشطر على K و f لا مختزلة على M .

الفصل التاسع عشر

النظرية الأساسية في الجبر
The Fundamental Theorem of Algebra

إذا كان لدينا حقل بحيث تنشطرّ أيّة كثيرة حدود معرفة عليه، فإنّ مثل هذا الحقل يسمى حقلاً جبريًا مغلقًا، والنظرية الأساسية في الجبر تنص على أن حقل الأعداد المركبة حقل جبري مغلق، و هذه النظرية لا تعتبر أساسية للجبر الحديث ولا هي تمامًا نظرية في الجبر، وهذا الذي دفعنا إلى وضع عنوان الباب بين علامتي تنصيص.

(١٩،١) الحقول المرتّبة وامتداداتها
Ordered Fields and their Extensions

إنّ أوّل من قدّم برهانًا لهذه النظريّة هو العالم جاوس (Gauss) في رسالته لنيل درجة الدكتوراه عام ١٧٩٩م وقد أعطى العنوان التالي لبحثه: «برهان جديد على أنّ كل دالّة مُنْطَقَة صحيحة في متغيّر واحد يمكن تفكيكها إلى عوامل حقيقيّة من الدرجة الأولى أو الثانية».

لقد كان جاوس متواضعًا عندما ذكر أنّ هذا هو برهان جديد حيث إنّ برهانه هو أول برهان حقيقي لهذه النظريّة، على الرغم من وجود فجوات في هذا البرهان «من وجهة النظر الحديثة» إلاّ أنّ طبيعة هذه الفجوات طبولوجية ومن السهل سدّها، ولكن لا تعتبر فجوات على الإطلاق في عصر جاوس. ويمكن الاطلاع على برهان جاوس في (Hardy, 1960).

لقد قدّمت بعد ذلك براهين أخرى، وأحد هذه البراهين يستخدم التحليل المركّب [انظر: Titchmarsh, 1960) وهو البرهان الشائع، وهناك برهان آخر قدّمه

كليفورد [Clifford, 1968] مستخدمًا الجبر فقط، وفكرة هذا البرهان تعتمد على إثبات أنّ درجة أيّة كثيرة حدود لا مختزلة على $\mathbb{R}$ هي 1 أو 2 . والبرهان الذّي سنقدّمه هنا ينسب إلى ليجندر (Legendre)، والبرهان الأصلي يحتوي على بعض الفجوات والتي نسدّها باستخدام نظرية جالوا.

ليس منطقيًا أن نجزم بوجود برهان جبري بحت لهذه النظريّة؛ وذلك لأنّ الأعداد الحقيقية (ومن ثم الأعداد المركّبة) تعرّف بدلالة مفاهيم من التحليل مثل متتابعة كوشي، أو قطوع ديدكند، أو إكمال الترتيبات. وسنبدأ بتجريد بعض خواص الأعداد الحقيقية.

تعريف

الحقل المرتّب هو عبارة عن حقل K معرف عليه علاقة $\leq$ بحيث يتحقق التالي:

(١) $k \leq k$ لكل $k \in K$.

(٢) إذا كان $k \leq l$ و $l \leq m$ فإنّ $k \leq m$ لكل $k,l,m \in K$

(٣) إذا كان $k \leq l$ و $l \leq m$ فإنّ $k = l$ لكل $k,l \in K$.

(٤) إذا كان $k,l, \in K$ فإمّا $k \leq l$ أو $l \leq k$.

(٥) إذا كان $k,l,m \in K$ و $k \leq l$ فإنّ $k+m \leq l+m$.

(٦) إذا كان $k,l,m \in K$ و $k \leq l$ و $m \geq 0$ فإنّ $km \leq lm$.

تسمى العلاقة $\leq$ علاقة ترتيب على K. ومن الواضح أيضًا أنّنا نستطيع تعريف العلاقات $<$ و $\geq$ و $>$. كل من الحقلين $\mathbb{R}$ و Q حقل مرتب.

وسنحتاج إلى التمهيديّات التاليّة على الحقول المرتّبة.

تمهيدية(١٩,١)

إذا كان $k \in K$ حيث K حقل مرتّب، فإنّ $k^2 \geq 0$ وكذلك مميّز K يساوي صفرًا.

إذا كان $k \geq 0$ فإنّه باستخدام فقرة (٦) يكون $k^2 \geq 0$ ، ومن ثمّ باستخدام (٣) و(٤) نستطيع أن نفرض أنّ $k < 0$. إذا كان $-k < 0$ فإنّ :

$$0 = k + (-k) > k + 0 = k$$

وهذا تناقض .

إذن $k \geq 0$ ، ومن ثمّ فإنه $k^2 \geq (-k)^2 \geq 0$.

إذن $0 < 1^2 = 1$ ، ومن ثمّ فإنّه لأيّ عدد صحيح موجب n لدينا

$n \times 1 = 1 + ... + 1 > 0$.

إذن $n \times 1 \neq 0$ وبالتالي فإنّ مميّز K هو صفر . Δ

سنقتبس الخاصيّة التاليّة للأعداد الحقيقية :

تمهيدية (١٩,٢)

الحقل $\mathbb{R}$ معرفًا عليه علاقة الترتيب المعتادة حقل مرتّب . كل عدد موجب في $\mathbb{R}$ يوجد له جذر تربيعي في $\mathbb{R}$، وكل كثيرة حدود درجتها عدد فردي على $\mathbb{R}$ يجب أن يكون لها صفر في $\mathbb{R}$.

جميع الخواص في التمهيديّة (٢ , ١٩) يبرهن عليها عادة في أي مقرر تحليل رياضي ويعتمد برهانها على أنّ دالّة كثيرة الحدود متّصلة على $\mathbb{R}$. Δ

الخطوة التالية تقدّم لنا ما نحتاجه من نظريّة جالوا .

