



منشورات جامعة دمشق

كلية العلوم

قسم الرياضيات

تمديدات الحقول نظرية غالوا

الدكتورة

نور موفق غازي

مدرسة في قسم الرياضيات

الدكتور

حمزة إبراهيم حاكمي

أستاذ في قسم الرياضيات

جامعة دمشق : 1437 - 1438
2016 - 2017



تمديدات الحقول ونظرية غالوا



تمديدات الحقول ونظرية غالوا
السنة الرابعة رياضيات
قسم الرياضيات



منشورات جامعة دمشق

كلية العلوم

قسم الرياضيات

تمديدات الحقول نظرية غالوا

الدكتورة

نور غازي

مدرسة في قسم الرياضيات

الدكتور

حمزة إبراهيم حاكمي

أستاذ في قسم الرياضيات

جامعة دمشق : 1437 - 1438
2016 - 2017



الفهرس

الفهرس	٥
المقدمة	٩
الفصل الأول	١٣
حلقة كثيرات الحدود (الحدوديات)	١٣
١ - ١. حلقة الحدوديات	١٣
١ - ٢. الحدوديات الأولية (غير الخزولة)	٢٨
تمارين محلولة (١)	٤١
تمارين (١)	٤٧
الفصل الثاني	٤٩
الحدوديات فوق حلقة الأعداد الصحيحة	٤٩
١ - ٢. الحدوديات الأولية في $Z[x]$	٤٩
تمارين محلولة (٢)	٦٦
تمارين (٢)	٧٣
الفصل الثالث	٧٥
تمديد الحقول	٧٥
١ - ٣. تمديد الحقول	٧٥
٢ - ٣. التمديدات المنتهية	٨٦
٣ - ٣. التمديدات الجبرية	٩٣
تمارين محلولة (٣)	١١١
تمارين (٣)	١٢١

١٢٣	الفصل الرابع
١٢٣	حقول التفريق
١٢٣	٤ - ١. مميزات الحقول.
١٣٢	٤ - ٢. حقول التفريق.
١٤٣	تمارين محلولة (٤)
١٤٩	تمارين (٤)
١٥١	الفصل الخامس
١٥١	التمديدات المنفصلة.
١٥١	٥ - ١. المشتق والأصفار.
١٦٠	٥ - ٢. التمديدات الجبرية المنفصلة.
١٧٠	٥ - ٣. التمديدات المنفصلة.
١٨٨	تمارين محلولة (٥)
١٩٣	تمارين (٥)
١٩٥	الفصل السادس
١٩٥	الحقول المنتهية.
١٩٥	٦ - ١. الحقول المنتهية .
٢٠٥	تمارين محلولة (٦)
٢٠٨	تمارين (٦)
٢٠٩	الفصل السابع
٢٠٩	التماثلات الذاتية للحقول
٢٠٩	٧ - ١. العناصر المترافقة .
٢١٨	٧ - ٢. التماثلات الذاتية.

٢٢٥	٧ - ٣. تمديد التباينات.
٢٣٨	تمارين محلولة (٧)
٢٤٦	تمارين (٧)
٢٤٧	الفصل الثامن
٢٤٧	التمديدات الناعمية
٢٤٧	٨ - ١. التمديدات الناعمية.
٢٦٧	٨ - ٢. تمديدات غالوا.
٢٧٩	تمارين محلولة (٨)
٢٨٣	الفصل التاسع.
٢٨٣	نظرية غالوا الحديثة.
٢٨٣	٩ - ١. نظرية غالوا والتمديدات المنتهية.
٢٩٢	٩ - ٢. نظرية غالوا وحقول التفريق.
٣١٢	٩ - ٣. تطبيقات على نظرية غالوا.
٣٣٠	تمارين (٩)
٣٣١	الفصل العاشر
٣٣١	نظرية غالوا الأساسية
٣٣١	١٠ - ١. نظرية غالوا الأساسية.
٣٥٥	تمارين محلولة (١٠)
٣٦٣	الفصل الحادي عشر
٣٦٣	الحقول الدوارة
٣٦٣	١١ - ١. الجذور الأولية للواحد.
٣٧١	١١ - ٢. الحدوديات الدوارة.

٣٨٤	١١ - ٣. الحقول الدوارة.
٣٩٦	١١ - ٤. التمديدات الدائرية.
٤٠٥	الفصل الثاني عشر
٤٠٥	التمديدات الجذرية.
٤٠٥	١٢ - ١. التمديدات الجذرية.
٤٢٣	١٢ - ٢. طرق حل بعض المعادلات.
٤٣١	الفصل الثالث عشر
٤٣١	الحقول الحقيقية.
٤٣١	١٣ - ١. الحقول المرتبة.
٤٤٣	١٣ - ٢. الحقول الحقيقية.
٤٤٦	المصطلحات العلمية
٤٥١	المراجع العلمية.

المقدمة

منذ القرن الثالث قبل الميلاد وحتى منتصف القرن الأول الميلادي اقتصرت العمليات الحسابية على مجموعة الأعداد الصحيحة والكسرية) العادية (فضلاً عن صياغة عدد من المسائل الإنشائية مثل تقسيم زاوية إلى ثلاثة أجزاء متساوية وغيرها.

وقرابة العام ٨٢٥ ميلادية وفي ظل الحضارة الإسلامية ظهر كتاب " حساب الجبر والمقابلة " لمحمد بن موسى الخوارزمي الذي أوجد فيه حلول المعادلتين من الدرجة الأولى والثانية ومن هنا بدأ علم الجبر وتطوره.

وفي عصر النهضة تم إيجاد حلول المعادلات الجبرية من الدرجتين الثالثة والرابعة، وتعد الفترة بين العامين ١١٧٠ - ١٥٧٠ ميلادية تقريباً فترة تأسيس علم الجبر الحديث من خلال الرموز. وتعد الفترة ما بين ١٦٠٠ - ١٨٠٠ ميلادية تقريباً الفترة التي ظهرت فيها الهندسة التحليلية ودمج الجبر الحديث مع الهندسة وفي هذه الفترة أيضاً تطور علم جبر الحدوديات (كثيرات الحدود) وتبلورت مسائل المعادلات الجبرية وتم إيجاد حلول لهذه المعادلات فضلاً عن نشأة نظرية المحددات.

وفي الفترة ما بين العامين ١٨٠٠ - ١٨٥٠ ميلادية تقريباً تم إثبات النظرية الأساسية حول وجود حلول لعدد من المعادلات الجبرية بأمثال عددية رافقه تطور كبير في نظرية الأعداد، وفي الفترة ما بين ١٨٥٠ - ١٨٧٠ ميلادية نشأت محاولات تقريبية لحل المعادلات الجبرية ضمن شروط على أمثال هذه المعادلات. وفي الفترة ما بين ١٨٧٠ - ١٩٠٠ ميلادية تم حل مسألة إيجاد حلول للمعادلات الجبرية من الدرجة الخامسة وأكبر من الخامسة، حيث تم إثبات عدم وجود حل لهذه المسألة بواسطة الجذور من قبل غالوا. وفي هذه الفترة تم تطوير نظرية التوابع الجبرية ونشأة دراسة الزمر المنتهية وتطورها وذلك من خلال زمرة التباديل. ومنذ ذلك الوقت توسع علم الجبر وتفرع إلى عدد كبير من الفروع.

يعد هذا الكتاب مدخلاً لدراسة تمديدات الحقول عموماً ونظرية غالوا خصوصاً ويضم ثلاثة عشر فصلاً كتبت جميعها بلغة علمية مبسطة قدر الإمكان وقد ألحق كل فصل بعدد كبير من التمارين المحلولة وغير المحلولة بحيث يمكن اعتباره مغطياً لكل من الناحيتين النظرية والعملية على حد سواء.

يبدأ الكتاب في فصله الأول وفي فقرته الأولى بدراسة حلقة الحدوديات (كثيرات الحدود) فوق حقل وفي فقرته الثانية بدراسة الحدوديات الأولية (غير القابلة للتفريق). أما الفصل الثاني فخصص لدراسة الحدوديات فوق حلقة الأعداد الصحيحة وألحق هذا الفصل بعدد كاف من الاختبارات لتبيان إن كانت حدودية ما قابلة للتفريق أم لا. وقد خصص الفصل الثالث لدراسة تمديدات الحقول بشكل عام فضلاً عن التمديدات المنتهية والتمديدات الجبرية لحقل ما.

يعد الفصل الرابع مدخلاً لدراسة حقول التفريق حيث درست فيه مميزات الحقول وحقول التفريق. أما الفصل الخامس فقد خصصت فقرته الأولى لدراسة المشتقات والأصفار لحدودية ما، أما فقرته الثانية فدرست فيها الحدوديات المنفصلة والفقرة الأخيرة منه خصصت لدراسة الحقول المنفصلة.

وخصص الفصل السادس لدراسة الحقول المنتهية والزمرة الضربية لهذه الحقول وألحق بعدد من التمارين المحلولة لتبيان كيفية التعامل مع الحقول المنتهية. وأما الفصل السابع فخصصت فقرته الأولى لدراسة العناصر المترافقة في حقل ما وفقرته الثانية خصصت لدراسة التماثلات الذاتية للحقول، أما فقرته الثالثة منه فخصصت لدراسة تمديد التشاكلات بين الحقول.

وأما الفصل الثامن فقد خصصت الفقرة الأولى منه لدراسة التمديدات النازمية لحقل ما وفقرته الثانية خصصت لدراسة تمديدات غالوا لحقل منتهي (مميزه لا يساوي الصفر). وأما الفصل التاسع فقد خصصت الفقرة الأولى منه لدراسة نظرية غالوا لأجل التمديدات المنتهية وفقرته الثانية خصصت لدراسة نظرية غالوا لأجل حقول التفريق والفقرة الثالثة منه

خصصت لعرض بعض التطبيقات على نظرية غالوا. أما نظرية غالوا الأساسية فدرست في الفصل العاشر.

في الفصل الحادي عشر درست التمديدات الجذرية لحقل ما فضلاً عن طرق إيجاد الجذور للمعادلات من الدرجة الثانية والثالثة والرابعة وذلك في الفقرة الثانية من هذا الفصل.

وخصص الفصل الثاني عشر وفي فقرته الأولى لدراسة جذور الواحد والجذور الأولية للواحد والفقرة الثانية منه خصصت لدراسة الحقول الدوارة وأما فقرته الثالثة فخصصت لدراسة التمديدات الدائرية.

وقد عرضنا في الفصل الثالث عشر وفي الفقرة الأولى منه لمحة عن الحقول المرتبة وفي الفقرة الثانية منه لمحة عن الحقول الحقيقية.

ونلفت الانتباه إلى أن الصيغ والعلاقات الرياضية يجب قراءتها من اليسار إلى اليمين.

هذا وإننا نأمل أن نكون قد وفقنا بتغطية كافة مفردات هذا المقرر بشكل مناسب وجيد وأن يؤدي هذا الكتاب الغاية والفائدة المرجوة منه وهي أن يحصل الطالب والقارئ لهذا الكتاب على أساس قوي ومتين في المواضيع التي تمت مناقشتها.

والله ولي التوفيق

دمشق في ١ / ٩ / ٢٠١٦ م

المؤلفان

د. نور غازي

أ. د. حمزة حاكمي



الفصل الأول

حلقة كثيرات الحدود (الحدوديات)

تعد الحدوديات (كثيرات الحدود) واحدة من المفاهيم الرياضية المهمة، في مراحل سابقة تمت دراسة الحدوديات بأمثال صحيحة أو بشكل أعم بأمثال حقيقية أو مركبة. في هذه المرحلة سنركز بشكل خاص على الحدوديات بأمثال من Z_n ($n \geq 1$ عدد صحيح) حلقة الأعداد الصحيحة بالنسبة لعمليتي الجمع والضرب بالمقاس n . بداية سنتعرف على عملية بناء حلقة الحدوديات من خلال الفقرة الآتية:

١ - ١. حلقة الحدوديات.

لتكن R حلقة واحدة و I مجموعة من الأدلة، لنأخذ المجموعة:

$$\mathfrak{I} = \{a = (a_0, a_1, a_2, a_3, \dots) : a_i \in R, \forall i \in I\}$$

مجموعة جميع الأسطر غير المنتهية والتي جميع مركباتها من الحلقة R والتي تحقق $a_i = 0$ وذلك أيّاً كان $i \in I$ باستثناء عدد منته، من الواضح أن المجموعة $\mathfrak{I}$ غير خالية. لنعرف على المجموعة $\mathfrak{I}$ عملية ثنائية تحولها إلى بنية جبرية وذلك من خلال التمهيدية الآتية:

تمهيدية ١-١-١.

لتكن R حلقة واحدة، لنعرف على المجموعة:

$$\mathfrak{I} = \{a = (a_0, a_1, a_2, a_3, \dots) : a_i \in R, a_i = 0, \forall i \in I \text{ باستثناء عدد منته}\}$$

عملية جمع (+) بالشكل الآتي: أيّاً كان $a = (a_0, a_1, a_2, \dots), b = (b_0, b_1, b_2, \dots) \in \mathfrak{I}$

$$a + b = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$$

فنجذ أن الثنائية $(\mathfrak{I}, +)$ هي زمرة جمعية تبديلية.

البرهان.

واضح من خلال تعريف عملية الجمع (+) بأنها ثنائية (داخلية) وهي أيضاً تجميعية لأنه

أيّاً كان $a = (a_0, a_1, a_2, \dots), b = (b_0, b_1, b_2, \dots), d = (d_0, d_1, d_2, \dots) \in \mathfrak{I}$ فإن

$$\begin{aligned}
(a+b)+d &= ((a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots)) + (d_0, d_1, d_2, \dots) = \\
&= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) + (d_0, d_1, d_2, \dots) = \\
&= ((a_0 + b_0) + d_0, (a_1 + b_1) + d_1, (a_2 + b_2) + d_2, \dots) = \\
&= (a_0 + (b_0 + d_0), a_1 + (b_1 + d_1), a_2 + (b_2 + d_2), \dots) = \\
&= (a_0, a_1, a_2, \dots) + (b_0 + d_0, b_1 + d_1, b_2 + d_2, \dots) = \\
&= (a_0, a_1, a_2, \dots) + ((b_0, b_1, b_2, \dots) + (d_0, d_1, d_2, \dots)) = a + (b + d)
\end{aligned}$$

كما أن عملية الجمع (+) تبديلية، لأن:

$$\begin{aligned}
a+b &= (a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) = \\
&= (b_0 + a_0, b_1 + a_1, b_2 + a_2, \dots) = b+a
\end{aligned}$$

كما أنه يوجد في المجموعة $\mathfrak{T}$ عنصر محايد بالنسبة لعملية الجمع (+) هو

$$0 = (0, 0, 0, \dots) \text{ أيضاً لكل عنصر } a = (a_0, a_1, a_2, \dots) \in \mathfrak{T} \text{ يوجد نظير هو:}$$

$$-a = (-a_0, -a_1, -a_2, \dots) \in \mathfrak{T}$$

مما سبق نجد أن الثنائية $(\mathfrak{T}, +)$ هي زمرة جمعية تبديلية. $\diamond$

لنتابع دراستنا للزمرة التبديلية $(\mathfrak{T}, +)$ بغية تحويلها إلى حلقة واحدة وذلك من خلال

التمهيدية الآتية:

تمهيدية ١-١-٢.

لتكن R حلقة واحدة، لنعرف على المجموعة:

$$\mathfrak{T} = \{a = (a_0, a_1, a_2, a_3, \dots) : a_i \in R, a_i = 0, \forall i \in I \text{ باستثناء عدد منته } \}$$

عملية ضرب (.) بالشكل الآتي: أيأ كان $a = (a_0, a_1, a_2, \dots), b = (b_0, b_1, b_2, \dots) \in \mathfrak{T}$

فإن $a \cdot b = d$ حيث $d = (d_0, d_1, d_2, \dots)$ وأن $d_k = \sum_{i+j=k} a_i b_j$ ، أي أن:

$$d_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \dots + a_{k-1} b_1 + a_k b_0$$

عندئذ:

١ - العملية (.) المعرفة على المجموعة $\mathfrak{T}$ هي عملية ثنائية (داخلية) وتجميعية.

٢ - يوجد غي المجموعة $\mathfrak{T}$ عنصر محايد بالنسبة لعملية الضرب هو $1 = (1, 0, 0, \dots)$.

٣ - عملية الضرب توزيعية على الجمع من اليمين واليسار.

٤ - الثلاثية $(\mathfrak{T}, +, \cdot)$ حلقة واحدة.

٥ - الحلقة R هي حلقة جزئية من الحلقة $(\mathfrak{T}, +, \cdot)$.

البرهان.

١ - واضح من خلال تعريف عملية الضرب $(\cdot)$ بأنها عملية ثنائية وهي أيضاً تجميعية، لأنه أياً كان:

$a = (a_0, a_1, a_2, \dots), b = (b_0, b_1, b_2, \dots), d = (d_0, d_1, d_2, \dots) \in \mathfrak{T}$
فإن $a \cdot b = h$ حيث $h = (h_0, h_1, h_2, \dots) \in \mathfrak{T}$ وأن $h_k = \sum_{i+j=k} a_i b_j$ ومنه فإن
 $(a \cdot b) \cdot d = h \cdot d = c$ حيث $c = (c_0, c_1, c_2, \dots) \in \mathfrak{T}$ وأن $c_s = \sum_{n+m=s} h_n d_m$ وهكذا نجد أن:

$$\begin{aligned} c_s &= \sum_{n+m=s} h_n d_m = \sum_{n+m=s} \left(\sum_{i+j=n} a_i b_j \right) \cdot d_m = \sum_{n+m=s} \sum_{i+j=n} (a_i b_j) \cdot d_m = \\ &= \sum_{i+j+m=s} a_i (b_j d_m) = \sum_{i+t=s} \sum_{j+m=t} a_i (b_j d_m) = \sum_{i+t=s} a_i \sum_{j+m=t} b_j d_m \end{aligned}$$

وهكذا نجد أن $(a \cdot b) \cdot d = a \cdot (b \cdot d)$.

٢ - واضح أن $1 = (1, 0, 0, \dots) \in \mathfrak{T}$ وأنه أياً كان $a = (a_0, a_1, a_2, \dots) \in \mathfrak{T}$ فإن $1 \cdot a = a \cdot 1 = a$.

٣ - ليكن $a = (a_0, a_1, a_2, \dots), b = (b_0, b_1, b_2, \dots), d = (d_0, d_1, d_2, \dots) \in \mathfrak{T}$ عندئذ فإن

$$a \cdot (b + d) = (a_0, a_1, a_2, \dots) \cdot (b_0 + d_0, b_1 + d_1, b_2 + d_2, \dots) = (h_0, h_1, h_2, \dots)$$

حيث

$$h_k = \sum_{i+j=k} a_i \cdot (b_j + d_j) = \sum_{i+j=k} (a_i \cdot b_j + a_i \cdot d_j) = \sum_{i+j=k} a_i \cdot b_j + \sum_{i+j=k} a_i \cdot d_j$$

وهذا يبين أن $a \cdot (b + d) = a \cdot b + a \cdot d$ ، أي أن الضرب توزيعي على الجمع من اليسار، بشكل مشابه نجد أن الضرب توزيعي على الجمع من اليمين.

٤ - بالاعتماد على ما سبق وعلى التمهيدية (١-١-١) نجد أن الثلاثية $(\mathfrak{T}, +, \cdot)$ حلقة واحدة.

٥ - لنأخذ المجموعة $\mathfrak{T}_0 = \{(a, 0, 0, \dots) : a \in R\}$ فنجد أن $\mathfrak{T}_0$ هي مجموعة جزئية من المجموعة $\mathfrak{T}$ وغير خالية، لأن $(1, 0, 0, \dots) \in \mathfrak{T}_0$. كما أن $\mathfrak{T}_0$ هي حلقة جزئية من

الحلقة $\mathfrak{S}$ ، لأنه أياً كان $x = (a, 0, 0, \dots), y = (b, 0, 0, \dots) \in \mathfrak{S}_0$ فإن $a, b \in R$ وبما أن $a - b \in R, ab \in R$ نجد أن:

$$x - y = (a, 0, 0, \dots) - (b, 0, 0, \dots) = (a - b, 0, 0, \dots) \in \mathfrak{S}_0$$

$$xy = (a, 0, 0, \dots)(b, 0, 0, \dots) = (ab, 0, 0, \dots) \in \mathfrak{S}_0$$

من جهة أخرى، إن التطبيق $\varphi: R \rightarrow \mathfrak{S}_0$ المعرف بالشكل الآتي: أياً كان $a \in R$ فإن $\varphi(a) = (a, 0, 0, \dots) \in \mathfrak{S}_0$ هو تشاكل حلقي متباين وغامر (تماثل حلقي)، لأنه إذا كان $a, b \in R$ فإن:

$$\varphi(a + b) = (a + b, 0, 0, \dots) = (a, 0, 0, \dots) + (b, 0, 0, \dots) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = (ab, 0, 0, \dots) = (a, 0, 0, \dots)(b, 0, 0, \dots) = \varphi(a)\varphi(b)$$

وهذا يبين أن φ تشاكل حلقي، كما أن φ متباين، لأنه إذا كان $\varphi(a) = \varphi(b)$ فإن $(a, 0, 0, \dots) = (b, 0, 0, \dots)$ ومنه يكون $a = b$ ، وكذلك فإن φ غامر لأنه إذا كان $(c, 0, 0, \dots) \in \mathfrak{S}_0$ فإن $c \in R$ وأن $\varphi(c) = (c, 0, 0, \dots)$. مما سبق نجد أن φ إيزومورفيزم، نطابق عادة بين الحلقتين $R, \mathfrak{S}_0$ وهكذا نجد أن R هي حلقة جزئية من الحلقة $(\mathfrak{S}, +, \cdot)$.

تعريف.

لتكن R حلقة ولنأخذ الحلقة $(\mathfrak{S}, +, \cdot)$ المعرفة في التمهيدية (١-١-٢)، بما أن $(0, 1, 0, 0, \dots) \in \mathfrak{S}$ ، لنضع $x = (0, 1, 0, 0, \dots)$ ، نسمي العنصر x متحولاً فوق الحلقة R أو على الحلقة R .

بعض الخواص للمتحول x نوردتها من خلال التمهيدية الآتية:

تمهيدية ١-١-٣.

لتكن R حلقة ولنأخذ الحلقة $(\mathfrak{S}, +, \cdot)$ المعرفة في التمهيدية (١-١-٢). عندئذ:

١ - أياً كان $n \in N$ فإن $x^n = (0, 0, \dots, 0, \underbrace{1}_n, 0, \dots)$ حيث العنصر 1 يظهر في المركبة ذات الرقم n .

٢ - أياً كان $a \in R$ فإن $ax = (0, a, 0, 0, \dots) = xa$ حيث العنصر a يظهر في

المركبة ذات الرقم 1.

٣ - أيضاً كان $a \in R$ و $n \in N^*$ فإن $ax^n = (0, 0, \dots, 0, \underbrace{a}_{n}, 0, \dots) = x^n a$ حيث

العنصر a يظهر في المركبة ذات الرقم n .

٤ - إذا كان $a = (a_0, a_1, a_2, \dots, a_n, \dots) \in \mathfrak{S}$ حيث أن a_n آخر مركبة مغايرة للصفر، فإن a يمكن تمثيله بالشكل الآتي: $a = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ وهذا التمثيل للعنصر a وحيد.

البرهان.

١ - البرهان بالاستقراء حسب n . من أجل $n = 1$ فإن $x = (0, 1, 0, 0, \dots)$.

من أجل $n = 2$ ، لنفرض أن $x^2 = xx = (c_0, c_1, c_2, \dots, c_m, 0, \dots)$ حيث $c_k = \sum_{i+j=k} a_i b_j$. بما أن $a_1 = b_1 = 1$ وأن $a_i = b_i = 0$ أيّاً كان $i \neq 1$ ، نجد أن $c_k = 0$

أيّاً كان $k \neq 2$ ، وأن $c_2 = a_0b_2 + a_1b_1 + a_2b_0 = 1$ ، وهكذا نجد أن:

$$x^2 = (0, 0, 1, 0, \dots)$$

لنفرض أن $x^{n-1} = (0, 0, \dots, 0, \underbrace{1}_{n-1}, 0, \dots)$ عندئذ يكون:

$$x^n = x^{n-1} \cdot x = (0, 0, \dots, 0, \underbrace{1}_{n-1}, 0, \dots) \cdot (0, 1, 0, \dots) = (h_0, h_1, h_2, 0, \dots)$$

حيث $h_k = \sum_{i+j=k} a_i b_j$ وأن $a_i = 0$ أيّاً كان $i \neq n-1$ و $a_{n-1} = 1$ وأيضاً $b_j = 0$ أيّاً كان

$j \neq 1$ و $b_1 = 1$ ، وهكذا نجد أن $h_i = 0$ أيّاً كان $i \neq n$ وأن:

$$h_n = a_0b_n + a_1b_{n-1} + \dots + a_{n-1}b_1 + a_nb_0 = 1$$

وهذا يبين لنا أن $x^n = (0, 0, \dots, 0, \underbrace{1}_n, 0, \dots)$.

٢ - ليكن $a \in R$ عندئذ فإن

$$(0, a, 0, 0, \dots) = (a, 0, 0, \dots) \cdot (0, 1, 0, \dots) = ax$$

$$(0, a, 0, 0, \dots) = (0, 1, 0, \dots) \cdot (a, 0, 0, \dots) = xa$$

وهكذا نجد أن $ax = xa$.

٣ - ليكن $a \in R$ و $n \in N^*$ عندئذ فإن:

$$(0,0,\dots,0, \underbrace{a,0,\dots}_n) = (a,0,0,\dots) \cdot (0,0,\dots,0, \underbrace{1,0,\dots}_n) = ax^n$$

$$(0,0,\dots,0, \underbrace{a,0,\dots}_n) = (0,0,\dots,0, \underbrace{1,0,\dots}_n) \cdot (a,0,0,\dots) = x^n a$$

وهكذا نجد أن $ax^n = x^n a$.

٤ - ليكن $a = (a_0, a_1, a_2, \dots, a_n, 0, \dots) \in \mathfrak{S}$ عندئذ فإن:

$$a = (a_0, 0, 0, \dots) + (0, a_1, 0, \dots) + (0, 0, a_2, 0, \dots) + \dots + (0, 0, \dots, 0, a_n, 0, \dots)$$

حيث أن a_n هي آخر مركبة مغايرة للصفر، عندئذ حسب (٢) و (٣) نجد أن:

$$a = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

لنفرض أن $a = b_0 + b_1 x + b_2 x^2 + \dots + b_n x^n$ حيث $b_i \in R$ وذلك لأجل $0 \leq i \leq n$

ف نجد حسب (٢) و (٣) أن:

$$\begin{aligned} a &= (b_0, 0, 0, \dots) + (0, b_1, 0, \dots) + (0, 0, b_2, 0, \dots) + \dots + (0, 0, \dots, 0, b_n, 0, \dots) = \\ &= (b_0, b_1, b_2, \dots, b_n, 0, \dots) \in \mathfrak{S} \end{aligned}$$

ومنه نجد أن $a_i = b_i$ وذلك لأجل $0 \leq i \leq n$ ، وهذا يبين لنا وحدانية هذا التمثيل. ◊

تعريف.

لتكن R حلقة نسمي الحلقة $(\mathfrak{S}, +, \cdot)$ والتي تم بناؤها في التمهيدية (١-٢-١)،

حلقة الحدوديات بالمتحول x فوق الحلقة R ونرمز لها $R[x]$ ونسمي عناصر الحلقة

$R[x]$ حدوديات على الحلقة R (فوق الحلقة R) ونرمز لها $f(x)$.

إذا كان $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n = \sum_{i=0}^n a_i x^i \in R[x]$ حيث $a_n \neq 0$

فإننا نسمي n بدرجة الحدودية $f(x)$ ونرمز لذلك $\partial f(x) = n$ ونسمي العناصر $a_i \in R$

حيث $0 \leq i \leq n$ بأمثال الحدودية $f(x)$.

بالاعتماد على التعريف السابق يمكننا صياغة النتيجة الهامة الآتية:

نتيجة.

لتكن $R[x]$ حلقة الحدوديات فوق الحلقة R . عندئذ:

١ - أيًا كان $a \in R$ فإن $\partial a = 0$.

٢ - نصلح على أن $\partial 0 = -\infty$.

٣ - إذا كان $f(x) = \sum_{i=0}^n a_i x^i$, $g(x) = \sum_{i=0}^m b_i x^i \in R[x]$ حيث $a_i, b_i \in R$ ، فإن:

$$f(x) + g(x) = \sum_{i=0}^r (a_i + b_i) x^i \in R[x]$$

حيث $r = \max\{n, m\}$.

$$f(x) \cdot g(x) = \sum_{k=0}^{n+m} d_k \cdot x^k \in R[x]$$

$$\diamond \cdot d_k = \sum_{i+j=k} a_i \cdot b_j \quad \text{حيث}$$

لنتابع دراستنا لخواص الحلقة $R[x]$ وذلك من خلال المبرهنة الآتية:

مبرهنة ١-١-٤.

لتكن $R[x]$ حلقة الحدوديات فوق الحلقة R وليكن $f(x) = \sum_{i=0}^n a_i x^i$, $g(x) = \sum_{i=0}^m b_i x^i$

عنصرين من الحلقة $R[x]$ ، حيث $a_i, b_i \in R$. عندئذ:

$$1. f(x) = g(x) \Leftrightarrow n = m, a_i = b_i \quad \forall 0 \leq i \leq n$$

$$2. \partial(f(x) + g(x)) \leq \max\{\partial f(x), \partial g(x)\}$$

$$3. \partial(f(x) \cdot g(x)) \leq \partial f(x) + \partial g(x)$$

٤ - إذا كانت الحلقة R منطقة تكاملية فإن الحلقة $R[x]$ تكون أيضاً منطقة تكاملية.

٥ - إذا كانت الحلقة R منطقة تكاملية فإن $\partial(f(x) \cdot g(x)) = \partial f(x) + \partial g(x)$

البرهان.

١ - لنزوم الشرط. لنفرض أن $f(x) = g(x)$ عندئذ يكون

$$a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m$$

$$(a_0, a_1, a_2, \dots, a_n, 0, \dots) = (b_0, b_1, b_2, \dots, b_m, 0, \dots)$$

ومنه نجد أن $n = m$ كما أن $a_i = b_i$ وذلك أيّاً كان $0 \leq i \leq n$.

كفاية الشرط. ينتج مباشرة من خلال التعريف.

٢ - لنفرض أن $a_n \neq 0, b_m \neq 0$ عندئذ يكون $\partial(f(x)) = n, \partial(g(x)) = m$ وهنا

نميز حالتين:

- الحالة الأولى. إذا كان $n = m$ وأن $a_n + b_m \neq 0$ عندئذ يكون:

$$\partial(f(x) + g(x)) = n = \max\{n, m\}$$

أما إذا كان $a_n + b_m = 0$ عندئذ يكون $\partial(f(x) + g(x)) < n = \max\{n, m\}$

- الحالة الثانية. إذا كان $n \neq m$ ، لنفرض أن $n > m$ ، عندئذ يكون:

$$\partial(f(x) + g(x)) = n = \max\{n, m\}$$

٣ - لنفرض أن $f(x) \cdot g(x) = \sum_{k=0}^{n+m} d_k \cdot x^k$ حيث $d_k = \sum_{i+j=k} a_i \cdot b_j$ عندئذ يكون:

$$\partial(f(x) \cdot g(x)) \leq n + m = \partial f(x) + \partial g(x)$$

٤ - لنفرض أن الحلقة R منطقة تكاملية، عندئذ تكون الحلقة R تبديلية فيها $1 \neq 0$

وبالتالي تكون الحلقة $R[x]$ تبديلية فيها $1 \neq 0$. لنفرض أن $f(x) \neq 0$ و $g(x) \neq 0$

عندئذ يوجد دليل $0 \leq i_0 \leq n$ وآخر $0 \leq j_0 \leq m$ بحيث $a_{i_0} \neq 0, b_{j_0} \neq 0$ ، ولما كانت

الحلقة R منطقة تكاملية ينتج أن $a_{i_0} \cdot b_{j_0} \neq 0$ وبالتالي يكون $f(x) \cdot g(x) \neq 0$ وهذا

يبين أن الحلقة $R[x]$ منطقة تكاملية.

٥ - لنفرض أن الحلقة R منطقة تكاملية وأن $a_n \neq 0, b_m \neq 0$ عندئذ يكون $a_n \cdot b_m \neq 0$

وأن $\partial f(x) = n, \partial g(x) = m$ ومنه يكون:

$$\partial(f(x) \cdot g(x)) = n + m = \partial f(x) + \partial g(x)$$

إضافة لذلك فإن $\partial(f(x) \cdot g(x)) = n + m$ عندما فقط عندما $a_n \cdot b_m \neq 0$

نعلم أن أهم الخواص التي تتمتع بها حلقة الأعداد الصحيحة Z هي خوارزمية

القسمة والتي يمكن صياغتها بالشكل الآتي:

خوارزمية القسمة.

ليكن $a, b \in Z$ وأن $b \neq 0$ ، عندئذ يوجد في $q, r \in Z$ بحيث $a = qb + r$ حيث

$0 \leq r < |b|$ ، إضافة لذلك فإن كلاً من q, r يتعين بشكل وحيد.

إن خوارزمية القسمة السابقة صحيحة لأجل حلقة الحدوديات على حقل وهذا ما تثبته

لنا المبرهنة الآتية:

مبرهنة ١-١-٥ (خوارزمية القسمة).

ليكن F حقلاً و $F[x]$ حلقة الحدوديات على الحقل F وليكن $f(x), g(x) \in F[x]$ بحيث $g(x) \neq 0$ عندئذ يوجد $q(x), r(x) \in F[x]$ يحققان:

$$f(x) = q(x) \cdot g(x) + r(x)$$

وأنه إما $r(x) = 0$ أو $\partial r(x) < \partial g(x)$. إضافة لذلك فإن كلاً من $q(x), r(x)$ يتعين بشكل وحيد.

البرهان.

البرهان سوف نورده بالاستقراء حسب درجة الحدودية $f(x)$.

- إذا كانت $\partial f(x) = -\infty$ فإن $f(x) = 0$ ومنه يكون $f(x) = 0 \cdot g(x) + 0$ وهنا نختار $q(x) = r(x) = 0$ والصفر معين بشكل وحيد.

- إذا كانت $\partial f(x) = 0$ فإن $f(x) = a$ حيث $a \in F, a \neq 0$ وهنا نميز حالتين:

- $\partial g(x) = 0$ عندئذ $g(x) = b$ حيث $b \in F, b \neq 0$. لنضع $q(x) = ab^{-1}$ و $r(x) = 0$ فنجد أن $f(x) = (ab^{-1}) \cdot b + 0$ ، أي أن $f(x) = q(x) \cdot g(x) + r(x)$.

- $\partial g(x) > 0$ وهنا نأخذ $q(x) = 0$ و $r(x) = a$ فنجد أن $f(x) = 0 \cdot g(x) + a$ أي أن $f(x) = q(x) \cdot g(x) + r(x)$ ، وأن $\partial r(x) = 0 < \partial g(x)$.

- لنفرض أن $\partial f(x) > 0$ وأن المبرهنة صحيحة لأجل جميع الحدوديات التي درجة كل منها أصغر من درجة $f(x)$. وهنا نميز حالتين:

- الحالة الأولى. إذا كان $\partial f(x) < \partial g(x)$ في هذه الحالة نأخذ $f(x) = r(x)$ و $q(x) = 0$ ، فنجد أن $f(x) = 0 \cdot g(x) + r(x)$ أي أن:

$$f(x) = q(x) \cdot g(x) + r(x)$$

- الحالة الثانية. إذا كان $\partial f(x) \geq \partial g(x)$ ، لنفرض أن $\partial g(x) = m, \partial f(x) = n$ فيكون $n \geq m$ وأن:

$$f(x) = \sum_{i=0}^n a_i x^i \quad : a_n \neq 0, a_i \in F, \forall 0 \leq i \leq n$$

$$g(x) = \sum_{i=0}^m b_i x^i \quad : b_m \neq 0, b_i \in F, \forall 0 \leq i \leq m$$

لنضع $C(x) = a_n \cdot b_m^{-1} x^{n-m} g(x) - f(x)$ فنجد أن $C(x) \in F[x]$ وأن $\partial C(x) < n$ وحسب الفرض الاستقرائي يوجد $q_1(x), r_1(x) \in F[x]$ يحققان:

$$C(x) = q_1(x) \cdot g(x) + r_1(x)$$

وأنه إما $r_1(x) = 0$ أو $\partial r_1(x) < \partial g(x)$.

لنفرض أن $q(x) = a_n \cdot b_m^{-1} x^{n-m} - q_1(x)$ وأن $r(x) = -r_1(x)$ فنجد أن:

$$q(x) \cdot g(x) + r(x) = a_n \cdot b_m^{-1} x^{n-m} g(x) - q_1(x) \cdot g(x) - r_1(x) =$$

$$= a_n \cdot b_m^{-1} x^{n-m} g(x) - C(x) =$$

$$= a_n \cdot b_m^{-1} x^{n-m} g(x) - [a_n \cdot b_m^{-1} x^{n-m} g(x) - f(x)] = f(x)$$

وأنه إما $r(x) = 0$ أو $\partial r_1(x) < \partial g(x)$.

الوحدانية. لنفرض أن $f(x) = q(x) \cdot g(x) + r(x) = q_1(x) \cdot g(x) + r_1(x)$ عندئذ

يكون $r_1(x) - r(x) = [q(x) - q_1(x)] \cdot g(x)$. لنفرض جدياً أن $r_1(x) - r(x) \neq 0$

عندئذ يكون $\partial(r_1(x) - r(x)) = \partial g(x) + \partial[q(x) - q_1(x)] \geq \partial g(x)$

من جهة أخرى، بما أن $\partial r_1(x), \partial r(x) < \partial g(x)$ نجد أن:

$$\partial(r_1(x) - r(x)) \leq \max \{\partial r_1(x), \partial r(x)\} < \partial g(x)$$

وهذا تناقض، مما سبق نجد أن $r_1(x) = r(x)$ ، وبما أن $F[x]$ منطقة تكاملية وأن

$$g(x) \neq 0 \text{ نجد أن } q(x) - q_1(x) = 0 \text{ أي أن } q(x) = q_1(x) \text{ .}$$

تعريف.

ليكن F حقلاً و $F[x]$ حلقة الحدوديات على الحقل F وليكن $f(x), g(x) \in F[x]$

بحيث $g(x) \neq 0$. وجدنا حسب خوارزمية القسمة أنه يوجد $q(x), r(x) \in F[x]$ يحققان

$$f(x) = q(x) \cdot g(x) + r(x) \text{ وأنه إما } r(x) = 0 \text{ أو } \partial r(x) < \partial g(x).$$

نسمي $q(x)$ ناتج قسمة $f(x)$ على $g(x)$ في $F[x]$ ، ونسمي أيضاً $r(x)$ باقي قسمة

$$f(x) \text{ على } g(x) \text{ في } F[x].$$

مثال.

لنأخذ الحقل Z_5 ولنفرض أن $f(x) = 3x^4 + x^3 + 2x^2 + 1$ و $g(x) = x^2 + 4x + 2$

عنصرين من $Z_5[x]$ ، عندئذ يكون

$3x^4 + x^3 + 2x^2 + 1 = (x^2 + 4x + 2) \cdot (3x^2 + 4x) + (2x + 1)$
 إن $q(x) = 3x^2 + 4x \in Z_5[x]$ يمثل ناتج قسمة $f(x)$ على $g(x)$ في $Z_5[x]$. كذلك
 فإن $r(x) = x^2 + 4x + 2 \in Z_5[x]$ يمثل باق قسمة $f(x)$ على $g(x)$ في $Z_5[x]$.
 نأتي الآن لدراسة التمهيدية الآتية:

تمهيدية ١-١-٦.

ليكن F حقلاً و $F[x]$ حلقة الحدوديات على الحقل F وليكن $a \in F$ و $f(x) \in F[x]$.
 عندئذ فإن $f(a)$ هو باقي قسمة $f(x)$ على $x - a$ في $F[x]$.
 البرهان.

بما أن $a \in F$ فإن $x - a \in F[x]$ و $0 \neq x - a$ وحسب خوارزمية القسمة لأجل $x - a$, $f(x)$,
 فإنه يوجد $q(x), r(x) \in F[x]$ يحققان $f(x) = q(x) \cdot (x - a) + r(x)$ وأنه إما
 $r(x) = 0$ أو $\partial r(x) < \partial(x - a)$.
 - إذا كان $r(x) = 0$ عندئذ يكون $r(a) = 0$ وأن:

$$f(a) = q(a) \cdot (a - a) = 0 = r(a)$$

- إذا كان $\partial r(x) < \partial(x - a)$ عندئذ يكون $\partial r(x) = 0$ ومنه فإن $r(x) = b \in F$ و $b \neq 0$
 وبالتالي يكون $f(a) = q(a) \cdot (a - a) + r(a) = r(a) = b = r(x)$ وهذا
 يبين لنا أن $f(a)$ هو باق قسمة $f(x)$ على $x - a$ في $F[x]$.

تعريف.

لتكن R حلقة و $f(x), g(x) \in R[x]$ بحيث $g(x) \neq 0$. نقول إن $g(x)$ يقسم
 $f(x)$ في $R[x]$ ($f(x)$ يقبل القسمة على $g(x)$ في $R[x]$) إذا وجد $h(x) \in R[x]$
 يحقق $f(x) = g(x) \cdot h(x)$.

تعريف.

لتكن R حلقة و $f(x) \in R[x]$. نقول عن العنصر $a \in R$ إنه صفر للحدودية $f(x)$
 إذا كان $f(a) = 0$.

تعريف.

ليكن F حقلاً و $a \in F$ وليكن $f(x) \in F[x]$. نقول عن العنصر $a \in F$ إنه صفر للحدودية $f(x)$ من المرتبة k ($k \geq 1$ عدد صحيح) إذا كان $(x-a)^k$ يقسم $f(x)$ في $F[x]$ وأن $(x-a)^{k+1}$ لا يقسم $f(x)$ في $F[x]$.

بالاعتماد على التعريف السابق يمكننا صياغة التمهيدية الآتية:

تمهيدية ٧-١-١.

ليكن F حقلاً و $F[x]$ حلقة الحدوديات على الحقل F وليكن $a \in F$ و $f(x) \in F[x]$. الشرط اللازم والكافي كي يكون a هو صفرًا للحدودية $f(x)$ هو أن يكون $x-a$ قاسماً للحدودية $f(x)$.

البرهان.

لزوم الشرط. لنفرض أن a صفر للحدودية $f(x)$ ، بما أن $a \in F$ فإن $x-a \in F[x]$ وحسب خوارزمية القسمة يوجد $q(x), r(x) \in F[x]$ يحققان:

$$f(x) = q(x) \cdot (x-a) + r(x)$$

وأنه إما $r(x) = 0$ أو أن $\partial r(x) < \partial(x-a)$. لنفرض جلاً أن $r(x) \neq 0$ عندئذ تكون $\partial r(x) = 0$ ومنه $r(x) = b \in F$ وأن $b \neq 0$.

من جهة أخرى، بما أن a صفر للحدودية $f(x)$ فإن $f(a) = 0$ وحسب التمهيدية (١-٦) فإن $0 = f(a) = r(x) = b$ وهذا غير ممكن، مما سبق نجد أن $r(x) = 0$ وبالتالي يكون $f(x) = q(x) \cdot (x-a)$.

كفاية الشرط. لنفرض أن $x-a$ قاسم للحدودية $f(x)$ في $F[x]$ عندئذ يوجد $h(x) \in F[x]$ بحيث $f(x) = h(x) \cdot (x-a)$ ومنه يكون $f(a) = 0$ وهذا يبين أن a صفر للحدودية $f(x)$.

المبرهنة الآتية تبين لنا عدد أصفار حدودية ما:

مبرهنة ٨-١-١.

ليكن F حقلاً و $F[x]$ حلقة الحدوديات على الحقل F وليكن $f(x) \in F[x]$. إذا كان

$\partial f(x) = n$ حيث $n \geq 1$ عدد صحيح، عندئذ الحدودية $f(x)$ تملك n صفراً على الأكثر.

البرهان.

نورده بالاستقراء حسب درجة $f(x)$.

- إذا كانت $\partial f(x) = 1$ عندئذ يكون $f(x) = a_0 + a_1x$ حيث $a_0, a_1 \in F$ وأن $a_1 \neq 0$ وبما أن F حقل فإن $b = a_0a_1^{-1} \in F$ وأن $f(b) = 0$ وبالتالي فإن b صفر للحدودية $f(x)$. لنفرض أن الحدودية $f(x)$ تملك صفراً آخر في F وليكن c عندئذ يكون $f(c) = a_0 + a_1c$ ومنه نجد أن $a_0 + a_1c = a_0 + a_1(a_0a_1^{-1})$ وبالتالي يكون $a_1c = a_0$ أي أن $c = a_0a_1^{-1} = b$ ، مما سبق نجد أن الحدودية $f(x)$ تملك صفراً واحداً في F .

- لنفرض أن المبرهنة صحيحة لأجل كل حدودية من $F[x]$ درجتها أصغر من درجة $f(x)$ ، وهنا نميز حالتين:

- إذا كانت $f(x)$ لا تملك أصفاراً في F ، يتم المطلوب.

- ليكن $a \in F$ أحد أصفار الحدودية $f(x)$ من المرتبة k ، عندئذ فإن $(x-a)^k$ يقسم $f(x)$ في $F[x]$ ومنه يوجد $g(x) \in F[x]$ يحقق $f(x) = (x-a)^k \cdot g(x)$ وأن $g(a) \neq 0$ ومنه $\partial f(x) = \partial(x-a)^k + \partial g(x)$ أي أن $\partial f(x) = k + \partial g(x)$ وهكذا نجد أن $\partial g(x) = \partial f(x) - k = n - k < n$ وحسب الفرض الاستقرائي نجد أن الحدودية $g(x)$ تملك على الأكثر $n - k$ صفراً في F وبما أن كل صفر للحدودية $g(x)$ هو صفر للحدودية $f(x)$ نجد أن $f(x)$ تملك على الأكثر $k + (n - k) = n$ صفراً في F .

ملاحظة.

إن المبرهنة الأخيرة غير صحيحة لأجل الحدوديات على الحلقات. فعلى سبيل المثال الحدودية $f(x) = x^2 + 3x + 2 \in Z_6[x]$ تملك أربعة أصفار في Z_6 هي 1, 2, 4, 5 لأن $f(1) = f(2) = f(4) = f(5) = 0$ بينما $\partial f(x) = 2$.

لندرس الآن بعض الخواص لحلقة الحدوديات على حقل والبدائية ستكون مع المبرهنة

الآتية:

مبرهنة ٩-١-١.

حلقة الحدوديات فوق أي حقل هي حلقة مثاليات رئيسية.

البرهان.

ليكن F حقلاً و $F[x]$ حلقة الحدوديات فوق F . بما أن F منطقة تكاملية فإنه حسب المبرهنة (١-١-٤) تكون الحلقة $F[x]$ منطقة تكاملية أيضاً. ليكن A مثالياً في $F[x]$.

- إذا كان $A = \{0\}$ عندئذ يكون $A = 0 \cdot F[x]$ وبالتالي يتم المطلوب.

- لنفرض أن $A \neq \{0\}$ ولنأخذ المجموعة $\mathfrak{S} = \{\partial f(x) : 0 \neq f(x) \in A\}$ فنجد أن $\mathfrak{S} \subseteq N$ وغير خالية. وبما أن أي مجموعة جزئية من N تملك عنصراً أصغر فإن المجموعة $\mathfrak{S}$ تحوي عنصراً أصغر وليكن n ، ومنه يوجد $0 \neq g(x) \in A$ بحيث $\partial g(x) = n$ وبالتالي يكون $g(x) \cdot F[x] \subseteq A$.

ليكن $\mu(x) \in A$ وحسب خوارزمية القسمة لأجل $\mu(x), g(x)$ فإنه يوجد $q(x), r(x)$ عنصران في $F[x]$ يحققان $\mu(x) = q(x) \cdot g(x) + r(x)$ وأنه إما $r(x) = 0$ أو أن $\partial r(x) < \partial g(x)$. لنفرض جديلاً أن $r(x) \neq 0$ عندئذ يكون $r(x) = -q(x) \cdot g(x) + \mu(x)$ وأن $r(x) \in A$ كما أن $\partial r(x) < \partial g(x)$ وهذا يناقض اختيار $g(x)$. وهكذا نجد أن $r(x) = 0$ ومنه يكون:

$$\mu(x) = q(x) \cdot g(x) \in g(x) \cdot F[x]$$

وبالتالي يكون $A \subseteq g(x) \cdot F[x]$ ، مما سبق نجد أن $A = g(x) \cdot F[x]$.

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن F حقلاً و $F[x]$ حلقة الحدوديات فوق F . إن كل مثالي A في الحلقة $F[x]$ هو مثالي رئيسي مولد بالحدودية ذات الدرجة الأصغر في A .

تعريف.

لتكن R حلقة. نقول عن الحلقة R إنها إقليدية إذا حققت الشروط الآتية:

١ - الحلقة R منطقة تكاملية.

٢ - يوجد تطبيق $\varphi: R^* \rightarrow N$ يحقق أيّاً كان $a, b \in R^*$ فإن $\varphi(a) \leq \varphi(ab)$ ، حيث $R^* = R \setminus \{0\}$.

٣ - لأجل أي عنصرين $a, b \in R$ بحيث $b \neq 0$ يوجد $q, r \in R$ يحققان $a = qb + r$ وأنه إما $r = 0$ أو أن $\varphi(r) < \varphi(b)$. نسمي التطبيق φ الدالة الإقليدية.

مبرهنة ١٠-١-١.

حلقة الحدوديات فوق أي حقل هي حلقة إقليدية.

البرهان.

ليكن F حقلاً و $F[x]$ حلقة الحدوديات فوق F . حسب المبرهنة (١-١-٤) فإن الحلقة $F[x]$ هي منطقة تكاملية. لنعرف العلاقة $\varphi: (F[x])^* \rightarrow N$ بالشكل الآتي: أيّاً كان $g(x) \in (F[x])^*$ فإن $\varphi(g(x)) = \partial g(x)$ ، فنجد أن φ تطبيقاً. ليكن $g(x), \mu(x) \in (F[x])^*$ عندئذ وبما أن $F[x]$ منطقة تكاملية فإنه حسب المبرهنة (١-١-٤) نجد أن

$$\begin{aligned} \varphi(g(x) \cdot \mu(x)) &= \partial(g(x) \cdot \mu(x)) = \partial(g(x)) + \partial(\mu(x)) \geq \\ &\geq \partial(g(x)) = \varphi(g(x)) \end{aligned}$$

ليكن $f(x), g(x) \in F[x]$ بحيث $g(x) \neq 0$ عندئذ حسب خوارزمية القسمة يوجد $q(x), r(x) \in F[x]$ بحيث $f(x) = q(x) \cdot g(x) + r(x)$ وأنه إما $r(x) = 0$ أو أن $\partial r(x) < \partial g(x)$ وبالتالي إما $r(x) = 0$ أو أن $\varphi(r(x)) < \varphi(g(x))$ ، مما سبق نجد أن الحلقة $F[x]$ هي حلقة إقليدية. ◊

١ - ٢. الحدوديات الأولية (غير الخزولة).

في هذه الفقرة سوف ندرس نوعاً مهماً من الحدوديات وهي الحدوديات الأولية (غير الخزولة) والبداية سوف تكون مع التعريف الآتي:

تعريف.

لتكن R منطقة تكاملية و $f(x) \in R[x]$ و $f(x) \neq 0$. نقول عن الحدودية $f(x)$ إنها أولية (غير خزولة) في $R[x]$ إذا حققت الشرطين الآتيين:

- ١ - الحدودية $f(x)$ غير قابلة للقلب في $R[x]$.
- ٢ - لا يمكن كتابة $f(x)$ على شكل جداء حدوديتين من $R[x]$ كل منهما غير قابلة للقلب في $R[x]$.

إذا لم تكن الحدودية $f(x)$ أولية (غير خزولة) قلنا إنها غير أولية (خزولة).
إن الشرط (٢) من التعريف يعني أنه إذا كانت $f(x) = g(x) \cdot p(x)$ حيث $g(x), p(x) \in R[x]$ عندئذ إما $g(x)$ أو $p(x)$ قابلة للقلب في $R[x]$.
لنبدأ الآن بتحديد أي الحدوديات هي حدوديات أولية وأيها غير أولية، والبداية سوف تكون مع بعض الأمثلة:

أمثلة.

- ١ - الحدودية $f(x) = 2x^2 + 4 \in Z[x]$ غير أولية في $Z[x]$ ، لأنه يمكن كتابة $f(x)$ بالشكل $f(x) = g(x) \cdot p(x)$ حيث $g(x) = 2$ و $p(x) = x^2 + 2$ وكل منهما غير قابلة للقلب في $Z[x]$.
- ٢ - الحدودية $f(x) = x + 2 \in Z[x]$ هي حدودية أولية في $Z[x]$.
- ٣ - الحدودية $f(x) = 6x + 3 \in Z[x]$ هي حدودية غير أولية في $Z[x]$.
- ٤ - الحدودية $f(x) = 6x + 3 \in Q[x]$ هي حدودية أولية في $Q[x]$.
- ٥ - الحدودية $f(x) = x^2 - 2 \in Q[x]$ هي حدودية أولية في $Q[x]$.
- ٦ - الحدودية $f(x) = x^2 - 2 \in R[x]$ هي حدودية غير أولية في $R[x]$.

مثال.

لنأخذ الحلقة Z_4 بالنسبة لعمليتي الجمع والضرب بالمقاس 4. الحدودية $f(x) = 2x + 1$ هي عنصر في $Z_4[x]$ وتحقق $(2x+1)(2x+1) = 1$ ، وهذا يبين لنا أن الحدودية $f(x)$ قابلة للقلب في $Z_4[x]$ مع العلم أن $\partial f(x) > 0$.

التمهيدية الآتية تبين لنا أنه في حلقة الحدوديات فوق أي منطقة تكاملية لا توجد حدوديات قابلة للقلب درجتها أكبر من الصفر.

تمهيدية ١-٢-١.

لتكن R منطقة تكاملية و $f(x) \in R[x]$ و $f(x) \neq 0$. إذا كانت $f(x)$ قابلة للقلب في $R[x]$ عندئذ تكون $\partial f(x) = 0$.

البرهان.

لنفرض أن الحدودية $f(x)$ قابلة للقلب في $R[x]$ عندئذ توجد $g(x) \in R[x]$ و $g(x) \neq 0$ بحيث $f(x) \cdot g(x) = 1$ وحسب المبرهنة (١-١-٤) نجد أن $\partial f(x) + \partial g(x) = 0$ ومنه يكون $\partial f(x) = \partial g(x) = 0$.

إن عكس التمهيدية الأخيرة غير صحيح لأنه ليس كل عنصر في منطقة تكاملية مغاير للصفر قابلاً للقلب.

بينما إذا كان F حقلاً فإن عكس التمهيدية الأخيرة يكون صحيحاً وهذا ما تبينه لنا المبرهنة الآتية:

مبرهنة ١-٢-٢.

ليكن F حقلاً و $f(x) \in F[x]$ و $f(x) \neq 0$. الشرط اللازم والكافي كي تكون الحدودية $f(x)$ قابلة للقلب في $F[x]$ هو أن تكون $\partial f(x) = 0$.

البرهان.

لزوم الشرط. لنفرض أن الحدودية $f(x)$ قابلة للقلب في $F[x]$. بما أن $F[x]$ منطقة تكاملية فإنه حسب التمهيدية (١-٢-١) فإن $\partial f(x) = 0$.

كفاية الشرط. لنفرض أن $\partial f(x) = 0$ عندئذ فإن $f(x) = a$ حيث $a \in F$ و $a \neq 0$ ولما كان F حقلاً فإن العنصر a قابل للقلب في F وبالتالي في $F[x]$.

لنورد الآن المبرهنة الآتية:

مبرهنة ١-٢-٣.

ليكن F حقلاً و $F[x]$ حلقة الحدوديات فوق F . عندئذ:

١ - كل حدودية في $F[x]$ درجتها تساوي الصفر هي حدودية غير أولية في $F[x]$.

٢ - كل حدودية في $F[x]$ درجتها تساوي الواحد هي حدودية أولية في $F[x]$.

البرهان.

١ - لتكن $f(x) \in F[x]$ بحيث $\partial f(x) = 0$ عندئذ حسب المبرهنة (١-٢-٢) الحدودية

$f(x)$ تكون قابلة للقلب في $F[x]$ وحسب التعريف تكون الحدودية $f(x)$ غير أولية.

٢ - لتكن $g(x) \in F[x]$ بحيث $\partial g(x) = 1$ عندئذ حسب المبرهنة (١-٢-٢) الحدودية

$g(x)$ تكون غير قابلة للقلب في $F[x]$.

لتكن $p(x), q(x) \in F[x]$ بحيث $g(x) = p(x) \cdot q(x)$ ، بما أن $F[x]$ منطقة تكاملية

فإن $\partial p(x) + \partial q(x) = 1$ ومنه إما $\partial p(x) = 0$ أو $\partial q(x) = 0$.

- إذا كانت $\partial p(x) = 0$ عندئذ حسب المبرهنة (١-٢-٢) تكون الحدودية $p(x)$ قابلة

للقلب في $F[x]$.

- إذا كانت $\partial q(x) = 0$ فإن الحدودية $q(x)$ تكون قابلة للقلب في $F[x]$.

مما سبق نجد أن الحدودية $g(x)$ أولية في $F[x]$.

اختبار آخر للحدوديات الأولية نورده من خلال المبرهنة الآتية:

مبرهنة ١-٢-٤.

ليكن F حقلاً و $f(x) \in F[x]$ بحيث $\partial f(x)$ تساوي 2 أو 3. عندئذ الشرط اللازم

والكافي كي تكون الحدودية $f(x)$ غير أولية في $F[x]$ هو أن تملك صفراً في F .

البرهان.

لزوم الشرط. لنفرض أن الحدودية $f(x)$ غير أولية فوق F ، بما أن $\partial f(x) > 0$ فإن

$f(x)$ غير قابلة للقلب في $F[x]$ وبالتالي يوجد $g(x), h(x) \in F[x]$ كل منهما غير

قابلة للقلب في $F[x]$ تحققان $f(x) = g(x) \cdot h(x)$ ومنه يكون:

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

ولما كانت $\partial g(x) > 0$ و $\partial h(x) > 0$ وأن $\partial f(x)$ تساوي 2 أو 3 فإن واحدة على الأقل من الحدوديتين $g(x)$ أو $h(x)$ درجتها تساوي الواحد.

لنفرض أن $\partial g(x) = 1$ عندئذ $g(x) = ax + b$ حيث $a, b \in F$ وأن $a \neq 0$ ومنه فإن $-ba^{-1} \in F$ هو صفراً للحدودية $g(x)$ وبالتالي صفراً للحدودية $f(x)$. كذلك الأمر إذا كانت $\partial h(x) = 1$. مما سبق نجد أن الحدودية $f(x)$ تملك صفراً في F .

كفاية الشرط. لنفرض أن الحدودية $f(x)$ تملك صفراً في F وليكن d ، عندئذ حسب التمهيدية (١-١-٧) فإن الحدودية $x - d$ تقسم $f(x)$ في $F[x]$ ومنه توجد $\lambda(x) \in F[x]$ بحيث $f(x) = (x - d) \cdot \lambda(x)$ وبما أن $\partial f(x)$ تساوي 2 أو 3 نجد أن $\partial \lambda(x) > 0$. ولما كانت $\partial \lambda(x) > 0$ و $\partial(x - d) > 0$ فإنه حسب المبرهنة (١-٢-٢) فإن كلاً من $\lambda(x)$ و $x - d$ غير قابلة للقلب في $F[x]$ ، وهذا يبين لنا أن $f(x)$ تكتب على شكل جداء حدوديتين كل منهما غير قابلة للقلب في $F[x]$ وحسب التعريف تكون الحدودية $f(x)$ غير أولية في $F[x]$. ◊

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة التمهيدية الآتية:

تمهيدية ١-٢-٥.

ليكن F حقلاً و $f(x) \in F[x]$ بحيث $\partial f(x)$ تساوي 2 أو 3. عندئذ الشرط اللازم والكافي كي تكون الحدودية $f(x)$ أولية في $F[x]$ هو أن لا تملك $f(x)$ صفراً في F .
البرهان.

نتركه للقارئ. ◊

أمثلة.

١ - الحدودية $f(x) = x^2 + 1$ هي حدودية أولية فوق Z_3 .
بما أن 3 عدداً أولياً فإن Z_3 حقلاً، كما أن $\partial f(x) = 2$. بملاحظة أن $f(0) = 1$ وأن $f(1) = f(2) = 2$ نجد أن $f(x)$ لا تملك أصفاراً في Z_3 وحسب التمهيدية (١-٢-٥) تكون الحدودية $f(x)$ أولية فوق Z_3 .

٢ - الحدودية $f(x) = x^2 + 1$ هي حدودية غير أولية فوق Z_5 .

بما أن Z_5 حقلاً وأن $\partial f(x) = 2$ وبملاحظة أن $f(2) = f(3) = 0$ نجد أن الحدودية $f(x)$ تملك أصفاراً في Z_5 وحسب المبرهنة (١-٢-٤) تكون الحدودية $f(x)$ غير أولية فوق Z_5 .

٣ - الحدودية $g(x) = x^2 - 3$ هي حدودية أولية فوق Q .
بما أن Q حقل وأن $\partial g(x) = 2$ وبملاحظة أن $x = \pm\sqrt{3} \notin Q$ هي جميع أصفار الحدودية $g(x)$ ، نجد أن الحدودية $g(x)$ لا تملك أصفاراً في الحقل Q وحسب التمهيدية (١-٢-٥) تكون الحدودية $g(x)$ أولية فوق Q . بينما فوق حقل الأعداد الحقيقية R فإن الحدودية $g(x)$ غير أولية في $R[x]$ لأن $x = \pm\sqrt{3} \in R$ وذلك حسب المبرهنة (١-٢-٤).

٤ - الحدودية $h(x) = 2x^2 + 4$ هي حدودية أولية فوق Q .
لأن Q حقل وأن $\partial h(x) = 2$ وبملاحظة أن $x = \pm\sqrt{2}i \notin Q$ هي جميع أصفار الحدودية $h(x)$ وبالتالي حسب التمهيدية (١-٢-٥) تكون الحدودية $h(x)$ أولية فوق Q .

تمهيدية ١-٢-٦.

ليكن F حقلاً و $a \in F$ ، ولتكن $f(x) \in F[x]$. عندئذ:

- ١ - إذا كانت الحدودية $a \cdot f(x)$ أولية فوق F فإن الحدودية $f(x)$ أولية فوق F .
 - ٢ - إذا كانت الحدودية $f(a \cdot x)$ أولية فوق F فإن الحدودية $f(x)$ أولية فوق F .
 - ٣ - إذا كانت الحدودية $f(a + x)$ أولية فوق F فإن الحدودية $f(x)$ أولية فوق F .
- البرهان.

١ - بما أن $f(x) \in F[x]$ فإن $a \cdot f(x) \in F[x]$ وأن $\partial(a \cdot f(x)) = \partial f(x)$. لنفرض أن الحدودية $a \cdot f(x)$ أولية فوق F عندئذ فإن $\partial(a \cdot f(x)) > 0$ ومنه فإن $\partial f(x) > 0$ وبالتالي فإن $f(x)$ غير قابلة للقلب فوق F .
لتكن $g(x), h(x) \in F[x]$ بحيث $f(x) = g(x) \cdot h(x)$ عندئذ يكون:

$$a \cdot f(x) = (a \cdot g(x)) \cdot h(x)$$

وبما أن الحدودية $a \cdot f(x)$ أولية فوق F نجد أنه إما $\partial(a \cdot g(x)) = 0$ ومنه فإن $\partial g(x) = 0$ أو $\partial h(x) = 0$ ، مما سبق نجد أن الحدودية $f(x)$ أولية فوق F .

٢ - بما أن $f(x) \in F[x]$ فإن $f(a \cdot x) \in F[x]$ وأن $\partial(f(a \cdot x)) = \partial f(x)$.
 لنفرض أن الحدودية $f(a \cdot x)$ أولية فوق F عندئذ فإن $\partial(f(a \cdot x)) > 0$ ومنه فإن $\partial f(x) > 0$ وبالتالي فإن $f(x)$ غير قابلة للقلب فوق F .

لتكن $q(x), \lambda(x) \in F[x]$ بحيث $f(x) = q(x) \cdot \lambda(x)$ عندئذ يكون:

$$f(a \cdot x) = q(a \cdot x) \cdot \lambda(a \cdot x)$$

وبما أن الحدودية $f(a \cdot x)$ أولية فوق F نجد أنه إما $\partial(q(a \cdot x)) = 0$ وبالتالي تكون $\partial q(x) = 0$ أو $\partial(\lambda(a \cdot x)) = 0$ وبالتالي تكون $\partial \lambda(x) = 0$ ، مما سبق نجد أن الحدودية $f(x)$ أولية فوق F .

٣ - البرهان يتم بطريق مشابهة للحالة (٢) وذلك لأن $f(x), f(a + x) \in F[x]$ وأن $\partial(f(a + x)) = \partial f(x)$.

لندرس الآن بعضاً من الخواص الجبرية للحدوديات الأولية وأول هذه الخواص نوردتها من خلال المبرهنة الآتية:

مبرهنة ١-٢-٧.

ليكن F حقلاً و $f(x) \in F[x]$. الشروط الآتية متكافئة:

١ - المثالي $A = f(x) \cdot F[x]$ أعظمي في الحلقة $F[x]$.

٢ - الحدودية $f(x)$ أولية في الحلقة $F[x]$.

البرهان.

(1) $\Leftrightarrow$ (2). لنفرض أن المثالي A أعظمي في $F[x]$ ، عندئذ $A \neq \{0\}$ لأن $\{0\}$ ليس مثالياً أعظمية في $F[x]$. بما أن $A \neq F[x]$ فإن $f(x)$ غير قابلة للقلب في $F[x]$ وبالتالي $\partial f(x) > 0$. ليكن $g(x), h(x) \in F[x]$ بحيث $f(x) = g(x) \cdot h(x)$ عندئذ $f(x) \in g(x) \cdot F[x]$ ومنه $A \subseteq g(x) \cdot F[x]$ ، وبما أن المثالي A أعظمي في $F[x]$ نجد أنه إما $g(x) \cdot F[x] = F[x]$ أو $g(x) \cdot F[x] = A$.
 - إذا كان $g(x) \cdot F[x] = F[x]$ عندئذ تكون الحدودية $g(x)$ قابلة للقلب في $F[x]$ ومنه فإن $\partial g(x) = 0$.

- إذا كان $g(x) \cdot F[x] = A$ نجد أن $\partial f(x) = \partial g(x)$ وهنا نجد أن $\partial h(x) = 0$.

وهذا يبين لنا أنه لا يمكن كتابة $f(x)$ على شكل جداء حدوديتين درجة كل منهما أكبر من الصفر، مما سبق نجد أن الحدودية $f(x)$ أولية في $F[x]$.
 $(2) \Leftarrow (1)$. لنفرض أن الحدودية $f(x)$ أولية في $F[x]$ وليكن B مثالياً في $F[x]$ بحيث $A \subseteq B \subseteq F[x]$. وبما أن F حقل فإنه حسب المبرهنة (١-١-٩) فإن الحلقة $F[x]$ هي حلقة مثاليات رئيسية وبالتالي يوجد $g(x) \in F[x]$ بحيث:

$$B = g(x) \cdot F[x]$$

وبما أن $f(x) \in A \subseteq B$ فإنه يوجد $h(x) \in F[x]$ بحيث $f(x) = g(x) \cdot h(x)$ وبما أن الحدودية $f(x)$ أولية في $F[x]$ فإنه إما $\partial g(x) = 0$ أو $\partial h(x) = 0$.
 - إذا كانت $\partial g(x) = 0$ عندئذ تكون الحدودية $g(x)$ قابلة للقلب في $F[x]$ وبالتالي يكون $B = F[x]$.

- إذا كانت $\partial h(x) = 0$ عندئذ يكون $h(x) = b$ وأن $0 \neq b \in F$ ومنه فإن:

$$g(x) = f(x) \cdot b^{-1} \in f(x) \cdot F[x] = A$$

وبالتالي يكون $B \subseteq A$ وهكذا نجد أن $B = A$ وهذا يبين أن المثالي $A = f(x) \cdot F[x]$ أعظمياً في $F[x]$. ◊

بالاعتماد على المبرهنة الأخيرة يمكننا الوصول إلى المبرهنة الآتية:

مبرهنة ١-٢-٨.

ليكن F حقلاً و $f(x) \in F[x]$. الشرط اللازم والكافي كي تكون الحدودية $f(x)$ أولية في $F[x]$ هو أن تكون الحلقة $\langle f(x) \rangle / F[x]$ حقلاً.
البرهان.

لزوم الشرط. لنفرض أن الحدودية $f(x)$ أولية في $F[x]$ عندئذ حسب المبرهنة (١-٢-٧) يكون المثالي $\langle f(x) \rangle$ أعظمياً في $F[x]$ وبالتالي الحلقة $\langle f(x) \rangle / F[x]$ تشكل حقلاً.

كفاية الشرط. لنفرض أن الحلقة $\langle f(x) \rangle / F[x]$ حقلاً عندئذ يكون المثالي $\langle f(x) \rangle$ أعظمياً في $F[x]$ وحسب المبرهنة (١-٢-٧) تكون الحدودية $f(x)$ أولية في $F[x]$. ◊

النتيجة الآتية مشابهة لتمهيدية إقليدس الخاصة بالأعداد الأولية في حلقة الأعداد الصحيحة Z والتي يمكن صيغتها من خلال المبرهنة الآتية:

مبرهنة ١-٢-٩.

ليكن F حقلاً و $f(x), g(x), p(x) \in F[x]$. إذا كانت الحدودية $p(x)$ أولية فوق F وكانت $p(x)$ تقسم الجداء $f(x) \cdot g(x)$ ، عندئذ إما $p(x)$ تقسم $f(x)$ أو $p(x)$ تقسم $g(x)$.

البرهان.

لنفرض أن الحدودية $p(x)$ أولية في $F[x]$ وأن $A = \langle p(x) \rangle$ ، حسب المبرهنة (١-٢-٢) (٧) يكون المثالي A أعظماً في $F[x]$ وبالتالي تكون الحلقة $F[x]/A$ حقلاً. من جهة أخرى، بما أن $f(x) \cdot g(x) = p(x) \cdot \varphi(x)$ حيث $\varphi(x) \in F[x]$ نجد أن $f(x) \cdot g(x) + A = A$ ومنه فإن $(f(x) + A) \cdot (g(x) + A) = A$ ولما كان $F[x]/A$ حقلاً نجد أنه إما $f(x) + A = A$ أو $g(x) + A = A$ وهذا يبين لنا أنه إما $f(x) \in A$ أو $g(x) \in A$.

- إذا كان $f(x) \in A$ عندئذ توجد $h(x) \in F[x]$ بحيث $f(x) = p(x) \cdot h(x)$.

- إذا كان $g(x) \in A$ عندئذ توجد $\lambda(x) \in F[x]$ بحيث $g(x) = p(x) \cdot \lambda(x)$.

ومنه نجد أنه إما $p(x)$ تقسم $f(x)$ أو $p(x)$ تقسم $g(x)$ في $F[x]$. ◊

المبرهنة الأخيرة يمكن تعميمها لأجل أي عدد منته من الحدوديات وهذا التعميم سوف نورده من خلال المبرهنة الآتية:

مبرهنة ١-٢-١٠.

ليكن F حقلاً و $f_1(x), f_2(x), \dots, f_n(x), p(x) \in F[x]$. إذا كانت الحدودية $p(x)$ أولية فوق F وكانت $p(x)$ تقسم الجداء $f_1(x) \cdot f_2(x) \cdots f_n(x)$ ، عندئذ فإن $p(x)$ تقسم واحداً على الأقل من الحدوديات $f_i(x)$ في $F[x]$ ، حيث $1 \leq i \leq n$.

البرهان.

يتم من خلال التطبيق المباشر للمبرهنة (١-٢-٩) ولذلك سوف نتركه للقارئ. ◊

مثال.

لتكن $Z_2[x]$ حلقة الحدوديات فوق الحقل Z_2 . ولتكن $p(x) = x^3 + x + 1 \in Z_2[x]$.

١ - أثبت أن الحدودية $p(x)$ أولية في $Z_2[x]$.

٢ - أثبت أن الحلقة $Z_2[x]/A$ حقلًا، حيث $A = \langle p(x) \rangle$ ، ثم عين هذا الحقل.

الحل.

١ - نلاحظ أولاً أن $p(0) = p(1) = 1$ وهذا يبين أن الحدودية $p(x)$ لا تملك أصفاراً في الحقل Z_2 ، ولم كانت $\partial p(x) = 3$ فإنه حسب التمهيدية (١-٢-٥) تكون الحدودية $p(x)$ أولية فوق الحقل Z_2 .

٢ - بما أن الحدودية $p(x)$ أولية فوق الحقل Z_2 فإنه حسب المبرهنة (١-٢-٨) تكون الحلقة $Z_2[x]/A$ حقلًا، حيث $A = \langle p(x) \rangle$.

ليكن $\overline{f(x)} \in Z_2[x]/A$ عندئذ توجد $f(x) \in Z_2[x]$ بحيث $\overline{f(x)} = f(x) + A$ وحسب خوارزمية القسمة لأجل العنصرين $f(x), p(x)$ نجد أنه توجد $q(x), r(x) \in Z_2[x]$ تحقق $f(x) = q(x) \cdot p(x) + r(x)$ وأنه إما $r(x) = 0$ أو أن $\partial r(x) < \partial p(x)$ ومنه

$$\begin{aligned}\overline{f(x)} &= f(x) + A = [q(x) \cdot p(x) + r(x)] + A = \\ &= (q(x) \cdot p(x) + A) + (r(x) + A) = r(x) + A\end{aligned}$$

وذلك لأن $q(x) \cdot p(x) \in A$.

بما أنه إما $r(x) = 0$ أو أن $\partial r(x) < \partial p(x) = 3$ نجد أنه إما $r(x) = 0$ أو أن $r(x) = ax^2 + bx + c$ حيث $a, b, c \in Z_2$ ومنه نجد أن

$$Z_2[x]/A = \{(ax^2 + bx + c) + A : a, b, c \in Z_2\}$$

وبما أن الحقل Z_2 يحوي عنصرين فقط نجد أنه للعناصر a, b, c ثمانية احتمالات فقط، ومنه فإن الحقل $Z_2[x]/A$ يتألف من ثمانية عناصر. ◊

بالاعتماد على المثال السابق يمكننا صياغة المبرهنة الآتية:

مبرهنة ١-٢-١١.

ليكن p عدداً أولياً ولتكن $Z_p[x]$ حلقة الحدوديات فوق الحقل Z_p . لنفرض أن $f(x) \in Z_p[x]$ وأن $\partial f(x) = n$ و $A = \langle f(x) \rangle$. إذا كانت الحدودية $f(x)$ أولية

في $Z_p[x]$ ، عندئذ فإن الحلقة $Z_p[x]/A$ تشكل حقلاً مؤلفاً من p^n عنصراً.
البرهان.

بما أن العدد p أولي فإن Z_p حقل. لنفرض أن الحدودية $f(x)$ أولية فوق Z_p ، عندئذ حسب المبرهنة (١-٢-٧) يكون المثالي $A = \langle f(x) \rangle$ أعظماً في $Z_p[x]$ وبالتالي تكون الحلقة $Z_p[x]/A$ حقلاً، لنفرض أن $\partial f(x) = n$.

ليكن $\overline{g(x)} \in Z_p[x]/A$ عندئذ $\overline{g(x)} = g(x) + A$ حيث $g(x) \in Z_p[x]$ وحسب خوارزمية القسمة لأجل العنصرين $f(x), g(x)$ يوجد $q(x), r(x) \in Z_p[x]$ بحيث $g(x) = q(x) \cdot f(x) + r(x)$ وأنه إما $r(x) = 0$ أو أن $\partial r(x) < \partial f(x) = n$ أي أن $r(x) = \sum_{i=0}^{n-1} a_i x^i$ ، حيث $a_i \in Z_p$ وبما أن العناصر a_i عددها يساوي n وأن كل عنصر من هذه العناصر يأخذ p قيمة، نجد أن عدد عناصر الحقل $Z_p[x]/A$ يساوي p^n عنصراً، أي أن:

$$Z_p[x]/A = \{a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0 : a_i \in Z, \forall 0 \leq i \leq n-1\}$$

وبالتالي يكون $\text{Card}(Z_p[x]/A) = p^n$. ♦

تعريف.

لتكن $F[x]$ حلقة الحدوديات فوق الحقل F ولتكن $f(x), g(x) \in F[x]$. نقول عن الحدوديتين $f(x), g(x)$ إنهما أوليتان فيما بينهما إذا حققنا الشرط الآتي: أيأ كانت $\theta(x) \in F[x]$ وكانت $\theta(x)$ تقسم كلاً من $f(x)$ و $g(x)$ فإن $\partial \theta(x) = 0$.

بالاعتماد على التعريف السابق يمكننا صياغة التمهيدية الآتية:

تمهيدية ١-٢-١٢.

لتكن $F[x]$ حلقة الحدوديات فوق الحقل F ولتكن $f(x), g(x) \in F[x]$. نقول عن الحدوديتين $f(x), g(x)$ إنهما أوليتان فيما بينهما في $F[x]$. عندئذ توجد $h(x), q(x)$ في $F[x]$ تحققان $f(x) \cdot q(x) + g(x) \cdot h(x) = 1$.
البرهان.

لنأخذ المجموعة

$$A = \{f(x) \cdot r(x) + g(x) \cdot p(x) : r(x), p(x) \in F[x]\}$$

فنجد أن المجموعة A تشكل مثالياً في $F[x]$ (أثبت ذلك)، وبما أن F حقل فإنه حسب المبرهنة (٩-١-١) تكون الحلقة $F[x]$ حلقة مثاليات رئيسية، ومنه فإن المثالي A يكون مثالياً رئيسياً في $F[x]$ وبالتالي توجد $\theta(x) \in F[x]$ بحيث $A = \theta(x) \cdot F[x]$ وبما أن

$$f(x) = f(x) \cdot 1 + g(x) \cdot 0 \in A$$

$$g(x) = f(x) \cdot 0 + g(x) \cdot 1 \in A$$

فإنه توجد $h_0(x), d_0(x) \in F[x]$ بحيث:

$$f(x) = h_0(x) \cdot \theta(x), \quad g(x) = d_0(x) \cdot \theta(x)$$

وهذا يبين لنا أن $\theta(x)$ تقسم كلياً من $f(x)$ و $g(x)$ وبما أن $f(x), g(x)$ أوليتان فيما بينهما ينتج أن $\partial \theta(x) = 0$ ، أي أن $\theta(x) = a$ حيث $a \in F$ و $a \neq 0$ ومنه فإن العنصر a قابل للقلب في $F[x]$ وأن $a \in A$ وبالتالي يكون $A = F[x]$ ، أي أن $1 \in A$ ومنه فإن $f(x) \cdot q(x) + g(x) \cdot h(x) = 1$ حيث $h(x), q(x) \in F[x]$.

تمهيدية ١-٢-١٣.

ليكن F حقلاً و $f(x) = \sum_{i=0}^n a_i x^i$ ، $g(x) = \sum_{i=0}^m b_i x^i \in F[x]$ إذا كان $a_n = 1$ و $b_m = 1$ وكانت $f(x)$ تقسم $g(x)$ و $g(x)$ تقسم $f(x)$ ، عندئذ يكون:

$$f(x) = g(x)$$

البرهان.

لما كان $f(x)$ تقسم $g(x)$ و $g(x)$ تقسم $f(x)$ فإنه يوجد $\lambda(x), \mu(x) \in F[x]$ بحيث يكون $g(x) = f(x) \cdot \lambda(x)$ ، $f(x) = g(x) \cdot \mu(x)$ ومنه يكون:

$$g(x) = g(x) \cdot \mu(x) \cdot \lambda(x)$$

وهذا يبين أن $\partial(\mu(x) \cdot \lambda(x)) = 0$ وبالتالي يكون $\partial \mu(x) = \partial \lambda(x) = 0$. أي أن $\mu(x) = c$ ، $\lambda(x) = d$ حيث $c, d \in F$ عناصر مغايرة للصفر. ومنه نجد أن:

$$g(x) = f(x) \cdot d$$

وهذا يبين أن $\partial f(x) = \partial g(x)$ أي أن $n = m$ ومنه نجد أن:

$$x^n + \sum_{i=0}^{n-1} b_i x^i = dx^n + \sum_{i=0}^{m-1} a_i x^i$$

ومنه نجد أن $d = 1$ وبالتالي يكون $f(x) = g(x)$.

تمهيدية ١-٢-١٤.