تمهيدية (١٩,٣)

إذا كان K حقلاً مميّزه صفر ، وكان M أي امتداد منته للحقل K بحيث $M \neq K$ و $[M : K]$ يقبل القسمة على عدد أولي p فإنّ درجة أي امتداد منته للحقل K يجب أن تكون قوة للعدد p.

البرهان

لنفرض أنّ N امتداد منته للحقل K ، بما أن المميّز صفر فـإنّ N : K قابل للفصل .

ومن الممكن أن نفرض أنّ $N : K$ ناظمي وذلك لأننا نستطيع أخذ الإغلاق الناظمي، ومن ثمّ فإنّ تقابل جالوا متباين وشامل . ولنفرض أن G هي زمرة جالوا للامتداد $N : K$ و P هي زمرة سايلو الجزئيّة من النوع p . وباستخدام نظرية (١ , ١١) نجد أن $[P^{\dagger}:K] = [G:P]$ ، ولكن هذه الدرجة أولية نسبيًا مع p ، إذن $P^{\dagger} = K$ ، ومن ثمّ فإنّ $P = G$ وبالتالي فإن $[N : K] = |G| = p^n$ حيث $n \in \mathbb{Z}$. Δ

نظرية (٤ , ١٩)

ليكن K حقلاً مرتبًا بحيث يوجد جذر تربيعي لكل عنصر موجب، وبحيث يوجد صفر لكل كثيرة حدود درجتها عدد فردي، عندئذ يكون $K(i)$ مغلقًا جبريًا حيث $i^2 = -1$.

البرهان

إذا كان M امتدادًا منتهيًا للحقل K فإنّه إمّا أن تكون $[M : K]$ تساوي 1 أو عددًا زوجيًا، ولإثبات ذلك نفرض أنّ $[M : K] = r > 1$ حيث r عدد فردي، ولنفرض أنّ $\alpha \in M \setminus K$ ، وأنّ m هي كثيرة حدود α الأصغرية. إذن ∂m يقسم r ، ومن ثمّ فإنّ m عدد فردي. وباستخدام الفرض نجد أن لكثيرة الحدود m صفرًا في K ومن ثمّ فهي قابلة للاختزال، وهذا يناقض تمهيدية (٢ , ٣). إذن درجة أيّ أمتداد منته للحقل K يجب أن تكون عددًا زوجيًا. وباستخدام تمهيدية (١ , ١٩) نجد أن مميز K صفر ومن ثم باستخدام تمهيدية (٣ , ١٩) نجد أنّ درجة أيّ امتداد منته للحقل K يجب أن تكون قوة للعدد 2 .

لنفرض أنّ $M \neq K(i)$ هو امتداد منته للحقل $K(i)$ حيث $i^2 = -1$. وبأخذ الإغلاق الناظمي نستطيع أن نفرض أنّ $M : K$ ناظمي، ومن ثمّ فإنّ زمرة جالو للامتداد $M : K$ هي زمرة من النوع 2 . وباستخدام تمهيدية (١٠ , ١٣)، وتقابل جالوا نستطيع أن نجد امتداد N للحقل $K(i)$ بحيث يكون $[N : K(i)] = 2$. وباستخدام قانون حلّ معادلة الدرجة الثانية نجد أنّ $N = K(i)(\alpha)$ حيث $\alpha^2 \in K(i)$. ولكن إذا كان

فإنّ $a, b \in K$

$$\sqrt{a+bi} = \sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}$$

حيث الجذر التربيعي للعدد $a^2 + b^2$ هو الجذر الموجب وإشارة الجذرين الآخرين تختار بحيث يكون حاصل ضربهما يساوي b، إذن هذه الجذور التربيعيّة تنتمي إلى K لأنّ العناصر التي داخلها موجبة. إذن $\alpha \in K(i)$ ، ومن ثمّ فإن $N = K(i)$ وهذا يناقض الفرضية على N . إذن $M = K(i)$، ومن ثم فإنه لا يوجد امتداد منته للحقل K(i) درجته أكبر من 1، إذن درجة أيّة كثيرة حدود لا مختزلة على K(i) تساوي 1 لأنّه ما عدا ذلك فإنّ أيّ حقل انشطار تكون درجته على K(i) أكبر من 1 . إذن K(i) مغلق جبريًا. Δ

نتيجة (١٩,٥) (النظريّة الأساسيّة في الجبر)

حقل الأعداد المركبة $\mathbb{C}$ مغلق جبريًا.

البرهان

خذ $K = \mathbb{R}$ في النظريّة (١٩,٤) واستخدم التمهيديّة (١٩,٢).

تمارين

(١٩,١) برهن على أنّ الحقل K مغلق جبريًا إذا وفقط إذا كان L : K جبريًا فإنّ $L = K$

(١٩,٢) برهن على أنّ أيّ أمتداد جبري للحقل $\mathbb{R}$ يماثل $\mathbb{R} : \mathbb{R}$ أو $\mathbb{C} : \mathbb{R}$.

(١٩,٣) استخدم الاستنتاج الموغل لإثبات أنّ لكلّ حقل K يوجد امتدادجبري مغلق- L . (اقرن أصفارًا لكثيرات حدود لا مختزلة حتى نفاذ هذه الأصفار).

(١٩,٤) أثبت أنّ الحقل $\mathbb{C}$ حقل غير مرتّب، إذا سمحنا بتغيير العمليّات المعرّفة على $\mathbb{C}$ فهل نستطيع جعل $\mathbb{C}$ حقلاً مرتّبًا؟

(١٩,٥) برهن على أن النظريّة التي قدّمها جاوس لنيل درجة الدكتوراه والتي ذكرنا

نصّها في بداية هذا الفصل .