ليكن F حقلاً و $f(x) = \sum_{i=0}^n a_i x^i$, $g(x) = \sum_{i=0}^m b_i x^i \in F[x]$ حدوديتان أوليتان فوق F . إذا كان $a_n = 1$ و $b_m = 1$ وكان d صفراً لكل من $f(x)$ و $g(x)$ ، عندئذ يكون $f(x) = g(x)$.

البرهان.

لما كان d صفراً للحدوديتين $f(x)$ و $g(x)$ ، عندئذ حسب التمهيدية (١-١-٧) فإن $x = d$ يقسم كل من $f(x)$ و $g(x)$ ، ومنه يوجد $\lambda(x), \mu(x) \in F[x]$ بحيث يكون:

$$g(x) = (x - d) \cdot \mu(x), \quad f(x) = (x - d) \cdot \lambda(x)$$

ولما كانت كل من $f(x)$ و $g(x)$ أولية فوق F نجد أن $\partial \mu(x) = \partial \lambda(x) = 0$ وهذا يبين أن $\lambda(x) = c$ حيث $\mu(x) = t$ حيث $c, t \in F$ عناصر مغايرة للصفر. ومنه نجد أن:

$$g(x) = (x - d) \cdot t, \quad f(x) = (x - d) \cdot c$$

وهذا يبين أن $f(x) = (x - d) \cdot c \cdot t^{-1} \cdot t$ وبالتالي يكون $f(x) = g(x) \cdot c \cdot t^{-1}$ ومنه يكون $\partial f(x) = \partial g(x)$ ، أي أن $n = m$ ولما كان $a_n = b_n = 1$ نجد أن $c \cdot t^{-1} = 1$ أي أن $t = 1$ وبالتالي $f(x) = g(x)$.

مبرهنة ١-٢-١٥.

ليكن F حقلاً و $f(x) = \sum_{i=0}^n a_i x^i \in F[x]$ عندئذ فإن $f(x)$ تملك نشرًا وحيداً على الشكل الآتي:

$$f(x) = a_n \cdot g_1(x)^{d_1} \cdot g_2(x)^{d_2} \cdots g_m(x)^{d_m}$$

حيث $g_i(x) \in F[x]$ حدوديات أولية فوق F لأجل كل $1 \leq i \leq m$ وأن d_i أعداد صحيحة موجبة لأجل كل $1 \leq i \leq m$.

البرهان.

إذا كانت الحدودية $f(x)$ أولية فوق F نجد أن $f(x) = a_n \sum_{i=0}^n a_i^{-1} a_i x^i$ لنفرض

أن $g(x) = \sum_{i=0}^n a_i^{-1} x^i$ فنجد أن $g(x) \in F[x]$. لما كانت $f(x)$ أولية فوق F فإنه حسب التمهيدية (١-٢-٦) تكون الحدودية $g(x)$ أولية في $F[x]$ وبذلك يتم المطلوب. لنفرض أن الحدودية $f(x)$ ليست أولية فوق F وأن $\partial f(x) = n$. سوف نورد البرهان بالاستقراء حسب n .

من أجل $n=1$ نجد أن $f(x) = a_1 x + a_0$ ومنه فإن $f(x) = a_1(x + a_1^{-1} a_0)$ وأن $x + a_1^{-1} a_0 \in F[x]$ حدودية أولية فوق F .

لنفرض أن المبرهنة صحيحة لأجل كل حدودية في $F[x]$ درجتها أصغر من n . لما كانت الحدودية $f(x)$ ليست أولية فوق F فإنه يوجد $\lambda(x), \mu(x) \in F[x]$ بحيث:

$$f(x) = \lambda(x) \cdot \mu(x)$$

وأن $0 < \partial \lambda(x), \partial \mu(x) < n$ وحسب الفرض الاستقرائي فإن كلا من $\lambda(x), \mu(x)$ يملك نشرًا على الشكل الآتي:

$$\lambda(x) = a \cdot \lambda_1(x)^{d_1} \cdot \lambda_2(x)^{d_2} \cdots \lambda_t(x)^{d_t}$$

$$\mu(x) = b \cdot \mu_1(x)^{s_1} \cdot \mu_2(x)^{s_2} \cdots \mu_m(x)^{s_m}$$

حيث $\lambda_i(x), \mu_i(x) \in F[x]$ حدوديات أولية فوق F لأجل كل i . وهذا يبين أن:

$$f(x) = a \cdot b \cdot \lambda_1(x)^{d_1} \cdot \lambda_2(x)^{d_2} \cdots \lambda_t(x)^{d_t} \cdot \mu_1(x)^{s_1} \cdot \mu_2(x)^{s_2} \cdots \mu_m(x)^{s_m}$$

وحدانية النشر ينتج من المبرهنة (١-٢-٩) والتمهيدية (١-٢-١٤) .

تمارين محلولة (١)

١ - لنأخذ الحقل $Z_3 = \{0,1,2\}$ ولتكن $p(x) = x^2 + 1 \in Z_3[x]$ ولنفرض أن $A = \langle p(x) \rangle$. أثبت أن الحلقة $Z_3[x]/A$ حقلاً ثم أوجد عناصر هذا الحقل.

الحل.
نلاحظ أن $p(0) = 1$ وأن $p(1) = p(2) = 2$ وهذا يبين لنا أن الحدودية $p(x)$ لا تملك أصفاراً في الحقل Z_3 ، ولما كانت $\partial p(x) = 2$ فإنه حسب التمهيدية (١-٢-٥) تكون الحدودية $p(x)$ أولية في $Z_3[x]$ وحسب المبرهنة (١-٢-٧) تكون الحلقة $Z_3[x]/A$ حقلاً. ليكن $\overline{f(x)} \in Z_3[x]/A$ عندئذ $\overline{f(x)} = f(x) + A$ حيث $f(x) \in Z_3[x]$ وحسب خوارزمية القسمة لأجل العنصرين $p(x), f(x)$ فإنه يوجد $q(x), r(x) \in Z_3[x]$ تحقق:
$$f(x) = q(x) \cdot p(x) + r(x)$$
 وأنه إما $r(x) = 0$ أو أن $\partial r(x) < \partial p(x) = 2$ ومنه نجد أن $r(x) = ax + b$ حيث $a, b \in Z_3$ وهكذا نجد أن:

$$\overline{f(x)} = f(x) + A = [q(x) \cdot p(x) + r(x)] + A = r(x) + A$$

وهذا يبين لنا أن $Z_3[x]/A = \{(ax+b) + A : a, b \in Z_3\}$ أي أن:

$$Z_3[x]/A = \{A, 1+A, 2+A, x+A, 2x+A, (x+1)+A, (x+2)+A, (2x+1)+A, (2x+2)+A\} \cdot \diamond$$

٢ - لتكن R حلقة و $R[x]$ حلقة الحدوديات فوق R . عندئذ:

١ - إذا كان A مثالياً في R فإن $A[x]$ يكون مثالياً في $R[x]$.

٢ - إذا كانت الحلقة R تبديلية وكان B مثالياً أولياً في R فإن $B[x]$ يكون مثالياً أولياً في $R[x]$.

الحل.

١ - لنفرض أن A مثالي في R . إن:

$$A[x] = \{f(x) : f(x) \in R[x], f(x) = \sum_{i=0}^n a_i x^i : a_i \in A, \forall 0 \leq i \leq n\}$$

بما أن $0 \in A$ فإن $0 \in A[x]$ وبالتالي المجموعة $A[x]$ غير خالية.
ليكن $f(x), g(x) \in A[x]$ ولنفرض أن $f(x) = \sum_{i=0}^n a_i x^i$, $g(x) = \sum_{i=0}^m b_i x^i$ عندئذ
 $a_i, b_i \in A$ وبما أن A مثالي في R نجد أن $a_i - b_i \in A$ ومنه:

$$f(x) - g(x) = \sum_{i=0}^{\max\{n,m\}} (a_i - b_i) x^i \in A[x]$$

ليكن $h(x) \in A[x]$ و $\varphi(x) \in R[x]$ ولنفرض $h(x) = \sum_{i=0}^s d_i x^i$, $\varphi(x) = \sum_{i=0}^t c_i x^i$ عندئذ

يكون $d_i \in A, c_i \in R$. بفرض أن $\mu(x) = \varphi(x) \cdot h(x) = \sum_{k=0}^{s+t} \mu_k x^k$ وأن $\mu(x) = \sum_{k=0}^{s+t} d_k x^k$ حيث

$$a_k = \sum_{i+j=k} c_i d_j$$

و $d_j \cdot c_i \in A$ وبالتالي يكون $a_k = \sum_{i+j=k} c_i d_j \in A$ ومنه فإن $\mu(x) = \sum_{k=0}^{s+t} d_k x^k \in A[x]$

بطريقة مشابهة نجد أنه أياً كان $\lambda(x) \in R[x]$, $\psi(x) \in A[x]$ فإن:

$$\psi(x) \cdot \lambda(x) \in A[x]$$

مما سبق نجد أن المجموعة $A[x]$ تشكل مثالياً في $R[x]$.

٢ - لنفرض أن الحلقة R تبديلية وأن B مثالي أولي في R عندئذ حسب (١) يكون $B[x]$ مثالياً في $R[x]$. من جهة أخرى، بما أن المثالي B مثالي أولي في R فإن $B \neq R$ ومنه يوجد $b \in R$ وأن $b \notin B$ ومنه فإن $f(x) = bx \in R[x]$ وأن $f(x) \notin B[x]$ وهذا يبين أن $B[x] \neq R[x]$.

ليكن $f(x), g(x) \in R[x]$ بحيث $f(x) \cdot g(x) \in B[x]$ ولنفرض أن:

$$f(x) = \sum_{i=0}^n a_i x^i, g(x) = \sum_{i=0}^m b_i x^i$$

حيث $a_i, b_i \in R$ وأن:

$$f(x) \cdot g(x) = h(x) = \sum_{i=0}^{n+m} c_i x^i$$

حيث $c_k = \sum_{i+j=k} a_i b_j$ وبما أن $h(x) \in B[x]$ فإن $c_k \in B$ وذلك لأجل جميع قيم k .

- لدينا $c_0 = a_0 b_0 \in B$ وبما أن المثالي B مثالي أولي في R عندئذ إما $a_0 \in B$ أو $b_0 \in B$. لنفرض أن $b_0 \notin B$ عندئذ يكون $a_0 \in B$ ، كما أنه في هذه الحالة يكون

$g(x) \notin B[x]$ لنبرهن على أن $f(x) \in B[x]$ ، أي لنبرهن على أن $a_i \in B$ وذلك أيأ
كان $0 \leq i \leq n$.

لدينا أيضاً $c_1 = a_0b_1 + a_1b_0 \in B$ وبما أن $a_0 \in B$ نجد أن $a_0b_1 \in B$ ومنه يكون
 $a_1b_0 = c_1 - a_0b_1 \in B$ وبما أن $b_0 \notin B$ وأن B أولي نجد أن $a_1 \in B$.
- أيضاً لدينا $c_2 = a_0b_2 + a_1b_1 + a_2b_0 \in B$ وبما أن $a_0, a_1 \in B$ نجد أن $a_0b_2 \in B$
وأيضاً $a_1b_1 \in B$ ومنه يكون $a_2b_0 = c_2 - a_0b_2 - a_1b_1 \in B$ وبما أن $b_0 \notin B$ وأن B
أولي نجد أن $a_2 \in B$. نتابع بهذا الشكل ومن خلال الاستقراء لأجل n ، لنفرض أنه تم
إثبات أن $a_0, a_1, a_2, \dots, a_{n-1} \in B$ ولنبرهن على أن $a_n \in B$.
بما أن $c_n = \sum_{i+j=n} a_ib_j \in B$ أي أن $c_n = a_0b_n + a_1b_{n-1} + \dots + a_nb_0 \in B$ وأن
 $a_0, a_1, a_2, \dots, a_{n-1} \in B$ نجد أن:

$$a_nb_0 = c_n - (a_0b_n + a_1b_{n-1} + \dots + a_{n-1}b_1) \in B$$

وبما أن $b_0 \notin B$ وأن B أولي نجد أن $a_n \in B$ وهكذا نجد أن $a_0, a_1, a_2, \dots, a_n \in B$
ومنه فإن $f(x) \in B[x]$ وهذا يبين لنا أن المثالي $B[x]$ أولي في $R[x]$.

٣ - ليكن F حقلاً وأن $F[x]$ حلقة الحدوديات فوق F ولتكن $p(x) \in F[x]$ وأن
 $A = \langle p(x) \rangle$. إذا كانت $f(x), g(x) \in F[x]$ وتحققان الشروط الآتية:

$$\partial f(x) < \partial p(x), \quad \partial g(x) < \partial p(x) \quad -$$

$$f(x) + A = g(x) + A \quad -$$

$$f(x) = g(x) \quad \text{أثبت أن}$$

الحل.

لنفرض جدياً أن $f(x) \neq g(x)$ عندئذ يكون $f(x) - g(x) \neq 0$ وحسب الشرط (١)
فإن $\partial(f(x) - g(x)) \leq \max\{\partial f(x), \partial g(x)\} < \partial p(x)$.

من جهة أخرى، بما أن $f(x) + A = g(x) + A$ فإن $f(x) - g(x) \in A$ وبما أن
 $A = \langle p(x) \rangle$ فإنه توجد $\lambda(x) \in F[x]$ بحيث $f(x) - g(x) = p(x) \cdot \lambda(x)$ ومنه
يكون $\partial(f(x) - g(x)) = \partial p(x) + \partial \lambda(x) \geq \partial p(x)$ وهذا تناقض. مما سبق نجد
أن $f(x) = g(x)$.

٤ - ليكن K, F حقلين وأن $\varphi: K \rightarrow F$ تشاكل حقيقي. عندئذ يوجد تشاكل حقيقي

$\varphi: K[x] \rightarrow F[x]$ معرف بالشكل الآتي: $\varphi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \varphi(a_i) x^i$ وذلك أيًا كان

$$\sum_{i=0}^n a_i x^i \in K[x]$$

الحل.

لنعرف $\varphi: K[x] \rightarrow F[x]$ بالشكل الآتي: $\varphi(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \varphi(a_i) x^i$ وذلك أيًا كان

$\sum_{i=0}^n a_i x^i \in K[x]$. واضح أن φ تطبيق. لنبرهن على أن φ تشاكل.

ليكن $\sum_{i=0}^n a_i x^i, \sum_{i=0}^m b_i x^i \in K[x]$ ولنفرض أن $n \geq m$ حيث $a_i, b_i \in K$ ذلك لأجل جميع

القيم $0 \leq i \leq n$. عندئذ يكون:

$$\begin{aligned} \varphi(\sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i) &= \varphi(\sum_{i=0}^n (a_i + b_i) x^i) = \sum_{i=0}^n \varphi(a_i + b_i) x^i = \\ &= \sum_{i=0}^n \varphi(a_i + b_i) x^i = \sum_{i=0}^n [\varphi(a_i) + \varphi(b_i)] x^i = \sum_{i=0}^n \varphi(a_i) x^i + \sum_{i=0}^m \varphi(b_i) x^i = \\ &= \varphi(\sum_{i=0}^n a_i x^i) + \varphi(\sum_{i=0}^m b_i x^i) \end{aligned}$$

لنفرض أن:

$$(\sum_{i=0}^n a_i x^i) \cdot (\sum_{i=0}^m b_i x^i) = \sum_{i=0}^{n+m} d_i x^i$$

حيث $d_k = \sum_{i+j=k} a_i b_j$ وأن $0 \leq k \leq n+m$ فنجد أن:

$$\varphi[(\sum_{i=0}^n a_i x^i) \cdot (\sum_{i=0}^m b_i x^i)] = \varphi(\sum_{k=0}^{n+m} d_k x^k) = \sum_{k=0}^{n+m} \varphi(d_k) x^k$$

وبما أن φ تشاكل فإن:

$$\varphi(d_k) = \varphi(\sum_{i+j=k} a_i b_j) = \sum_{i+j=k} \varphi(a_i b_j) = \sum_{i+j=k} \varphi(a_i) \cdot \varphi(b_j)$$

وهكذا نجد أن:

$$\varphi[(\sum_{i=0}^n a_i x^i) \cdot (\sum_{i=0}^m b_i x^i)] = (\sum_{i=0}^n \varphi(a_i) x^i) \cdot (\sum_{i=0}^m \varphi(b_i) x^i) = \varphi(\sum_{i=0}^n a_i x^i) \cdot \varphi(\sum_{i=0}^m b_i x^i)$$

مما سبق نجد أن التطبيق $\varphi: K[x] \rightarrow F[x]$ تشاكل حقيقي. ♦

٥ - ليكن K, F حقلين متماثلين، عندئذ تكون الحلقتان $K[x], F[x]$ متماثلتين أيضاً.
الحل.

نفرض أن K, F حقلين وأن $\varphi: K \rightarrow F$ تماثل، بما أن φ تشاكل حقلي عندئذ حسب التمرين الأخير يكون التطبيق $\varphi: K[x] \rightarrow F[x]$ المعروف بالشكل الآتي:

أياً كان $\sum_{i=0}^n a_i x^i \in K[x]$ فإن $\sum_{i=0}^n \varphi(a_i) x^i = \varphi(\sum_{i=0}^n a_i x^i)$ ، تشاكل حقلي. لنبرهن على

أن التشاكل φ تماثل. تلاحظ أولاً أن التشاكل φ متباين، لأنه إذا كان $\sum_{i=0}^n a_i x^i \in K[x]$

و $\sum_{i=0}^m b_i x^i \in K[x]$ بحيث أن $\varphi(\sum_{i=0}^n a_i x^i) = \varphi(\sum_{i=0}^m b_i x^i)$ فإن:

$$\sum_{i=0}^n \varphi(a_i) x^i = \sum_{i=0}^m \varphi(b_i) x^i$$

وهذا يبين لنا أن $n = m$ وأن $\varphi(a_i) = \varphi(b_i)$ وذلك لأجل جميع القيم $0 \leq i \leq n$. وبما

أن $\varphi: K \rightarrow F$ تماثل نجد أن $a_i = b_i$ وذلك لأجل جميع القيم $0 \leq i \leq n$. وهذا يبين

$$\sum_{i=0}^n a_i x^i = \sum_{i=0}^m b_i x^i$$

كما أن التشاكل $\varphi: K[x] \rightarrow F[x]$ غامر، لأنه إذا كان $\sum_{i=0}^t c_i x^i \in F[x]$ فإن $c_i \in F$

أياً كان $0 \leq i \leq t$ وبما أن التشاكل $\varphi: K \rightarrow F$ غامر فإنه توجد عناصر $d_i \in K$

لأجل جميع القيم $0 \leq i \leq t$ تحقق $\varphi(d_i) = c_i$ ، ومنه نجد أن $\sum_{i=0}^t d_i x^i \in K[x]$ وأن:

$$\varphi(\sum_{i=0}^t d_i x^i) = \sum_{i=0}^t \varphi(d_i) x^i = \sum_{i=0}^t c_i x^i$$

مما سبق نجد أن التطبيق $\varphi: K[x] \rightarrow F[x]$ تماثل. ◊

٦ - ليكن K, F حقلين. إذا كان $\varphi: K \rightarrow F$ تماثلاً وكانت الحدودية $p(x) \in K[x]$

أولية فوق K ، عندئذ تكون الحدودية $\varphi(p(x))$ أولية فوق F .

الحل.

نفرض أن $\varphi: K \rightarrow F$ تماثل، عندئذ حسب التمرين المحلول (١-٥) يمكن تمديد هذا

التماثل إلى تماثل حقلي $\varphi: K[x] \rightarrow F[x]$ المعروف بالشكل الآتي:

أيّاً كان $\sum_{i=0}^n c_i x^i \in K[x]$ فإن $\sum_{i=0}^n \varphi(c_i) x^i = \varphi(\sum_{i=0}^n c_i x^i)$. لنفرض أن $p(x) \in K[x]$ حدودية أولية فوق الحقل K ، عندئذ تكون الحدودية $p(x)$ غير قابلة للقلب في $K[x]$ وحسب المبرهنة (٢-٢-١) تكون $\partial p(x) \geq 1$. لنفرض أن $\partial p(x) = m \geq 1$ عندئذ يكون $p(x) = \sum_{i=0}^m d_i x^i$ حيث $d_i \in K$ وأن $d_m \neq 0$ ومنه يكون:

$$\varphi(p(x)) = \sum_{i=0}^m \varphi(d_i) x^i \in F[x]$$

لأن $\varphi(d_i) \in F$ وذلك لأجل جميع القيم $0 \leq i \leq m$ وبما أن $\varphi: K \rightarrow F$ تماثل وأن $d_m \neq 0$ نجد أن $\varphi(d_m) \neq 0$ وبالتالي فإن $\partial \varphi(p(x)) = m \geq 1$ وحسب المبرهنة (٢-٢-١) فإن الحدودية $\varphi(p(x))$ تكون غير قابلة للقلب في $F[x]$. من جهة أخرى، ليكن $\theta_0(x), g_0(x) \in F[x]$ بحيث $\varphi(p(x)) = \theta_0(x) \cdot g_0(x)$ ولنفرض جدلاً أن كلاً من $\theta_0(x)$ و $g_0(x)$ غير قابلة للقلب في $F[x]$ عندئذ حسب المبرهنة (٢-٢-١) فإن $\partial \theta_0(x) \geq 1$ و $\partial g_0(x) \geq 1$ ولكون $\varphi: K[x] \rightarrow F[x]$ تماثلاً فإنه توجد $\theta(x), g(x) \in K[x]$ بحيث $\varphi(\theta(x)) = \theta_0(x), \varphi(g(x)) = g_0(x)$ ومنه يكون:

$$\varphi(p(x)) = \theta_0(x) \cdot g_0(x) = \varphi(\theta(x)) \cdot \varphi(g(x)) = \varphi(\theta(x) \cdot g(x))$$

ولما كان التطبيق $\varphi: K[x] \rightarrow F[x]$ تماثلاً ينتج أن $p(x) = \theta(x) \cdot g(x)$ وبما أن $\partial \theta_0(x) \geq 1$ و $\partial g_0(x) \geq 1$ ينتج أن $\partial \theta(x) \geq 1$ و $\partial g(x) \geq 1$ وحسب المبرهنة (٢-٢-١) فإن كلاً من $\theta(x)$ و $g(x)$ غير قابلة للقلب في $F[x]$ وهذا يناقض كون الحدودية $p(x)$ أولية فوق K ، وهذا يبين لنا أنه إما $\theta_0(x)$ أو $g_0(x)$ قابلة للقلب في $K[x]$. مما سبق نجد أن الحدودية $\varphi(p(x))$ أولية فوق الحقل F .

تمارين (١)

- ١ - ليكن $f(x), g(x) \in Z_5[x]$ حيث $f(x) = 4x^3 + 2x^2 + x + 3$ وأن $g(x) = 3x^4 + 3x^3 + 3x^2 + x + 4$. أوجد $f(x) + g(x)$, $f(x) \cdot g(x)$.
- ٢ - أثبت أن الحدودية $x^2 + 3x + 2$ تملك أربعة أصفار في الحلقة Z_6 .
- ٣ - ليكن $f(x) = x^3 + 2x + 4$, $g(x) = 3x + 2 \in Z_5[x]$. أوجد ناتج وباقي قسمة $f(x)$ على $g(x)$ في $Z_5[x]$.
- ٤ - ليكن $f(x) = 5x^4 + 3x^3 + 1$, $g(x) = 3x^2 + 2x + 1 \in Z_7[x]$. أوجد ناتج وباقي قسمة $f(x)$ على $g(x)$ في $Z_7[x]$.
- ٥ - ليكن $f(x) = x^4 + x$, $g(x) = x^2 + x \in Z_3[x]$. أثبت أن كلا من f, g يعرف تطبيقاً من Z_3 إلى Z_3 وأن $f = g$ على Z_3 .
- ٦ - أثبت أن الحدودية $2x + 1 \in Z_4[x]$ تملك مقلوباً بالنسبة للضرب (قابلية للقلب) في $Z_4[x]$.
- ٧ - أوجد جميع الحدوديات من الدرجة 2 في الحلقة Z_2 .
- ٨ - ليكن p عدداً أولياً، أوجد $U(Z_p[x])$.
- ٩ - أوجد جميع حلول المعادلة $x^2 - x + 2 = 0$ في الحلقة $Z_3[i]$.
- ١٠ - أثبت أن الحدودية $g(x) = x^2 + x + 4$ أولية فوق Z_{11} .
- ١١ - لتكن $f(x) = x^3 + 6 \in Z_7[x]$. اكتب $f(x)$ على شكل جداء لحدوديات أولية فوق Z_7 .
- ١٢ - لتكن $f(x) = x^3 + x^2 + x + 1 \in Z_2[x]$. اكتب الحدودية $f(x)$ على شكل جداء لحدوديات أولية فوق Z_7 .
- ١٣ - أثبت أن المثالي $\langle x^2 + 1 \rangle$ أولي في $Z[x]$ ولكنه ليس أعظماً.
- ١٤ - أثبت أن الحلقة $R[x]/\langle x^2 + 1 \rangle$ حقل، حيث R هو حقل الأعداد الحقيقية.
- ١٥ - لأجل أي عدد أولي p أثبت أن الحدودية $x^4 + 1$ ليست أولية في $Z_p[x]$.

- ١٦ - لتكن $Z_2[x]$ حلقة الحدوديات فوق الحقل Z_2 وليكن $A = \langle x^2 + x + 1 \rangle$. أثبت أن الحلقة $Z_2[x]/A$ حقل ثم أوجد جميع عناصره.
- ١٧ - لتكن $Z_5[x]$ حلقة الحدوديات فوق الحقل Z_5 وليكن $A = \langle x^2 + x + 1 \rangle$. أوجد مقلوب العنصر $(2x + 3) + A$ في الحلقة $Z_5[x]/A$.
- ١٨ - لتكن $Z_3[x]$ حلقة الحدوديات فوق الحقل Z_3 وليكن $B = \langle x^2 + x + 1 \rangle$. أثبت أن الحلقة $Z_3[x]/B$ ليست حقلاً.
- ١٩ - أوجد جميع الحدوديات الأولية من الدرجة الثانية في الحلقة $Z_3[x]$.
- ٢٠ - ليكن F حقلاً و $F[x]$ حلقة الحدوديات فوق الحقل F ولنأخذ المجموعة $K = \{f(x) : f(x) \in F[x], f(a) = 0, \forall a \in F\}$
- أثبت أن المجموعة K تشكل مثاليًا في $F[x]$.
- إذا كان الحقل F منتهياً أثبت أن المثالي K ليس منتهياً.
- إذا كان الحقل F ليس منتهياً أثبت أن المثالي K منتهياً.
- ٢١ - ليكن F حقلاً و $f(x) = \sum_{i=0}^n a_i x^i \in F[x]$. أثبت أن الشرط اللازم والكافي كي تكون الحدودية $g(x) = x - 1$ تقسم الحدودية $f(x)$ في $F[x]$ هو أن يكون $\sum_{i=0}^n a_i = 0$.
- ٢٢ - ليكن F حقلاً و $p(x) \in F[x]$. إذا كانت الحدودية $p(x)$ أولية فوق F وكان $A = \langle p(x) \rangle$. أثبت أن المجموعة $I = \{a + I : a \in F\}$ تشكل حقلاً جزئياً من الحقل $F[x]/A$ يماثل F .

الفصل الثاني

الحدوديات فوق حلقة الأعداد الصحيحة

في هذا الفصل سوف ندرس الحدوديات فوق حلقة الأعداد الصحيحة Z .

٢ - ١. الحدوديات الأولية في $Z[x]$.

سوف نخصص هذه الفقرة لدراسة الحدوديات الأولية في الحلقة $Z[x]$ والبدائية ستكون مع التمهيدية الآتية:

تمهيدية ٢-١-١.

لتكن $0 \neq f(x) \in Z[x]$. عندئذ القضايا الآتية صحيحة:

١ - الشرط اللازم والكافي كي تكون الحدودية $f(x)$ قابلة للقلب في $Z[x]$ هو أن تكون $f(x) = 1$ أو $f(x) = -1$.

٢ - كل عدد أولي في Z هو حدودية أولية في $Z[x]$ ودرجتها تساوي الصفر.

٣ - كل عدد غير أولي في Z ولا يساوي الصفر هو حدودية غير أولية في $Z[x]$ ودرجتها تساوي الصفر.

البرهان.

١ - لزوم الشرط. لنفرض أن الحدودية $f(x)$ قابلة للقلب في $Z[x]$ ، بما أن $Z[x]$ منطقة

تكاملية فإنه حسب التمهيدية (١-٢-١) فإن $\partial f(x) = 0$ ومنه فإن $f(x) = a$ حيث

$a \in Z$ ، $a \neq 0$ ، وبما أن العناصر القابلة للقلب في Z هي فقط $1, -1$ نجد أنه إما

$$f(x) = 1 \text{ أو } f(x) = -1.$$

كفاية الشرط واضح.

٢ - ليكن p عدداً أولياً في Z ولنفرض أن $g(x) = p$ فنجد أن $0 \neq g(x) \in Z[x]$

وأن $\partial g(x) = 0$ ، وبما أن $p \neq \pm 1$ عندئذ حسب (١) فإن الحدودية $g(x)$ غير قابلة

للقلب في $Z[x]$. لنفرض أن $g(x) = h(x) \cdot \lambda(x)$ حيث $h(x), \lambda(x) \in F[x]$ عندئذ

يكون $\partial h(x) = \partial \lambda(x) = 0$ وذلك لأن $Z[x]$ منطقة تكاملية، ومنه فإن $h(x) = a$ و

$\lambda(x) = b$ حيث a, b أعداد صحيحة مغايرة للصفر، ومنه نجد أن $p = a \cdot b$ وبما أن a يقسم p فإنه إما $a = \pm 1$ أو $a = \pm p$.

- إذا كان $a = \pm 1$ فإنه حسب (١) تكون الحدودية $h(x)$ قابلة للقلب في $Z[x]$.
 - إذا كان $a = \pm p$ عندئذ يكون $b = \pm 1$ وحسب (١) تكون الحدودية $\lambda(x)$ قابلة للقلب في $Z[x]$. مما سبق وحسب التعريف نجد أن $g(x)$ أولية في $Z[x]$.

٣ - لنفرض أن $n \neq 0$ عدد صحيح ليس أولياً وأن $\mu(x) = n$ ، عندئذ $\mu(x) \in Z[x]$ وأن $\mu(x) \neq 0$ ، كما أن $\partial \mu(x) = 0$. وهنا نميز حالتين:

- $n = \pm 1$ عندئذ حسب (١) تكون الحدودية $\mu(x)$ قابلة للقلب في $Z[x]$ وبالتالي فهي غير أولية في $Z[x]$ حسب التعريف.

- $n \neq \pm 1$ عندئذ حسب (١) تكون الحدودية $\mu(x)$ غير قابلة للقلب في $Z[x]$ وبما أن الحلقة Z حلقة مثاليات رئيسية فإنه بالإمكان كتابة العنصر n بالشكل $n = c \cdot d$ حيث $c, d \in Z$ وأن كلاً منهما غير قابل للقلب في Z . لنفرض أن $h_1(x) = d$ و $g_1(x) = c$ فنجد أن $\mu(x) = g_1(x) \cdot h_1(x)$ وأن كلاً من $g_1(x), h_1(x)$ غير قابل للقلب في $Z[x]$. مما سبق نجد أن الحدودية $\mu(x)$ غير أولية في $Z[x]$.

قبل المتابعة في دراسة الحدوديات الأولية في $Z[x]$ سنورد عدداً من الأمثلة:

أمثلة.

١ - الحدودية $f(x) = 3x + 6$ غير أولية في $Z[x]$.
 بما أن $\partial f(x) > 0$ فإنه حسب التمهيدية (٢-١-١) تكون الحدودية $f(x)$ غير قابلة للقلب في $Z[x]$. نلاحظ أيضاً أن $f(x) = 3(x + 2)$ ، بفرض أن $h(x) = x + 2$ و $g(x) = 3$ نجد أن $f(x) = g(x) \cdot h(x)$ وأن الحدودية $g(x) = 3$ غير قابلة للقلب في $Z[x]$ وأيضاً الحدودية $h(x) = x + 2$ غير قابلة للقلب في $Z[x]$ وذلك حسب التمهيدية (٢-١-١)، مما سبق وحسب التعريف نجد أن الحدودية $f(x)$ ليست أولية في $Z[x]$.

٢ - الحدودية $f(x) = 5x + 2$ هي حدودية أولية في $Z[x]$.
 بما أن $\partial f(x) > 0$ فإن $f(x)$ غير قابلة للقلب في $Z[x]$. لنفرض أن:

$$f(x) = g(x) \cdot \lambda(x)$$

عندئذ وبما أن $Z[x]$ منطقة تكاملية نجد أن $\partial f(x) = \partial g(x) + \partial \lambda(x)$ و $1 = \partial f(x)$ ومنه إما $\partial g(x) = 0$ أو $\partial \lambda(x) = 0$.

- إذا كانت $\partial g(x) = 0$ نجد أن $g(x) = a$ حيث $a \in Z$ و $a \neq 0$ وفي هذه الحالة تكون $\partial \lambda(x) = 1$ وبالتالي يكون $\lambda(x) = bx + d$ حيث $b, d \in Z$ وأن $b \neq 0$ ومنه فإن:

$$5x + 2 = a(bx + d) = abx + ad$$

وبالتالي يكون $2 = ad$ و $5 = ab$ وهذا يبين أن العدد a هو قاسم مشترك للعددين 2,5 وبما أن العددين 2,5 أوليان فيما بينهما، فإن القاسم المشترك الوحيد لهما هو الواحد ومنه نجد أن الحدودية $g(x) = 1$ وحسب التمهيدية (٢-١-١) فإن الحدودية $g(x)$ قابلة للقلب في $Z[x]$.

- إذا كانت $\partial \lambda(x) = 0$ بطريقة مشابهة نجد أن الحدودية $\lambda(x)$ قابلة للقلب في $Z[x]$. وحسب التعريف نجد أن الحدودية $f(x)$ أولية في $Z[x]$.

بالعودة إلى المثالين السابقين نجد أنه في المثال رقم (١) لدينا $\gcd(3,6) = 3 > 1$ بينما في المثال رقم (٢) فإن $\gcd(2,5) = 1$. وهكذا نجد أن القاسم المشترك الأعظم لأمثال الحدودية يمكن أن يلعب دوراً في كونها أولية أم لا، وذلك فقط في الحلقة $Z[x]$. لأجل ذلك سوف نورد التعريف الآتي:

تعريف.

ليكن $f(x) = \sum_{i=0}^n a_i x^i \in Z[x]$ و $0 \neq f(x)$. نسمي القاسم المشترك الأعظم للعناصر:

$$a_0, a_1, \dots, a_n \in Z$$

برئيس الحدودية $f(x)$ ، أي أن رئيس الحدودية $f(x)$ هو $\gcd(a_0, a_1, \dots, a_n)$. إذا كان $\gcd(a_0, a_1, \dots, a_n) = 1$ نقول عن الحدودية $f(x)$ في هذه الحالة إنها رئيسية.

بالاعتماد على التعريف السابق يمكننا صياغة النتيجة الآتية:

نتيجة.

إذا كانت $f(x) = \sum_{i=0}^n a_i x^i \in Z[x]$ وكان أحد الأمثال $a_i = \pm 1$ عندئذ تكون الحدودية $f(x)$ رئيسية. ◊

العلاقة بين الحدوديات الأولية والرئيسية نوردتها من خلال التمهيدية الآتية:

تمهيدية ٢-١-٢.

كل حدودية أولية في $Z[x]$ ودرجتها أكبر من الصفر هي حدودية رئيسية.
البرهان.

لتكن $f(x) = \sum_{i=0}^n a_i x^i \in Z[x]$ حدودية أولية فوق Z وأن $\partial f(x) > 0$. لنفرض جدلاً أن $f(x)$ ليست رئيسية، عندئذ يكون $\gcd(a_0, a_1, a_2, \dots, a_n) = b > 1$ ومنه توجد عناصر $d_i \in Z$ بحيث $a_i = b d_i$ وذلك لأجل جميع القيم $0 \leq i \leq n$ ، ومنه

$$f(x) = \sum_{i=0}^n a_i x^i = \sum_{i=0}^n (b d_i) x^i = b \left(\sum_{i=0}^n d_i x^i \right)$$

لنفرض أن $h(x) = \sum_{i=0}^n d_i x^i$ وأن $g(x) = b$ فنجد أن $\partial h(x) = \partial f(x) > 0$ وأن $g(x) \neq \pm 1$ وحسب التمهيدية (٢-٢-١) فإن الحدوديتين $g(x), h(x)$ كل منهما غير قابلة للقلب في $Z[x]$ وهذا يناقض كون الحدودية $f(x)$ أولية في $Z[x]$. مما سبق نجد أن $\gcd(a_0, a_1, a_2, \dots, a_n) = 1$ وبالتالي تكون الحدودية $f(x)$ رئيسية في $Z[x]$. ◊

لأجل متابعة دراستنا للحدوديات الرئيسية لا بد لنا من المبرهنة الآتية:

مبرهنة ٢-١-٣.

جداء حدوديتين رئيسيتين هو حدودية رئيسية.

البرهان.

لتكن $f(x) = \sum_{i=0}^n a_i x^i$, $g(x) = \sum_{i=0}^m b_i x^i \in Z[x]$ حيث $a_i, b_i \in Z$ حدوديتان رئيسيتان ولنفرض جدلاً أن الحدودية $f(x) \cdot g(x) = \sum_{k=0}^{n+m} c_k x^k \in Z[x]$ ليست رئيسية، حيث $c_k \in Z$ أيّاً كان $0 \leq k \leq n+m$ ، عندئذ يكون $\gcd(c_0, c_1, c_2, \dots, c_{n+m}) = u > 1$.

بما أن كل عدد صحيح أكبر من الواحد يقبل القسمة على عدد أولي، لنفرض أن العدد الأولي p يقسم u ولنفرض أن $\overline{a_i} = a_i \bmod -p$, $\overline{b_j} = b_j \bmod -p$ عندئذ يكون $\overline{a_i}, \overline{b_j} \in Z_p$ وذلك أياً كان $0 \leq i \leq n$ و $0 \leq j \leq m$. وبالتالي يكون:

$$\overline{f(x)} = \sum_{i=0}^n \overline{a_i} x^i, \quad \overline{g(x)} = \sum_{i=0}^m \overline{b_i} x^i \in Z_p[x]$$

من جهة أخرى، بما أن p يقسم u فإن p يقسم c_i ومنه فإن $\overline{c_i} = c_i \bmod -p = 0$ وذلك أياً كان $0 \leq i \leq n+m$ ، ومنه فإن $\overline{f(x)} \cdot \overline{g(x)} = \overline{f(x) \cdot g(x)} = 0$ ولما كانت $Z_p[x]$ منطقة تكاملية نجد أنه إما $\overline{f(x)} = 0$ أو $\overline{g(x)} = 0$.

- إذا كان $\overline{f(x)} = 0$ عندئذ يكون $\overline{a_i} = 0$ وبالتالي فإن a_i يقبل القسمة على p وذلك أياً كان $0 \leq i \leq n$ ، ومنه يكون $\gcd(a_0, a_1, a_2, \dots, a_n) = p \neq 1$ وهذا يناقض كون الحدودية $f(x)$ رئيسية.

- كذلك الأمر إذا كان $\overline{g(x)} = 0$ فإن الحدودية $g(x)$ تكون غير رئيسية وهذا أيضاً غير ممكن، مما سبق نجد أن الحدودية $f(x) \cdot g(x)$ هي حدودية رئيسية. ◊

يمكن تعميم المبرهنة الأخيرة بالشكل الآتي:

نتيجة.

جداء أي عدد منته من الحدوديات الرئيسية هو حدودية رئيسية. ◊

نأتي الآن إلى دراسة المبرهنة الآتية والتي تبين لنا متى تكون الحدودية الرئيسية أولية:

مبرهنة ٢-١-٤.

القضايا الآتية صحيحة:

١ - كل حدودية رئيسية في $Z[x]$ وغير أولية فوق Q تكون غير أولية في $Z[x]$.

٢ - كل حدودية في $Z[x]$ وغير أولية فوق Q تكون غير أولية في $Z[x]$.

البرهان.