(١٩, ٦) لنفرض أنّ $K : Q$ امتداد منته التوليد، برهن على وجود تشاكل متباين من K إلى $\mathbb{C}$ بالنسبة إلى Q. (**إرشاد:** خذ بعين الاعتبار الأعداد الرئيسة لإقران عناصر متسامية والإغلاق الجبري للحقل $\mathbb{C}$ لإقران عناصر جبريّة). هل تبقى النظرية صحيحة لو أخذنا $\mathbb{R}$ بدلاً من $\mathbb{C}$ ؟

(١٩, ٧) ليكن K حقلاً مرتّبًا . نقول إن المجموعة الجزئيّة S من K محدودة من الأعلى إذاوجد عنصر $k \in K$ بحيث يكون $s \le k$ لكل $s \in S$ ونسمى k بحدّ أعلى للمجموعة S . ونقول إنّ العنصر l هو أصغر حدّ أعلى للمجموعة S إذا كان l حدًا أعلى وكان $l \le m$ لأي حد أعلى آخر m. برهن على أنّه من الممكن إيجاد حقل K ومجموعة جزئية S من K بحيث يكون للمجموعة S حدّ أعلى ولا يكون لها أصغر حد أعلى .

(١٩, ٨) يسمّى الحقل المرتّب K تامًا إذا كان لكلّ مجموعة جزئيّة محدودة S من K أصغر حدّ أعلى . برهن على أنّ أيّ حقل مرتّب تامّ يجب أن يماثل الحقل $\mathbb{R}$ وهذا التماثل يحافظ على الترتيب . (**إرشاد:** يحتوي K على حقل جزئي يماثل Q باستخدام الترتيب المعتاد . افرض أنّ T هي مجموعة جميع الحدود العليا الأصغرية للمجموعات الجزئية المحدودة من Q . أثبت أنّ T تماثل $\mathbb{R}$ وأن T هي الحقل K) .

(١٩, ٩) باستخدام تعريف $\mathbb{R}$ كحقل تامّ مرتّب اثبت الخواص المذكورة في التمهيدية (١٩, ٢) .

(١٩, ١٠) ضع علامة صح أو خطأ أمام كل مما يلي :

(أ) الحقل $\mathbb{C}$ مغلق جبريًا .

(ب) حقل الأعداد الجبرية A مغلق جبريًا .

(ج) الحقل A حقل مرتّب .

(د) الحقل $\mathbb{C}$ حقل غير مرتّب .

(هـ) أية كثيرة حدود على $\mathbb{R}$ تنشطر في $\mathbb{C}$.

(و) إذا كانت f كثيرة حدود على $\mathbb{R}$ وكان K حقل انشطار لها فإنّ $K = \mathbb{R}$ أو $K = \mathbb{C}$.

(ز) مميّز أيّ حقل مرتّب يساوي صفرًا .

(ح) أي حقل مميزه صفر حقل مرتّب .

(ط) كل جذر تربيعي في حقل مرتّب يجب أن يكون موجبًا .

(ي) إذا كان لكل عنصر في حقل K جذر تربيعي في K فإنّه لا يمكن أن يكون K حقلاً مرتبًا .

حلول مختارة

Selected Solutions

في هذا البند سنقدم حلولاً أو إرشادات لبعض تمارين مختارة من التمارين التي وردت في الكتاب.

(١ , ٢) لا . لا يوجد محايد ضربي للحلقة $2\mathbb{Z}$.

(١ , ٣) $\mathbb{Z}_7$ حقل ومجال كامل . كلّ من $\mathbb{Z}_6$ و $\mathbb{Z}_8$ ليس حقلاً ولا مجالاً كاملاً .

(١ , ٤) عمليتا الجمع والضرب إبداليتان .

(١ , ٦) لا يماثل $\mathbb{Z}_4$ لأنّ $\mathbb{Z}_4$ ليس حقلاً . يوجد حقل واحد فقط عدد عناصره 4 (تحت سقف التماثل) .

(١ , ٩) (ا) $r = 49t + 12$, $q = t^4 - 7t - 1$.

(ب) $r = 1$, $q = 1$.

(ج) $q = 2t^2 - \frac{27}{2}t + \frac{137}{4}$, $r = -\frac{697}{4}$

(د) $r = 0$, $q = t^2 - 1$.

(هـ) $q = 4t^4 - 2t^3 + 4t + 2$, $r = -2t + 2$.

(١ , ١٠) (ا) 1، (ب) 1، (ج) 1، (د) $t+2$، (هـ) $t-1$.

(١ , ١٣) $C_2 \times C_2 \times C_2$, $C_2 \times C_2$, C_2 , C_4 .

(١ , ١٤) 2 ، 3 ، 4 ، 6 ، 8 ، 12 و 24 فقط .

(١ , ١٥) FFFTTFTFF ؟.

(٢ , ١) كثيرات الحدود اللا مختزلة هي (ب) ، (ج) ، (د) ، (ز) .

(٢,٢) (أ) $(t^2+\sqrt{2t}+1)(t^2-\sqrt{2t}+1)$.

(هـ) $(t-1)(t^2-6t-3)$

(ز) $(t-3)(t^2+3t+9)$

(ح) $(t+1)(t+\beta)$.

(٢,٣) استخدم نظريّة (٢,٨).

(٢,٦) a^2-4b مربّع كامل إذا وفقط إذا كانت كثيرة الحدود قابلة للاختزال.

(٢,٧) كما في التمرين (٢,٦).

(٢,٨) غير متماثلين لأنّ $\mathbb{Z}_p$ منته، و $\mathbb{Z}_p(t)$ غير منته.

(٢,٩)(أ) $s_1^2-2s_2$

(ب) $s_1^3-3s_1s_2+3s_3$

(ج) $s_1s_2-3s_3$

(د) s_3^2

(هـ) $2s_1^2-6s_2$

(و) $18s_1s_2s_3+s_1^2s_2^2-4s_1^3s_3-4s_2^3-27s_3^2$

(ز) جميع كثيرات الحدود غير متناظرة.