١ - لتكن $f(x) \in Z[x]$ حدودية رئيسية وغير أولية في $Q[x]$ عندئذ يوجد $g(x), h(x)$ عناصر في $Q[x]$ تحقق $f(x) = g(x) \cdot h(x)$. لنفرض أن a هو جداء المقامات لأمثال الحدودية $g(x)$ وأن b هو جداء المقامات لأمثال الحدودية $h(x)$ ، عندئذ يكون

$a \cdot g(x), b \cdot h(x) \in Z[x]$. لنفرض أن c_1 رئيس الحدودية $a \cdot g(x)$ و c_2 رئيس الحدودية $b \cdot h(x)$ ، عندئذ يكون:

$$a \cdot g(x) = c_1 \cdot g_1(x) \text{ و } b \cdot h(x) = c_2 \cdot h_1(x)$$

بما أن $\partial g(x) > 0, \partial h(x) > 0$ فإن $\partial g_1(x) > 0, \partial h_1(x) > 0$ كما أن كلا من $g_1(x)$ و $h_1(x)$ هي حدوديات رئيسية ولما كان:

$$a \cdot b \cdot f(x) = c_1 \cdot g_1(x) \cdot c_2 \cdot h_1(x) = c_1 \cdot c_2 \cdot g_1(x) \cdot h_1(x)$$

وبما أن جداء حدوديتين رئيسيتين هو حدودية رئيسية وذلك حسب المبرهنة (٢-١-٣) فإن الحدودية $g_1(x) \cdot h_1(x)$ هي حدودية رئيسية ومنه فإن $c_1 \cdot c_2$ هو رئيس الحدودية $c_1 \cdot c_2 \cdot g_1(x) \cdot h_1(x)$

من جهة أخرى، بما أن الحدودية $f(x)$ رئيسية فإن رئيس الحدودية $a \cdot b \cdot f(x)$ هو $a \cdot b$ وبما أن $a \cdot b \cdot f(x) = c_1 \cdot c_2 \cdot g_1(x) \cdot h_1(x)$ نجد أن $a \cdot b = c_1 \cdot c_2$. مما سبق نجد أن $f(x) = g_1(x) \cdot h_1(x)$ حيث $\partial g_1(x) > 0, \partial h_1(x) > 0$ وهذا يبين أن الحدودية $f(x)$ ليست أولية في $Z[x]$.

٢ - لتكن $\varphi(x) \in Z[x]$ حدودية غير أولية في $Q[x]$ ولنفرض أن α هو رئيس الحدودية $\varphi(x)$ ، عندئذ $\varphi(x) = \alpha \cdot \mu(x)$ حيث $\mu(x) \in Z[x]$ حدودية رئيسية، وبما أن $\varphi(x)$ حدودية غير أولية فوق Q فإن الحدودية $\mu(x)$ تكون غير أولية فوق Q ، لأنه إذا كانت $\mu(x) = \alpha^{-1} \cdot \varphi(x)$ فإنه حسب المبرهنة (١-٢-٦) تكون الحدودية $\varphi(x)$ أولية في $Q[x]$ ، وهذا غير ممكن. أصبح لدينا $\mu(x)$ حدودية رئيسية في $Z[x]$ وغير أولية وحسب (١) نجد أن الحدودية $\mu(x)$ غير أولية في $Z[x]$ ، ومنه يوجد $g_2(x)$ و $h_2(x)$ عناصر في $Z[x]$ بحيث $\partial g_2(x) > 0, \partial h_2(x) > 0$ وتحققان

$$\mu(x) = g_2(x) \cdot h_2(x)$$

ومنه يكون $\varphi(x) = [\alpha \cdot g_2(x)] \cdot h_2(x)$ وهذا يبين لنا أن الحدودية $\varphi(x)$ غير أولية في $Z[x]$.

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة المبرهنة الآتية والتي تبين لنا متى تكون الحدوديات فوق Z أولية:

مبرهنة ٢-١-٥.

لتكن $f(x) \in Z[x]$ وأن $\partial f(x) > 0$. الشرط اللازم والكافي كي تكون الحدودية $f(x)$ أولية في $Q[x]$ هو أن تكون $f(x)$ أولية في $Z[x]$.

البرهان.

لنزم الشرط. لنفرض أن الحدودية $f(x)$ أولية في $Q[x]$ وأنها غير أولية في $Z[x]$ ، عندئذ تكون الحدودية $f(x)$ غير أولية في $Q[x]$ وهذا غير ممكن. ومنه فإن $f(x)$ أولية في $Z[x]$.

كفاية الشرط. لنفرض أن الحدودية $f(x)$ أولية في $Z[x]$ وأنها غير أولية في $Q[x]$ ، عندئذ حسب المبرهنة (٢-١-٤) تكون الحدودية $f(x)$ غير أولية في $Z[x]$ وهذا غير ممكن. ومنه فإن $f(x)$ أولية في $Q[x]$. ◊

بسبب أهمية الحدوديات الأولية في $Z[x]$ ودورها في دراسة الحقول فقد تم إيجاد عدد من الاختبارات للحدوديات الأولية في $Z[x]$. أحد هذه الاختبارات سوف نورد من خلال المبرهنة الآتية:

مبرهنة ٢-١-٦.

ليكن p عدداً أولياً ولتكن $f(x) = \sum_{i=0}^n a_i x^i \in Z[x]$ وأن $\partial f(x) > 0$. لنفرض أن $\overline{f(x)} = \sum_{i=0}^n \overline{a_i} x^i \in Z_p[x]$ عندئذ تكون $\overline{a_i} = a_i \bmod p$. إذا كانت الحدودية $\overline{f(x)}$ أولية في $Z_p[x]$ وكان $\partial \overline{f(x)} = \partial f(x)$ ، عندها تكون الحدودية $f(x)$ أولية فوق Q ، (وبالتالي فوق Z).

البرهان.

لنفرض جديلاً أن الحدودية $f(x)$ غير أولية فوق Q ، عندئذ حسب المبرهنة (٢-١-٤) تكون الحدودية $f(x)$ غير أولية فوق Z ، وبالتالي يوجد $g(x), h(x) \in Z[x]$ بحيث $\partial g(x) > 0, \partial h(x) > 0$ وتحققان $f(x) = g(x) \cdot h(x)$ ، ومنه يكون:

$$\partial g(x) < \partial f(x), \partial h(x) < \partial f(x)$$

لنفرض أن $h(x) = \sum_{i=0}^n d_i x^i, g(x) = \sum_{j=0}^m b_j x^j$ حيث $d_i, b_j \in Z$ وذلك لأجل جميع

القيم $0 \leq i \leq n, 0 \leq j \leq m$ لنفرض أن $\overline{b_j} = b_j \bmod -p, \overline{d_i} = d_i \bmod -p$ عندئذ تكون $\overline{f(x)} = \overline{g(x) \cdot h(x)}$ وأن $\overline{g(x)} = \sum_{j=0}^m \overline{b_j} x^j, \overline{h(x)} = \sum_{i=0}^n \overline{d_i} x^i \in Z_p[x]$ وبما أن $\partial \overline{f(x)} = \partial f(x)$ نجد أن:

$$\partial \overline{g(x)} \leq \partial g(x) < \partial f(x)$$

$$\partial \overline{h(x)} \leq \partial h(x) < \partial f(x)$$

ومنه يكون $\partial \overline{g(x)} > 0, \partial \overline{h(x)} > 0$ وهذا يناقض كون الحدودية $\overline{f(x)}$ أولية في $Z_p[x]$. مما سبق نجد أن الحدودية $f(x)$ أولية في $Q[x]$ وبالتالي أولية في $Z[x]$.

لنورد الآن عدداً من الأمثلة كتطبيق على المبرهنات السابقة.

أمثلة.

١ - أثبت أن الحدودية $f(x) = 21x^3 - 3x^2 + 2x + 9 \in Z[x]$ أولية في $Z[x]$.
نلاحظ أنه من أجل $p = 2$ فإن $2 \bmod -2 = 0$ وأن

$$21 \bmod -2 = -3 \bmod -2 = 9 \bmod -2 = 1$$

ومنه تكون $\overline{f(x)} = x^3 + x^2 + 1 \in Z_2[x]$ كما أن $\partial \overline{f(x)} = \partial f(x) = 3$.
من جهة أخرى، بما أن $Z_2 = \{0,1\}$ حقل وأن $\overline{f(1)} = \overline{f(0)} = 1$ نجد أن الحدودية $\overline{f(x)}$ لا تملك أصفاراً في الحقل Z_2 وحسب التمهيدية (١-٢-٥) نجد أن الحدودية $\overline{f(x)}$ أولية فوق Z_2 وحسب المبرهنة (٢-١-٦) تكون الحدودية $f(x)$ أولية في $Z[x]$.

٢ - أثبت أن الحدودية $f(x) = 21x^3 - 3x^2 + 2x + 8 \in Z[x]$ أولية في $Z[x]$.
نلاحظ أنه من أجل $p = 2$ فإن $21 \bmod -2 = -3 \bmod -2 = 1$ وأن

$$2 \bmod -2 = 8 \bmod -2 = 0$$

ومنه تكون $\overline{f(x)} = x^3 + x^2 = x^2(x+1) \in Z_2[x]$ وأن $\partial \overline{f(x)} = \partial f(x) = 3$.
من جهة أخرى، بما أن $Z_2 = \{0,1\}$ حقل وأن $\overline{f(1)} = \overline{f(0)} = 0$ نجد أن الحدودية $\overline{f(x)}$ تملك أصفاراً في الحقل Z_2 ، وحسب المبرهنة (١-٢-٤) نجد أن الحدودية $\overline{f(x)}$ غير أولية فوق Z_2 .

وهنا نلاحظ أن المبرهنة (١-٢-٤) لا تعطينا جواباً حول الحدودية $f(x)$ إن كانت أولية في $Z[x]$ أم لا. ؟ لأجل ذلك لابد من البحث عن عدد أولي آخر.

نلاحظ أنه من أجل $p = 5$ فإن $21 \bmod -5 = 1$ وأن $8 \bmod -5 = 3$ كما أن:

$$2 \bmod -5 = -3 \bmod -5 = 2$$

ومنه تكون $\overline{f(x)} = \partial f(x) = 3$ وأن $\overline{f(x)} = x^3 + 2x^2 + 2x + 3 \in Z_5[x]$ من جهة أخرى، بما أن $Z_5 = \{0,1,2,3,4\}$ حقل وأن $\overline{f(0)} = \overline{f(1)} = \overline{f(2)} = 3$ كما أن $\overline{f(3)} = 4$, $\overline{f(4)} = 2$ نجد أن الحدودية $\overline{f(x)}$ لا تملك أصفاراً في الحقل Z_5 ، وبما أن $\partial \overline{f(x)} = 3$ فإنه حسب التمهيدية (١-٢-٥) تكون الحدودية $\overline{f(x)}$ أولية فوق Z_5 وحسب المبرهنة (٢-١-٦) تكون الحدودية $f(x)$ أولية في $Q[x]$ وبالتالي أولية في $Z[x]$. ♦

٣ - أثبت أن الحدودية $f(x) = 3/7x^4 - 2/7x^2 + 9/35x + 3/5 \in Q[x]$ أولية في $Q[x]$.

لنأخذ الحدودية $h(x) = 35 \cdot f(x) = 15x^4 - 10x^2 + 9x + 21 \in Z[x]$

نلاحظ أنه من أجل العدد الأولي $p = 2$ أن $-10 \bmod -2 = 0$ وأن:

$$15 \bmod -2 = 9 \bmod -2 = 21 \bmod -2 = 1$$

ومنه تكون $\overline{h(x)} = \partial h(x) = 4$ وأن $\overline{h(x)} = x^4 + x + 1 \in Z_2[x]$

من جهة أخرى، بما أن $Z_2 = \{0,1\}$ حقل وأن $\overline{h(1)} = \overline{h(0)} = 1$ نجد أن الحدودية

$\overline{h(x)}$ لا تملك أصفاراً في الحقل Z_2 . لنفرض جدلاً أن الحدودية $\overline{h(x)}$ غير أولية في

$Z_2[x]$. عندئذ توجد $g(x), \varphi(x) \in Z_2[x]$ بحيث $\overline{h(x)} = g(x) \cdot \varphi(x)$ وأن

$\partial \overline{h(x)} = 4$ وبما أن $\partial g(x) > 0, \partial \varphi(x) > 0$ سوف نميز الحالتين:

- الحالة الأولى. $\partial g(x) = 3, \partial \varphi(x) = 1$ عندها نجد أن الحدودية $\varphi(x)$ تملك صفراً

في الحقل Z_2 وبالتالي فإن الحدودية $\overline{h(x)}$ تملك صفراً في الحقل Z_2 وهذا غير ممكن.

- الحالة الثانية. $\partial g(x) = 2, \partial \varphi(x) = 2$ وهنا نجد أن $\varphi(x) = a_2x^2 + a_1x + a_0$

وأن $g(x) = b_2x^2 + b_1x + b_0$ حيث $a_2, a_1, a_0, b_2, b_1, b_0 \in Z_2$ ومنه يكون:

$$\overline{h(x)} = a_2b_2x^4 + (a_2b_1 + a_1b_2)x^3 + (a_2b_0 + a_1b_1 + a_0b_2)x^2 +$$

$$+ (a_1b_0 + a_0b_1)x + a_0b_0$$

وبالتالي يكون

$$- a_2 = b_2 = 1 \text{ أي أن } a_2b_2 = 1$$

$$- a_1 = b_1 = 0 \text{ أي أن } a_2b_1 + a_1b_2 = 0$$

$$- b_0 + a_1b_1 + a_0 = 0 \text{ أي أن } a_2b_0 + a_1b_1 + a_0b_2 = 0$$

$$- a_1b_0 + a_0b_1 = 1$$

$$- a_0 = b_0 = 1 \text{ ومنه يكون } a_0b_0 = 1$$

بالتعويض في المعادلات السابقة نجد أن $a_1b_1 = 0$ وأن $a_1 + b_1 = 1$ و $a_1 + b_1 = 0$

وهذا غير ممكن في الحقل Z_2 . مما سبق نجد أن الحدودية $\overline{h(x)}$ أولية في $Z_2[x]$

وحسب المبرهنة (٦-١-٢) تكون الحدودية $h(x)$ أولية في $Q[x]$ وحسب التمهيدية (١-)

(٦-٢) تكون الحدودية $f(x) = 1/35 \cdot h(x)$ أولية في $Q[x]$.

لنورد الآن اختباراً هاماً آخر للحدوديات الأولية والذي يسمى اختبار إيرنشتاين

1852 - 1823 *Fredinand Eisenstein* وذلك من خلال المبرهنة الآتية:

مبرهنة ٦-١-٢. (اختبار إيرنشتاين 1850).

لتكن $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in Z[x]$. إذا وجد عدد أولي p

يحقق الآتي:

$$١ - p \text{ لا يقسم } a_n$$

$$٢ - p \text{ يقسم } a_{n-1}, a_{n-2}, \dots, a_1, a_0$$

$$٣ - p^2 \text{ لا يقسم } a_0$$

عندئذ تكون الحدودية $f(x)$ أولية فوق Q ، (وبالتالي فوق Z).

البرهان.

لنفرض جلاً أن الحدودية $f(x)$ غير أولية في $Q[x]$ عندئذ تكون الحدودية $f(x)$ غير

أولية في $Z[x]$ عندئذ توجد $g(x), h(x) \in Z[x]$ بحيث $\partial g(x) > 0, \partial h(x) > 0$

تحققان $f(x) = g(x) \cdot h(x)$ ومنه تكون $\partial f(x) < \partial g(x), \partial h(x) < \partial f(x)$.

لنفرض أن:

$$g(x) = b_r x^r + b_{r-1} x^{r-1} + \dots + b_1 x + b_0 : b_i \in \mathbb{Z}, \forall 0 \leq i \leq r$$

$$h(x) = c_s x^s + c_{s-1} x^{s-1} + \dots + c_1 x + c_0 : c_i \in \mathbb{Z}, \forall 0 \leq i \leq s$$

بما أن $f(x) = g(x) \cdot h(x)$ نجد أن $n = r + s$ وأن $a_n = b_r \cdot c_s$ ، $a_0 = b_0 \cdot c_0$. لنفرض أن p يقسم b_0 عندئذ a_0 يقسم p إما p يقسم b_0 أو p يقسم c_0 . لنفرض أن p يقسم b_0 عندئذ p لا يقسم c_0 ، لأنه إذا كان p يقسم c_0 نجد أن p^2 يقسم a_0 وهذا مرفوض فرضاً. كذلك بما أن p لا يقسم a_n فإن p لا يقسم b_r . لنفرض أن أول معاملات $g(x)$ التي لا تقبل القسمة على p هو b_i وبما أن:

$$a_i = b_i c_0 + b_{i-1} c_1 + \dots + b_1 c_{i-1} + b_0 c_i$$

وبما أن p يقسم a_i فرضاً نجد أن p يقسم الطرف الأيمن من المساواة الأخيرة وبالتالي فهو يقسم جميع الحدود في هذه المساواة وبالتالي يكون p قاسماً للحد $b_i c_0$ وبما أن p لا يقسم b_i ينتج أن p يقسم c_0 وهذا غير ممكن فرضاً. مما سبق نجد أن الحدودية $f(x)$ أولية فوق $Q[x]$ ، وبالتالي فوق $\mathbb{Z}[x]$. ◊

لنورد الآن عدداً من الأمثلة كتطبيق على المعيار الأخير.

أمثلة.

١ - أثبت أن الحدودية $f(x) = x^6 + 9x^4 + 12x^2 + 6 \in \mathbb{Z}[x]$ أولية في $\mathbb{Z}[x]$.

نلاحظ أنه من أجل $p = 3$ فإن p لا يقسم $a_6 = 1$ وأن p يقسم كلاً من

$$a_4 = 9, a_2 = 12, a_0 = 6$$

كما أن $p^2 = 9$ لا يقسم $a_0 = 6$ وحسب معيار إيرنشتاين تكون الحدودية $f(x)$ أولية فوق $Q[x]$ ، وبالتالي فوق $\mathbb{Z}[x]$. ◊

٢ - أثبت أن الحدودية $\varphi(x) = x^4 + 3x^2 + 3$ أولية في $Q[x]$.

نلاحظ أنه من أجل $p = 3$ فإن p لا يقسم $a_4 = 1$ وأن p يقسم كلاً من

$$a_2 = 3, a_0 = 3$$

كما أن $p^2 = 9$ لا يقسم $a_0 = 3$ وحسب معيار إيرنشتاين تكون الحدودية $\varphi(x)$ أولية فوق $Q[x]$ ، وبالتالي فوق $\mathbb{Z}[x]$. ◊

٣ - أثبت أن الحدودية $\psi(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$ أولية في $Q[x]$.

نلاحظ أنه من أجل $p = 5$ فإن p لا يقسم $a_5 = 3$ وأن p يقسم كلاً من:

$$a_4 = 15, a_3 = -20, a_1 = 10, a_0 = 20$$

كما أن $p^2 = 25$ لا يقسم $a_0 = 20$ وحسب معيار إيزنشتاين تكون الحدودية $\psi(x)$ أولية فوق $Q[x]$ ، وبالتالي فوق $Z[x]$. ♦

تعريف.

ليكن p عدداً أولياً. نسمي الحدودية:

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

الحدودية الدوارة من المرتبة p .

مبرهنة ٢-١-٨.

ليكن p عدداً أولياً. الحدودية الدوارة من المرتبة p هي حدودية أولية فوق Q ، وبالتالي فوق Z .

البرهان.

حسب التعريف فإن الحدودية الدوارة من المرتبة p هي:

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

لنضع

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

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

$$= x^{p-1} + px^{p-2} + px^{p-3} + \dots + px + p$$

عندئذ حسب معيار إيزنشتاين، نجد أنه من أجل العدد الأولي p فإن p لا يقسم $a_{p-1} = 1$ وأن p يقسم كلاً من:

$$a_{p-2} = a_{p-3} = \dots = a_1 = a_0 = p$$

كما أن p^2 لا يقسم $a_0 = p$ وحسب معيار إيزنشتاين تكون الحدودية $f(x)$ أولية فوق Q وبالتالي تكون الحدودية $\Phi_p(x+1)$ أولية فوق Q وحسب التمهيدية (١-٢-٦) تكون الحدودية $\Phi_p(x)$ أولية فوق Q (وبالتالي فوق Z). ◊

وجدنا من خلال دراستنا السابقة، أن حلقة الحدوديات على أي حقل هي حلقة تحليل وحيد. الخطوة الآتية من دراستنا تتضمن إثبات أن حلقة الحدوديات $Z[x]$ هي حلقة تحليل وحيد. والبدائية ستكون مع المبرهنة الآتية:

مبرهنة ١-٢-٩.

كل حدودية رئيسية في $Z[x]$ ودرجتها أكبر من الصفر تكتب على شكل جداء منته لحدوديات أولية في $Z[x]$ درجة كل منها أكبر من الصفر.

البرهان.

لتكن $f(x) \in Z[x]$ حدودية رئيسية وأن $\partial f(x) > 0$. سوف نورد البرهان بالاستقراء حسب درجة $f(x)$.

- لنفرض أن $\partial f(x) = 1$. بما أن $f(x) \neq \pm 1$ فإنه حسب التمهيدية (١-٢-١) تكون الحدودية $f(x)$ غير قابلة للقلب في $Z[x]$.

لتكن $g(x), h(x) \in Z[x]$ بحيث $f(x) = g(x) \cdot h(x)$ وبما أن $\partial f(x) = 1$ فإنه إما $\partial g(x) = 0$ أو $\partial h(x) = 0$.

- إذا كانت $\partial g(x) = 0$ عندئذ $g(x) = a$ حيث $a \in Z$ و $a \neq 0$ وأن $\partial h(x) = 1$. بفرض أن b هو رئيس الحدودية $h(x)$ عندئذ تكون $h(x) = b \cdot h_1(x)$ حيث $h_1(x)$ حدودية رئيسية في $Z[x]$ ، ومنه $f(x) = a \cdot b \cdot h_1(x)$ وبما أن الحدودية $f(x)$ رئيسية نجد أن $a \cdot b = 1$ ومنه يكون $a = b = 1$ وهذا بين لنا حسب التمهيدية (١-٢-١) أن الحدودية $g(x)$ قابلة للقلب في $Z[x]$.

- بشكل مشابه نجد أنه إذا كانت $\partial h(x) = 0$ فإن الحدودية $h(x)$ تكون قابلة للقلب في $Z[x]$. مما سبق نجد أن الحدودية $f(x)$ أولية في $Z[x]$.

- لنفرض الآن أن المبرهنة صحيحة لأجل كل حدودية رئيسية في $Z[x]$ ودرجتها أصغر من درجة $f(x)$. بما أن $\partial f(x) > 0$ عندئذ الحدودية $f(x)$ غير قابلة للقلب في $Z[x]$.

إذا كانت الحدودية $f(x)$ أولية في $Z[x]$ عندها يتم المطلوب.

لنفرض أن الحدودية $f(x)$ غير أولية في $Z[x]$ عندئذ يوجد $p(x), h(x) \in Z[x]$ بحيث $f(x) = p(x) \cdot h(x)$ وأن $\partial p(x) > 0, \partial h(x) > 0$. لنفرض أن b_1 هو رئيس الحدودية $h(x)$ وأن b_2 هو رئيس الحدودية $p(x)$ عندئذ يكون $h(x) = b_1 \cdot h_1(x)$ وأن $p(x) = b_2 \cdot p_1(x)$ حيث $h_1(x), p_1(x) \in Z[x]$ وأن كلاهما حدودية رئيسية ومنه يكون $f(x) = b_1 \cdot b_2 \cdot h_1(x) \cdot p_1(x)$ وبما أن الحدودية $f(x)$ رئيسية نجد أن $b_1 = b_2 = 1$ وبالتالي يكون $h(x) = h_1(x)$ و $p(x) = p_1(x)$ وهذا يبين لنا أن كلا من $p(x), h(x)$ هي حدوديات رئيسية ودرجة كل منهما أكبر من الصفر وأصغر من درجة $f(x)$ وحسب الفرض الاستقرائي فإن كلا من الحدوديتين $p(x), h(x)$ تكتب على شكل جداء لحدوديات أولية في $Z[x]$ ودرجة كل منهما أكبر من الصفر، وهكذا نجد أن الحدودية $f(x)$ تكتب على شكل جداء لحدوديات أولية في $Z[x]$ ودرجة كل منها أكبر من الصفر. ♦

لنورد الآن نص المبرهنة الأساسية في الحساب:

مبرهنة ١-٢-١٠.

كل عدد صحيح أكبر من الواحد هو إما عدد أولي أو هو جداء منته لأعداد أولية وهذا الجداء وحيد، بمعنى أنه إذا كان $n > 1$ عدداً صحيحاً وكان

$$n = q_1 \cdot q_2 \cdots q_t = p_1 \cdot p_2 \cdots p_r$$

حيث q_i, p_j أعداد أولية أيّاً كان $1 \leq i \leq t, 1 \leq j \leq r$ فإن $t = r$ وبعد إجراء تبديل على الأدلة يكون $q_i = p_i$ أيّاً كان $1 \leq i \leq t$.

البرهان.

لأجل البرهان يمكن العودة إلى كتاب البنى الجبرية (١). ♦

نأتي الآن لإثبات أن حلقة الحدوديات $Z[x]$ هي حلقة تحليل وحيد.

مبرهنة ١-٢-١١.

كل حدودية في $Z[x]$ مغايرة للصفر وغير قابلة للقلب في $Z[x]$ يمكن كتابتها على الشكل

$$b_1 \cdot b_2 \cdots b_s \cdot p_1(x) \cdot p_2(x) \cdots p_m(x)$$

حيث b_i حدوديات أولية درجتها تساوي الصفر وأن $p_j(x)$ حدوديات أولية درجتها أكبر من الصفر وذلك أياً كان $1 \leq i \leq s, 1 \leq j \leq m$. إضافة لذلك، إذا كان:

$$\begin{aligned} b_1 \cdot b_2 \cdots b_s \cdot p_1(x) \cdot p_2(x) \cdots p_m(x) &= \\ = c_1 \cdot c_2 \cdots c_t \cdot q_1(x) \cdot q_2(x) \cdots q_n(x) \end{aligned}$$

حيث c_i حدوديات أولية درجتها تساوي الصفر وأن $q_j(x)$ حدوديات أولية درجتها أكبر من الصفر وذلك أياً كان $1 \leq i \leq n, 1 \leq j \leq t$ فإن $1 \leq i \leq n, 1 \leq j \leq t$. وبعد إعادة الترتيب يكون $b_i = \pm c_i$ و $p_i(x) = q_i(x)$ أياً كان $1 \leq i \leq n$.

البرهان.

لتكن $f(x) \in Z[x]$ حدودية مغايرة للصفر وغير قابلة للقلب في $Z[x]$. نميز حالتين:

- إذا كانت $\partial f(x) = 0$ عندئذ $f(x) = a$ حيث $a \in Z, a \neq 0$ وحسب المبرهنة (٢-١٠) يتم المطلوب.

- إذا كانت $\partial f(x) > 0$ ، لنفرض أن b رئيس الحدودية $f(x)$ عندئذ $f(x) = b \cdot f_1(x)$ حيث $f_1(x) \in Z[x]$ حدودية رئيسية وأن $\partial f_1(x) > 0$ وحسب المبرهنة (٢-١٠-٩) نجد

$$f_1(x) = p_1(x) \cdot p_2(x) \cdots p_m(x)$$

حيث $p_j(x)$ حدوديات أولية في $Z[x]$ درجتها أكبر من الصفر وذلك لأجل جميع قيم $1 \leq j \leq m$ ، وحسب المبرهنة (٢-١٠-٩) نجد أن $b = b_1 \cdot b_2 \cdots b_s$ حيث $b_i \in Z$ حدوديات أولية درجة كل منها تساوي الصفر وذلك لأجل جميع القيم $1 \leq i \leq s$ ، ومنه:

$$f(x) = b_1 \cdot b_2 \cdots b_s \cdot p_1(x) \cdot p_2(x) \cdots p_m(x)$$

الوحدانية. لنفرض أن:

$$\begin{aligned} f(x) &= b_1 \cdot b_2 \cdots b_s \cdot p_1(x) \cdot p_2(x) \cdots p_m(x) = \\ &= c_1 \cdot c_2 \cdots c_t \cdot q_1(x) \cdot q_2(x) \cdots q_n(x) \end{aligned}$$

حيث b_i, c_i حدوديات أولية درجتها تساوي الصفر وأن $p_i(x), q_j(x)$ حدوديات أولية درجتها أكبر من الصفر. لنفرض أن $b = b_1 \cdot b_2 \cdots b_s$ وأن $c = c_1 \cdot c_2 \cdots c_t$ بما أن الحدوديات $p_i(x), q_j(x)$ حدوديات أولية درجتها أكبر من الصفر فإنه حسب

التمهيدية (٢-١-٢) فإن كلاً من $p_i(x), q_j(x)$ هي حدوديات رئيسية وحسب نتيجة المبرهنة (٣-١-٢) فإن كلاً من:

$$p_1(x) \cdot p_2(x) \cdots p_m(x), \quad q_1(x) \cdot q_2(x) \cdots q_n(x)$$

هو حدودية رئيسية. وهذا يؤدي بدوره إلى أن:

$$b_1 \cdot b_2 \cdots b_s = c_1 \cdot c_2 \cdots c_t$$

وحسب المبرهنة (١٠-١-٢) نجد أن $s = t$ وأن $b_i = \pm c_i$ وذلك أيّاً كان $1 \leq i \leq s$ وبما أن الحلقة Z منطقة تكاملية نجد أن:

$$p_1(x) \cdot p_2(x) \cdots p_m(x) = \pm q_1(x) \cdot q_2(x) \cdots q_n(x)$$

بالنظر إلى الحدوديات $p_i(x), q_j(x)$ على أنها عناصر من $Q[x]$ وبملاحظة أن $p_1(x)$ تقسم الجداء $q_1(x) \cdot q_2(x) \cdots q_n(x)$ فإنه حسب المبرهنة (١٠-٢-١) نجد أن الحدودية $p_1(x)$ تقسم إحدى الحدوديات $q_j(x)$.

لنفرض أن الحدودية $p_1(x)$ تقسم الحدودية $q_i(x)$ ، نعيد ترقيم الحدوديات $q_j(x)$ بحيث تكون $p_1(x)$ تقسم $q_1(x)$ ، وبما أن الحدودية $q_1(x)$ أولية في $Q[x]$ وذلك حسب المبرهنة (٥-١-٢) نجد أن $q_1(x) = \alpha/\beta \cdot p_1(x)$ حيث $\alpha, \beta \in Z$ وأن $\beta \neq 0$ وبما أن كلاً من الحدوديتين $p_i(x), q_j(x)$ رئيسية نجد أن $\alpha/\beta = \pm 1$ ومنه يكون $q_1(x) = \pm p_1(x)$ وبما أن الحلقة $Z[x]$ منطقة تكاملية نجد أن:

$$p_2(x) \cdots p_m(x) = \pm q_2(x) \cdots q_n(x)$$

لنكرر العملية السابقة لأجل الحدودية $p_2(x)$ ثم $p_3(x)$ وهكذا.

- إذا كان $m < n$ عندئذ بعد m من الخطوات نجد أن:

$$1 = \pm q_{m+1}(x) \cdot q_{m+2}(x) \cdots q_n(x)$$

وهذا غير ممكن.

- - إذا كان $m > n$ عندئذ بعد n من الخطوات نجد أن:

$$p_{n+1}(x) \cdot p_{n+2}(x) \cdots p_m(x) = \pm 1$$

وهذا أيضاً غير ممكن. مما سبق نجد أن $p_i(x) = \pm q_i(x)$ وذلك لأجل جميع القيم

$$1 \leq i \leq n$$

لنورد الآن مثلاً نبين من خلاله أن حلقة الحدوديات $Z[x]$ ليست حلقة مثاليات رئيسية:

مثال.

الحلقة $Z[x]$ ليست حلقة مثاليات رئيسية.

البرهان.

لنأخذ المجموعة $I = \{f(x) : f(x) \in Z[x], f(0) = 0 \bmod -2\}$. إن المجموعة

I تشكل مثالياً في $Z[x]$ ، انظر التمرين المحلول (٢-٤). لنبرهن على أنه لا يوجد في

$Z[x]$ عنصر $h(x)$ يحقق $I = \langle h(x) \rangle$.

لنفرض جدلاً أن $I = \langle h(x) \rangle$ حيث $h(x) \in Z[x]$. بما أن $2 \in I$ فإنه يوجد $f(x)$

عنصر في $Z[x]$ بحيث $2 = f(x) \cdot h(x)$ ومنه فإن:

$$\partial(f(x) \cdot h(x)) = \partial f(x) + \partial h(x) = \partial 2 = 0$$

وبالتالي يكون $\partial h(x) = 0$ أي أن $h(x) = a$ حيث $a \in Z$ و $a \neq 0$. لنوجد قيمة العنصر

a . بما أن $2 = f(1) \cdot h(1)$ فإنه إما $h(1) = \pm 1$ أو $h(1) = \pm 2$.

بما أن $1 \notin I$ نجد أن $h(1) = \pm 2$.

من جهة أخرى، بما أن $x \in I$ فإنه يوجد $g(x) \in Z[x]$ بحيث $x = g(x) \cdot h(x)$ ومنه

نجد أن $x = \pm 2 \cdot h(x)$ وهذا غير ممكن.

مما سبق نجد أنه لا توجد $h(x) \in Z[x]$ بحيث $I = \langle h(x) \rangle$ ، وهذا يبين لنا أن المثالي

I ليس رئيسياً وبالتالي الحلقة $Z[x]$ ليست حلقة مثاليات رئيسية. ◊

بالاعتماد على المثال الأخير يمكننا صياغة النتيجة الآتية:

نتيجة.

إذا كانت D حلقة مثاليات رئيسية فإن $D[x]$ ليست بالضرورة حلقة مثاليات رئيسية.

تمارين محلولة (٢)

١ - أثبت أن المثالي $A = \langle x \rangle$ هو مثالي أولي في الحلقة $Z[x]$ وليس أعظمية.

الحل.

نلاحظ أولاً أن $A = \langle x \rangle = x \cdot Z[x]$ بمعنى آخر، أيًا كان $f(x) \in A$ فإنه إما $f(x) = 0$ أو $\partial f(x) > 0$. كما أن $A \neq Z[x]$ ، لأنه أيًا كان $0 \neq a \in Z$ فإن $a \in Z[x]$ وأن $\partial a = 0$ وبالتالي $a \notin A$. لنعرف العلاقة $\varphi: Z \rightarrow Z[x]/A$ بالشكل الآتي أيًا كان $a \in Z$ فإن $\varphi(a) = a + A$ فنجد أن φ تشاكل حلقي، لأنه أيًا كان $a, b \in Z$

$$\varphi(a+b) = (a+b) + A = (a+A) + (b+A) = \varphi(a) + \varphi(b)$$

$$\varphi(a \cdot b) = (a \cdot b) + A = (a+A) \cdot (b+A) = \varphi(a) \cdot \varphi(b)$$

كما أن التطبيق φ متباين، لأنه إذا كان $c, d \in Z$ بحيث $\varphi(c) = \varphi(d)$ فإن $c + A = d + A$ وبالتالي يكون $c - d \in A$ ومنه يكون $c - d = x \cdot f(x)$ حيث $f(x) \in Z[x]$.

لنفرض أن $f(x) = \sum_{i=0}^n d_i x^i$ حيث $d_i \in Z$ فنجد أن:

$$c - d = d_n x^{n+1} + d_{n-1} x^n + \dots + d_1 x^2 + d_0 x$$

ومنه يكون $d_n = d_{n-1} = \dots = d_1 = d_0 = 0$ أي أن $c - d = 0$ وبالتالي $c = d$ وهذا يبين أن التطبيق φ متباين.

كما أن التطبيق φ غامر، لأنه إذا كان $\overline{\lambda(x)} \in Z[x]/A$ فإن $\overline{\lambda(x)} = \lambda(x) + A$

حيث $\lambda(x) \in Z[x]$. لنفرض أن $\lambda(x) = \sum_{i=0}^m c_i x^i$ حيث $c_i \in Z$ ، عندئذ:

$$\begin{aligned} \lambda(x) &= c_m x^m + c_{m-1} x^{m-1} + \dots + c_1 x + c_0 = \\ &= x(c_m x^{m-1} + c_{m-1} x^{m-2} + \dots + c_2 x + c_1) + c_0 \end{aligned}$$

لنفرض أن:

$$\mu(x) = c_m x^{m-1} + c_{m-1} x^{m-2} + \dots + c_2 x + c_1$$

فنجـد أن $\mu(x) \in Z[x]$ وأن $\lambda(x) = x \cdot \mu(x) + c_0$ ومنه يكون:

$$\begin{aligned}\overline{\lambda(x)} &= \lambda(x) + A = (x \cdot \mu(x) + c_0) + A = \\ &= (x \cdot \mu(x) + A) + (c_0 + A) = c_0 + A\end{aligned}$$

وبما أن $c_0 \in Z$ نجد أن $c_0 + A = \overline{\lambda(x)}$ ، وهذا يبين أن التطبيق φ غامر. مما سبق نجد أن φ تماثل. بما أن الحلقة Z منطقة تكاملية نجد أن الحلقة $Z[x]/A$ منطقة تكاملية ومنه يكون المثالي A أولياً في الحلقة $Z[x]$.

لنفرض جـدلاً أن المثالي A أعظمي في الحلقة $Z[x]$ عندئذ تكون الحلقة $Z[x]/A$ حقلاً. وبما أن $Z[x]/A \cong Z$ نجد أن Z حقل وهذا غير صحيح، مما سبق نجد أن المثالي A ليس أعظمياً في الحلقة $Z[x]$.

٢ - لتكن $Q[x]$ حلقة الحدوديات فوق الحقل Q أثبت أن المثالي $B = \langle x \rangle$ مثالي أعظمي في الحلقة $Q[x]$.

الحل.

نعلم أن $B = \langle x \rangle = x \cdot Q[x]$ بمعنى آخر، أياً كان $g(x) \in B$ فإنه إما $g(x) = 0$ أو $\partial g(x) > 0$. كما أن $B \neq Q[x]$ ، لأنه أياً كان $b \in Q$ فإن $b \notin B$ وبالتالي $\partial b = 0$.

لنعرف العلاقة $\varphi: Q \rightarrow Q[x]/B$ بالشكل الآتي أياً كان $b \in Q$ فإن $\varphi(b) = b + B$ فنجد أن φ تشاكل حلقي، لأنه أياً كان $a, b \in Q$ فإن:

$$\varphi(a + b) = (a + b) + B = (a + B) + (b + B) = \varphi(a) + \varphi(b)$$

$$\varphi(a \cdot b) = (a \cdot b) + B = (a + B) \cdot (b + B) = \varphi(a) \cdot \varphi(b)$$

كما أن التطبيق φ متباين، لأنه إذا كان $c, d \in Q$ بحيث $\varphi(c) = \varphi(d)$ فإن $c + B = d + B$ وبالتالي يكون $c - d \in B$ ومنه يكون $c - d = x \cdot q(x)$ حيث

$$q(x) \in Q[x]. \text{ لنفرض أن } q(x) = \sum_{i=0}^n d_i x^i \text{ حيث } d_i \in Q \text{ فنجد أن:}$$

$$c - d = d_n x^{n+1} + d_{n-1} x^n + \dots + d_1 x^2 + d_0 x$$

ومنـه يكون $d_n = d_{n-1} = \dots = d_1 = d_0 = 0$ أي أن $c - d = 0$ وبالتالي $c = d$ وهذا

يبين أن التطبيق φ متباين.

كما أن التطبيق φ غامر، لأنه إذا كان $\overline{\lambda(x)} \in Q[x]/B$ فإن $\overline{\lambda(x)} = \lambda(x) + B$

حيث $\lambda(x) \in Q[x]$. لنفرض أن $\lambda(x) = \sum_{i=0}^m c_i x^i$ حيث $c_i \in Q$ ، عندئذ:

$$\begin{aligned}\lambda(x) &= c_m x^m + c_{m-1} x^{m-1} + \cdots + c_1 x + c_0 = \\ &= x(c_m x^{m-1} + c_{m-1} x^{m-2} + \cdots + c_2 x + c_1) + c_0\end{aligned}$$

لنفرض أن:

$$\mu(x) = c_m x^{m-1} + c_{m-1} x^{m-2} + \cdots + c_2 x + c_1$$

ف نجد أن $\mu(x) \in Q[x]$ وأن $\lambda(x) = x \cdot \mu(x) + c_0$ ومنه يكون:

$$\begin{aligned}\overline{\lambda(x)} &= \lambda(x) + B = (x \cdot \mu(x) + c_0) + B = \\ &= (x \cdot \mu(x) + B) + (c_0 + B) = c_0 + B\end{aligned}$$

وبما أن $c_i \in Q$ نجد أن $\overline{\lambda(x)} = c_0 + B = \varphi(c_0)$ ، وهذا يبين أن التطبيق φ غامر. مما سبق نجد أن φ تماثل. بما أن Q حقل ينتج أن الحلقة $Q[x]/B$ حقل وبالتالي يكون المثالي B أعظمية في الحلقة $Q[x]$.