(٢,١٠) ستحصل على كثيرة الحدود من الدرجة الثالثة الأصليّة.

(٢,١١) FFTTFTTFFF .

(٣,٢) (أ) Q.

(ب) Q.

(ج) $\{p+qi : p, q \in Q\}$.

(د) $\{p+q\sqrt{2}+ri+si\sqrt{2} \;\; p,q,r,s \in Q\}$

(هـ) $\{p+q\sqrt{2}+r\sqrt{3}+s\sqrt{6} : p,q,r,s \in Q\}$

(ل) $\mathbb{R}$.

(ك) $\mathbb{C}$.

(٣,٣) (ا) $\{ p + q\sqrt{2} : p,q \in Q \}$

(ب) $\{ p + qi : p,q \in Q \}$

(ج) $\{p + q\alpha + r \alpha^2 : p,q,r \in Q \}$

(د) $\{ p + q\sqrt{5} + r\sqrt{7} + s\sqrt{35} : p,q,r,s \in Q \}$

(هـ) $\{ p + qi\sqrt{11} : p,q \in Q \}$

(٣,٤) (ا) العبارات التي لا تحتوي على قوى t الفردية.

(ب) $K(t)$.

(ج) العبارات التي تحتوي فقط على t^n حيث n مضاعف العدد 5 .

(د) (ا) نفسه.

(٣,٥) **الجبرية**: امتدادات تمرين (٣,٣). **المتسامية**: امتدادات تمرين (٣,٤) جميعها بسيطة على الرغم من عدم وضوح تمرين (٣,٣د).

(٣,٨) (ا) $t^2 + 1$.

(ب) $t^2 + 1$.

(ج) $t^2 - 2$.

(د) $t^2 - t - 1$.

(هـ) $t^2 + t + 1$.

(و) $t^2 + t + 1$.

(ز) $u^2 - t - 1$ (على اعتبار أنّها كثيرة حدود في u).

(٣,١٠) فقط الفقرة (ب).

(٣,١٨) نعم.

(٣,١٩) لا.

(٣,٢٠) TFFFFTTFFF.

(٤,١) (ا) ∞ ، (ب) ∞ ، (ج) 1، (د) 3 ، (هـ) 8، (و) 2 ، (ز) 7 .

(٧ , ٤) لا توجد أيّة دالّة بافتراض الاتّصال .

(١١ , ٤) عندما يكون العنصر في L غير صفري .

(١٣ , ٤) نعم .

(١٦ , ٤) الدرجة تساوي 4 .

(١٨ , ٤) FTFTTFFTTF .

(٤ , ٥) نعم .

(١٠ , ٥) TTTFTTTFFT .

(٩ , ٦) TFTTTFFTFT .

(١ , ٧) (أ) $\sqrt{2} \to \pm\sqrt{2}$

(ب) $\alpha \to \alpha$.

(ج) $\sqrt{2} \to \pm\sqrt{2}$ ، $\sqrt{3} \to \pm\sqrt{3}$

(٢ , ٧) $C_2 \times C_2, C_1, C_2$.

(٣ , ٧) (أ) و (ج) .

(٤ , ٧) الزمرة هي C_2 وتقابل جالوا متباين وشامل .

(٧ , ٧) TTFTFFFTFT .

(١ , ٨) $Q(e^{2\pi i/3})$ ، $Q(i\sqrt{2}, i\sqrt{3})$ ، $Q(\sqrt{2}, e^{\pi i/3})$.

(٢ , ٨) 2, 4, 12 .

(٥ , ٨) جميع الحقول التي عدد عناصرها 25 متماثلة .

(٧ , ٨) خذ حذرك عند التحليل إلى كثيرات حدود لا مختزلة قبل تطبيق النظرية

(٦ , ٨) عندما يكون المميز $p > 0$.

(٨ , ٨) (ب)، (د)، (هـ) .

(٩ , ٨) خطأ لأي درجة > 2 . (اقرن الجذر الحقيقي النوني للعدد 2 مع Q)

(١٢ , ٨) TTTFFTTTFF .

(٤ , ٩) يوجد واحد فقط .

(٥ , ٩) يوجد واحد فقط .

(٦ , ٩) خطأ إذا لم يكن K حقلاً .

(٩,٧) TFTFFTFTTT .

(١٠,١) خطأ للحقل $K(t)$ ، خذ $t \to t^2$.

(١٠,٢) (أ) $Q(\alpha, e^{2\pi i/5})$.

(ب) $Q(\beta, e^{2\pi i/7})$.

(ج) $Q(\sqrt{2}, \sqrt{3})$

(د) $Q(\alpha, \sqrt{2}, e^{2\pi i/3})$.

(هـ) حقل انشطار $t^3 - 3t + 3$.

(١٠,٣) (أ) C_1 ، (ب) C_1 ، (ج) $C_2 \times C_2$ ، (د) C_2 .

(١٠,٤) (أ) $<\gamma, \delta : \gamma^5 = \delta^4 = 1 \;,\; \delta^{-1}\gamma\delta = \gamma^3>$

(ب) $<\gamma, \delta : \gamma^7 = \delta^6 = 1 \;,\; \gamma^{-1}\delta\gamma = \gamma^3>$

(ج) $C_2 \times C_2$

(د) $C_2 \times S_3$.

(١٠,٦) 8 .

(١٠,٧) FTTFFTFTTF .

(١٢,١) (أ) $C_2 \times C_2$ ، (ب) C_2 ، (ج) $C_2 \times C_2$.

(١٣,١) $\{1, a, \ldots, a^{n-1}\}$ دورية ناظمية خارجها C_2.

(١٣,٢) يوجد زمرة جزئيّة من S_n تماثل A_5 .

(١٣,٦) استخدم نظرية كوشي (١٣,١٤).

(١٣,١٤) FTTTFFFTTT .

(١٤,٣) C_{p-1} .

(١٤,٤) قلِّد برهان النظرية (١٤,٨).

(١٤,٨) TTFTTTTTT.

(١٥,٢) (أ) 4 ، (ب) 2 ، (ح) 0 .

(١٥,١١) TFTTFFFFFT .

(١٦,١) 2 ، 3 ، 4 ، 5 ، 17 ، 65536 ، 65537 ، 83521 ، 103823 ، $2^{216091} - 1$
العدد الأخير هو أكبر عدد أوّلي معلوم لوقت كتابة هذا الكتاب .

(١٦,١١) 2 أو n = 1 فقط .

(١٦,١٢) FTTTTTTFFF .

(١٧,٤) 641 يقسم كل من $5^4 \times 2^{28} + 2^{32}$ و $5^4 \times 2^{28} - 1$. حاصل طرحهما هو F_5 . (ينسب البرهان إلى G.T. Bennett) .

(١٧,٦) 1 ، 2 ، 3 ، 4 ، 5 ، 6 ، 8 ، 10 ، 12 ، 15 ، 16 ، 17 ، 20 ، 24 ، 30 ، 32 ، 34 ، 40 ، 48 ، 51 ، 60 ، 64 ، 68 ، 80 ، 96 .

(١٧,٨) TFTTFTTTTF .

(١٩,٤) $i^2 = -1$ مربعًا كاملاً ومن ثمّ فهو موجب وهذا تناقض . وإذا غيّرنا تعريف العمليات على $\mathbb{C}$ ، نستطيع أن نجعله حقلاً مرتبًا : جد تقابل بين $\mathbb{C}$ و $\mathbb{R}$ ثمّ استخدم العمليات على $\mathbb{R}$ لتحصل على عمليات على $\mathbb{C}$.

(١٩,١٠) TTFTTTTFTT .

المراجع
References

GALOIS THEORY

Adamson. I. T. (1964) Introduction to Field Theory. Oliver and Boyd. Edinburg.

Artin. E. (1948) Galois Theory, Notre Dame University Press. Notre Dame.

Carling, d.J. H. (1960) A Course in Galois Theory, Cambridge Univesity Press. Cambridge.

Hadlock, C.R. (1978) Field Theory and its Classical Problems, Carus Mathematical Monographs 19. mathematical Association of America. Washington DC.

Jacobson, N. (1964) Theory of Fields and Galois Theory (Lectures in Abstract Algebra. Vol.3). Van Nostrand. Princeton.

Kaplansky. I. (1969) Fields and Rings. University of Chicago Press. Chicago.

Tignol. Jean-Pierre (1988) Galois Theory of Algebraic Equations. Longman. Lodnon.

Van der Waerden. B.L. (1953) Modern Algebra (2 vols). Ungar. New York.

ADDITIONAL MATHERMATICAL MATERIAL

Cundy. H.M. and Rollett. A.P. (1961) Mathematical Models. Oxford University Press. Oxford.

Halmos. P.R. (1958) Finite-dimensional Vector Space, Van Nostrand, Princeton.

Hardy. G.H. (1960) A Course of Pure Mathematics. Cambridge University Press. Cambridge.

Hardy. G.H. and Wright, E.M. (1962) The Theory of Numbers. Oxford University Press. Oxford.

Ledermann, W. (1961) The Theory of finite Groups. Oliver and Boyd, Edinburgh.

MacDonald. I.D. (1968) The Theory of Groups. Oxford Univeristy Press, Oxford.

Oldroyd. J.C. (1955) Approximate constructions for 7, 9, 11 and 13-sided polygons, Eureka, 18, 20.

Rammanujan. S. (1962) Collected Papers of Srinvasa Ramanujan, Chelsea, New York.

Salmon, G. (1885) Lessons Introductory to the Modern Higher Algebra, Hodges, Figgis,

Dublin.
Titchmarsh, E.C. (1960) The Theroy of Functions, Oxford University Press, Oxford.

HISTORICAL MATERIAL

Bell, E.T. (1965) Men of Mathematics (2 vols). Penguin, Harmonds-worth, Middlesex.
Bertrand. J. (1899) La Vie d'Evariste Galois, par P. Dupuy, Bull. des sciences mathematiques, 23, 198-212.
Bortolotti, E. (1925) L'algebra nella scuola matematica bolognese det secolo XVI, Periodico di Matematica, 5(4), 147-84.
Boubaki, N. (1969) Elements d'Histoire des Mathematiques, Hermann, Paris.
Bourgne, R. and Azra, J.P. (1962) Ecrits et memories mathematiques d'Evarise Galois, Gauthier-Villars. Paris.
Cardano, G. (1931) The Book of my Life, Dent, London.
Clifford, W.K. (1968) Mathematical Papers, Chelsea. New York.
Coolidge, J.L. (1963) The Mathematics of Great Amateurs. Dover. New York.
Dalmas, A. (1956) Evariste Galois revolutionnair et geometre. Fasquelle, Paris.
Dupuy, P. (1896) L vie d'Evariste Galois, Annales of Ecole Normale, 13(3), 197-266.
Galois, E. (1987) Oeuvres mathematiques d'Evariste Galois. Gauthier-Villars. Paris.
Gauss, C.F. (1966) Disquisitiones Arithmetricae, Yale University Press, New Haven.
Huntingdon, E.V. (1905) Trans. Amer. Math. Soc., 6, 181.
Klein F. (1913) Lectures on the Icosahedron and the Solution of Equations of the fifth Degree. Kegan Paul. London.
Klein, F. et al (1962) Famous Problems and other Monographs. Chelsea. new York.
Kollros, L. (1949) Evariste Galosis, Birkhauser, Basle.
Midonick, H. (1965) The Treasury of Mathematics (2 vols). Penguin. Harmondsworth, Middlesex.
Richelot, F.J. (1932) De resolutione algebraica aequationis $x^{257} = 1$, sive de divisione circuli per bisectionam anguli septies repetitam in partes 257 inter se aequales commentatio coronata, Crelle's Journal, IX, 1 - 26. 146-61, 209-30, 337-56.
Richmond, H.W. (1893) Quart, J. Math., 26, 206-7 and Math. Ann., 67(1909), 459-61.
Rothman, A. (1982) The short life of Evariste Galois. Scientific American, April, 112-20.
Taton, R. (1947) Les relations d'Evariste Galois avec les mathematiciens de son temps. Cercle International de synthese, Revue d'histoire des sciences et de leurs applications, 1, 114.