٣ - أثبت أنه لا توجد حدوديات $f(x)$ في $Z[x]$ تحقق $\partial f(x) > 0$ وأن $f(x)$ قابلة للقلب في $Z[x]$.

الحل.

لنفرض جلاً أنه توجد $f(x) \in Z[x]$ تحقق أن $\partial f(x) > 0$ وأن $f(x)$ قابلة للقلب في $Z[x]$ ، عندئذ توجد $h(x) \in Z[x]$ وأن $h(x) \neq 0$ و $f(x) \cdot h(x) = 1$ وبما أن Z منطقة تكاملية فإنه حسب المبرهنة (١-١-٤) تكون $Z[x]$ منطقة تكاملية ومنه نجد أن:

$$\partial f(x) + \partial h(x) = 0$$

وبالتالي يكون $\partial f(x) = \partial h(x) = 0$ وهذا يناقض الفرض، إذاً لا توجد في $Z[x]$ حدوديات $f(x)$ تحقق $\partial f(x) > 0$ وأن $f(x)$ قابلة للقلب في $Z[x]$.

٤ - لتكن $Z[x]$ حلقة الحدوديات فوق الحقل Z ولتكن:

$$K = \{f(x) : f(x) \in Z[x], f(0) = 0 \text{ mod } -2\}$$

والمطلوب:

١ - أثبت أن المجموعة K تشكل مثاليًا في $Z[x]$.

٢ - أثبت أن المثالي K أولي في $Z[x]$.

الحل.

١ - نلاحظ أن المجموعة K غير خالية لأن $0 \in K$. ليكن $f(x), g(x) \in K$ عندئذ كل من $f(0), g(0)$ هي أعداد زوجية، وبما أن فرق عددين زوجيين هو عدد زوجي نجد أن:

$$(f - g)(0) = f(0) - g(0) = 0 \mod -2$$

ومنه $f(x) - g(x) \in K$

ليكن $\varphi(x) \in K$ عندئذ أيًا كان $\mu(x) \in Z[x]$ فإن:

$$(\mu \cdot \varphi)(0) = \mu(0) \cdot \varphi(0) = 0 \mod -2$$

وذلك لأن جداء عددين أحدهما زوجي يكون الناتج عددًا زوجيًا وهذا يبين لنا أن:

$$\mu(x) \cdot \varphi(x) \in K$$

مما سبق نجد أن المجموعة K تشكل مثاليًا في $Z[x]$.

٢ - نلاحظ على سبيل المثال أن $f(x) = x + 1 \in Z[x]$ وأن $f(0) = 1 \neq 0 \mod -2$

أي أن $f(x) \notin K$ وهذا يبين لنا أن $K \neq Z[x]$.

ليكن $f(x), g(x) \in Z[x]$ بحيث $f(x) \cdot g(x) \in K$ عندئذ يكون:

$$(f \cdot g)(0) = f(0) \cdot g(0) = 0 \mod -2$$

ومنه فإن الجداء $f(0) \cdot g(0)$ هو عدد زوجي وبالتالي فإن أحد العددين $f(0)$ أو $g(0)$

على الأقل هو عدد زوجي، وهذا يبين أنه إما $f(0) = 0 \mod -2$ أو أن

$g(0) = 0 \mod -2$ وبالتالي إما $f(x) \in K$ أو أن $g(x) \in K$. مما سبق نجد أن

المثالي K أولي في $Z[x]$.

٥ - لنكن $Z[x]$ حلقة الحدوديات فوق الحقل Z ولنأخذ المجموعة:

$$I = \{f(x) : f(x) \in Z[x], f(0) = 0\}$$

والمطلوب:

١ - أثبت أن المجموعة I تشكل مثاليًا في $Z[x]$.

٢ - أثبت أن المثالي I أولي في $Z[x]$.

٣ - أثبت أن المثالي I ليس أعظمياً في $Z[x]$.

الحل.

١ - نتركه كتمرين للقارئ.

٢ - بما أن $f(x) = x+1 \in Z[x]$ وأن $f(0) = 1 \neq 0$ نجد أن $f(x) \notin I$ وهذا يبين لنا أن $I \neq Z[x]$.

ليكن $h(x), g(x) \in Z[x]$ بحيث $h(x) \cdot g(x) \in I$ عندئذ يكون $f(0) \cdot g(0) = 0$.

لنفرض أن $h(x) = \sum_{i=0}^m b_i x^i$, $g(x) = \sum_{i=0}^n a_i x^i$ حيث $a_i, b_i \in Z$ ولنفرض أن:

$$g(x) \cdot h(x) = \sum_{k=0}^{n+m} c_k x^k$$

حيث $c_k = \sum_{i+j=k} a_i b_j$. بما أن $f(0) \cdot g(0) = 0$ نجد أن $c_0 = 0$ وذلك لأجل جميع القيم

$0 \leq k \leq n+m$ ومنه يكون $c_0 = a_0 b_0 = 0$ وبما أن $a_0, b_0 \in Z$ وأن Z منطقة تكاملية نجد أنه إما $a_0 = 0$ أو $b_0 = 0$.

- إذا كان $a_0 = 0$ عندئذ يكون $g(x) = \sum_{i=1}^n a_i x^i$ ومنه فإن $g(0) = 0$ وبالتالي يكون $g(x) \in I$.

- إذا كان $b_0 = 0$ عندئذ يكون $h(x) = \sum_{i=1}^m b_i x^i$ ومنه فإن $h(0) = 0$ وبالتالي يكون $h(x) \in I$. مما سبق نجد أن المثالي I أولي في $Z[x]$.

٣ - لنفرض جـدلاً أن المثالي I أعظمي في $Z[x]$ ، عندئذ تكون الحلقة $Z[x]/I$ حقلاً.

لنعرف التطبيق $\varphi: Z[x] \rightarrow Z$ بالشكل الآتي: أيّاً كان $h(x) = \sum_{i=1}^n d_i x^i \in Z[x]$ فإن

$\varphi(h(x)) = d_0$ فنجد أن التطبيق φ تشاكل حلقي، لأنه إذا كان $f(x), g(x) \in Z[x]$

بحيث:

$$f(x) = \sum_{i=0}^n a_i x^i, g(x) = \sum_{i=0}^m b_i x^i$$

حيث $a_i, b_i \in Z$ لأجل جميع قيم i, j ، عندئذ:

$$\begin{aligned}\varphi(f(x) + g(x)) &= \varphi\left(\sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i\right) = \varphi\left(\sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i\right) = \\ &= a_0 + b_0 = \varphi(f(x)) + \varphi(g(x))\end{aligned}$$

لنفرض أن $f(x) \cdot g(x) = \sum_{k=0}^{n+m} c_k x^k$ حيث $c_k = \sum_{i+j=k} a_i b_j$ عندئذ يكون:

$$\varphi(f(x) \cdot g(x)) = \varphi\left(\sum_{k=0}^{n+m} c_k x^k\right) = c_0 = a_0 \cdot b_0 = \varphi(f(x)) \cdot \varphi(g(x))$$

مما سبق نجد أن التطبيق φ تشاكل حلقي، وهو أيضاً غامر، لأنه أياً كان $d \in Z$ فإن $x + d \in Z[x]$ ويحقق $\varphi(x + d) = d$ وحسب نظرية التماثل الأولى نجد أن $Z[x]/Ker \varphi \cong Z$. لنبرهن الآن على أن $Ker \varphi = I$.

ليكن $\lambda(x) \in Ker \varphi$ عندئذ $\lambda(x) \in Z[x]$ ، بفرض أن $\lambda(x) = \sum_{i=0}^s c_i x^i$ حيث $c_i \in Z$ عندئذ يكون $\varphi(\lambda(x)) = c_0$ وأن $\varphi(\lambda(x)) = 0$ ومنه نجد أن $c_0 = 0$ وبالتالي يكون $\lambda(x) = \sum_{i=1}^s c_i x^i$ وهذا يبين لنا أن $\lambda(0) = 0$ وبالتالي فإن $\lambda(x) \in I$. ومنه نجد أن $Ker \varphi \subseteq I$. ليكن $\mu(x) \in I$ عندئذ يكون $\mu(x) \in Z[x]$ وأن $\mu(0) = 0$ وهذا يبين لنا أن $\mu(x) = \sum_{i=1}^t r_i x^i$ ومنه يكون $\varphi(\mu(x)) = r_0 = 0$ ومنه أن $\mu(x) \in Ker \varphi$ أي $\mu(x) \in Ker \varphi \subseteq I$. مما سبق نجد أن $Ker \varphi = I$. وهكذا نجد أن $Z[x]/I \cong Z$ وبما أن $Z[x]/I$ حقل نجد أن Z حقل وهذا غير صحيح. ومنه فإن المثالي I ليس أعظمية في $Z[x]$. $\diamond$

٦ - ليكن $m \geq 1$ عدداً صحيحاً ولنفرض أنه أياً كان $a \in Z$ فإن $\bar{a} = a \bmod m$. أثبت أن التطبيق $\varphi: Z[x] \rightarrow Z_m[x]$ المعرف بالشكل الآتي:

أياً كان $\sum_{i=0}^n a_i x^i \in Z[x]$ فإن:

$$\varphi\left(\sum_{i=0}^n a_i x^i\right) = \sum_{i=0}^n \bar{a}_i x^i$$

هو تشاكل حلقي غامر.

الحل.

ليكن $\sum_{i=0}^n a_i x^i, \sum_{i=0}^m b_i x^i \in Z[x]$ حيث $a_i, b_j \in Z$ لأجل جميع قيم i, j . عندئذ يكون:

$$\begin{aligned} \varphi\left(\sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i\right) &= \varphi\left(\sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i\right) = \sum_{i=0}^{\max\{n,m\}} \overline{(a_i + b_i)} x^i = \\ &= \sum_{i=0}^{\max\{n,m\}} \overline{(a_i + b_i)} x^i = \sum_{i=0}^{\max\{n,m\}} (\overline{a_i} + \overline{b_i}) x^i = \sum_{i=0}^n \overline{a_i} x^i + \sum_{i=0}^m \overline{b_i} x^i = \\ &= \varphi\left(\sum_{i=0}^n a_i x^i\right) + \varphi\left(\sum_{i=0}^m b_i x^i\right) \end{aligned}$$

$$\varphi\left[\left(\sum_{i=0}^n a_i x^i\right) \cdot \left(\sum_{i=0}^m b_i x^i\right)\right] = \varphi\left(\sum_{k=0}^{n+m} c_k x^k\right) = \sum_{k=0}^{n+m} \overline{c_k} x^k$$

وبما أن $c_k = \sum_{i+j=k} a_i \cdot b_j$ فإن:

$$\overline{c_k} = \overline{\sum_{i+j=k} a_i \cdot b_j} = \sum_{i+j=k} \overline{a_i \cdot b_j} = \sum_{i+j=k} \overline{a_i} \cdot \overline{b_j}$$

ومنه نجد أن:

$$\begin{aligned} \varphi\left[\left(\sum_{i=0}^n a_i x^i\right) \cdot \left(\sum_{i=0}^m b_i x^i\right)\right] &= \sum_{k=0}^{n+m} \overline{c_k} x^k = \left(\sum_{k=0}^n \overline{a_i} x^i\right) \cdot \left(\sum_{k=0}^m \overline{b_i} x^i\right) = \\ &= \varphi\left(\sum_{i=0}^n a_i x^i\right) \cdot \varphi\left(\sum_{i=0}^m b_i x^i\right) \end{aligned}$$

وهذا يبين أن φ تشاكل حلقي. لنبرهن على أن التطبيق φ غامر.

ليكن $\sum_{i=0}^t d_i x^i \in Z_m[x]$ عندئذ يكون $d_i \in Z_m$ أيأً كان $0 \leq i \leq t$ ومنه فإن $d_i \in Z$

وبالتالي $\sum_{i=0}^t d_i x^i \in Z[x]$ ، وبما أن $\overline{d_i} = d_i \bmod -m$ أيأً كان $0 \leq i \leq t$ نجد أن:

$$\varphi\left(\sum_{i=0}^t d_i x^i\right) = \sum_{i=0}^t \overline{d_i} x^i = \sum_{i=0}^t d_i x^i$$

مما سبق نجد أن φ تشاكل حلقي غامر. ♦

تمارين (٢)

١ - عين كلاً من $U(Z[x])$ و $U(R[x])$ حيث Z حلقة الأعداد الصحيحة و R حقل الأعداد الحقيقية.

٢ - أوجد الحدودية $f(x) \in Z[x]$ والتي تحقق $f(1/2) = f(-1/3) = 0$.

٣ - أثبت أن الحدودية $f(x) = x^3 + x^2 + x + 1$ ليست أولية فوق الحقل Q .

٤ - بين أيّاً من الحدوديات الآتية أولية فوق الحقل Q :

$$f(x) = x^5 + 9x^4 + 12x^2 + 6$$

$$g(x) = x^4 + x + 1$$

$$h(x) = x^4 + 3x^2 + 3$$

$$q(x) = x^5 + 5x^2 + 1$$

$$\mu(x) = 8x^3 - 6x^2 + 1$$

$$\lambda(x) = 5/2x^5 + 9/2x^4 + 15x^3 + 7/3x^2 + 6x + 3/14$$

٥ - أثبت أن الحدودية $f(x) = x^5 + 2x + 4 \in Z[x]$ أولية فوق Z .

٦ - أوجد كلاً من $q(x), r(x)$ اللتين تحققان $f(x) = q(x) \cdot g(x) + r(x)$ حيث

$$f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2, \quad g(x) = x^2 + 2x - 3$$

في $Z_7[x]$.

٧ - أثبت أن الحدودية $x^4 + 1$ أولية فوق Q وليست أولية فوق حقل الأعداد الحقيقية R .

٨ - لتكن $f(x) = 3x^2 + 4x + 3 \in Z_5[x]$. أثبت أن الحدودية $f(x)$ يمكن كتابتها

على الشكل $(3x + 2)(x + 4)$ وأيضاً على الشكل $(4x + 1)(2x + 3)$.

٩ - أثبت أن الحدودية $f(x) = x^4 + 15x^3 + 7$ أولية فوق Q .

١٠ - ليكن p عدداً أولياً. هل توجد حدوديات $f(x) \in Z_p[x]$ بحيث $\partial f(x) > 0$

تكون قابلة للقلب في $Z_p[x]$ ؟

١١ - لتكن $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in Z[x]$ وأن $d \in Q$. إذا كان

$x - d$ يقسم $f(x)$ في $Z[x]$ ، أثبت أن $d \in Z$.

١٢ - أوجد الحدودية $p(x) \in Q[x]$ والتي لأجلها $\langle p(x) \rangle \cong Q(\sqrt{1+\sqrt{5}})$.

١٣ - أوجد الحدودية $f(x) \in Q[x]$ والتي لأجلها $f(1+\sqrt{2})=0$.

١٤ - أوجد جميع أصفار الحدودية $6x^4 + 17x^3 + 7x^2 + x - 10$ في Q .

١٥ - بين أياً من الحدوديات الآتية:

$$\begin{array}{cc} x^2 - 12 & 8x^3 + 6x^2 - 9x + 24 \\ 4x^{10} - 9x^3 + 24x - 18 & 2x^{10} - 25x^3 + 10x^2 - 30 \end{array}$$

أولية فوق Q .

١٦ - اكتب كل من الحدوديات الآتية على شكل جداء لحدوديات أولية:

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

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

$$- 2x^2 - 3x + 6 \text{ في } Z[x].$$

$$- 2x^2 - 3x + 6 \text{ في } Z_7[x].$$

١٧ - لتكن $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ و $g(x) = x^2 - 2x + 3$ حدوديتين

في الحلقة $Z_5[x]$. أوجد الحدوديتين $q(x), r(x) \in Z_5[x]$ اللتين تحققان أن:

$$f(x) = q(x) \cdot g(x) + r(x).$$

١٨ - أثبت أن حلقة الخارج $\langle x^2 - 5x + 6 \rangle$ تشكل حقلاً.

١٩ - في أي من الحلقات الآتية: $Z[x]$, $Q[x]$, $Z_{11}[x]$ يمكن كتابة الحدودية:

$$4x^2 - 4x + 8$$

على شكل جداء لحدوديات أولية.

٢٠ - أوجد الحدودية $f(x) \in Q[x]$ التي لأجلها $f(\alpha) = 0$ حيث:

$$\alpha = 1 + \sqrt{2}, \alpha = \sqrt{2} + \sqrt{3}, \alpha = \sqrt{1 + \sqrt[3]{2}}$$

الفصل الثالث

تمديد الحقول

من خلال دراستنا السابقة للحلقات يمكننا القول إنه أصبح بمقدورنا التمييز بين نوعين من الحقول، حقول منتهية وحقول غير منتهية. فعلى سبيل المثال، وجدنا أن $Z_3[x]/\langle x^2 + 1 \rangle$ هو حقل منته مرتبته 9 بينما $R[x]/\langle x^2 + 1 \rangle$ هو حقل غير منته لأنه يماثل حقل الأعداد العقدية (المركبة).

في هذا الفصل والفصول القادمة سوف نورد عدداً من المفاهيم والمبرهنات المتعلقة بنظرية الحقول عموماً وبالحقول المنتهية خصوصاً والذي يمثل الجزء الأكثر متعة في الجبر المجرد.

٣ - ١. تمديد الحقول.

تعريف.

نقول عن الحقل E إنه تمديد (ممدد) للحقل F إذا وجد تشاكلاً (حلقياً) متبايناً $\varphi: F \rightarrow E$.

بالاعتماد على التعريف السابق يمكننا صياغة النتيجة الآتية:

نتيجة.

- ١ - يكون الحقل E تمديداً للحقل F إذا كان $F \subseteq E$ ، بمعنى آخر، يكون الحقل E تمديداً للحقل F إذا كان F حقلاً جزئياً من الحقل E .
- ٢ - كل حقل يعد تمديداً لأي حقل جزئي منه.

ملاحظة.

لابد من الإشارة إلى أنه إذا كان الحقل E تمديداً للحقل F فإن العمليات الثنائية المعرفة على F هي ذاتها العمليات الثنائية المعرفة على الحقل E .

أمثلة.

١ - حقل الأعداد الحقيقية R هو تمديد لحقل الأعداد النسبية Q وأيضاً حقل الأعداد المركبة (العقدية) هو تمديد لحقل الأعداد الحقيقية R .

٢ - الحقل $Z_7 = \{0,1,2,3,4,5,6\}$ بالنسبة لعمليتي الجمع والضرب بالمقاس 7 لا يعد تمديداً للحقل $Z_5 = \{0,1,2,3,4\}$ بالنسبة لعمليتي الجمع والضرب بالمقاس 5 ويعود السبب في ذلك لاختلاف العمليات الثنائية المعرفة على الحقلين Z_5 و Z_7 ، على الرغم من أن $Z_5 \subset Z_7$ (احتواء مجموعات).

٣ - لنأخذ المجموعة

$$Q(\sqrt{2}) = \{a + b\sqrt{2} ; a, b \in Q\}$$

أ - إن المجموعة $Q(\sqrt{2})$ تشكل حقلاً بالنسبة لعمليتي الجمع (+) والضرب (·) المعرفتين بالشكل الآتي: أيأ كان $a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2} \in Q(\sqrt{2})$ فإن

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in Q(\sqrt{2})$$

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in Q(\sqrt{2})$$

ب - $Q \subset Q(\sqrt{2})$ لأنه أيأ كان $a \in Q$ فإن $a = a + 0\sqrt{2} \in Q(\sqrt{2})$.

ج - الحقل $Q(\sqrt{2})$ يعد تمديداً للحقل Q .

سوف ندرس الآن نوعاً خاصاً من الحقول الجزئية.

تعريف.

ليكن الحقل E تمديداً للحقل F و $a_1, a_2, \dots, a_n \in E$ ، سوف نرمز لأصغر حقل جزئي في E يحوي كلاً من F والمجموعة $\{a_1, a_2, \dots, a_n\}$ بالرمز $F(a_1, a_2, \dots, a_n)$.
لندرس الآن طبيعة الحقل $F(a_1, a_2, \dots, a_n)$ وذلك من خلال التمهيدية التالية:

تمهيدية ٣-١-١.

ليكن الحقل E تمديداً للحقل F و $a_1, a_2, \dots, a_n \in E$. إن الحقل $F(a_1, a_2, \dots, a_n)$ يساوي إلى تقاطع جميع الحقول الجزئية في E والتي كل منها يحوي الحقل F والمجموعة $\{a_1, a_2, \dots, a_n\}$.

البرهان.

لنفرض أن $\mathfrak{F}$ هي مجموعة كل الحقول الجزئية في الحقل E والتي كل منها يحوي F والمجموعة $\{a_1, a_2, \dots, a_n\}$. إن المجموعة $\mathfrak{F}$ ليست خالية لأن $E \in \mathfrak{F}$. بما أن $F(a_1, a_2, \dots, a_n) \in \mathfrak{F}$ فإن $K \subseteq F(a_1, a_2, \dots, a_n) \subseteq \bigcap_{K \in \mathfrak{F}} K$. من جهة أخرى، حسب التعريف فإن $F(a_1, a_2, \dots, a_n)$ هو أصغر حقل جزئي في E يحوي كلاً من F والمجموعة $\{a_1, a_2, \dots, a_n\}$ عندئذ أياً كان $D \in \mathfrak{F}$ فإن $F(a_1, a_2, \dots, a_n) \subseteq D$ وبالتالي يكون $F(a_1, a_2, \dots, a_n) \subseteq \bigcap_{K \in \mathfrak{F}} K$. نجد أن $F(a_1, a_2, \dots, a_n) = \bigcap_{K \in \mathfrak{F}} K$.

نأتي الآن لدراسة المبرهنة التالية:

مبرهنة ٣-١-٢.

ليكن الحقل E تمديداً للحقل F . عندئذ:

- ١ - أياً كان $a \in F$ فإن $F(a) = F$.
- ٢ - أياً كان $a, b \in E$ فإن $F(a, b) = F(a)(b) = F(b)(a)$.
- ٣ - أياً كان $a, b \in F$ بحيث $a \neq 0$ وكان $d \in E$ فإن $F(d) = F(ad + b)$.

البرهان.

- ١ - لنفرض أن $a \in F$ عندئذ يكون F هو أصغر حقل جزئي في E يحوي كلاً من الحقل F والعنصر a ومنه $F(a) = F$.
- ٢ - ليكن $a, b \in E$. حسب التعريف فإن $F(a)$ هو أصغر حقل جزئي في E يحوي كلاً من F و a ، وأن $F(a, b)$ حقل جزئي في E يحوي كلاً من F و a ومنه نجد أن $F(a) \subseteq F(a, b)$.
- لنضع $K = F(a)$. فنجد أن $K \subseteq F(a, b)$ وأن $b \in F(a, b)$. بما أن $K(b)$ هو أصغر حقل جزئي في E يحوي كلاً من K و b نجد أن $K(b) \subseteq F(a, b)$.
- من جهة أخرى، لدينا $a, b \in K(b) = F(a)(b)$ وأن $F \subseteq K(b)$ ولكون $F(a, b)$ هو أصغر حقل جزئي في E يحوي كلاً من F والعناصر a, b نجد أن:

$$F(a, b) \subseteq K(b) = F(a)(b)$$

مما سبق نجد أن $F(a,b) = F(a)(b)$.

بطريقة مشابهة نجد أن $F(a,b) = F(b)(a)$.

٣ - ليكن $a, b \in F$ بحيث $a \neq 0$ و $d \in E$ عندئذ يكون $a, b \in F \subseteq F(d)$ ومنه
فإن $a, b, d \in F(d)$ وبما أن $F(d)$ حقل فإن $ad \in F(d)$ وأن $ad + b \in F(d)$ وحسب (١) نجد أن $F(d) = F(ad + b)$.

تعريف.

ليكن الحقل E تمديداً للحقل F و $a \in E$ ، نسمي كل تمديد للحقل F من الشكل $F(a)$ تمديداً بسيطاً للحقل F .

أمثلة.

١ - الحقل $Q(\sqrt{2})$ يعد تمديداً بسيطاً للحقل Q .

ليكن K حقلاً يحوي كلاً من Q والعنصر $\sqrt{2}$. عندئذ أيّاً كان $a, b \in Q$ فإن $a, b, \sqrt{2} \in K$ ، ومنه $a + b\sqrt{2} \in K$ ، أي أن $Q(\sqrt{2}) \subseteq K$.

٢ - أوجد عناصر الحقل $Q(\sqrt{3}, \sqrt{5})$.

لدينا حسب المبرهنة (٣-١-٢) أن $Q(\sqrt{3}, \sqrt{5}) = Q(\sqrt{3})(\sqrt{5})$.

ليكن $x \in Q(\sqrt{3})(\sqrt{5})$ عندئذ فإن $x = a + b\sqrt{5}$ حيث $a, b \in Q(\sqrt{3})$ وبالتالي فإن

$a = a_1 + a_2\sqrt{3}$ وأن $b = b_1 + b_2\sqrt{3}$ حيث $a_1, a_2, b_1, b_2 \in Q$ وهكذا نجد أن

$$\begin{aligned} x &= a_1 + a_2\sqrt{3} + (b_1 + b_2\sqrt{3})\sqrt{5} = \\ &= a_1 + a_2\sqrt{3} + b_1\sqrt{5} + b_2\sqrt{15} \end{aligned}$$

ومنه فإن $Q(\sqrt{3}, \sqrt{5}) = \{a_1 + a_2\sqrt{3} + b_1 + b_2\sqrt{15}, : a_1, a_2, b_1, b_2 \in Q\}$.

٣ - أثبت أن $Q(\sqrt{2}) = Q(3 + \sqrt{2})$.

الحل.

ليكن $x \in Q(\sqrt{2})$ عندئذ بحسب التعريف يكون $x = a + b\sqrt{2}$ حيث $a, b \in Q$ ومنه
فإن:

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

بفرض أن $a_1 = a - 3b \in Q$ نجد أن $x \in Q(3 + \sqrt{2})$ ومنه يكون:

$$Q(\sqrt{2}) \subseteq Q(3 + \sqrt{2})$$

ليكن $y \in Q(3 + \sqrt{2})$ عندئذ $y = a_1 + b_1(3 + \sqrt{2})$ حيث $a_1, b_1 \in Q$ ومنه يكون:

$$y = (a_1 + 3b_1) + b_1\sqrt{2} \quad \text{بفرض أن } a_2 = a_1 + 3b_1 \in Q(\sqrt{2}) \text{ نجد أن:}$$

$$y = a_2 + b_1\sqrt{2} \in Q(\sqrt{2})$$

وهذا يبين أن $Q(3 + \sqrt{2}) \subseteq Q(\sqrt{2})$.

أو مباشرة حسب المبرهنة (٣-١-٢) ومن أجل $d = \sqrt{2}, b = 3, a = 1$ نجد أن:

$$Q(\sqrt{2}) = Q(3 + \sqrt{2})$$

قبل البدء في البحث عن مسألة وجود التمديد لحقل ما لابد لنا من التمهيدية الأساسية

الآتية:

تمهيدية ٣-١-٣.

ليكن F, K حقليين و $g: F \rightarrow K$ تطبيق يحقق الشروط: أياً كان $a, b \in F$ فإن:

$$g(a + b) = g(a) + g(b), \quad g(ab) = g(a)g(b)$$

عندئذ نتحقق واحدة فقط من الحالات الآتية:

$$١ - \quad g(0) = 0 \text{ و } g(1) = 0 \text{ وفي هذه الحالة يكون } g = 0.$$

$$٢ - \quad g(0) = 0 \text{ و } g(1) = 1 \text{ وفي هذه الحالة يكون } g \text{ متبايناً.}$$

البرهان.

$$\text{لدينا } g(0) = g(0 + 0) = g(0) + g(0) \text{ ومنه فإن } g(0) = 0.$$

$$\text{كما أن } g(1) = g(1.1) = g(1).g(1), \text{ ومنه فإن } g(1)(1 - g(1)) = 0. \text{ بما أن } K \text{ حقل}$$

$$\text{فإنه إما } g(1) = 0 \text{ أو } 1 - g(1) = 0.$$

$$١ - \text{ إذا كان } g(1) = 0 \text{ عندئذ أياً كان } a \in F \text{ فإن:}$$

$$g(a) = g(a.1) = g(a).g(1) = g(a).0 = 0$$

وهذا يبين لنا أن $g = 0$.

$$٢ - \text{ إذا كان } 1 - g(1) = 0 \text{ عندئذ } g(1) = 1. \text{ وهنا نجد أنه أياً كان } b \in F, b \neq 0 \text{ فإن}$$

$$1 = g(1) = g(bb^{-1}) = g(b)g(b^{-1}) \text{ وهذا يبين لنا أن } g(b) \neq 0. \text{ لنبرهن أن } g$$

متباين. ليكن $a, b \in F$ بحيث $g(a) = g(b)$ عندئذ يكون $g(a - b) = 0$ ومنه فإن

$a - b = 0$ ، أي أن $a = b$ وبالتالي g متباين. ٥

السؤال الذي يتبادر إلى الذهن مباشرة هل بالإمكان تمديد أي حقل، أو بمعنى آخر هل يوجد تمديد ما لأي حقل. المبرهنة الآتية تجيب على هذا السؤال:

مبرهنة ٣-١-٤.

ليكن F حقلاً و $p(x)$ حدودية أولية في الحلقة $F[x]$ ، عندئذ يوجد تمديد E للحقل F يحوي صفراً للحدودية $p(x)$.

البرهان.

لنفرض أن الحدودية $p(x)$ أولية في الحلقة $F[x]$ ، عندئذ وحسب المبرهنة (١-٢-٢) فإن المثالي $A = \langle p(x) \rangle$ يكون أعظمية في $F[x]$ وبالتالي تكون حلقة الخارج $F[x]/A$ حقلاً. لنفرض أن $E = F[x]/A$ ولنعرّف التطبيق $\varphi: F \rightarrow E$ بالشكل التالي: أيّاً كان $a \in F$ فإن $\varphi(a) = a + A$ فنجد أن φ هو تشاكل حلقى لأنه أيّاً كان $a, b \in F$

$$\varphi(a+b) = (a+b) + A = (a+A) + (b+A) = \varphi(a) + \varphi(b)$$

$$\varphi(a \cdot b) = (a \cdot b) + A = (a+A) \cdot (b+A) = \varphi(a) \cdot \varphi(b)$$

كما أن $\varphi(1) = 1 + A \neq A$ ، وحسب التمهيدية (٣-١-٣) يكون التشاكل φ متبايناً.

لنضع $Im \varphi = K$ فنجد أن $\varphi: F \rightarrow K$ هو تشاكل متباين وغامر أي تماثل وبما أن F حقل فإن K يكون حقلاً جزئياً في E ، أي $K \subseteq E$. بما أن الحقلين F, K متماثلان فإنه يمكن المطابقة بينهما واعتبار أن الحقل F هو حقل جزئي في الحقل E . مما سبق نجد أن الحقل E هو تمديد للحقل F .

لنبرهن الآن على أن الحقل E يحوي صفراً للحدودية $p(x)$. بما أن $p(x) \in F[x]$ لنفرض أن $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ حيث $a_n, a_{n-1}, \dots, a_1, a_0$ ولنبرهن على أن العنصر $x + A \in E$ هو صفر للحدودية $p(x)$. إن:

$$\begin{aligned} p(x+A) &= a_n (x+A)^n + a_{n-1} (x+A)^{n-1} + \dots + a_1 (x+A) + a_0 (x+A)^0 = \\ &= a_n (x^n + A) + a_{n-1} (x^{n-1} + A) + \dots + a_1 (x+A) + a_0 (x^0 + A) = \\ &= (a_n x^n + A) + (a_{n-1} x^{n-1} + A) + \dots + (a_1 x + A) + (a_0 + A) = \end{aligned}$$

$$= (a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) + A = p(x) + A = A$$

وهذا يبين لنا أن العنصر $x + A \in E$ هو صفر للحدودية $p(x)$.

المبرهنة الآتية تعد تعميماً للمبرهنة السابقة والتي توصف بأنها المبرهنة الأساسية في نظرية الحقول و تسمى *Kroneker's Theorem 1887*.

مبرهنة ٣-١-٥.

ليكن F حقلاً و $f(x) \in F[x]$ بحيث $\partial f(x) > 0$. عندئذ يوجد تمديد E للحقل F يحوي صفراً للحدودية $f(x)$.

البرهان.

بما أن F حقل عندئذ الحلقة $F[x]$ هي حلقة تحليل وحيد. من جهة أخرى، بما أن $f(x) \in F[x]$ وأن $\partial f(x) > 0$ فإنه حسب المبرهنة (٢-٢-١) تكون $f(x)$ غير قابلة للقلب في $F[x]$ وبالتالي يوجد في $F[x]$ عنصر أولي وليكن $p(x)$ يقسم $f(x)$ في $F[x]$ ، ومنه يوجد $\lambda(x) \in F[x]$ بحيث $f(x) = p(x) \cdot \lambda(x)$. وبما أن الحدودية $p(x)$ أولية في $F[x]$ فإنه حسب المبرهنة (٣-١-٤) يوجد تمديد E للحقل F يحوي صفراً للحدودية $p(x)$ وليكن α .

إن $\alpha \in E$ وأن $f(\alpha) = p(\alpha) \cdot \lambda(\alpha) = 0$ أي أن α هو صفر للحدودية $f(x)$. مما سبق نجد أنه يوجد تمديد E للحقل F يحوي صفراً للحدودية $f(x)$.

لنورد الآن بعضاً من الأمثلة توضح لنا فكرة المبرهنات السابقة.

أمثلة.

١ - لتكن $f(x) = x^2 + 2 \in Q[x]$. واضح أن الحدودية $f(x)$ هي حدودية أولية في

$Q[x]$ وحسب المبرهنة (٣-١-٤) يوجد تمديد E للحقل Q هو $E = Q[x]/A$ حيث

$A = \langle f(x) \rangle$ وهذا الحقل يحوي صفراً للحدودية $f(x)$ هو $x + A \in E$. لأن

$$f(x + A) = (x + A)^2 + (x + A)^0 = (x^2 + A) + (x^0 + A) =$$

$$= (x^2 + 1) + A = f(x) + A = A$$

نعلم أن الحدودية $f(x) = x^2 + 2$ تملك جذراً (صفاً) عقدياً (مركباً) هو $i = \sqrt{-1}$

ولكن ما نرغب بتوضيحه هنا أننا نبني حقلاً يحوي حقل الأعداد النسبية Q وجذر للحدودية $x^2 + 2$ وذلك باستخدام الحقل Q فقط. ◊

٢ - لنأخذ الحودية $f(x) = x^5 + 2x^2 + 2x + 2 \in Z_3[x]$. واضح أن الحودية $f(x)$ غير أولية فوق Z_3 (تأكد من ذلك). وبما أن Z_3 حقلاً عندئذ تكون الحلقة $Z_3[x]$ حلقة تحليل وحيد وبما أن $\partial f(x) > 0$ فإن الحودية $f(x)$ يمكن كتابتها بصورة وحيدة على شكل جداء منته لعناصر أولية من الحلقة $Z_3[x]$ بالشكل الآتي: $f(x) = (x^2 + 1)(x^3 + 2x + 2) \in Z_3[x]$ وبما أن الحودية $x^2 + 2$ هي حودية أولية في الحلقة $Z_3[x]$ فإنه حسب المبرهنة (٣-١-٤) يوجد تمديد $E = Z_3[x]/\langle x^2 + 1 \rangle$ للحقل Z_3 يحوي صفراً للحودية $x^2 + 1$ ، وبما أن أي صفر للحودية $x^2 + 1$ هو صفر للحودية $f(x)$ نجد أن الحقل $E = Z_3[x]/\langle x^2 + 1 \rangle$ هو تمديد للحقل Z_3 ويحوي صفراً للحودية $f(x)$ وهذا الحقل منته ومؤلف من تسعة عناصر.

من جهة أخرى، بما أن الحودية $x^3 + 2x + 2 \in Z_3[x]$ هي حودية أولية في $Z_3[x]$ فإنه حسب المبرهنة (٣-١-٤) يوجد تمديد $E_1 = Z_3[x]/\langle x^3 + 2x + 2 \rangle$ للحقل Z_3 يحوي صفراً للحودية $x^3 + 2x + 2$ وبالتالي يكون E_1 تمديداً للحقل Z_3 ويحوي صفراً للحودية $f(x)$ وهذا الحقل مؤلف من 27 عنصراً.

إن المثال الأخير يبين لنا أنه يوجد أكثر من تمديد للحقل الواحد.

نأتي الآن إلى دراسة المبرهنة الهامة الآتية:

مبرهنة ٣-١-٦.

ليكن F حقلاً و $p(x)$ حودية أولية في الحلقة $F[x]$ ، وليكن E تمديد ما للحقل F و $a \in E$ صفراً للحودية $p(x)$. عندئذ فإن:

$$١ - F(a) \cong F[x]/\langle p(x) \rangle.$$

٢ - إذا كانت $\partial p(x) = n$ عندئذ أيّاً كان $b \in F(a)$ فإن العنصر b يمكن التعبير عنه بصورة وحيدة على النحو الآتي:

$$b = c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1a + c_0$$

حيث $c_{n-1}, c_{n-2}, \dots, c_1, c_0 \in F$

البرهان.

١ - إن $F(a)$ حقل وهو أصغر حقل جزئي في E يحوي كلاً من F والعنصر a .
من جهة أخرى، بما أن الحدودية $p(x)$ أولية فوق الحقل F فإنه حسب المبرهنة (١-٧-٢) فإن المثالي $\langle p(x) \rangle$ هو مثالي أعظمي في الحلقة $F[x]$ وبالتالي تكون حلقة الخارج $F[x]/\langle p(x) \rangle$ حقلاً.

لنعرف التطبيق $\varphi: F[x] \rightarrow F(a)$ بالشكل الآتي: أيّاً كان $f(x) \in F[x]$ فإن $\varphi(f(x)) = f(a)$ فنجد أن التطبيق φ هو تشاكل حلقي وذلك بحسب التمرين المحلول (٣-٤). لنبرهن الآن على أن $\langle p(x) \rangle = \text{Ker } \varphi$. بما أن العنصر a هو صفر للحدودية $p(x)$ أي $p(a) = 0$ نجد أن $p(x) \in \text{Ker } \varphi$ ومنه يكون $\langle p(x) \rangle \subseteq \text{Ker } \varphi$.
من جهة أخرى، بما أن الحدودية $\mu(x) = 1 \in F[x]$ وأن $\mu(a) = 1 \neq 0$ نجد أن $\mu(x) \notin \text{Ker } \varphi$ وهذا يبين لنا أن المثالي $\langle p(x) \rangle \subsetneq \text{Ker } \varphi$ وبما أن المثالي $\langle p(x) \rangle$ أعظمي في الحلقة $F[x]$ نجد أن $\text{Ker } \varphi = \langle p(x) \rangle$ ، وهكذا نجد أن:

$$F[x]/\text{Ker } \varphi \cong \text{Im } \varphi$$

وبالتالي يكون $F[x]/\langle p(x) \rangle \cong \text{Im } \varphi$

من جهة ثالثة، بما أن $F[x]/\langle p(x) \rangle$ حقل فإن $\text{Im } \varphi$ حقل أيضاً، بالإضافة لذلك فإن $\text{Im } \varphi \subseteq F(a)$. لنبرهن الآن على أن $\text{Im } \varphi = F(a)$.
ليكن $d \in F$ عندئذ الحدودية $\lambda(x) = d \in F[x]$ وأن $\lambda(a) = d \in \text{Im } \varphi$ وأن $\varphi(\lambda(x)) = \lambda(a) = d \in \text{Im } \varphi$.
وهذا يبين لنا $F \subseteq \text{Im } \varphi$.

كذلك بما أن الحدودية $\theta(x) = x \in F[x]$ وأن $\theta(a) = a \in \text{Im } \varphi$ فإن $\varphi(\theta(x)) = \theta(a) = a \in \text{Im } \varphi$ وبما أن a والعنصر F يحوي كلاً من $F(a)$ هو أصغر حقل يحوي $F(a)$ والعنصر a نجد أن $F(a) \subseteq \text{Im } \varphi$. مما سبق نجد أن $F(a) = \text{Im } \varphi$ وهكذا فإن $F(a) \cong F[x]/\langle p(x) \rangle$.

٢ - وجدنا حسب (١) أن $\varphi: F[x] \rightarrow F(a)$ هو تشاكل غامر.

ليكن $b \in F(a)$ عندئذ يوجد $g(x) \in F[x]$ بحيث $\varphi(g(x)) = b$. حسب تعريف φ فإن $g(a) = b$.