دليل الرموز

Symbol Index

الرمز	المعنى
i	$\sqrt{-1}$
$\begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & \alpha & \delta & \gamma \end{pmatrix}$	تبديل
$\mathbb{Z}$	الأعداد الصحيحة
Q	الأعداد النسبية
$\mathbb{R}$	الأعداد الحقيقية
$\mathbb{C}$	الأعداد المركبة
$I + r$	مجموعة مشاركة $\{i+r : i \in I\}$
R/I	حلقة الخارج
$n\mathbb{Z}$	مضاعفات العدد n
$\mathbb{Z}_n$	الأعداد الصحيحة قياس n
n^*	$(1+...+1+1)$ n من المرّات
$r_0+r_1t+...+r_nt^n$	كثيرة حدود
$\sum r_i t^i$	كثيرة حدود
$R[t]$	حلقة كثيرات الحدود في t
$R[t_1,...,t_n]$	حلقة كثيرات الحدود في n من المجاهيل
$R(t)$	حقل العبارات الكسرية في t

الرمز	المعنى
$R(t_1,\ldots,t_n)$	حقل العبارات الكسرية في n من المجاهيل
∂f	درجة f
$-\infty$	ناقص ما لانهاية
$f \mid g$	f تقسم g
$f \nmid g$	f لا تقسم g
$S_r(t_1,\ldots,t_n)$	كثيرات الحدود المتناظرة الابتدائيّة الرائيّة
$L : K$	امتداد حقلي
$K(Y)$	امتداد حقلي مولَّد من Y
$K(y)$	امتداد حقلي مولَّد من $\{y\}$
$K(y_1,\ldots,y_n)$	امتداد حقلي مولَّد من $\{y_1,\ldots,y_n\}$
(λ, μ)	تماثل امتدادات حقلية
$\mu\vert_K$	اقتصار μ على K
$\ker(\varphi)$	نواة φ
$[L : K]$	درجة امتداد
∞	مالانهاية
A	حقل الأعداد الجبرية
$\Gamma(L : K)$	زمرة جالوا للامتداد $L : K$
M^*	زمرة جالوا للامتداد $M : K$ عندما $K \subseteq M \subseteq L$
$H^\dagger$	حقل H الثابت
$\mathfrak{I}$	مجموعة الحقول الوسطية
$\mathcal{G}$	مجموعة الزمر الجزئية من زمرة جالوا
*	تطبيق في تقابل جالوا
†	تطبيق في تقابل جالوا

الرمز	المعنى
$\binom{P}{r}$	معامل ذات الحدين
Df	تفاضل f
$\|S\|$	عدد S الرئيس
D_8	زمرة ذو الوجهين من الرتبة 8
C_n	زمرة دورية رتبتها n
$H \triangleleft G$	H زمرة جزئيّة ناظميّة من G
V	زمرة كلاين الرباعية
S_n	زمرة التبديلات
A_n	الزمرة المتناوبة
$C_G(x)$	مركز x في G
$Z(G)$	مركز G
$Im(\varphi)$	صورة φ
$N(a)$	معيار a
$T(a)$	أثر a
$GL_2(K)$	زمرة المصفوفات الغير شاذّة من الرتبة 2 X 2 على K
$PGL_2(K)$	زمرة الاسقاطات الخطّية العامة
$GF(q)$	حقل جالوا من الرتبة q
$e(G)$	أس G
F_n	عدد فيرما من الرتبة n
G	زمرة جالوا المنشأة بواسطة التبديلات.

ثبت المصطلحات

● عربي – إنجليزي
● إنجليزي – عربي

أولاً: عربي – إنجليزي

أ

إبدالي	Commutative
ابل	Abel
أثر	Trace
أرخميدس	Archimedes
أس (قوة)	Exponent
أفلاطون	Blato
الإغريق	Greeks
امتداد بسيط	Simple extension
جبري	Algebraic extension
بسيط	Simple algebraic extension
جذري	Radical extension
حقلي	Field extension
الزمر	Extension of groups
قابل للفصل	Separable extension
متسام بسيط	Simple transcendental extension

امتداد منته	Finite Extension
التوليد	Finitely generated extension
ناظمي	Normal extension
الإنشاء باستخدام المسطرة والفرجار	Construction by ruler and compass
إنشائي	Constructive
انغلاق ناظمي	Normal closure
أوّليان نسبيًا	Coprime
أولي لـ	Prime to
أويلر	Euler

ب

البابليون	Babylonians
باق	Remainder
بريانشون	Brianchon
بواسون	Poisson
بونكليلي	Poncelet
بيونكير	Poincare

ت

تبديل	Permutation
تثليث الزاوية	Trisection of the angle
تحويل	Transformation
ترافق مركب	Complex conjugation
تربيع الدائرة	Quadrature of the circle
تسامي e	Transcendence of e

Transcendence of π	تسامي π
Frobenius monomorphism	فروبيناس المتباين
Monomorphism	متباين
K-monomorphism	بالنسبة إلى K
Galois correspondence	تقابل جالوا
Cubic resolvent	تكعيبة مفككة
Automorphism	تماثل ذاتي
K-automorphism	بالنسبة إلى K
Frobenius automorphism	فروبيناس الذاتي

ث

Constant	ثابت

ج

Jacobi	جاكوبي
Galois	جالوا
Gauss	جاوس
Algebraic	جبري
Grossmann	جروسمان
Gordan	جوردان
Jerrard	جيرارد

ح

Splitting field	حقل انشطار

حقل ثابت	Fixed field
جالوا	Galois field
جزئي أولي	Prime subfield
العبارات الكسرية	Field of rational expressions
الكسور	Field of fractions
مغلق جبريًا	Algebraically closed field
منته	Finite field
وسطي	Intermediate field
حلقـة	Ring
كثيرات الحدود	Ring of polynomials

خ

خارج	Quotient
خط مستقيم	Line
خوارزمية أقليدس	Euclidean algorithm
زمرة جالوا	Algorithm for Galois group
القسمة	Division algorithm

د

دائرة	Circle
دالّة ناقصيّة	Elliptic function
درجة امتداد حقلي	Degree of field extension
التسامي	Transcendence degree

درجة كثيرة الحدود	Degree of polynomial
دلاّل منسي	Forgetful functor
دودل	Doodle
ديدكاند	Dedekind

ر

رامانجان	Ramanujan
روفيني	Ruffini

ز

زمرة بسيطة	Simple group
التبديلات	Symmetric group
التماثلات الذاتية	Automorphism group
التناوب	Alternating group
التناظرات	Symmetry group
جالوا	Galois group
دورية	Cyclic group
سايلو الجزئية من النوع P	Sylow p - subgroup
ضربية	Multiplicative group
قابلة للحل	Soluble group
من النوع p	p-group

س

سايلو	Sylow

ستاينتز	Steinitz
ستاينر	Steiner

ش

شكل شبكي	Lattice diagram

ص

صفر	Zero
بسيط	Simple zero
مضاعف	Multiple zero
مكرر	Repeated zero

ع

عبارة جذريّة	Radical expression
كسريّة	Rational expression
عدد جبري	Algebraic number
رئيس غير منته	Infinite cardinal
فيرما	Fermat number

غ

غير قابل للاختزال	Irreducibe
غير قابل للفصل	Inseparable

ف

فاستراس	Weierstrass
فصل ترافق	Conjugacy class
فضاء متّجهات	Vector space
فورير	Fourier
فونتانا	Fontana
فيراري	Ferrari
فيرما	Fermat
فيرو	Ferro
فيور	Fior

ق

قابل للاختزال	Reducible
للحل باستخلاص الجذور	Soluble by radicals
للفصل	Separable
قاسم	Factor
مشترك أعظم	Highest common factor
قاعدة لايبنز	Leibniz's rule
قانون البرج	Tower law

ك

كاردانو	Cardano
كارول	Carroll

كانتور	Cantor
كايلي	Cayley
كثيرة حدود	Polynomial
أصغريّة	Minimum polynomial
العامة	General polynomial
متناظرة	Symmetric plynomial
متناظرة ابتدائية	Elementary symmetric polynomial
كثيرة حدود واحدية	Monic polynomial
كرونكر	Kronecker
كلاين	Klein
كليفورد	Clifford
كوشي	Cauchy

ل

لاجرانج	Lagrange
لاكسرية π	Irrationality of π
لاكسرية π^2	Irrationality of π^2
لامبرت	Lambert
لايبنز	Leibniz
لجندر	Legendre
ليوفايل	Liouville

م

ماستشروني	Mascheroni

مبارزة	Duel
متتالية جذريّة	Radical Sequence
متسام	Transcendental
متعدّي	Transitive
مجال كامل	Integral domain
مجهول	Indeterminate
محدد فاندرموند	Vandermonde determinant
مرافق	Conjugate
مركز	Centre
مشتقّة شكليّة	Formal derivative
مضاعف	Multiple
مضاعفة المكعّب	Duplication of the cube
مضلّع	Polygon
معادلة خطيّة	Linear equation
الدرجة الثالثة	Cubic equation
الثانية	Quadratic equation
الخامسة	Quintic equation
الرابعة	Quartic equation
الفصول	Class equation
كثيرة حدود	Polynomial equation
معامل	Coefficient
ممايز	Discriminant
ممركز	Centralizer
مميّز	Characteristic
مناقلات	Transpositions
مور	Mohr

ميزان ايزنستاين	Eisenstein's criterion

ن

ناظمي	Normal
نظريّة التماثل الأولى	First isomorphism theorem
الثانية	Second isomorphism theorem
جالوا لاساسية	Fundamental theorem of Galois
الجبر الأساسية	Fundamental theorem of algebra
رول	Roll's theorem
قابلة للإنشاء	Constructible point

هـ

هندسة	Geometry
هوبير	Hobbes
هورويتز	Hurwitz
هيرمايت	Hermite
هيلبرت	Hilbert

ي

يقرن	Adjoin
يقسّم	Divide
ينشطر	Split

ثانيًا: إنجليزي عربي

A

Able	ابل
Adjoin	يقرن
Algebraic	جبري
Algebraically closed field	حقل مغلق جبريًا
Algebraic extention	امتداد جبري
number	عدد جبري
Algorithm for Galois group	خوارزمية زمرة جالوا
Alternating group	زمرة التناوب
Archimedes	أرخميدس
Automorphism	تماثل ذاتي
group	زمرة التماثلات الذاتية

B

Babylonians	البابليون
Blato	أفلاطون

Brianchon	بريانشون

C

Cantor	كانتور
Cardano	كاردانو
Carroll	كارول
Cauchy	كوشي
Cayley	كايلي
Centre	مركز
Centralizer	ممركز
Characteristic	مميز
Circle	دائرة
Class equation	معادلة الفصول
Clifford	كليفورد
Coefficient	معامل
Commutative	إبدالي
Complex conjugation	ترافق مركب
Conjugacy class	فصل ترافق
Conjugate	مرافق
Constant	ثابت
Constructible point	نظرية قابلة لإنشاء
Construction by ruler and compass	الإنشاء باستخدام المسطرة والفرجار
Constructive	إنشائي
Coprime	أوليان نسبيًا
Cubic equation	معادلة الدرجة الثالثة