حسب خوارزمية القسمة لأجل $g(x), p(x) \in F[x]$ يوجد $q(x), r(x) \in F[x]$ بحيث:

$$g(x) = q(x)p(x) + r(x)$$

حيث إما $r(x) = 0$ أو $\partial r(x) < \partial p(x)$. ومنه:

$$\begin{aligned} g(x) + \langle p(x) \rangle &= (q(x)p(x) + r(x)) + \langle p(x) \rangle = \\ &= (q(x)p(x) + \langle p(x) \rangle) + (r(x) + \langle p(x) \rangle) = \\ &= r(x) + \langle p(x) \rangle \end{aligned}$$

ومنه نجد أن $g(x) - r(x) \in \langle p(x) \rangle$ وبالتالي يوجد $f(x) \in F[x]$ بحيث:

$$g(x) - r(x) = f(x)p(x)$$

وحسب تعريف φ نجد أن $g(a) - r(a) = f(a)p(a) = 0$ ومنه $g(a) = r(a) = b$.

نفرض أن $\partial p(x) = n$ وبما أنه إما $r(x) = 0$ أو $\partial r(x) < \partial p(x)$ ، نجد أن:

$$r(x) = \sum_{i=0}^{n-1} c_i x^i$$

حيث $c_{n-1}, c_{n-2}, \dots, c_1, c_0 \in F$ ، وهكذا نجد أن $b = r(a) = \sum_{i=0}^{n-1} c_i a^i$.

وبالتالي يكون $b = c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \dots + c_1a + c_0$ وهذه الكتابة وحيدة لكون

$r(x)$ معين بشكل وحيد. ♦

أمثلة.

١ - لنأخذ الحدودية $f(x) = x^6 - 2 \in Q[x]$.

حسب اختبار أيزنشتاين فإن الحدودية $f(x)$ هي حدودية أولية فوق الحقل Q وأن $a = \sqrt[6]{2} = 2^{1/6}$ هو صفر للحدودية $f(x)$ وحسب المبرهنة (٣-١-٦) فإن

$Q(\sqrt[6]{2}) \cong Q[x]/\langle f(x) \rangle$ كما أن المجموعة:

$$\{1, 2^{1/6}, 2^{2/6}, 2^{3/6}, 2^{4/6}, 2^{5/6}\}$$

تشكل قاعدة للحقل $Q(\sqrt[6]{2})$ فوق الحقل Q وبالتالي يكون:

$$Q[x]/\langle f(x) \rangle \cong Q(\sqrt[6]{2}) = \{c_0 + c_1 2^{1/6} + c_2 2^{2/6} + c_3 2^{3/6} + c_4 2^{4/6} + c_5 2^{5/6} : \}$$

$$c_i \in Q, i = 0,1,2,3,4,5\}.$$

٢ - أوجد جميع عناصر الحقل $Q(\sqrt[3]{5})$.

حسب اختبار أيزنشتاين فإن الحدودية $p(x) = x^5 - 5 \in Q[x]$ هي حدودية أولية فوق Q وأن $a = \sqrt[3]{5} = 5^{1/3}$ هو صفر للحدودية $p(x)$ وحسب المبرهنة (٣-١-٦) فإن $Q(\sqrt[3]{5}) \cong Q[x]/\langle p(x) \rangle$ كما أن المجموعة $\{1, 5^{1/3}, 5^{2/3}\}$ تشكل قاعدة للحقل $Q(\sqrt[3]{5})$ فوق الحقل Q وبالتالي يكون:

$$Q[x]/\langle p(x) \rangle \cong Q(\sqrt[3]{5}) = \{c_0 + c_1 5^{1/3} + c_2 5^{2/3} : c_0, c_1, c_2 \in Q\}.$$

٣ - أثبت أن $Q(\sqrt{2}) = Q(3 + \sqrt{2})$.

الحل.

ليكن $x \in Q(\sqrt{2})$ عندئذ بحسب التعريف يكون $x = a + b\sqrt{2}$ حيث $a, b \in Q$ ومنه فإن:

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

بفرض أن $a_1 = a - 3b \in Q$ نجد أن $x \in Q(3 + \sqrt{2})$ ومنه يكون:

$$Q(\sqrt{2}) \subseteq Q(3 + \sqrt{2})$$

ليكن $y \in Q(3 + \sqrt{2})$ عندئذ فإن $y = a_1 + b_1(3 + \sqrt{2})$ حيث $a_1, b_1 \in Q$ ومنه

يكون $y = (a_1 + 3b_1) + b_1\sqrt{2}$. بفرض أن $a_3 = a_1 + 3b_1 \in Q$ نجد أن:

$$y = a_3 + b_1\sqrt{2} \in Q(\sqrt{2})$$

وهذا يبين أن $Q(3 + \sqrt{2}) \subseteq Q(\sqrt{2})$ ، ومنه يكون $Q(\sqrt{2}) = Q(3 + \sqrt{2})$.

أو مباشرة حسب المبرهنة (٣-١-٢) ومن أجل $a=1, b=1$ و $d = \sqrt{2}$ نجد أن:

$$Q(\sqrt{2}) = Q(d) = Q(3 + \sqrt{2})$$

٣ - ٢. التمديدات المنتهية.

ليكن الحقل E تمديداً للحقل F ، في هذه الحالة يمكن النظر إلى الحقل E على أنه فضاء شعاعي فوق F . بالاعتماد على هذه الحقيقة يمكننا صياغة التعريف الآتي:

تعريف.

ليكن الحقل E تمديداً للحقل F .

- نقول عن التمديد E إنه تمديد منته للحقل F من الدرجة n إذا كان بعد الفضاء الشعاعي E فوق F يساوي n ، ونرمز لذلك $[E : F] = n$.
- إذا لم يكن التمديد E للحقل F منتهياً، نقول في هذه الحالة إن التمديد E هو تمديد غير منته للحقل F .

بالاعتماد على التعريف السابق نقول عن الحقل E إنه تمديد منته للحقل F درجته تساوي n إذا وجدت مجموعة جزئية من الحقل E مؤلفة من n عنصر

$$S = \{x_1, x_2, \dots, x_n\} \subset E$$

تحقق الشرطين التاليين:

- ١ - أن تكون المجموعة S مولدة للحقل E فوق الحقل F ، أي أنه أي $y \in E$ فإن $y = a_1x_1 + a_2x_2 + \dots + a_nx_n$ حيث $a_1, a_2, \dots, a_n \in F$.
- ٢ - أن تكون المجموعة S مستقلة خطياً فوق F ، أي أنه من أجل أي مجموعة من العناصر $a_1, a_2, \dots, a_n \in F$ تحقق الشرط $a_1x_1 + a_2x_2 + \dots + a_nx_n = 0$ ينتج أن $a_1 = a_2 = \dots = a_n = 0$.

نسمي المجموعة S قاعدة للحقل E فوق الحقل F .

بمعنى آخر، نقول عن التمديد E للحقل F إنه تمديد منته درجته تساوي n إذا وجدت مجموعة من عناصر الحقل E مؤلفة من n عنصر تحقق: أن كل عنصر من الحقل E يكتب بصورة وحيدة على شكل تركيب خطي لعناصر هذه المجموعة بأمثال من الحقل F .

أمثلة.

١ - إن حقل الأعداد العقدية (المركبة) $C = \{a + bi : a, b \in R\}$ هو تمديد منته لحقل الأعداد الحقيقية R من الدرجة الثانية قاعدته المجموعة $\{1, i\}$. لأن هذه المجموعة تولد الحقل C فوق الحقل R وهي أيضاً مستقلة خطياً لأنه أياً كان $\alpha, \beta \in R$ بحيث $\alpha + \beta i = 0$ فإن $\alpha + \beta i = 0 + 0i$ ومنه يكون $\alpha = \beta = 0$. بينما حقل الأعداد العقدية هو تمديد غير منته لحقل الأعداد النسبية Q .

٢ - الحقل $Q(\sqrt{2}) = \{a + b\sqrt{2} ; a, b \in Q\}$ هو تمديد منته للحقل Q . لأنه كما هو واضح من تعريف الحقل $Q(\sqrt{2})$ فإن المجموعة $\{1, \sqrt{2}\}$ تولد الحقل $Q(\sqrt{2})$ فوق الحقل Q وهي أيضاً مستقلة خطياً فوق Q لأنه أياً كان $a, b \in Q$ بحيث $a + b\sqrt{2} = 0$ فإن $b = 0$ لأنه إذا كان $b \neq 0$ فإن $\sqrt{2} = -a/b = -ab^{-1} \in Q$ وهذا غير ممكن.

واحدة من الخواص الهامة للتمديدات المنتهية وهي خاصية التعدي نوردتها من خلال المبرهنة الآتية:

مبرهنة ١-٢-٣.

ليكن الحقل K تمديداً منتهياً للحقل E والحقل E تمديداً منتهياً للحقل F ، عندئذ يكون الحقل K تمديداً منتهياً للحقل F ويحقق $[K : F] = [K : E] \cdot [E : F]$.
البرهان.

بما أن الحقل K تمديد للحقل E فإن $E \subseteq K$ ، كذلك بما أن الحقل E هو تمديد للحقل F فإن $F \subseteq E$ ، مما سبق نجد أن $F \subseteq K$ ، أي أن الحقل K هو تمديد للحقل F . من جهة أخرى، بما أن الحقل K هو تمديد منته للحقل E وأن الحقل E هو تمديد منته للحقل F ، لنفرض أن $[K : E] = n$ وأن $[E : F] = m$ ومنه توجد قاعدة للحقل K فوق E ومؤلفة من n عنصر ولتكن $X = \{x_1, x_2, \dots, x_n\} \subset K$ وقاعدة للحقل E فوق الحقل F ومؤلفة من m عنصر ولتكن $Y = \{y_1, y_2, \dots, y_m\} \subset E$. لنبرهن الآن على أن المجموعة $X \cdot Y = \{y_j \cdot x_i : 1 \leq j \leq m, 1 \leq i \leq n\}$ تشكل قاعدة للحقل K فوق الحقل F .

ليكن $a \in K$ ، بما أن الحقل K تمديد منته للحقل E قاعدته المجموعة X فإن:

$$a = a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

حيث $a_i \in E$ وذلك من أجل جميع القيم $1 \leq i \leq n$.

من جهة أخرى، بما أن $a_i \in E$ وأن الحقل E تمديد منته للحقل F قاعدته المجموعة Y فإن $a_i = c_{i1}y_1 + c_{i2}y_2 + \cdots + c_{im}y_m$ حيث $c_{ij} \in F$ أيضاً كان $1 \leq j \leq m$ و $1 \leq i \leq n$. وهكذا نجد أن:

$$a = \sum_{i=1}^n a_i x_i = \sum_{i=1}^n \left(\sum_{j=1}^m c_{ij} y_j \right) x_i = \sum_{i,j} c_{ij} (y_j x_i)$$

إن هذا يبين لنا أن المجموعة $Y \cdot X$ تولد الحقل K فوق الحقل F .

من جهة ثالثة، لنفرض أن $\sum_{i,j} c_{ij} (y_j x_i) = 0$ عندئذ يكون $\sum_{i=1}^n \left(\sum_{j=1}^m c_{ij} y_j \right) x_i = 0$. وبما أن المجموعة X تشكل قاعدة للحقل K فوق E نجد أن $\sum_{j=1}^m c_{ij} y_j = 0$ وبما أن المجموعة Y تشكل قاعدة للحقل E فوق الحقل F نجد أن $c_{ij} = 0$ وذلك لأجل جميع القيم $1 \leq i \leq n$ و $1 \leq j \leq m$. مما سبق نجد أن المجموعة $Y \cdot X$ تشكل قاعدة للحقل K فوق F وهذه المجموعة مؤلفة من $m \cdot n$ عنصراً، وبالتالي يكون لدينا:

$$[K:F] = m \cdot n = [K:E] \cdot [E:F]$$

إن المبرهنة الأخيرة تتشابه إلى حد كبير مع مبرهنة لاگرانج الخاصة بالزمر المنتهية، وهذه المبرهنة يمكن صياغتها بشكل آخر كما يلي: إذا كان $F \subseteq E \subseteq K$ وكان الحقل K تمديداً منتهياً للحقل E والحقل E تمديداً منتهياً للحقل F فإن:

- كلاً من درجتي تمديد الحقل K فوق الحقل E ودرجة تمديد E فوق F تقسم $[K:F]$.

- درجة تمديد الحقل K فوق F تقبل القسمة على كل من درجتي تمديد K فوق E و E فوق F ، أي أن $[K:F]$ تقبل القسمة على $[K:E]$ و $[E:F]$.

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة المبرهنة التالية:

مبرهنة ٢-٢-٣.

ليكن الحقل K تمديداً للحقل E والحقل E تمديداً للحقل F ، $(F \subseteq E \subseteq K)$.
الشرط اللازم والكافي كي يكون الحقل K تمديداً منتهياً للحقل F هو أن يكون الحقل K
تمديداً منتهياً للحقل E وأن يكون الحقل E تمديداً منتهياً للحقل F .
البرهان.

لزوم الشرط. لنفرض أن الحقل K تمديد منته للحقل F ولنفرض أن $[K : F] = n$. بما
أن بعد الفضاء K فوق F يساوي إلى n وأن الفضاء E فوق F هو فضاء جزئي من
الفضاء K فإن $[E : F] \leq [K : F] = n$ وهكذا نجد أن التمديد E للحقل F هو تمديد
منته. لنفرض أن $[E : F] = m$ حيث $m \leq n$ عندئذ يكون $[K : E] \leq n$ لأنه إذا
كانت $[K : E] = s$ حيث $s > n$ فإن $[K : F] = s \cdot m > n$ فإن $[K : E] \cdot [E : F] = s \cdot m > n$
وهذا غير ممكن، ومنه نجد أن $[K : E] \leq n$ وبالتالي يكون K تمديداً منتهياً للحقل E .
كفاية الشرط. لنفرض أن الحقل K تمديد منته للحقل E وأن الحقل E تمديد منته للحقل
 F عندئذ حسب المبرهنة (٣-٢-١) يكون الحقل K تمديداً منتهياً للحقل F . ◊

يمكن تعميم المبرهنة الأخيرة لأجل أي عدد منته من التمديدات المنتهية بالشكل
الآتي:

مبرهنة ٣-٢-٣.

لنأخذ السلسلة الآتية من الحقول $F_1 \subseteq F_2 \subseteq \dots \subseteq F_n$. الشرط اللازم والكافي كي
يكون الحقل F_n تمديداً منتهياً للحقل F_1 هو أن يكون الحقل F_i تمديداً منتهياً للحقل F_{i-1}
وذلك لأجل جميع القيم $i = 1, 2, \dots, n$ ، بالإضافة لذلك يكون:

$$[F_n : F_1] = [F_n : F_{n-1}] \cdot [F_{n-1} : F_{n-2}] \cdot \dots \cdot [F_2 : F_1]$$

البرهان.

لزوم الشرط. لنفرض أن الحقل F_n تمديد منته للحقل F_1 وأن $[F_n : F_1] = m$. بما أن
 F_n فضاء شعاعي فوق F_1 وأن $F_1 \subseteq F_{i-1}$ فإن F_n فضاء شعاعي فوق F_{i-1} وأن
 $[F_n : F_{i-1}] \leq m$. من جهة أخرى، الحقل F_i هو فضاء شعاعي فوق F_{i-1} وأن
 $F_i \subseteq F_n$ ومنه فإن F_i فوق F_{i-1} هو فضاء جزئي من الفضاء F_n فوق F_{i-1} ومنه

ولذلك $[F_i : F_{i-1}] \leq [F_n : F_{i-1}] \leq m$ وهذا يبين لنا أن الحقل F_i تمديد منته للحقل F_{i-1} وذلك لأجل جميع القيم $i = 2, 3, \dots, n$.

كفاية الشرط. لنفرض أن الحقل F_i تمديد منته للحقل F_{i-1} وذلك لأجل جميع القيم $i = 2, 3, \dots, n$ ، ولنبرهن على أن الحقل F_n تمديد منته للحقل F_1 . بالاستقراء على n . واضح أنه من أجل $n = 2$ فإن $F_1 \subseteq F_2$ وأن الحقل F_2 هو تمديد منته للحقل F_1 . لنفرض أن النص صحيح لأجل $(n-1)$ أي أن الحقل F_{n-1} هو تمديد منته للحقل F_1 . وبما أن الحقل F_n تمديد منته للحقل F_{n-1} وحسب المبرهنة (٢-٢-١) يكون F_n تمديداً منتهياً للحقل F_1 . ◊

أمثلة.

١ - أثبت أن الحقل $Q(\sqrt{5})$ هو تمديد منته للحقل Q درجته تساوي 2. بما أن $Q \subseteq Q(\sqrt{5})$ فإن الحقل $Q(\sqrt{5})$ هو تمديد للحقل Q ، كما أن المجموعة $\{1, \sqrt{5}\}$ تشكل قاعدة للحقل $Q(\sqrt{5})$ فوق Q ، لأنه أياً كان $x \in Q(\sqrt{5})$ فإن $x = a + b\sqrt{5} = a \cdot 1 + b \cdot \sqrt{5}$ حيث $a, b \in Q$. كذلك إذا كان $x = a + b\sqrt{5} = 0$ حيث $a, b \in Q$ فإن $b = 0$ لأنه إذا كان $b \neq 0$ فإن $b \in Q$ $-a/b = -ab^{-1} \in Q$ وهذا غير ممكن.

مما سبق نجد أن $Q(\sqrt{5})$ هو تمديد منته للحقل Q وأن $[Q(\sqrt{5}) : Q] = 2$.

٢ - أثبت أن الحقل $Q(\sqrt{5}, \sqrt{3})$ هو تمديد منته للحقل $Q(\sqrt{5})$ درجته تساوي 2. بما أن $\sqrt{5} \in Q(\sqrt{5}, \sqrt{3})$ نجد أن $Q(\sqrt{5}) \subseteq Q(\sqrt{5}, \sqrt{3})$ وهذا يبين لنا أن الحقل $Q(\sqrt{5}, \sqrt{3})$ هو تمديد للحقل $Q(\sqrt{5})$.

من جهة أخرى، حسب المبرهنة (٣-١-٢) فإن $Q(\sqrt{5}, \sqrt{3}) = Q(\sqrt{5})(\sqrt{3})$ وبالتالي أياً كان $x \in Q(\sqrt{5}, \sqrt{3})$ فإن $x \in Q(\sqrt{5})(\sqrt{3})$ ومنه:

$$x = a + b\sqrt{3} = a \cdot 1 + b \cdot \sqrt{3}$$

حيث $a, b \in Q(\sqrt{5})$ وهذا يبين لنا أن المجموعة $\{1, \sqrt{3}\}$ تولد الحقل $Q(\sqrt{5}, \sqrt{3})$ فوق الحقل $Q(\sqrt{5})$ وهذه المجموعة مستقلة، لأنه إذا كان $a + b\sqrt{3} = 0$ حيث $a, b \in Q(\sqrt{5})$ فإن $b = 0$ لأنه إذا كان $b \neq 0$ فإن $-a/b = -ab^{-1} \in Q(\sqrt{5})$ $\sqrt{3} = -a/b = -ab^{-1} \in Q(\sqrt{5})$

وهذا غير صحيح، لأنه أيضاً إذا كان $\sqrt{3} \in Q(\sqrt{5})$ فإن $\sqrt{3} = a_1 + b_1\sqrt{5}$ حيث $a_1, b_1 \in Q$ ومنه يكون $a_1 = \sqrt{3} - b_1\sqrt{5} \notin Q$ وهذا غير ممكن. مما سبق نجد أن $b = 0$ وبالتالي $a = 0$ ، أي أن الحقل $Q(\sqrt{5}, \sqrt{3})$ هو تمديد منته للحقل $Q(\sqrt{5})$ وأن:

$$[Q(\sqrt{5}, \sqrt{3}) : Q(\sqrt{5})] = 2$$

٣ - أثبت أن الحقل $Q(\sqrt{5}, \sqrt{3})$ هو تمديد منته للحقل Q درجته تساوي 4.
نلاحظ أن $Q \subseteq Q(\sqrt{5}) \subseteq Q(\sqrt{5}, \sqrt{3})$ وهذا يبين لنا أن الحقل $Q(\sqrt{5}, \sqrt{3})$ هو تمديد للحقل Q . من جهة أخرى، وجدنا حسب المثال (١) أن الحقل $Q(\sqrt{5})$ هو تمديد منته للحقل Q وأن $[Q(\sqrt{5}) : Q] = 2$ ، وحسب المثال رقم (٢) أن الحقل $Q(\sqrt{5}, \sqrt{3})$ هو تمديد منته للحقل $Q(\sqrt{5})$ وأن $[Q(\sqrt{5}, \sqrt{3}) : Q(\sqrt{5})] = 2$ ، وحسب المبرهنة (٣-٢-١) نجد أن الحقل $Q(\sqrt{5}, \sqrt{3})$ هو تمديد منته للحقل Q وأن
 $[Q(\sqrt{5}, \sqrt{3}) : Q] = [Q(\sqrt{5}, \sqrt{3}) : Q(\sqrt{5})] \cdot [Q(\sqrt{5}) : Q] = 2 \cdot 2 = 4$
وأن قاعدة التمديد $Q(\sqrt{5}, \sqrt{3})$ فوق الحقل Q هي المجموعة $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$.

$$٤ - أثبت أن $[Q(\sqrt[6]{2}, \sqrt[3]{2}) : Q] = 6$$$

لنأخذ الحقل $Q(\sqrt[6]{2})$ ولنأخذ الحدودية $f(x) = x^6 - 2 \in Q[x]$ فنجد أن $f(x) \neq 0$ وحسب معيار ايزنشتاين فإن الحدودية $f(x)$ هي حدودية أولية فوق Q وأن $\sqrt[6]{2}$ هو صفر للحدودية $f(x)$ في الحقل $Q(\sqrt[6]{2})$ وحسب المبرهنة (٣-١-٦) فإن المجموعة $\{1, 2^{1/6}, 2^{2/6}, 2^{3/6}, 2^{4/6}, 2^{5/6}\} \subseteq Q(\sqrt[6]{2})$

تشكل قاعدة للحقل $Q(\sqrt[6]{2})$ فوق الحقل Q وبالتالي يكون $[Q(\sqrt[6]{2}) : Q] = 6$.

من جهة أخرى، نلاحظ أن $Q(\sqrt{2}, \sqrt[3]{2}) \subseteq Q(\sqrt[6]{2})$ لأن

$$\sqrt{2} = (\sqrt[6]{2})(\sqrt[6]{2})(\sqrt[6]{2}) \in Q(\sqrt[6]{2})$$

$$\sqrt[3]{2} = (\sqrt[6]{2})(\sqrt[6]{2}) \in Q(\sqrt[6]{2})$$

كما أن $Q \subseteq Q(\sqrt{2}, \sqrt[3]{2}) \subseteq Q(\sqrt[6]{2})$ وبما أن $[Q(\sqrt[6]{2}) : Q] = 6$ فإن الحقل $Q(\sqrt[6]{2})$ هو تمديد منته للحقل Q وحسب المبرهنة (٣-٢-٢) فإن الحقل $Q(\sqrt{2}, \sqrt[3]{2})$ هو تمديد منته للحقل Q ، كما أن $[Q(\sqrt{2}, \sqrt[3]{2}) : Q] \leq [Q(\sqrt[6]{2}) : Q] = 6$.

من جهة ثانية، بما أن $\sqrt{2}, \sqrt[3]{2} \in Q(\sqrt{2}, \sqrt[3]{2})$ فإن $Q(\sqrt[3]{2}) \subseteq Q(\sqrt{2}, \sqrt[3]{2})$ وأما $Q(\sqrt{2}) \subseteq Q(\sqrt{2}, \sqrt[3]{2})$ ، وبما أن الحقل $Q(\sqrt{2}, \sqrt[3]{2})$ هو تمديد منته للحقل Q فإنه حسب المبرهنة (٣-٢-٢) يكون

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

وبما أن $[Q(\sqrt{2}) : Q] = 2$ نجد أن 2 تقسم $[Q(\sqrt{2}, \sqrt[3]{2}) : Q]$. أيضاً بما أن

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

وأن $[Q(\sqrt[3]{2}) : Q] = 3$ وتقسم $[Q(\sqrt{2}, \sqrt[3]{2}) : Q]$ ينتج أن

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

٣ - ٣. التمديدات الجبرية.

ليكن الحقل K تمديداً للحقل F و $a \in K$ ، وجدنا حسب التمرين المحلول (٣-٤) أن التطبيق $\varphi: F[x] \rightarrow F(a)$ المعرفة بالشكل التالي $\varphi(f(x)) = f(a)$ وذلك أيّاً كان $f(x)$ من $F[x]$ ، هو تشاكل حلقي، وبما أن $F(a) \subseteq K$ فإن التطبيق $\varphi: F[x] \rightarrow K$ المعرفة بالشكل $\varphi(f(x)) = f(a)$ وذلك أيّاً كان $f(x) \in F[x]$ هو تشاكل حلقي. بالاعتماد على ما سبق يمكننا صياغة المبرهنة الآتية:

مبرهنة ٣-٣-١.

ليكن الحقل K تمديداً للحقل F و $a \in K$. وأن $\varphi: F[x] \rightarrow K$ هو التشاكل المعرفة بالشكل الآتي: $\varphi(f(x)) = f(a)$ وذلك أيّاً كان $f(x) \in F[x]$. عندئذٍ القضايا الآتية متكافئة:

- ١ - التشاكل φ ليس متبايناً.
- ٢ - يوجد في $F[x]$ عنصر واحد على الأقل $h(x) \neq 0$ من أجله $h(a) = 0$.
- ٣ - يوجد في F عناصر $c_0, c_1, c_2, \dots, c_n \in F$ حيث $n \geq 1$ ليست جميعها معدومة من أجلها $\sum_{i=0}^n c_i a^i = 0$.

البرهان.

(1) $\Leftrightarrow$ (2). لنفرض أن التشاكل φ ليس متبايناً، عندئذٍ $\text{Ker } \varphi \neq \{0\}$ ومنه يوجد $h(x) \in \text{Ker } \varphi$ بحيث $h(x) \neq 0$ وبالتالي يكون $\varphi(h(x)) = h(a) = 0$ وهذا يبين لنا أنه يوجد $h(x) \in F[x]$ و $h(x) \neq 0$ من أجله $h(a) = 0$.

(2) $\Leftrightarrow$ (3). لنفرض أنه يوجد $h(x) \in F[x]$ بحيث $h(x) \neq 0$ من أجله $h(a) = 0$ ، ولنفرض أن $\partial h(x) = n$ عندئذٍ $h(x) = \sum_{i=0}^n c_i x^i$ حيث $c_i \in F$ لأجل جميع القيم $0 \leq i \leq n$ وبما أن $h(x) \neq 0$ فإن العناصر $c_0, c_1, c_2, \dots, c_n$ ليست جميعها معدومة. من جهة أخرى، بما أن $h(a) = 0$ نجد أن $\sum_{i=0}^n c_i a^i = 0$. لنبرهن الآن على أن $n \geq 1$.

لنفرض أن $n = 0$ عندئذٍ يكون $h(x) = c_0$ ، وبما أن $0 = h(a) = c_0$ نحصل على

تناقض، وهذا يبين لنا أن $n \geq 1$.

(3) $\Leftarrow$ (1). لنفرض أنه يوجد في F عناصر $c_0, c_1, c_2, \dots, c_n$ حيث $n \geq 1$ ليست

جميعها معدومة تحقق $\sum_{i=0}^n c_i a^i = 0$ عندئذ يكون $g(x) = \sum_{i=0}^n c_i x^i \in F[x]$ وأن $0 \neq g(x)$:

$$\phi(g(x)) = g(a) = \sum_{i=0}^n c_i a^i = 0$$

ومنه فإن $g(x) \in \text{Ker } \phi$ وبالتالي تكون $\text{Ker } \phi \neq \{0\}$ وهذا يبين لنا أن التشاكل $\phi: F[x] \rightarrow K$ ليس متبايناً. $\diamond$

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة التعريف الآتي:

تعريف.

ليكن الحقل K تمديداً للحقل F .

- نقول عن العنصر $a \in K$ إنه عنصر جبري فوق الحقل F إذا وجدت حدودية

$f(x) \in F[x]$ حيث $0 \neq f(x)$ ، أو بمعنى آخر، نقول عن العنصر

$a \in K$ إنه جبرياً فوق F إذا وجدت عناصر $c_0, c_1, c_2, \dots, c_n \in F$ حيث $n \geq 1$

ليست جميعها معدومة تحقق $\sum_{i=0}^n c_i a^i = 0$.

- ونقول عن التمديد K للحقل F إنه تمديد جبري إذا كان كل عنصر من الحقل K هو

عنصر جبري فوق الحقل F .

بالاعتماد على التعريف السابق يمكننا صياغة التمهيدية الآتية:

تمهيدية ٣-٣-٢.

ليكن F حقل. عندئذ أياً كان $a \in F$ فإن العنصر a هو عنصر جبري فوق الحقل F .

البرهان.

ليكن $a \in F$ ، عندئذ الحدودية $f(x) = x - a$ هي عنصر من الحلقة $F[x]$ وأن

$f(x) \neq 0$ ، بالإضافة لذلك فإن $f(a) = 0$ وحسب التعريف نجد أن العنصر a هو

عنصر جبري فوق الحقل F . $\diamond$

نأتي الآن إلى دراسة المبرهنة الهامة الآتية:

مبرهنة ٣-٣-٣.

ليكن الحقل K تمديداً للحقل F وليكن $a \in K$ عنصراً جبرياً فوق F . عندئذ توجد حدودية $p(x) \in F[x]$ أولية في $F[x]$ من أجلها $p(a) = 0$.
البرهان.

لنفرض أن العنصر $a \in K$ عنصر جبري فوق الحقل F ، عندئذ حسب التعريف يوجد في $F[x]$ عنصر واحد على الأقل $f(x) \in F[x]$ من أجله $f(a) = 0$. لنفرض أن $\partial f(x) = m$ عندئذ حسب المبرهنة (٣-٣-١) فإن $m \geq 1$. لنأخذ المجموعة:

$$M = \{\lambda(x) : \lambda(x) \in F[x]; \partial \lambda(x) \geq 1, \lambda(a) = 0\}$$

ف نجد أن المجموعة M غير خالية لأن $f(x) \in M$. لنأخذ المجموعة:

$$\mathfrak{N} = \{s : s \in N^*; s = \partial \lambda(x), \forall \lambda(a) \in M\}$$

ف نجد أن المجموعة $\mathfrak{N}$ هي مجموعة جزئية من N^* وغير خالية، لأن $m \in \mathfrak{N}$ ، ومنه فإن المجموعة $\mathfrak{N}$ تحوي عنصراً أصغر وليكن n ، إن $n \geq 1$.

من جهة أخرى، بما أن $n \in \mathfrak{N}$ فإنه توجد حدودية $p(x) \in M \subseteq F[x]$ بحيث $0 \neq p(x)$ بحيث $\partial p(x) = n$ وبما أن $p(x) \in M$ فإن $p(a) = 0$. لنبرهن الآن على أن الحدودية $p(x)$ هي حدودية أولية في $F[x]$. بما أن $\partial p(x) = n \geq 1$ فإنه حسب المبرهنة (١-٢-٢) تكون الحدودية $p(x)$ غير قابلة للقلب في $F[x]$.

لنتكن $g(x), \mu(x) \in F[x]$ بحيث $p(x) = g(x) \cdot \mu(x)$ عندئذ $g(x) \neq 0$ و $\mu(x) \neq 0$ وذلك لأن $p(x) \neq 0$. لنفرض جلاً أن كلا من $g(x)$ و $\mu(x)$ غير قابلين للقلب في $F[x]$ ، عندئذ حسب المبرهنة (١-٢-٢) فإن $\partial g(x) \geq 1$ و $\partial \mu(x) \geq 1$. وبما أن $\partial p(x) = \partial g(x) + \partial \mu(x)$ ينتج أن:

$$\partial p(x) \geq \partial g(x), \partial p(x) \geq \partial \mu(x)$$

من جهة أخرى، بما أن التطبيق $\varphi : F[x] \rightarrow K$ المعرف بالشكل الآتي: أيأ كان $f(x) \in F[x]$ فإن $\varphi(f(x)) = f(a)$ هو تشاكل حلقي نجد أن:

$$\varphi(p(x)) = \varphi(g(x) \cdot \mu(x)) = \varphi(g(x)) \cdot \varphi(\mu(x))$$

$$p(a) = g(a) \cdot \mu(a)$$

وبما أن $p(a) = 0$ وأن K حقل نجد أنه إما $g(a) = 0$ أو $\mu(a) = 0$. لنفرض أن $g(a) = 0$ ، أصبح لدينا $g(x) \in F[x]$ و $0 \neq g(x)$ وأن $\partial g(x) \geq 1$ كما أن $g(a) = 0$ و $\partial p(x) > \partial g(x)$ وهذا يناقض كون أن الحدودية $p(x)$ هي الحدودية ذات الدرجة الأصغر في $F[x]$ والتي من أجلها $p(a) = 0$ وهذا يبين لنا أنه إما $g(x)$ قابلة للقلب أو $\mu(x)$ قابلة للقلب في $F[x]$ ، مما سبق نجد أن الحدودية $p(x)$ أولية في $F[x]$. ◊

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة التعريف الآتي:

تعريف.

وجدنا حسب المبرهنة الأخيرة أنه إذا كان K تمديداً للحقل F وكان $a \in K$ عنصراً جبرياً فوق الحقل F عندئذ يوجد في الحلقة $F[x]$ حدودية $p(x) \neq 0$ أولية في $F[x]$ تحقق $p(a) = 0$ وهي الحدودية ذات الدرجة الأصغر من بين جميع الحدوديات $f(x) \in F[x]$ و $0 \neq f(x)$ والتي من أجلها $\partial f(x) > 0$ و $f(a) = 0$. نسمي هذه الحدودية بالحدودية الأصغرية للعنصر الجبري a فوق الحقل F .

واحدة من الخواص الهامة للحدودية الأصغرية نوردتها من خلال المبرهنة الآتية:

مبرهنة ٣-٣-٤.

ليكن الحقل K تمديداً للحقل F و $a \in K$ عنصر جبري فوق الحقل F ، ولتكن $p(x)$ هي الحدودية الأصغرية للعنصر a فوق F . إذا كانت $f(x) \in F[x]$ و $0 \neq f(x)$ بحيث $f(a) = 0$ عندئذ فإن $p(x)$ تقسم $f(x)$ في $F[x]$.

البرهان.

لنفرض أن $f(x) \in F[x]$ بحيث $f(a) = 0$ عندئذ حسب خوارزمية القسمة لأجل العنصرين $f(x), p(x)$ فإنه يوجد $q(x), r(x) \in F[x]$ تحقق

$$f(x) = q(x) \cdot p(x) + r(x)$$

حيث إما $r(x) = 0$ أو $\partial r(x) < \partial p(x)$. لنفرض جديلاً أن $r(x) \neq 0$ عندئذ يكون $\partial r(x) < \partial p(x)$. من جهة أخرى، بما أن التطبيق $\varphi: F[x] \rightarrow K$ المعروف بالشكل $\varphi(\lambda(x)) = \lambda(a)$ وذلك أيأ كان $\lambda(x) \in F[x]$ هو تشاكل حلقي نجد أن:

$$\begin{aligned}\varphi(f(x)) &= \varphi(q(x) \cdot p(x) + r(x)) = \varphi(q(x) \cdot p(x)) + \varphi(r(x)) = \\ &= \varphi(q(x)) \cdot \varphi(p(x)) + \varphi(r(x))\end{aligned}$$

ومنه يكون $f(a) = q(a) \cdot p(a) + r(a)$ وبالتالي فإن $r(a) = 0$.
أصبح لدينا $0 \neq r(x) \in F[x]$ و $\partial r(x) < \partial p(x)$ و $r(a) = 0$ وهذا يناقض كون
أن $p(x)$ هي الحدودية الأصغرية للعنصر الجبري a فوق الحقل F . مما سبق نجد أن
 $r(x) = 0$ وبالتالي يكون $f(x) = q(x) \cdot p(x)$ وهذا يبين لنا أن الحدودية $p(x)$
تقسم الحدودية $f(x)$ فوق F . ◊

خاصة هامة أخرى من خواص الحدودية الأصغرية لعنصر جبري نوردها من خلال
المبرهنة الآتية:

مبرهنة ٣-٣-٥.

ليكن الحقل K تمديداً للحقل F و $a \in K$ عنصر جبري فوق F . إذا كانت درجة
الحدودية الأصغرية للعنصر a فوق الحقل F تساوي n عندئذ يكون $[F(a) : F] = n$.
البرهان.

لنفرض أن العنصر $a \in K$ عنصر جبري فوق الحقل F ولنفرض أن $p(x) \in F[x]$
هي الحدودية الأصغرية للعنصر a فوق F وأن $\partial p(x) = n$. بما أن الحدودية $p(x)$
أولية فوق F وأن العنصر a هو صفر للحدودية $p(x)$ عندئذ حسب المبرهنة (٣-١-٦)
أيضاً كان $b \in F(a)$ فإن العنصر b يمكن التعبير عنه بصورة وحيدة على النحو
الآتي:

$$b = c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1a + c_0$$

حيث $c_{n-1}, c_{n-2}, \dots, c_1, c_0 \in F$.

وهكذا نجد أن المجموعة $\{1, a, a^2, \dots, a^{n-1}\} \subseteq F(a)$ تشكل قاعدة للحقل $F(a)$
فوق F ومؤلفة من n عنصر، وهذا يبين لنا أن $[F(a) : F] = n$. ◊

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة النتيجة الهامة الآتية:

نتيجة.

إذا كان الحقل K تمديداً للحقل F و $a \in K$ عنصر جبري فوق F ، عندئذ يكون الحقل $F(a)$ تمديداً منتهياً للحقل F . ◊

أيضاً بالاعتماد على المبرهنة الأخيرة يمكننا صياغة التعريف الآتي:

تعريف.

ليكن الحقل K تمديداً للحقل F و $a \in K$ عنصر جبري فوق F . إذا كان $[F(a):F] = n$ فإننا سنقول إن للعنصر a درجة تساوي n فوق F ، أو بمعنى آخر، نسمي n بدرجة العنصر a فوق F .

نأتي الآن إلى دراسة المبرهنة الهامة الآتية:

مبرهنة ٦-٣-٣.

ليكن F حقلاً. عندئذ كل تمديد منته للحقل F هو تمديد جبري للحقل F .

البرهان.

لنفرض أن الحقل K تمديد منته للحقل F وأن $[K:F] = n$ وليكن $a \in K$ عندئذ تكون المجموعة $\{1, a, a^2, \dots, a^{n-1}, a^n\} \subset K$ مرتبطة خطياً فوق الحقل F وبالتالي توجد عناصر $c_n, c_{n-1}, c_{n-2}, \dots, c_1, c_0 \in F$ ليست جميعها معدومة تحقق

$$\sum_{i=0}^n c_i a^i = 0$$

بما أن العناصر $c_n, c_{n-1}, c_{n-2}, \dots, c_1, c_0 \in F$ ليست جميعها معدومة فإن:

$$f(x) = \sum_{i=0}^n c_i x^i \in F[x]$$

وأن $f(x) \neq 0$ كما أن $f(a) = \sum_{i=0}^n c_i a^i = 0$ وحسب التعريف نجد أن العنصر a هو عنصر جبري فوق الحقل F وبالتالي يكون الحقل K تمديداً جبرياً للحقل F . ◊

ملاحظة.

إن عكس المبرهنة الأخيرة غير صحيح، أي أنه ليس كل تمديد جبري هو تمديد منته، ويعود السبب في ذلك إلى أنه إذا كان الحقل K تمديداً جبرياً للحقل F فإن كل

عنصر $a \in K$ ذو درجة منتهية فوق F وذلك حسب التعريف الأخير، بينما لو أخذنا الحقل $Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots)$ فنجد أن هذا الحقل هو تمديد جبري للحقل Q ولكنه يحوي عناصر لأجل كل درجة فوق Q .

نأتي الآن إلى دراسة خواص التمديدات الجبرية والبدائية سوف تكون مع المبرهنة الآتية:

مبرهنة ٣-٣-٧.

ليكن الحقل K تمديداً للحقل F و $a \in K$. الشرط اللازم والكافي كي يكون العنصر a جبرياً فوق الحقل F هو أن يكون الحقل $F(a)$ تمديداً منتهياً للحقل F .
البرهان.

لنلزم الشرط. لنفرض أن العنصر a هو عنصر جبري فوق الحقل F ولتكن $p(x) \in F[x]$ الحدودية الأصغرية للعنصر الجبري a فوق F وأن $\partial p(x) = n$ ، عندئذ حسب المبرهنة (٣-٣-٥) يكون $[F(a) : F] = n$ وهذا يبين لنا أن الحقل $F(a)$ هو تمديد منته للحقل F .

كفاية الشرط. لنفرض أن الحقل $F(a)$ هو تمديد منته للحقل F ، عندئذ حسب المبرهنة (٣-٣-٦) يكون الحقل $F(a)$ تمديداً جبرياً للحقل F وبالتالي يكون العنصر a جبرياً فوق الحقل F . ♦

خاصة هامة أخرى للتمديدات الجبرية نردها من خلال المبرهنة الآتية:

مبرهنة ٣-٣-٨.

ليكن الحقل K تمديداً جبرياً للحقل E و E تمديداً جبرياً للحقل F ، عندئذ يكون K تمديداً جبرياً للحقل F .
البرهان.

بما أن الحقل K هو تمديد للحقل E وأن الحقل E هو تمديد للحقل F عندئذ يكون K تمديداً للحقل F . ليكن $a \in K$ عندئذ فإن a هو عنصر جبري فوق الحقل E . لنفرض أن $p(x) \in F[x]$ هي الحدودية الأصغرية للعنصر الجبري a فوق E وأن

$\partial p(x) = n$ عندئذ $p(x) = \sum_{i=0}^n b_i x^i$ حيث $b_0, b_1, b_2, \dots, b_n \in E$. لنضع:

$$F_0 = F(b_0), \quad F_1 = F_0(b_1), \quad F_2 = F_1(b_2), \dots, F_n = F_{n-1}(b_n)$$

أصبح لدينا $F \subseteq F_0 \subseteq F_1 \subseteq \dots \subseteq F_{n-1} \subseteq F_n$.

بما أن $b_0 \in E$ وأن الحقل E هو تمديد جبري للحقل F فإن العنصر b_0 هو عنصر جبري فوق F وحسب المبرهنة (٧-٣-٣) يكون الحقل $F_0 = F(b_0)$ تمديداً منتهياً للحقل F . أيضاً، بما أن $b_1 \in E$ وأن E هو تمديد جبري للحقل F فإن العنصر b_1 هو عنصر جبري فوق F وبالتالي فوق الحقل F_0 لأن $F \subseteq F_0 \subseteq E$ وحسب المبرهنة (٣-٣-٣) F_0 يكون الحقل $F_1 = F_0(b_1)$ تمديداً منتهياً للحقل F_0 .

وهكذا نجد أنه أياً كان $i = 1, 2, \dots, n$ فإن $b_i \in E$ وبما أن الحقل E هو تمديد جبري للحقل F فإن العنصر b_i هو عنصر جبري فوق الحقل F وبالتالي جبري فوق F_{i-1} وذلك لأن $F \subseteq F_{i-1} \subseteq E$ وحسب المبرهنة (٧-٣-٣) يكون الحقل $F_i = F_{i-1}(b_i)$ تمديداً منتهياً للحقل F_{i-1} . أصبح لدينا $F_0 \subseteq F_1 \subseteq \dots \subseteq F_{i-1} \subseteq F_i \subseteq \dots \subseteq F_n$ وأن الحقل F_i هو تمديد منته للحقل F_{i-1} وحسب المبرهنة (٣-٢-٣) يكون الحقل F_n تمديداً منتهياً للحقل F_0 . وبما أن الحقل F_0 هو تمديد منته للحقل F فإنه حسب المبرهنة (١-٢-٣) يكون الحقل F_n تمديداً منتهياً للحقل F .

من جهة أخرى، بما أنه أياً كان $i = 0, 1, 2, \dots, n$ فإن $b_i \in F_i$ وبالتالي فإن

$$p(a) = 0 \text{ وتحقق } o \neq p(x) = \sum_{i=0}^n b_i x^i \in F_n[x] \text{ وهكذا نجد أن } b_0, b_1, \dots, b_n \in F_n$$

وهذا يبين لنا أن العنصر a هو عنصر جبري فوق الحقل F_n وحسب المبرهنة (٣-٣-٣) $F_n(a)$ يكون الحقل $F_n(a)$ هو تمديد منته للحقل F_n وبما أن الحقل F_n هو تمديد منته للحقل F وحسب المبرهنة (١-٢-٣) يكون الحقل $F_n(a)$ هو تمديد منته للحقل F وحسب المبرهنة (٧-٣-٣) يكون العنصر a جبرياً فوق F وهذا يبين لنا أن الحقل K هو تمديد جبري للحقل F . ♦

خاصة جديدة أخرى للتمديدات الجبرية وعلاقتها بالتمديدات المنتهية نوردتها من خلال

المبرهنة الآتية:

مبرهنة ٣-٣-٩.

ليكن الحقل E تمديداً للحقل F . الشرط اللازم والكافي كي يكون التمديد E للحقل F تمديداً منتهياً هو أن يكون $E = F(a_1, a_2, \dots, a_n)$ حيث $a_1, a_2, \dots, a_n \in E$ هي عناصر جبرية فوق F .
البرهان.

لزوم الشرط. لنفرض أن الحقل E هو تمديد منته للحقل F وأن $[E : F] = n$ عندئذ توجد قاعدة $\{a_1, a_2, \dots, a_n\} \subseteq E$ للحقل E فوق F . بما أن $\{a_1, a_2, \dots, a_n\} \subseteq E$ فإن $F(a_1, a_2, \dots, a_n) \subseteq E$.
من جهة أخرى، ليكن $y \in E$ عندئذ فإن العنصر y يكتب بشكل وحيد على النحو:
 $y = c_1 a_1 + c_2 a_2 + \dots + c_n a_n$ حيث $c_1, c_2, \dots, c_n \in F$ ومنه نجد أن:
 $y = c_1 a_1 + c_2 a_2 + \dots + c_n a_n \in F(a_1, a_2, \dots, a_n)$
وهذا يبين لنا أن $E \subseteq F(a_1, a_2, \dots, a_n)$ ، مما سبق نجد أن $E = F(a_1, a_2, \dots, a_n)$.
وبما أن E هو تمديد منته للحقل F فإنه حسب المبرهنة (٣-٣-٦) يكون E تمديداً جبرياً للحقل F وبالتالي فإن العناصر $a_1, a_2, \dots, a_n \in E$ هي عناصر جبرية فوق الحقل F .

كفاية الشرط. لنفرض أن $a_1, a_2, \dots, a_n \in E$ هي عناصر جبرية فوق الحقل F وأن $E = F(a_1, a_2, \dots, a_n)$.

لنضع $F_1 = F(a_1)$, $F_2 = F_1(a_2)$, $F_3 = F_2(a_3)$, $\dots$, $F_n = F_{n-1}(a_n)$ فنجد أن $F \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_n = E$. من جهة أخرى، بما أن العنصر a_1 هو عنصر جبري فوق F فإنه حسب المبرهنة (٣-٣-٧) يكون الحقل $F_1 = F(a_1)$ تمديداً منتهياً للحقل F . كذلك بما أن العنصر a_2 جبري فوق F فإن العنصر a_2 هو عنصر جبري فوق F_1 لأن $F \subseteq F_1$ وبالتالي حسب المبرهنة (٣-٣-٧) يكون $F_2 = F_1(a_2)$ تمديداً منتهياً للحقل F_1 . وبما أن العنصر a_i جبري فوق الحقل F فإن العنصر a_i يكون جبرياً فوق الحقل F_{i-1} لأن $F \subseteq F_{i-1}$ وبالتالي المبرهنة (٣-٣-٧) يكون الحقل $F_i = F_{i-1}(a_i)$ تمديداً منتهياً للحقل F_{i-1} وذلك لأجل جميع القيم $i = 1, 2, \dots, n$ حيث

$F_0 = F$. ومنه حسب المبرهنة (٣-٢-٣) يكون الحقل $F_n = E$ تمديداً منتهياً للحقل F . وحسب المبرهنة (٦-٣-٢) يكون الحقل E تمديداً جبرياً للحقل F .

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن الحقل K تمديداً للحقل F و $a_1, a_2, \dots, a_n \in K$ عناصر جبرية فوق الحقل F . عندئذ يكون الحقل $F(a_1, a_2, \dots, a_n)$ تمديداً جبرياً للحقل F .

البرهان.

لنفرض أن $a_1, a_2, \dots, a_n \in K$ عناصر جبرية فوق الحقل F ولنضع $E = F(a_1, a_2, \dots, a_n)$ فنجد أن $a_1, a_2, \dots, a_n \in E$ هي عناصر جبرية فوق الحقل F وحسب المبرهنة (٩-٣-٣) يكون E تمديداً جبرياً للحقل F .

إن النتيجة الأخيرة يمكن صياغتها على الشكل الآتي: إذا كان الحقل K تمديداً للحقل F وكان K مولداً بعدد منته من العناصر الجبرية فوق F فإن الحقل K يكون تمديداً جبرياً للحقل F .

نأتي الآن لدراسة مجموعة العناصر الجبرية فوق حقل ما.

تعريف.

ليكن الحقل K تمديداً للحقل F . نسمي المجموعة:

$$\bar{F} = \{a : a \in K; \text{ حيث } a \text{ عنصر جبري فوق الحقل } F\}$$

العلاقة الجبرية للحقل F في الحقل K .

البنية الجبرية لمجموعة العناصر الجبرية فوق حقل نوردها من خلال المبرهنة الآتية:

مبرهنة ٣-٣-١٠.

ليكن الحقل K تمديداً للحقل F . العلاقة الجبرية $\bar{F}$ للحقل F في الحقل K تشكل حقلاً جزئياً في K يحوي الحقل F .

البرهان.

واضح أن $\bar{F} \subseteq K$ كما أن $\bar{F} \neq \Phi$ لأن $0,1 \in \bar{F}$ ، وذلك لأن $f(x) = x \in F[x]$ و $0 \neq f(0) = 0$ ، أيضاً $g(x) = x-1 \in F[x]$ و $0 \neq g(1) = 0$.
 ليكن $a, b \in \bar{F}$ عندئذ $a, b \in K$ وأن كلاً من a و b هي عناصر جبرية فوق F .
 وحسب النتيجة الأخيرة، فإن الحقل $F(a, b)$ هو تمديد جبري للحقل F وأن $F(a, b) \subseteq K$. بما أن $a, b \in F(a, b)$ عندئذ فإن $a - b \in F(a, b)$ وهذا يبين لنا أن $a - b \in K$ وأن العنصر $a - b$ جبري فوق F وبالتالي فإن $a - b \in \bar{F}$.
 ليكن $c, d \in \bar{F}$ وأن $d \neq 0$ عندئذ $c, d \in K$ وأن كلاً من c و d هي عناصر جبرية فوق F . وحسب النتيجة الأخيرة، فإن الحقل $F(c, d)$ هو تمديد جبري للحقل F وأن $F(c, d) \subseteq K$. بما أن $c, d \in F(c, d)$ عندئذ فإن $c \cdot d^{-1} \in F(c, d)$ وبالتالي يكون $c \cdot d^{-1} \in K$ وهذا يبين لنا أن $c \cdot d^{-1} \in K$ وأن العنصر $c \cdot d^{-1}$ جبري فوق F وبالتالي فإن $cd^{-1} \in \bar{F}$. كما أن $F \subseteq \bar{F}$ لأن كل عنصر من الحقل F هو عنصر جبري فوق F وذلك حسب التمهيدية (٣-٣-٢). ◊

تعريف.

ليكن الحقل K تمديداً للحقل F . نقول عن الحقل F إنه مغلق جبرياً في K إذا كان $\bar{F} = F$ ، حيث $\bar{F}$ هي الغلابة الجبرية للحقل F في K .

لندرس الآن واحدة من الحالات التي يكون فيها حقل ما مغلقاً جبرياً وذلك من خلال المبرهنة الآتية:

مبرهنة ٣-٣-١١.

ليكن F حقل. إذا كانت درجة كل حدودية أولية في $F[x]$ تساوي الواحد فإن الحقل F يكون مغلقاً جبرياً.

البرهان.

ليكن K تمديداً للحقل F وأن $\bar{F}$ هي الغلابة الجبرية للحقل F في K ، حسب المبرهنة (٣-٣-١٠) فإن $F \subseteq \bar{F}$. ليكن $a \in \bar{F}$ عندئذ $a \in K$ ، كما أن العنصر a جبري فوق F . لنفرض أن $p(x) \in F[x]$ هي الحدودية الأصغرية للعنصر a فوق الحقل F ،

عندئذ فإن $p(x)$ هي حدودية أولية فوق F وحسب الفرض فإن $\partial p(x) = 1$ وبالتالي يكون $p(x) = b_1x + b_0$ حيث $b_1, b_0 \in F$ ، وأن $b_1 \neq 0$ ، بالإضافة لذلك فإن $p(a) = 1$ ومنه يكون $b_1a + b_0 = 0$ وبالتالي $a = b_0b_1^{-1} \in F$ وهذا يبين لنا أن $\bar{F} \subseteq F$. مما سبق نجد أن $F = \bar{F}$ وبالتالي الحقل F مغلق جبرياً. ◊

تبين لنا المبرهنة الآتية بعضاً من الخواص المهمة للحقول المغلقة جبرياً:

مبرهنة ٣-٣-١٢.

لأجل أي حقل F الشروط الآتية متكافئة:

١ - كل حدودية أولية في $F[x]$ درجتها تساوي الواحد.

٢ - الحقل F مغلق جبرياً.

٣ - إذا كان K تمديداً منتهياً للحقل F فإن $K = F$.

البرهان.

(1) $\Leftrightarrow$ (2). حسب المبرهنة (١١-٣-٢).

(2) $\Leftrightarrow$ (3). لنفرض أن K تمديد منته للحقل F عندئذ فإن $F \subseteq K$.

من جهة أخرى، حسب المبرهنة (٦-٣-٣) يكون K تمديداً جبرياً للحقل F ، ومنه أيّاً كان $a \in K$ فإن العنصر يكون جبرياً فوق F وبالتالي فإن $a \in \bar{F} = F$ ومنه نجد أن $K \subseteq F$ ، وهذا يبين لنا أن $K = F$.

(3) $\Leftrightarrow$ (1). لتكن $p(x) \in F[x]$ حدودية أولية فوق F ، عندئذ حسب المبرهنة (٣-٣-٣)

(٤-١) يوجد تمديد K للحقل F يحوي صفراً للحدودية $p(x)$ وليكن a . إن العنصر a جبري فوق F وحسب المبرهنة (٥-٣-٣) فإن $\partial p(x) = [F(a) : F]$ وهذا يبين أن

$F(a)$ تمديد منته للحقل F وحسب الفرض يكون $F(a) = F$ ومنه نجد أن:

$$\partial p(x) = [F(a) : F] = [F : F] = 1$$

لنورد مبرهنة أخرى تتضمن خواص جديدة للحقول المغلقة جبرياً:

مبرهنة ٣-٣-١٣.

لأجل أي حقل F الشروط الآتية متكافئة:

١ - الحقل F مغلق جبرياً.

٢ - كل حدودية في $F[x]$ درجتها أكبر من الصفر تملك صفراً واحداً على الأقل في F .

٣ - كل حدودية في $F[x]$ درجتها أكبر من الصفر تكتب على شكل جداء منته لحدوديات من $F[x]$ درجة كل منها تساوي الصفر.

البرهان.

(1) $\Leftrightarrow$ (2). لنفرض أن الحقل F مغلق جبرياً، ولتكن $f(x) \in F[x]$ وأن $\partial f(x) > 0$ عندئذ حسب المبرهنة (٣-١-٥) يوجد تمديد K للحقل F يحوي صفراً للحدودية $f(x)$ وليكن a . إن العنصر a جبري فوق F . لنفرض أن $p(x)$ هي الحدودية الأصغرية للعنصر a فوق F وحسب المبرهنة (٣-٣-٥) يكون $[F(a) : F] = \partial p(x)$ وهذا يبين أن الحقل $F(a)$ تمديد منته للحقل F وحسب المبرهنة (٣-٣-١٢) يكون $F(a) = F$ وبالتالي يكون $a \in F$.

(2) $\Leftrightarrow$ (3). لتكن $g(x) \in F[x]$ وأن $\partial g(x) = n > 0$. البرهان بالاستقراء حسب n . - إذا كانت $n = 1$ عندئذ $g(x) = a_1x + a_0$ حيث $a_1, a_0 \in F$ وأن $a_1 \neq 0$ وبذلك يتم المطلوب.

- لنفرض أن القضية صحيحة لأجل كل حدودية في $F[x]$ درجتها أكبر من الصفر وأصغر من n . لدينا حسب الفرض أن الحدودية $g(x)$ تملك صفراً واحداً على الأقل في F وليكن a_1 ، ومنه فإن $x - a_1 \in F[x]$ وتقسم $g(x)$ في $F[x]$ وبالتالي توجد $q(x)$ في $F[x]$ بحيث $g(x) = (x - a_1) \cdot q(x)$ ومنه فإن:

$$\partial q(x) = \partial g(x) - 1 = n - 1 < n$$

وحسب الفرض الاستقرائي فإن $q(x)$ تكتب على الشكل:

$$q(x) = h_2(x) \cdot h_3(x) \cdots h_n(x)$$

حيث $h_i(x) \in F[x]$ وأن $\partial h_i(x) = 1$ أيأ كان $2 \leq i \leq n$ ، ومنه فإن

$$g(x) = (x - a_1) \cdot h_2(x) \cdot h_3(x) \cdots h_n(x)$$

(3) $\Leftrightarrow$ (1). لنفرض أن $\bar{F}$ الغلاقة الجبرية للحقل F ، لدينا $F \subseteq \bar{F}$. ليكن $b \in \bar{F}$

عندئذ b هو عنصر جبري فوق F . لتكن أن $p(x) \in F[x]$ هي الحدودية الأصغرية

للعنصر b فوق F وأن $\partial p(x) = m$ وحسب الفرض فإن $p(x)$ تكتب بالشكل:

$$p(x) = p_1(x) \cdot p_2(x) \cdots p_m(x)$$

حيث $p_i(x) \in F[x]$ وأن $\partial p_i(x) = 1$ أيّاً كان $1 \leq i \leq m$ ، وبما أن $p(b) = 0$ وأن $F(b)$ حقل نجد فإنه يوجد دليل واحد على الأقل $1 \leq j \leq m$ لأجله $p_j(b) = 0$ وبما أن $\partial p_j(x) = 1$ فإن $p_j(x) = c_1x + c_0$ حيث $c_1, c_0 \in F$ وأن $c_1 \neq 0$ ، ولما كان $p_j(b) = 0$ نجد أن $c_1b + c_0 = 0$ ومنه فإن $c_1b + c_0 \in F$ وهذا يبين لنا أن $\bar{F} \subseteq F$ ومنه فإن $\bar{F} = F$ وبالتالي الحقل F مغلق جبرياً. ◊

تمهيدية ٣-٣-١٤.

ليكن الحقل K تمديداً جبرياً للحقل F . إذا كان L حقلاً جزئياً في K ويحوي F ، عندئذ يكون الحقل K تمديداً جبرياً للحقل L .
البرهان.

لنفرض أن الحقل K تمديد جبري للحقل F وأن $F \subseteq L \subseteq K$. ليكن $a \in K$ عندئذ فإن a هو عنصر جبري فوق F ومنه توجد $h(x) \in F[x]$ $0 \neq h(x)$ بحيث $h(a) = 0$ ، ولما كان $F \subseteq L$ فإن $F[x] \subseteq L[x]$ وبالتالي فإن $h(x) \in L[x]$ $0 \neq h(x)$ وأن $h(a) = 0$ وهذا يبين أن a عنصر جبري فوق L ، ومنه نجد أن الحقل K هو تمديد جبري للحقل L . ◊

مبرهنة ٣-٣-١٥.

ليكن الحقل K تمديداً للحقل F وأن $a \in K$ عنصر جبري فوق F . لنفرض أن $f(x) \in F[x]$ $0 \neq f(x)$ وأن $f(a) = 0$. الشروط الآتية متكافئة:

$$1 - [F(a) : F] \leq \partial f(x)$$

$$2 - \text{الحدودية } f(x) \text{ تكون أولية فوق } F \text{ عندما وفقط عندما } [F(a) : F] = \partial f(x)$$

$$3 - \text{إذا كان } E \text{ تمديداً آخر للحقل } F \text{ عندئذ يكون:}$$

$$[E(a) : E] \leq [F(a) : F]$$

البرهان.

١ - لما كان العنصر $a \in K$ جبرياً فوق F ، لنفرض أن $g(x)$ الحدودية الأصغرية

للعنصر a فوق F ، عندئذ $g(x) \in F[x]$ وحسب المبرهنة (٣-٣-٥) نجد أن:

$$[F(a):F] = \partial g(x)$$

من جهة أخرى، لما كان $f(a)=0$ نجد حسب المبرهنة (٣-٣-٤) أن $g(x)$ تقسم $f(x)$ في $F[x]$ ومنه فإن $\partial g(x) \leq \partial f(x)$ ، مما سبق نجد أن:

$$[F(a):F] \leq \partial f(x)$$

٢ - لزوم الشرط. لنفرض أن الحدودية $f(x)$ أولية فوق F . لما كان $f(a)=0$ نجد أن $f(x)$ هي الحدودية الأصغرية للعنصر a فوق F وحسب المبرهنة (٣-٣-٥) نجد أن $[F(a):F] = \partial f(x)$.

كفاية الشرط. لنفرض أن $[F(a):F] = \partial f(x)$. لما كان $a \in K$ عنصراً جبرياً فوق F ، لنفرض أن $g(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F . لما كان $f(a)=0$ نجد أن $g(x)$ تقسم $f(x)$ في $F[x]$ ومنه توجد $\lambda(x) \in F[x]$ بحيث:

$$f(x) = g(x) \cdot \lambda(x)$$

من جهة أخرى، لما كانت $g(x)$ الحدودية الأصغرية للعنصر a فوق F فإنه حسب المبرهنة (٣-٣-٥) فإن $[F(a):F] = \partial g(x)$ وحسب الفرض نجد أن:

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

وبالتالي يكون $\partial \lambda(x) = 0$ ومنه فإن $\lambda(x) = b$ حيث $b \in F$ و $b \neq 0$ وهكذا نجد أن:

$$f(x) = g(x) \cdot b$$

وبالتالي يكون $g(x) = f(x) \cdot b^{-1}$ ولما كانت الحدودية $g(x)$ أولية فوق F فإنه حسب التمهيدية (١-٢-٦) تكون الحدودية $f(x)$ أولية فوق F .

٣ - لنفرض أن $h(x) \in E[x]$ الحدودية الأصغرية للعنصر a فوق E ولنفرض أيضاً أن $g(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F ، لما كان $F \subseteq E$ نجد أن $g(x) \in E[x]$ ومنه فإن $h(x)$ تقسم $f(x)$ في $E[x]$ وبالتالي فإن $\partial h(x) \leq \partial g(x)$ وهكذا نجد أن:

$$\diamond. [E(a):E] = \partial h(x) \leq \partial g(x) = [F(a):F]$$

تعريف.

ليكن F حقلاً و $f(x) \in F[x]$ درجتها تساوي n . لنفرض أن $f(x) = \sum_{i=0}^n a_i x^i$ حيث $a_i \in F$ من أجل كل $1 \leq i \leq n$. نقول عن الحدودية $f(x)$ إنها وحيدة إذا كان $a_n = 1$.

مبرهنة ٣-٣-١٦.

ليكن الحقل K تمديداً للحقل F وليكن $a \in K$ عنصراً جبرياً فوق F . عندئذ توجد حدودية أولية وحيدة $f(x) \in F[x]$ لأجلها $f(a) = 0$.

البرهان.

لنفرض أن العنصر $a \in K$ جبري فوق F ، عندئذ حسب المبرهنة (٣-٣-٣) توجد حدودية أولية $p(x) \in F[x]$ لأجلها $p(a) = 0$. لنفرض أن $\partial p(x) = n$ ، عندئذ يكون

$$p(x) = \sum_{i=0}^n b_i x^i : b_i \in F, \forall 1 \leq i \leq n$$

لما كانت $\partial p(x) = n$ نجد أن $b_n \neq 0$. لنأخذ الحدودية $f(x) = b_n^{-1} \cdot p(x)$ فنجد أن $f(x) \in F[x]$ وأن $\partial p(x) = \partial f(x) = n$ ، كما أن $f(a) = 0$ ، فضلاً عن ذلك فإن $f(x)$ حدودية وحيدة، لأن:

$$f(x) = x^n + b_n^{-1} \cdot b_{n-1} x^{n-1} + \cdots + b_n^{-1} \cdot b_1 x + b_n^{-1} \cdot b_0$$

ولما كانت الحدودية $p(x) = b_n \cdot f(x)$ أولية فوق F فإنه حسب التمهيدية (١-٢-٦) تكون الحدودية $f(x)$ أولية فوق F . وهكذا نجد أن $f(x) \in F[x]$ حدودية أولية وواحدة فوق F لأجلها $f(a) = 0$. لنبرهن على أنها وحيدة.

لتكن $g(x) \in F[x]$ حدودية أولية وواحدة فوق F لأجلها $g(a) = 0$ ، لما كانت الحدودية $f(x)$ أولية فوق F وأن $f(a) = 0$ نجد أن $f(x)$ تقسم $g(x)$ في $F[x]$ ومنه توجد حدودية $h(x) \in F[x]$ بحيث $0 \neq h(x)$ و $g(x) = f(x) \cdot h(x)$ ، ولما كانت الحدودية $g(x)$ أولية وأن $f(x)$ غير قابلة للقلب في $F[x]$ نجد أن الحدودية $h(x)$ قابلة للقلب في $F[x]$ ومنه فإن $\partial h(x) = 0$ ، أي أن $h(x) = c$ حيث $0 \neq c \in F$ ومنه نجد أن $g(x) = c \cdot f(x)$ ولما كانت كل من الحدوديتين $f(x)$ و $g(x)$ وحيدة نجد أن $f(x) = g(x)$.

مبرهنة ٣-٣-١٧.

لتكن أعداداً أولية مختلفة. عندئذ:

$$1 - [Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}) : Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}})] = 2$$

$$2 - [Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}) : Q] = 2^n$$

$$3 - \sqrt{p_n} \notin Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}})$$

البرهان.

$$1 - \text{نفرض أن } K = Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}})$$

لما كان العنصر $\sqrt{p_n} \in K(\sqrt{p_n})$ صفراً للحدودية $K[x]$ $x^2 - \sqrt{p_n} \in K[x]$ وأن الحدودية أولية فوق K حسب معيار إيرنشتاين نجد أن $x^2 - p_n$ هي الحدودية الأصغرية للعنصر $\sqrt{p_n}$ فوق K ومنه فإن:

$$[K(\sqrt{p_n}) : K] = \partial(x^2 - p_n) = 2$$

$$2 - \text{سوف نورد البرهان بالاستقراء حسب } n.$$

من أجل $n=1$. إن $[Q(\sqrt{p_1}) : Q] = 2$ وذلك لأن العنصر $\sqrt{p_1}$ هو صفر للحدودية $x^2 - p_1 \in Q[x]$ ، ولما كانت الحدودية $x^2 - p_1$ أولية فوق Q وذلك حسب معيار إيرنشتاين نجد أن $x^2 - p_1$ هي الحدودية الأصغرية للعنصر $\sqrt{p_1}$ فوق Q وهذا يبين أن $[Q(\sqrt{p_1}) : Q] = 2$.

نفرض أن القضية صحيحة لأجل $n-1$. لدينا:

$$Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}}) \subseteq Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$$

ولدينا حسب (١) أن:

$$[Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}) : Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}})] = 2$$

وهذا يبين أن الحقل $Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$ هو تمديد منته للحقل

$$Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}})$$

ولدينا أيضاً حسب الفرض الاستقرائي أن:

$$[Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}}) : Q] = 2^{n-1}$$

وهذا يبين أن الحقل $Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}})$ هو تمديد منته للحقل Q ومنه نجد

أن الحقل $Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$ هو تمديد منتهي للحقل Q وبالتالي يكون:

$$\begin{aligned} [Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}) : Q] &= \\ &= [Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}) : Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}})] \cdot \\ &\quad \cdot [Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}}) : Q] = 2 \cdot 2^{n-1} = 2^n \end{aligned}$$

٣ - لنفرض جدلاً أن $\sqrt{p_n} \in Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}})$ عندئذ يكون:

$$Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}) = Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}})$$

وهذا يناقض (١)، ومنه نجد أن $\sqrt{p_n} \notin Q(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{n-1}})$ ♦

تمارين محلولة (٣)

١ - أثبت أن $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$.

الحل.

بما أن $Q(\sqrt{2}, \sqrt{3})$ حقل وأن $\sqrt{2}, \sqrt{3} \in Q(\sqrt{2}, \sqrt{3})$ فإن :

$$\sqrt{2} + \sqrt{3} \in Q(\sqrt{2}, \sqrt{3})$$

وحسب التعريف نجد أن $Q(\sqrt{2} + \sqrt{3}) \subseteq Q(\sqrt{2}, \sqrt{3})$.

من جهة أخرى، بما أن $Q(\sqrt{2} + \sqrt{3})^3 \subseteq Q(\sqrt{2} + \sqrt{3})$ فإن :

$$Q(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{5} \in Q(\sqrt{2} + \sqrt{3})$$

كذلك بما أن $9, \sqrt{2} + \sqrt{3} \in Q(\sqrt{2} + \sqrt{3})$ فإن :

$$9(\sqrt{2} + \sqrt{3}) = 9\sqrt{2} + 9\sqrt{3} \in Q(\sqrt{2} + \sqrt{3})$$

وبما أن $Q(\sqrt{2} + \sqrt{3})$ حقل فإن $-9\sqrt{2} - 9\sqrt{3} \in Q(\sqrt{2} + \sqrt{3})$ وهكذا نجد أن :

$$(11\sqrt{2} + 9\sqrt{5}) + (-9\sqrt{2} - 9\sqrt{3}) = 2\sqrt{2} \in Q(\sqrt{2} + \sqrt{3})$$

ولكون $1/2 \in Q$ نجد أن $1/2 \cdot 2 \cdot \sqrt{2} \in Q(\sqrt{2} + \sqrt{3})$ وبما أن :

$$\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2} \in Q(\sqrt{2} + \sqrt{3})$$

نجد أن $\sqrt{2}, \sqrt{3} \in Q(\sqrt{2} + \sqrt{3})$ وحسب التعريف يكون لدينا :

$$Q(\sqrt{2}, \sqrt{3}) \subseteq Q(\sqrt{2} + \sqrt{3})$$

مما سبق نجد أن $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$.

٢ - أثبت أن $Q(4-i) = Q(1+i)$.

الحل.

بما أن $Q(4-i)$ حقل وأن $4-i \in Q(4-i)$ فإن

$$-(4-i) = -4+i \in Q(4-i)$$

وبما أن $5, -4+i \in Q(4-i)$ نجد أن $1+i \in Q(4-i)$ وبالتالي

$$Q(1+i) \subseteq Q(4-i)$$

من جهة أخرى، بما أن $Q(1+i)$ حقل وأن $1+i \in Q(1+i)$ فإن:
 $-(1+i) \in Q(1+i)$. أيضاً بما أن $5, -(1+i) \in Q(1+i)$ نجد أن:

$$5 - (1+i) = 4 - i \in Q(1+i)$$

وبالتالي يكون $Q(4-i) \subseteq Q(1+i)$. مما سبق نجد أن $Q(4-i) = Q(1+i)$.

٣ - ليكن p عدداً أولياً ولتكن $Z_p[x]$ حلقة الحدوديات فوق الحقل Z_p . أثبت أن:

$$x^{p-1} - 1 = (x-1) \cdot (x-2) \cdot (x-3) \cdots (x-(p-1))$$

في $Z_p[x]$.

الحل.

بما أن p عدد أولي فإن الحلقة $Z_p = \{0,1,2,3,\dots,(p-1)\}$ حقلاً ومنه فإن كل عنصر من Z_p مغاير للصفر يملك مقلوباً في Z_p ، أي أن $U(p) = Z_p \setminus \{0\}$ ، وبما أن المجموعة $U(p)$ هي زمرة تبديلية بالنسبة لعملية الضرب بالمقاس p وأن مرتبتها $(p-1)$. كما أنه أيّاً كان $a \in U(p)$ فإن $a^{p-1} = 1$ ، أي أنه أيّاً كان $a \in Z_p$ $0 \neq a$ فإن $a^{p-1} = 1$ ومنه $a^{p-1} - 1 = 0$.

لنأخذ الحدودية $f(x) = x^{p-1} - 1$ فنجد أن $f(x) \in Z_p[x]$ وأنه أيّاً كان $a \in Z_p$ $0 \neq a$ فإن $f(a) = 0$ وهذا يبين لنا أن كل عنصر $a \in Z_p$ $0 \neq a$ هو صفر للحدودية $f(x)$ وبالتالي حسب التمهيدية (٦-١-١) فإن $x-a$ يقسم الحدودية $f(x)$ في $Z_p[x]$. بما أن $f(1) = 0$ فإن $x-1$ يقسم الحدودية $f(x)$ في $Z_p[x]$ ومنه يوجد $\varphi_1(x) \in Z_p[x]$ بحيث $f(x) = (x-1) \cdot \varphi_1(x)$ وبما أن $f(2) = 0$ نجد أن $\varphi_1(2) = 0$ ومنه فإن $x-2$ يقسم الحدودية $\varphi_1(x)$ في $Z_p[x]$ وبالتالي يوجد $\varphi_2(x) \in Z_p[x]$ بحيث يكون $\varphi_1(x) = (x-2) \cdot \varphi_2(x)$ ومنه فإن:

$$f(x) = (x-1) \cdot (x-2) \cdot \varphi_2(x)$$

وبما أن $f(3) = 0$ نجد أن $2 \cdot \varphi_2(3) = 0$ ومنه فإن $\varphi_2(3) = 0$ وذلك لأن Z_p حقل وبالتالي فإن $x-3$ يقسم الحدودية $\varphi_2(x)$ في $Z_p[x]$ وبالتالي يوجد $\varphi_3(x) \in Z_p[x]$ بحيث يكون $\varphi_2(x) = (x-3) \cdot \varphi_3(x)$ وبالتالي يكون:

$$f(x) = (x-1) \cdot (x-2) \cdot (x-3) \cdot \varphi_3(x)$$

نتابع بهذا الشكل إلى أن نصل إلى العنصر $a = p-1$ ومنه يكون:

$$\diamond \cdot x^{p-1} - 1 = (x-1) \cdot (x-2) \cdot (x-3) \cdots (x-(p-1))$$

٤ - ليكن الحقل E تمديداً للحقل F و $a \in E$. أثبت أن التطبيق $\varphi: F[X] \rightarrow F(a)$ المعروف بالشكل: أيّاً كان $f(x) \in F[X]$ فإن $\varphi(f(x)) = f(a)$ هو تشاكل حلقي. **الحل.**

ليكن $f(x), g(x) \in F[X]$ بحيث $f(x) = \sum_{i=0}^n a_i x^i$, $g(x) = \sum_{i=0}^m b_i x^i$ حيث $a_i, b_i \in F$ وذلك لأجل جميع القيم $0 \leq i \leq n, m$. بفرض أن $n \geq m$ عندئذ يكون:

$$\begin{aligned} \varphi(f(x) + g(x)) &= \varphi\left(\sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i\right) = \varphi\left(\sum_{i=0}^n (a_i + b_i) x^i\right) = \\ &= \sum_{i=0}^n (a_i + b_i) a^i = \sum_{i=0}^n a_i a^i + \sum_{i=0}^m b_i a^i = f(a) + g(a) = \\ &= \varphi(f(x)) + \varphi(g(x)) \end{aligned}$$

بالإضافة لذلك فإن:

$$\begin{aligned} \varphi(f(x) \cdot g(x)) &= \varphi\left(\left(\sum_{i=0}^n a_i x^i\right) \cdot \left(\sum_{i=0}^m b_i x^i\right)\right) = \varphi\left(\sum_{k=0}^{n+m} d_k x^k\right) = \\ &= \sum_{k=0}^{n+m} d_k a^k = \left(\sum_{i=0}^n a_i a^i\right) \cdot \left(\sum_{i=0}^m b_i a^i\right) = f(a) \cdot g(a) = \\ &= \varphi(f(x)) \cdot \varphi(g(x)) \end{aligned}$$

مما سبق نجد أن التطبيق φ هو تشاكل حلقي. $\diamond$

٥ - ليكن $a, b \in Q$ بحيث $b \neq 0$. أثبت أن الشرط اللازم والكافي كي يكون $Q(\sqrt{a}) = Q(\sqrt{b})$ هو أن يوجد $c \in Q$ من أجله $a = b \cdot c^2$. **الحل.**

لزوم الشرط. لنفرض أن $Q(\sqrt{a}) = Q(\sqrt{b})$. نميز حالتين:
الحالة الأولى: إذا كان $\sqrt{b} \in Q$ عندئذ يكون $Q(\sqrt{a}) = Q(\sqrt{b}) = Q$ وهذا يبين لنا أن $\sqrt{a} \in Q$ وبما أن $b \neq 0$ ، لنضع $c = \sqrt{a}/\sqrt{b}$ فنجد أن $c \in Q$ وأن $a = b \cdot c^2$.

الحالة الثانية: إذا كان $\sqrt{b} \notin Q$ عندئذ يكون $Q(\sqrt{b}) \neq Q$ وبالتالي يكون $Q(\sqrt{a}) \neq Q$ وهذا يبين لنا أن $\sqrt{a} \notin Q$ ، وبما أن $Q(\sqrt{a}) = Q(\sqrt{b})$ فإنه يوجد $r, c \in Q$ بحيث $\sqrt{a} = r + c\sqrt{b}$. إن $c \neq 0$ لأنه إذا كان $c = 0$ نجد أن $\sqrt{a} = r \in Q$ وهذا غير ممكن. كما أن $r = 0$ لأنه إذا كان $r \neq 0$ فإن:

$$a = \sqrt{a} \cdot \sqrt{a} = (r + c\sqrt{b}) \cdot (r + c\sqrt{b}) = r^2 + c^2b + 2rc\sqrt{b}$$

ومنه يكون:

$$\sqrt{b} = (a - (r^2 + c^2b)) / 2rc \in Q$$

وهذا غير ممكن. ومنه $r = 0$ وبالتالي $\sqrt{a} = c\sqrt{b}$ أي أن $a = b \cdot c^2$. كفاية الشرط. لنفرض أن $a = b \cdot c^2$ حيث $c \in Q$ فنجد أن $\sqrt{a} = c\sqrt{b} \in Q(\sqrt{b})$ ، عندئذ حسب المبرهنة (٣-١-٢) نجد أن $Q(\sqrt{a}) = Q(c\sqrt{b}) = Q(\sqrt{b})$.

٦ - أوجد جميع عناصر الحقل $\{a + bi : a, b \in Z_3; i^2 = -1\}$. $Z_3(i)$.
الحل.

لدينا $Z_3 = \{0, 1, 2\}$ ومنه فإن:

$$Z_3(i) = \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$$

٧ - لنأخذ الحقل $Z_2 = \{0, 1\}$ بالنسبة لعمليتي الجمع والضرب بالمقاس 2. ولنأخذ المجموعة:

$$Z_2(i) = \{a + bi : a, b \in Z_2 : i = \sqrt{-1}\}$$

والمطلوب:

١. أوجد جميع عناصر المجموعة $Z_2(i)$.

٢. أثبت أن المجموعة $Z_2(i)$ لا تشكل حقلاً.

الحل.

١ - $Z_2(i) = \{0, 1, i, 1+i\}$.

٢ - لنشكل جدولاً لعملية الضرب:

	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$1+i$
i	0	i	1	$1+i$
$1+i$	0	$1+i$	$1+i$	0

من خلال الجدول السابق نجد أن $(1+i)(1+i) = 0$ على الرغم من أن $(1+i) \neq 0$ وهذا يبين أن المجموعة $Z_2(i)$ لا تشكل حقلاً، لأن الحقل لا يحوي قواسم للصفر. ◊

٨ - أثبت أن الحقل $Q(\sqrt{2})$ يماثل الحقل $Q[x]/\langle x^2 - 2 \rangle$.

الحل.

بما أن $Q \subseteq Q(\sqrt{2})$ فإن الحقل $Q(\sqrt{2})$ هو تمديد للحقل Q وأن $\sqrt{2} \in Q(\sqrt{2})$ وحسب التمرين المحلول (٣-٤) فإن العلاقة $\varphi: Q[x] \rightarrow Q(\sqrt{2})$ المعرفة بالشكل الآتي: $\varphi(f(x)) = f(\sqrt{2})$ وذلك أيأ كان $f(x) \in Q[x]$ هو تشاكل حقيقي. من جهة أخرى، بما أن الحدودية $x^2 - 2 \in Q[x]$ أولية في $Q[x]$ فإنه حسب المبرهنة (١-٢-٧) يكون المثالي $\langle x^2 - 2 \rangle$ أعظمية في $Q[x]$ وبالتالي الحلقة $Q[x]/\langle x^2 - 2 \rangle$ تشكل حقلاً.