المفككة التكعيبية	resolvent
زمرة دورية	Cyclic group

D

ديدكاند	Dedekind
درجة امتداد حقلي	Degree of field extension
درجة كثيرة الحدود	of polynominal
ممايز	Discriminant
يقسم	Divide
خوارزمية القسمة	Division algorithm
دودل	Doodle
مبارزة	Duel
مضاعفة المعكب	Duplication of the cube

E

ميزان ايزنستاين	Eisenstein's criterion
كثيرة حدود متناظرة ابتدائية	Elementary symmetric polynomial
دالّة ناقصيّة	Elliptic function
خوارزمية أقليدس	Euclidean algorithm
أويلر	Euler
أس (قوة)	Exponent
امتداد الزمر	Extension of groups

F

قاسم	Factor
فيرما	Fermat

number	عدد فيرما
Ferrari	فيراري
Ferro	فيرو
Field extension	امتداد حقلي
of fractions	حقل الكسور
of rational expressions	حقل العبارات الكسرية
Finite extension	امتداد منته
field	حقل منته
Finitely generated extension	امتداد منته التوليد
Fior	فيور
First isomorphism theorem	نظريّة التماثل الأولي
Fixed field	حقل ثابت
Fontana	فونتانا
Forgetful functor	دلال منسي
Formal derivative	مشتقّة شكليّة
Fourier	فورير
Frobenious automorphism	تماثل فروبيناس الذاتي
monomorphism	تشاكل فروبيناس المتباين
Fundamental theorem of algebra	نظريّة الجبر الأساسيّة
theorem of Galois	نظريّة جالوا الأساسيّة

G

Galois	جالوا
Galois correspondence	تقابل جالوا
field	حقل جالوا

group	زمرة جالوا
Gauss	جاوس
General polynomial	كثيرة الحدود العامة
Geometry	هندسة
Gordan	جوردان
Greeks	الإغريق
Grossmann	جروسمان

H

Hermite	هيرمايت
Highest common factor	قاسم مشترك أعظم
Hilbert	هيلبرت
Hobbes	هوبير
Hurwitz	هورويتز

I

Indeterminate	مجهول
Infinite cardinal	عدد رئيس غير منته
Inseparable	غير قابل للفصل
Intergral domain	مجال كامل
Intermediate field	حقل وسطي
Irrationality of π	لا كسرية π
of π^2	لا كسرية π^2
Irreducible	غير قابل للاختزال

J

جاكوبي	Jacobi
جيرارد	Jerrard

K

تماثل ذاتي بالنسبة إلى K	K-automorphism
كلاين	Klein
تشاكل متباين بالنسبة إلى K	K-monomorphism
كرونكر	Kronecker

L

لاجرانج	Lagrange
لامبرت	Lambert
شكل شبكي	Lattice diagram
لجندر	Legendre
لايبنز	Leibniz
قاعدة لايبنز	Leibniz's rule
خط مستقيم	Line
معادلة خطية	Linear equation
ليوفايل	Liouville

M

ماستشروني	Mascheroni

Minimum polynomial	كثيرة حدود أصغرية
Mohr	مور
Monic polynomial	كثيرة حدود واحدية
Monomorphism	تشاكل متباين
Multiple	مضاعف
zero	صفر مضاعف
Multiplicative group	زمرة ضربيّة

N

Normal	ناظمي
closure	انغلاق ناظمي
extension	متداد ناظمي

P

Permutation	تبديل
P-group	زمرة من نوع p
Poincare	يونكير
Poisson	بواسون
Polygon	مضلع
Polynomial	كثيرة حدود
equation	معادلة كثيرة حدود
Poncelet	بونكليلي
Prime subfield	حقل جزئي أولي
Prime to	أوّلي لـ

Q

Quadratic equation	معالة الدرجة الثانية
Quadrature of the circle	تربيع الدائرة
Quartic equation	معادلة الدرجة الرابعة
Quintic equation	معادلة الدرجة الخامسة
Quotient	خارج

R

Radical expression	عبارة جذريّة
extension	امتداد جذري
sequence	متتالية جذريّة
Ramanujan	رامانجان
Rational expression	عبارة كسريّة
Reducible	قابل للاختزال
Remainder	باق
Repeated zero	صفرٌ مكرر
Ring	حلقه
of polynmials	حلقة كثيرات الحدود
Rols's theorem	نظريّة رول
Ruffini	روفيني

S

Secand isomorphism theorem	نظريّة التماثل الثانية

Separable	قابل للفصل
extension	امتداد قابل للفصل
Simple algebraic extension	امتداد جبري بسيط
extension	امتداد بسيط
group	زمرة بسيطة
transcendental extension	امتداد متسام بسيط
zero	صفر بسيط
Soluble by radicals	قابل للحل باستخلاص الجذور
group	زمرة قابلة للحل
Split	ينشطر
Splitting field	حقل انشطار
Steiner	ستاينر
Steinitz	ستاينتز
Sylow	سايلو
p-subgroup	زمرة سايلو الجزئيّة من النوع p
Symmetric group	زمرة التبديلات
polynomial	كثيرة حدود متناظرة
Symmetry group	زمرة التناظرات

T

Tower law	قانون البرج
Trace	أثـر
Transcendence degree	درجة التسامي
of π	تسامي π
of e	تسامي e

Transcendental	متسام
Transformation	تحويل
Transitive	متعدي
Transpositions	مناقلات
Trisection of the angle	تثليث الزاوية

U

Vandermonde determinant	محدّد فاندر موند
Vector space	فضاء متّجهات

W

Weierstrass	فاستراس

Z

Zero	صفر

كشاف الموضوعات

Subject Index

أ

ت

ح

خ

د

ر

ز

ع

غ