إضافة لذلك، فإن $\varphi(x^2 - 2) = (\sqrt{2})^2 - 2 = 0$ وهذا يبين أن $x^2 - 2 \in \text{Ker } \varphi$ وبالتالي يكون $\langle x^2 - 2 \rangle \subseteq \text{Ker } \varphi$ ، وبما أن $\varphi \neq 0$ فإن $\text{Ker } \varphi \neq F[x]$ ولما كان المثالي $\langle x^2 - 2 \rangle$ أعظمية في $Q[x]$ ، نجد أن $\langle x^2 - 2 \rangle = \text{Ker } \varphi$.

لنبرهن على أن التشاكل φ غامر. ليكن $d \in Q(\sqrt{2})$ عندئذ $d = a + b\sqrt{2}$ حيث $a, b \in Q$ ومنه فإن $g(x) = a + bx \in Q[x]$ وأن:

$$\varphi(g(x)) = g(\sqrt{2}) = a + b\sqrt{2} = d$$

أي أن φ غامر وحسب مبرهنة التماثل الأولى نجد أن $Q[x]/\text{Ker } \varphi \cong Q(\sqrt{2})$ ومنه:

$$\diamond \cdot Q[x]/\langle x^2 - 2 \rangle \cong Q(\sqrt{2})$$

٩ - أثبت أن العدد $\sqrt{1+\sqrt{3}} \notin Q$ وأن العنصر $\sqrt{1+\sqrt{3}}$ جبري فوق Q . ثم أثبت أن المثالي $B = \langle g(x) \rangle$ حيث $g(x) = x^4 - 2x - 2 \in Q[x]$ أعظمي في $Q[x]$ وأن الحقل $Q(\sqrt{3})/B$ يماثل الحقل $Q[x]/B$.

الحل.

واضح أن العدد $\sqrt{1+\sqrt{3}}$ عدداً حقيقياً. لنفرض جديلاً أن $\sqrt{1+\sqrt{3}} \in Q$ عندئذ يكون $\sqrt{1+\sqrt{3}} = a/b$ حيث $a, b \in Z$ وأن $b \neq 0$ ، ومنه فإن $1+\sqrt{3} = a^2/b^2$ وهذا يبين أن $\sqrt{3} = a^2 - b^2/b^2 \in Q$ وهذا غير ممكن، ومنه $\sqrt{1+\sqrt{3}} \notin Q$. لنأخذ الحدودية $g(x) = x^4 - 2x - 2 \in Q[x]$ فنجد أن $g(x) \neq 0$ وأن $g(\sqrt{1+\sqrt{3}}) = 0$ ومنه يكون العنصر $\sqrt{1+\sqrt{3}}$ جبرياً فوق Q . وحسب معيار إيرنشتاين نجد أن الحدودية $g(x)$ أولية في $Q[x]$ ومنه يكون المثالي $B = \langle g(x) \rangle$ أعظمياً في الحلقة $Q[x]$ وبالتالي تكون الحلقة $Q[x]/B$ حقلاً.

بما أن $Q \subseteq Q(\sqrt{1+\sqrt{3}})$ فإن الحقل $Q(\sqrt{1+\sqrt{3}})$ هو تمديد للحقل Q وحسب التمرين المحلول (٣-٤) فإن التطبيق:

$$\varphi: Q[x] \rightarrow Q(\sqrt{1+\sqrt{3}})$$

المعرف بالشكل الآتي: $\varphi(f(x)) = f(\sqrt{1+\sqrt{3}})$ وذلك أيأ كان $f(x) \in Q[x]$ هو تشاكل حلقي، وهو أيضاً غامر، لأنه إذا كان $d \in Q(\sqrt{1+\sqrt{3}})$ فإن:

$$d = a + b\sqrt{1+\sqrt{3}}$$

حيث $a, b \in Q$ ومنه فإن $a + bx \in Q[x]$ وأن:

$$\varphi(a + bx) = a + b\sqrt{1+\sqrt{3}} = d$$

وأن $g(x) = x^4 - 2x - 2 \in \text{Ker } \varphi$ وذلك لأن $g(\sqrt{1+\sqrt{3}}) = 0$ وبما أن $\varphi \neq 0$ فإن $\text{Ker } \varphi \neq Q[x]$ ولما كان المثالي $B = \langle g(x) \rangle \subseteq \text{Ker } \varphi$ أعظمياً في $Q[x]$ ، نجد أن $B = \text{Ker } \varphi$. وحسب مبرهنة التماثل الأولى نجد أن:

$$Q[x]/\text{Ker } \varphi \cong Q(\sqrt{1+\sqrt{3}})$$

ومنه فإن $Q[x]/B \cong Q(\sqrt{1+\sqrt{3}})$.

١٠ - ليكن K حقل و E, F حقول جزئية في K . أثبت أن $E \cdot F$ حقل جزئي في K يحوي كلا من E و F .

الحل.

نعلم أن $E \cdot F = \{x : x = \sum a_i b_i : a_i \in E, b_i \in F\}$ حيث أن المجاميع في $E \cdot F$ هي مجاميع منتهية. واضح أن $\Phi \neq E \cdot F \subseteq K$ لأن $1 = 1 \cdot 1 \in E \cdot F$.
ليكن $x, y \in E \cdot F$ عندئذ $x = \sum a_i b_i$ و $y = \sum c_i d_i$ و $a_i, c_i \in E$ و $b_i, d_i \in F$ ومنه فإن:

$$x - y = \sum a_i b_i - \sum c_i d_i \in E \cdot F$$

لأنه مجموع منته وذلك لأن كلا من x, y يمثل مجموعاً منتهياً. من جهة أخرى، إن كلا من E^*, F^* يمثل زمرة جزئية من الزمرة التبديلية $(K^*, \cdot)$ وبالتالي فإن $E^* \cdot F^*$ هو زمرة جزئية في الزمرة $(K^*, \cdot)$.

مما سبق نجد أن المجموعة $E \cdot F$ هي حقل جزئي في K . كما أن $F \subseteq E \cdot F$ لأنه أي $a \in F$ فإن $a = 1 \cdot a \in E \cdot F$ أيضاً أي $b \in E$ فإن $b = b \cdot 1 \in E \cdot F$ ومنه نجد أن $E, F \subseteq E \cdot F$. ♦

١١ - أثبت أن الحقلين $Q(\sqrt{3})$ و $Q(\sqrt{-3})$ غير متماثلين.

الحل.

لنفرض جلاً أن الحقلين $Q(\sqrt{3})$ و $Q(\sqrt{-3})$ متماثلان.
ولنفرض أن $\varphi : Q(\sqrt{-3}) \rightarrow Q(\sqrt{3})$ هو التماثل المفروض. بما أن $\varphi(1) = 1$ نجد أن $\varphi(-1) = -1$ ومنه يكون $\varphi(-3) = -3$ وبالتالي نجد أن:
 $-3 = \varphi(-3) = \varphi(\sqrt{-3} \cdot \sqrt{-3}) = \varphi(\sqrt{-3}) \cdot \varphi(\sqrt{-3}) = (\varphi(\sqrt{-3}))^2$
وهذا غير ممكن، لأنه بما أن $\varphi(\sqrt{-3}) \in Q(\sqrt{3})$ فإن $\varphi(\sqrt{-3})^2$ هو عدد حقيقي موجب وبالتالي المساواة $-3 = (\varphi(\sqrt{-3}))^2$ ليست صحيحة ومنه نجد أن الحقلين $Q(\sqrt{3})$ و $Q(\sqrt{-3})$ غير متماثلين. ♦

١٢ - ليكن $a, b \in Q$ بحيث $\sqrt{a} + \sqrt{b} \neq 0$. أثبت أن:

$$Q(\sqrt{a}, \sqrt{b}) = Q(\sqrt{a} + \sqrt{b})$$

الحل.

لدينا $\sqrt{a}, \sqrt{b} \in Q(\sqrt{a}, \sqrt{b})$ وأن $Q(\sqrt{a}, \sqrt{b})$ حقلاً عندئذ:

$$\sqrt{a} + \sqrt{b} \in Q(\sqrt{a}, \sqrt{b})$$

ومنه فإن $Q(\sqrt{a} + \sqrt{b}) \subseteq Q(\sqrt{a}, \sqrt{b})$.

لأجل البرهان على الاحتواء المعاكس لنبرهن أولاً أن $\sqrt{a}, \sqrt{b} \in Q(\sqrt{a} + \sqrt{b})$.

بما أن $\sqrt{a} + \sqrt{b} \in Q(\sqrt{a} + \sqrt{b})$ وأن $Q(\sqrt{a} + \sqrt{b})$ حقلاً فإن:

$$(\sqrt{a} + \sqrt{b})^3 \in Q(\sqrt{a} + \sqrt{b})$$

وبالتالي يكون:

$$(a + 3b)\sqrt{a} + (b + 3a)\sqrt{b} = (\sqrt{a} + \sqrt{b})^3 \in Q(\sqrt{a} + \sqrt{b})$$

ولما كان $a + 3b \in Q(\sqrt{a} + \sqrt{b})$ نجد أن:

$$-(a + 3b) \in Q(\sqrt{a} + \sqrt{b})$$

ومنه فإن:

$$(a + 3b)\sqrt{a} + (b + 3a)\sqrt{b} - (a + 3b)(\sqrt{a} + \sqrt{b}) \in Q(\sqrt{a} + \sqrt{b})$$

وهكذا نجد أن $-2(a + b)\sqrt{b} \in Q(\sqrt{a} + \sqrt{b})$ وبالتالي يكون:

$$\sqrt{b} = \sqrt{b} / -2(a + b) \in Q(\sqrt{a} + \sqrt{b})$$

بما أن $\sqrt{a} + \sqrt{b} \neq 0$ فإن $a + b \neq 0$. بالطريقة نفسها نجد أن:

$$\sqrt{a} \in Q(\sqrt{a} + \sqrt{b})$$

وهكذا نجد:

$$Q(\sqrt{a}, \sqrt{b}) \in Q(\sqrt{a} + \sqrt{b})$$

وبالتالي $Q(\sqrt{a}, \sqrt{b}) = Q(\sqrt{a} + \sqrt{b})$.

١٣ - أوجد درجة تمديد الحقل $Q(\sqrt{2}, \sqrt{6} + \sqrt{10})$ فوق الحقل $Q(\sqrt{3} + \sqrt{5})$.

الحل.

لنبرهن أولاً أن $Q(\sqrt{2}, \sqrt{6} + \sqrt{10}) = Q(\sqrt{2}, \sqrt{3} + \sqrt{5})$. ليكن:

$$x \in Q(\sqrt{2}, \sqrt{6} + \sqrt{10}) = Q(\sqrt{2})(\sqrt{6} + \sqrt{10})$$

عندئذ فإن:

$$x = a + b(\sqrt{6} + \sqrt{10})$$

حيث $a, b \in Q(\sqrt{2})$ ومنه فإن $x = a + b\sqrt{2}(\sqrt{3} + \sqrt{5})$ وأن $b = b_1 + b_2\sqrt{2}$ حيث $b_1, b_2 \in Q$ ومنه فإن:

$$b\sqrt{2} = b_1\sqrt{2} + 2b_2 \in Q(\sqrt{2}) + Q \subseteq Q(\sqrt{2})$$

وهكذا فإن:

$$x = a + b\sqrt{2}(\sqrt{3} + \sqrt{5}) = a + (b_1\sqrt{2} + 2b_2)(\sqrt{3} + \sqrt{5}) \in$$

$$\in Q(\sqrt{2})(\sqrt{3} + \sqrt{5})$$

$$\text{أي أن } Q(\sqrt{2}, \sqrt{6} + \sqrt{10}) \subseteq Q(\sqrt{2})(\sqrt{6} + \sqrt{10})$$

ليكن $y \in Q(\sqrt{2}, \sqrt{3} + \sqrt{5}) \subseteq Q(\sqrt{2})(\sqrt{3} + \sqrt{5})$ عندئذ فإن:

$$y = y_1 + y_2(\sqrt{3} + \sqrt{5})$$

حيث $y_1, y_2 \in Q(\sqrt{2})$. ولما كان $y_2 = y_2(\sqrt{2})^{-1}\sqrt{2} \in Q(\sqrt{2})$ نجد أن:

$$y = y_1 + y_2(\sqrt{3} + \sqrt{5}) = y_1 + y_2(\sqrt{2})^{-1}(\sqrt{6} + \sqrt{10})$$

$$\in Q(\sqrt{2})(\sqrt{6} + \sqrt{10}) = Q(\sqrt{2}, \sqrt{6} + \sqrt{10})$$

ومنه يكون $Q(\sqrt{2})(\sqrt{6} + \sqrt{10}) \subseteq Q(\sqrt{2}, \sqrt{6} + \sqrt{10})$.

مما سبق نجد أن:

$$Q(\sqrt{2}, \sqrt{6} + \sqrt{10}) = Q(\sqrt{2}, \sqrt{3} + \sqrt{5})$$

وهكذا يكون:

$$[Q(\sqrt{2}, \sqrt{6} + \sqrt{10}) : Q(\sqrt{3} + \sqrt{5})] =$$

$$= [Q(\sqrt{2}, \sqrt{3} + \sqrt{5}) : Q(\sqrt{3} + \sqrt{5})] = 2$$

١٤ - ليكن الحقل K تمديداً للحقل F وليكن $a \in K$. إذا كان $[F(a) : F]$ عدداً فردياً،

عندئذ يكون $F(a) = F(a^2)$.

الحل.

لنفرض أن $[F(a):F] = n$ ، حيث n عدد فردي، عندئذ يكون الحقل $F(a)$ تمديداً منتهياً للحقل F . من جهة أخرى، لما كان $a \in F(a)$ عندئذ فإن $a^2 \in F(a)$ وهذا يبين أن $F(a^2) \subseteq F(a)$.
أصبح لدينا $F \subseteq F(a^2) \subseteq F(a)$ ولما كان الحقل $F(a)$ تمديداً منتهياً للحقل F نجد أن:

$$[F(a):F] = [F(a):F(a^2)] \cdot [F(a^2):F]$$

أيضاً لما كان العنصر a^2 هو صفر للحدودية $[x] \in F(a^2)$ فإنه حسب المبرهنة (٣-٣-١٥) يكون:

$$[F(a):F(a^2)] \leq \partial(x^2 - a^2) = 2$$

ولما كان $[F(a):F]$ عدداً فردياً نجد أن $[F(a):F(a^2)] = 1$ وهذا يبين أن:
 $F(a) = F(a^2)$.

تمارين (٣)

- ١ - اكتب العنصر $(3+4\sqrt{2})^{-1}$ على الشكل $a+b\sqrt{2}$ حيث $a, b \in Q$.
- ٢ - أثبت أن $Q(\sqrt{3}, \sqrt{5}) = Q(\sqrt{3} + \sqrt{5})$.
- ٣ - أثبت أن الحقل $Q(\sqrt{3})$ لا يماثل الحقل $Q(\sqrt{2})$.
- ٤ - حدد جميع عناصر الحقل $Q(\sqrt[3]{5})$.
- ٥ - أوجد العناصر $a, b, c \in Q$ والتي من أجلها $(1 + \sqrt[3]{4})(2 - \sqrt[3]{2}) = a + b\sqrt[3]{2} + c\sqrt[3]{4}$.
- ٦ - لنفرض أن R حقل الأعداد الحقيقية و $a, b \in R$. أثبت أن $R = R(a + bi)$ ، حيث C هو حقل الأعداد المركبة.
- ٧ - عين جميع الحقول الجزئية في الحقل $Q(\sqrt{2})$.
- ٨ - أثبت أن المجموعة $Q(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in Q\}$ تشكل حقلاً، وذلك لأجل أي عدد صحيح موجب d من أجله $\sqrt{d} \notin Z$.
- ٩ - أوجد درجة التمديد $Q(\sqrt{3} + \sqrt{5})$ فوق الحقل $Q(\sqrt{15})$ ، ثم أوجد قاعدة هذا التمديد.
- ١٠ - أوجد درجة التمديد $Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2})$ فوق الحقل Q ، ثم أوجد قاعدة هذا التمديد.
- ١١ - لنأخذ الحقل $Z_3 = \{0, 1, 2\}$ بالنسبة لعمليتي الجمع والضرب بالمقاس 3، ولنأخذ المجموعة

$$Z_3(i) = \{a + bi : a, b \in Z_3, i^2 = -1\}$$

والمطلوب: أ - أوجد جميع عناصر المجموعة $Z_3(i)$.

ب - أثبت أن المجموعة $Z_3(i)$ تشكل حقلاً.

١٢ - لنأخذ الحقل Z_5 بالنسبة لعمليتي الجمع والضرب بالمقاس 5، ولنأخذ المجموعة

$$Z_5(i) = \{a + bi : a, b \in Z_5, i^2 = -1\}$$

والمطلوب: أ - أوجد جميع عناصر المجموعة $Z_5(i)$.

ب - أثبت أن المجموعة $Z_5(i)$ لا تشكل حقلاً.

١٣ - أوجد درجة تمديد الحقل $Q(\sqrt{1+\sqrt{3}})$ فوق الحقل Q .

١٤ - ليكن الحقل K تمديداً منتهياً للحقل F درجته عدد أولي. أثبت أنه أياً كان $a \in K$ فإنه إما $F(a) = F$ أو $F(a) = K$.

١٥ - ليكن الحقل K تمديداً للحقل F وأن $a \in K$. أثبت أن $[F(a):F(a^3)]$ إما تساوي الواحد أو تساوي 3.

١٦ - ليكن الحقل K تمديداً للحقل F وليكن E_1, E_2 حقليْن جزئيين في K بحيث $F \subseteq E_1 \subseteq K$ و $F \subseteq E_2 \subseteq K$. إذا كان كل من العددين $[E_1:F]$ و $[E_2:F]$ هو عدد أولي فأثبت أنه إما $E_1 = E_2$ أو $E_1 \cap E_2 = F$.

١٧ - ليكن الحقل K تمديداً للحقل F و $a, b \in K$. إذا كان العنصر a جبرياً فوق F درجته n وكان العنصر b جبرياً فوق F درجته m حيث $\gcd(a, b) = 1$. أثبت أن $[F(a, b):F] = n.m$.

١٨ - ليكن الحقل K تمديداً للحقل F و $a \in K$. إذا كان $[F(a):F] = 5$ أوجد $[F(a^3):F]$.

١٩ - أوجد درجة تمديد الحقل $Q(\sqrt{2}, \sqrt{6})$ فوق الحقل $Q(\sqrt{3})$.

٢٠ - أوجد درجة تمديد الحقل $Q(\sqrt{2}, \sqrt{5})$ فوق الحقل Q .

٢١ - أوجد درجة تمديد الحقل $Q(\sqrt{2}, \sqrt{6} + \sqrt{10})$ فوق الحقل $Q(\sqrt{3}, \sqrt{5})$.

٢٢ - أثبت أن $Q(\sqrt{3}, \sqrt{7}) = Q(\sqrt{3} + \sqrt{7})$.

٢٣ - أوجد درجة تمديد الحقل $Q(\sqrt{3} + \sqrt{7})$ فوق الحقل Q .

الفصل الرابع

حقول التفریق

٤ - ١. مميزات الحقول.

وجدنا سابقاً من خلال دراستنا لحقول الأعداد الحقيقية، النسبية، العقدية أن الصفر هو العدد الوحيد الذي إذا ضرب بأي عدد آخر يكون الناتج صفراً، بينما توجد حقول أخرى لا تحقق هذه الخاصة، فعلى سبيل المثال لو أخذنا الحقل $Z_5 = \{0,1,2,3,4\}$ بالنسبة لعمليتي الجمع والضرب بالمقاس 5 لوجدنا أن $1.5 = 2.5 = 3.5 = 4.5 = 0$. لأجل ذلك سوف ندرس هذه الخاصة بشكل موسع والبدائية ستكون مع التمهيدية الآتية:

تمهيدية ٤-١-١.

ليكن $(F, +, \cdot)$ حقلاً. ولنأخذ المجموعة:

$$E = \{a : a \in F; a = n \cdot 1_F : n \in Z\}$$

حيث أنه أيّاً كان $n \in Z$ فإن:

$$n \cdot 1_F = \begin{cases} \underbrace{1_F + 1_F \cdots + 1_F}_{n \text{ once}} & n > 0 \\ 0_F & n = 0 \\ \underbrace{(-1_F) + (-1_F) + \cdots + (-1_F)}_{-n \text{ once}} & n < 0 \end{cases}$$

ف نجد أن:

١ - $(E, +, \cdot)$ حلقة جزئية واحدة في الحقل $(F, +, \cdot)$.

٢ - التطبيق $\varphi : (Z, +, \cdot) \rightarrow (E, +, \cdot)$ المعرف بالشكل الآتي: أيّاً كان $n \in Z$ فإن

$\varphi(n) = n \cdot 1_F$ ، هو تشاكل حلقي غامر.

٣ - $\text{Ker } \varphi = \{n : n \in Z; n \cdot 1_F = 0_F\}$.

البرهان.

١ - واضح أن $E \subseteq F$ لأن $0 \in E$ كما أن $1_F \in E$ لأن $1_F = 1_Z \cdot 1_F \in E$.

ليكن $x, y \in E$ عندئذ $x = n \cdot 1_F, y = m \cdot 1_F$ حيث $n, m \in Z$ ومنه:

$$x - y = n \cdot 1_F - m \cdot 1_F = (n - m) \cdot 1_F \in E$$

$$x \cdot y = (n \cdot 1_F) \cdot (m \cdot 1_F) = (n \cdot m) \cdot (1_F \cdot 1_F) = (n \cdot m) \cdot 1_F \in E$$

وهذا يبين لنا أن E حلقة جزئية واحدة في F .

٢ - إن التطبيق φ هو تشاكل حلقي لأنه أياً كان $n, m \in Z$ عندئذ فإن:

$$\varphi(n + m) = (n + m) \cdot 1_F = n \cdot 1_F + m \cdot 1_F = \varphi(n) + \varphi(m)$$

$$\varphi(n \cdot m) = (n \cdot m) \cdot 1_F = (n \cdot m) \cdot (1_F \cdot 1_F) =$$

$$= (n \cdot 1_F) \cdot (m \cdot 1_F) = \varphi(n) \cdot \varphi(m)$$

كما أن التشاكل φ غامر، لأنه أياً كان $a \in E$ فإن $a = n \cdot 1_F$ حيث $n \in Z$ ومنه $\varphi(n) = n \cdot 1_F = a$

٣ - واضح أن $\text{Ker } \varphi = \{n : n \in Z; n \cdot 1_F = 0_F\}$

بالاعتماد على التمهيدية الأخيرة لنورد التعريف الآتي:

تعريف.

ليكن F حقلاً.

- سوف نقول إن للحقل F مميزاً يساوي الصفر إذا كان التشاكل الغامر φ الوارد في التمهيدية (١-١-٤) متبايناً (أي تماثل حلقي).

- سوف نقول إن للحقل F مميزاً لا يساوي الصفر إذا كان التشاكل الغامر φ الوارد في التمهيدية (١-١-٤) ليس متبايناً.

- سوف نقول إن للحقل F مميزاً يساوي 0_Z إذا كان p أصغر عدد صحيح موجب ينتمي إلى نواة التشاكل الغامر φ .

بالاعتماد على التعريف السابق يمكننا صياغة التمهيدية الآتية:

تمهيدية ١-١-٤.

ليكن F حقلاً مميزه يساوي الصفر. عندئذ:

$$١. 0_Z \cdot 1_F = 0_F$$

٢. أياً كان $n \in Z \setminus \{0\}$ فإن $n \cdot 1_F \neq 0_F$

٣. الحقل F غير منته.

البرهان.

١ - بما أن مميز الحقل F يساوي الصفر عندئذ وحسب التعريف يكون التشاكل φ

متبايناً ومنه تكون $\text{Ker } \varphi = \{0_Z\}$ وبالتالي يكون $0_Z \cdot 1_F = 0_F$.

٢ - ليكن $n \in Z \setminus \{0\}$ عندئذ بما أن التشاكل φ متباين فإن $n \notin \text{Ker } \varphi = \{0_Z\}$ ومنه يكون $n \cdot 1_F \neq 0_F$.

٣ - بما أن التشاكل φ متباين فإن φ هو تماثل حقيقي وبما أن الحلقة Z غير منتهية فإن الحلقة E تكون غير منتهية أيضاً، وبما أن $E \subseteq F$ فإن الحقل F هو حقل غير منته. ◊

بالاعتماد على التعريف الأخير يمكننا صياغة التمهيدية الآتي:

تمهيدية ٤-١-٣.

ليكن F حقلاً مميزه يساوي $p \neq 0_Z$. عندئذ:

١. $p \cdot 1_F = 0_F$.

٢. $p > 1$.

٣. العدد p هو عدد أولي.

البرهان.

١ - واضح.

٢ - إن $p \neq 1_Z$ لأنه إذا كان $p = 1_Z$ فإنه حسب (١) يكون $p \cdot 1_F = 1_Z \cdot 1_F = 0_F$ من جهة أخرى، لدينا $p \cdot 1_F = 1_Z \cdot 1_F = 1_F$ وهكذا نجد أن $1_F = 0_F$ وهذا غير ممكن، وبالتالي يكون $p > 1$.

٣ - ليكن $m_1 \in Z$ قاسم للعدد p عندئذ يوجد $m_2 \in Z$ بحيث $p = m_1 \cdot m_2$ وبما أن العدد p موجب فإننا نكون أمام حالتين إما أن $m_1, m_2 > 0$ أو أن $m_1, m_2 < 0$.
- الحالة الأولى: إذا كان $m_1, m_2 > 0$ بالإضافة لذلك فإن $m_1, m_2 \leq p$ ، كما أن:

$$\varphi(p) = \varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$$

حيث φ هو التشاكل المعروف في التمهيدية (٤-١-١) ومنه يكون $p \cdot 1_F = (m_1 \cdot 1_F) \cdot (m_2 \cdot 1_F) = 0_F$ وبالتالي فإن $(m_1 \cdot 1_F) \cdot (m_2 \cdot 1_F) = 0_F$ وهكذا نجد

أنه إما $m_1 \cdot 1_F = 0_F$ أو $m_2 \cdot 1_F = 0_F$.

- إذا كان $m_1 \cdot 1_F = 0_F$ عندئذ يكون $\varphi(m_1) = 0_F$ وبالتالي فإن $m_1 \in \text{Ker } \varphi$ وبما أن p هو أصغر عدد صحيح موجب في $\text{Ker } \varphi$ وأن $m_1 \leq p$ نجد أن $m_1 = p$.
- إذا كان $m_2 \cdot 1_F = 0_F$ عندئذ يكون $\varphi(m_2) = 0_F$ وبالتالي فإن $m_2 \in \text{Ker } \varphi$ وبما أن p هو أصغر عدد صحيح موجب في $\text{Ker } \varphi$ وأن $m_2 \leq p$ نجد أن $m_2 = p$ وبالتالي يكون $m_1 = 1$.

- الحالة الثانية: إذا كان $m_1, m_2 < 0$ عندئذ يوجد $r_1, r_2 \in \mathbb{Z}$ بحيث $r_1, r_2 > 0$ وأن $m_1 = -r_1, m_2 = -r_2$ ومنه يكون $p = m_1 \cdot m_2 = (-r_1) \cdot (-r_2) = r_1 \cdot r_2$ وحسب الحالة الأولى نجد أنه إما $r_1 = p$ أو $r_1 = 1$ وبالتالي إما $m_1 = -p$ أو $m_1 = -1$.
مما سبق نجد أن أي قاسم $m_1 \in \mathbb{Z}$ للعدد p ينتمي للمجموعة $\{\pm 1, \pm p\}$ وهذا يبين لنا أن العدد p هو عدد أولي. ◊

بالاعتماد على ما سبق يمكننا صياغة المبرهنة الهامة الآتية:

مبرهنة ٤-١-٤.

ليكن F حقلاً مميزه يساوي $p \neq 0_Z$ عندئذ:

١ - العناصر $0_F, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, (p-1) \cdot 1_F \in F$ مختلفة مثني مثني.

٢ - $E = \{0_F, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, (p-1) \cdot 1_F\} \subseteq F$

٣ - $E = \{0_F, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, (p-1) \cdot 1_F\} \subseteq F$ تشكل حقلاً جزئياً في F .
البرهان.

١ - ليكن $x, y \in \{0_F, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, (p-1) \cdot 1_F\}$ عندئذ يوجد $n, m \in \mathbb{Z}$ بحيث $0 \leq n, m < p$ وأن $x = n \cdot 1_F, y = m \cdot 1_F$. لنفرض أن $x = y$ عندئذ يكون $n = m$ لأنه إذا كان $n \neq m$ فإن $0 < n - m < p$ وبما أن $n \cdot 1_F = m \cdot 1_F$ نجد أن $(n - m) \cdot 1_F = n \cdot 1_F - m \cdot 1_F = 0$

وحسب التمهيدية (٤-١-١) يكون $n - m \in \text{Ker } \varphi$ وهذا يناقض كون p هو أصغر عدد صحيح موجب في $\text{Ker } \varphi$. مما سبق نجد أن $n \cdot 1_F = m \cdot 1_F$ عندما وفقط عندما $n = m$ وهذا يبين لنا أن العناصر

$$0_F, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, (p-1) \cdot 1_F \in F$$

مختلفة مثنى مثنى.

٢ - لدينا حسب التمهيدية (١-١-٤) أن $E = \{a : a \in F; a = n \cdot 1_F : n \in \mathbb{Z}\}$ ومنه يكون $\{0_F, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, (p-1) \cdot 1_F\} \subseteq E$. ليكن $x \in E$ عندئذ يوجد $n \in \mathbb{Z}$ بحيث $x = n \cdot 1_F$ وحسب خوارزمية القسمة لأجل العددين n, p يوجد $q, r \in \mathbb{Z}$ يحققان $n = qp + r$ حيث $0 \leq r < p$ ومنه فإن:

$$\varphi(n) = \varphi(qp + r) = \varphi(qp) + \varphi(r) = \varphi(q)\varphi(p) + \varphi(r)$$

ومنه نجد أن $n \cdot 1_F = (q \cdot 1_F) \cdot (p \cdot 1_F) + (r \cdot 1_F) = r \cdot 1_F$ وبما أن $0 \leq r < p$ يكون $x = n \cdot 1_F = r \cdot 1_F \in \{0_F, 1_F, 2 \cdot 1_F, \dots, (p-1) \cdot 1_F\}$ وهذا يبين لنا أن:

$$E \subseteq \{0_F, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, (p-1) \cdot 1_F\}$$

مما سبق نجد أن $E = \{0_F, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, (p-1) \cdot 1_F\}$

٣ - وجدنا حسب التمهيدية (١-١-٤) أن E هي حلقة جزئية واحدة في $(F, +, \cdot)$. لنبرهن الآن على أن كل عنصر من E مغاير للصفر يوجد له مقلوب في E . ليكن $y \in E, y \neq 0$ عندئذ يوجد $m \in \mathbb{Z}$ بحيث $y = m \cdot 1_F$. إن p لا يقسم m ، لأنه إذا كان p يقسم m يوجد $s \in \mathbb{Z}$ تحقق $m = ps$ ومنه يكون $\varphi(m) = \varphi(ps) = \varphi(p)\varphi(s)$ وبالتالي يكون $m \cdot 1_F = (p \cdot 1_F) \cdot (s \cdot 1_F) = 0 = 0 \cdot 1_F$ وحسب قانون الاختصار نجد أن $m = 0$ وهذا غير ممكن. وهكذا نجد أن العددين m, p أوليان فيما بينهما وبالتالي يوجد $q, r \in \mathbb{Z}$ يحققان $p \cdot q + m \cdot r = 1_{\mathbb{Z}}$ وبالتالي فإن:

$$\varphi(1_{\mathbb{Z}}) = \varphi(p \cdot q + m \cdot r) = \varphi(q \cdot p) + \varphi(m \cdot r) =$$

$$= \varphi(q) \cdot \varphi(p) + \varphi(m) \cdot \varphi(r)$$

$$1_F = 1_{\mathbb{Z}} \cdot 1_F = (p \cdot 1_F) \cdot (q \cdot 1_F) + (m \cdot 1_F) \cdot (r \cdot 1_F) = (m \cdot 1_F) \cdot (r \cdot 1_F)$$

وهكذا نجد أن $r \cdot 1_F \in E$ ويمثل مقلوباً للعنصر $y = m \cdot 1_F$ في E . مما سبق نجد أن

$$E = \{0_F, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, (p-1) \cdot 1_F\} \text{ تشكل حقلاً. } \diamond$$

لنورد الآن عدداً من الأمثلة:

أمثلة.

- ١ - كل من الحقول التالية: حقل الأعداد الحقيقية $(R, +, \cdot)$ ، حقل الأعداد النسبية $(Q, +, \cdot)$ ، حقل الأعداد العقدية $(C, +, \cdot)$ هي حقول مميز كل منها يساوي الصفر.
 - ٢ - الحقل $Q(\sqrt{2})$ مميزه يساوي الصفر.
 - ٣ - الحقل $Z_p = \{0, 1, 2, \dots, (p-1)\}$ بالنسبة لعمليتي الجمع والضرب بالمقاس p ، حيث p عدد أولي هو حقل مميزه يساوي $p \neq 0$.
 - ٤ - أي حقل منته مميزه لا يساوي الصفر.
- لنفرض أن F حقل منته عندئذ مميزه لا يساوي الصفر، لأنه إذا كان مميز الحقل F يساوي الصفر، فإنه حسب التمهيدية (٤-١-٢) يكون الحقل F غير منته.

نأتي الآن إلى دراسة التمهيدية الآتية:

تمهيدية ٤-١-٥.

ليكن F حقلاً مميزه يساوي $p \neq 0_Z$. عندئذ أياً كان $a, b \in F$ فإن:

١. $p \cdot a = 0_F$.
٢. $(a+b)^p = a^p + b^p$.
٣. $(a-b)^p = a^p - b^p$.
٤. لأجل أي عدد صحيح موجب n فإن $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

البرهان.

$$١ - p \cdot a = p \cdot (1_F \cdot a) = (p \cdot 1_F) \cdot a = 0_F \cdot a = 0_F$$

٢ - حسب دستور ثنائي الحد فإن:

$$(a+b)^p = \sum_{i=0}^p C_i^p \cdot a^i \cdot b^{p-i} = a^p + \sum_{i=1}^{p-1} C_i^p \cdot a^i \cdot b^{p-i} + b^p$$

وبما أن $C_i^p = \frac{p!}{i!(p-i)!}$ نجد أنه لأجل جميع القيم $0 < i < p$ فإن:

$$C_i^p \cdot a^i \cdot b^{p-i} = \frac{(p-1)!}{i!(p-i)!} \cdot (p \cdot a) \cdot a^{i-1} \cdot b^{p-i} = 0$$

وهذا يبين لنا أن $(a+b)^p = a^p + b^p$

٣ - يبرهن بطريقة مشابهة.

٤ - ليكن n عدداً صحيحاً موجباً. بالاستقراء حسب n . نلاحظ أنه من أجل $n=1$ حسب (٢) فإن $(a+b)^p = a^p + b^p$. لنفرض أن المساواة صحيحة من أجل $n-1$ عندئذ يكون $(a+b)^{p^{n-1}} = a^{p^{n-1}} + b^{p^{n-1}}$ ومنه فإن:

$$(a+b)^{p^n} = [(a+b)^{p^{n-1}}]^p = [a^{p^{n-1}} + b^{p^{n-1}}]^p = (a^{p^{n-1}})^p + (b^{p^{n-1}})^p = a^{p^n} + b^{p^n}$$

لندرس الآن التمهيدية الآتية:

تمهيدية ٤-١-٦.

ليكن F حقلاً مميزه يساوي $p \neq 0_Z$. عندئذ:

١. المجموعة $F^p = \{a^p : \forall a \in F\}$ تشكل حقل جزئي في F .

٢. $F \cong F^p$.

البرهان.

١ - واضح أن $F^p \subseteq F$ لأن $0_F^p = 0_F, 1_F^p = 1_F \in F^p$ كما أن $0_F \neq 1_F$.

ليكن $x, y \in F^p$ عندئذ يوجد $a, b \in F$ بحيث $x = a^p, y = b^p$ ومنه يكون:

$$x - y = a^p - b^p = (a - b)^p \in F^p$$

ليكن $x, y \in F^p$ بحيث $y \neq 0$ عندئذ يوجد $a, b \in F$ بحيث $x = a^p, y = b^p$ وأن

$b \neq 0$ ومنه يكون:

$$x \cdot y^{-1} = a^p \cdot (b^p)^{-1} = a^p \cdot b^{-p} = (ab^{-1})^p \in F^p$$

مما سبق نجد أن المجموعة F^p تشكل حقلاً جزئياً في F .

٢ - لنعرف التطبيق $f: F \rightarrow F^p$ بالشكل الآتي: أيأ كان $a \in F$ فإن $f(a) = a^p$ ،

فنجد أن التطبيق f هو تشاكل حلقي، لأنه أيأ كان $a, b \in F$ فإن:

$$f(a+b) = (a+b)^p = a^p + b^p = f(a) + f(b)$$

$$f(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = f(a) \cdot f(b)$$

بالإضافة لذلك فإن $f(1) = 1^p = 1$ كما أن التطبيق f متباين، لأنه إذا كان $a, b \in F$

بحيث $f(a) = f(b)$ فإن $a^p = b^p$ ومنه يكون $a = b$. أيضاً التطبيق f غامر، لأنه

إذا كان $x \in F^p$ فإنه يوجد $a \in F$ بحيث يكون $x = a^p$ ومنه فإن $f(a) = a^p x$.
مما سبق نجد أن التشاكل f هو تماثل وبالتالي يكون $F \cong F^p$.

إن التمهيدية الأخيرة تبين لنا أن أي حقل F مميزه $p \neq 0_Z$ يماثل الحقل F^p . وهنا يتبادر إلى الذهن السؤال الآتي: هل يوجد حقل F مميزه $p \neq 0_Z$ يحقق $F = F^p$.
نلاحظ على سبيل المثال أن الحقل $Z_3 = \{0,1,2\}$ بالنسبة لعمليتي الجمع والضرب بالمقامس 3 هو حقل مميزه يساوي 3، ويحقق أن $Z_3^3 = \{0,1,2\} = Z_3$. لأجل ذلك سوف نورد التعريف الآتي:

تعريف.

ليكن F حقلاً.

١. نقول عن الحقل F إنه حقل كامل إذا كان مميزه يساوي الصفر.
٢. إذا كان مميز الحقل F لا يساوي الصفر، نقول عن الحقل F إنه حقل كامل إذا كان $F = F^p$.

بالاعتماد على التعريف الأخير يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن F حقلاً مميزه يساوي $p \neq 0_Z$. الشرط اللازم والكافي كي يكون الحقل F حقلاً كاملاً هو أن يتحقق الشرط: أي أن كان $x \in F$ يوجد $y \in F$ بحيث $x = y^p$.

أمثلة.

١ - كل من الحقول التالية: حقل الأعداد الحقيقية $(R, +, \cdot)$ ، حقل الأعداد النسبية $(Q, +, \cdot)$ ، حقل الأعداد العقدية $(C, +, \cdot)$ هي حقول كاملة لأن مميز كل منها يساوي الصفر.

٢ - الحقل $Z_p = \{0,1,2,\dots,(p-1)\}$ بالنسبة لعمليتي الجمع والضرب بالمقامس p ، حيث p عدد أولي، هو حقل كامل.

نعلم أن مميز الحقل Z_p يساوي p . لنبرهن على أن $Z_p = (Z_p)^p$.

واضح أن $(Z_p)^p \subseteq Z_p$. ليكن $a \in Z_p$ عندئذ بما أن $a^p \in Z$ فإنه حسب خوارزمية القسمة لأجل العددين a^p, p يوجد $q, r \in Z$ بحيث $a^p = q \cdot p + r$ حيث $0 \leq r < p$ ، ومنه:

$$\varphi(a^p) = \varphi(q \cdot p + r) = \varphi(q \cdot p) + \varphi(r) = \varphi(q) \cdot \varphi(p) + \varphi(r)$$

حيث أن φ هو التشاكل المعرف في التمهيدية (٤-١-١) ومنه يكون:

$$a^p \cdot 1_F = (q \cdot 1_F) \cdot (p \cdot 1_F) + r \cdot 1_F = r \cdot 1_F$$

وهكذا نجد أن $a^p = r \cdot 1_F \in Z_p$ حيث $0 \leq r < p$ أي أن $a^p = r \cdot 1_F \in Z_p$ وبالتالي يكون $Z_p \subseteq (Z_p)^p$. مما سبق نجد أن $Z_p = (Z_p)^p$ ، وهذا يبين لنا أن الحقل Z_p هو حقل كامل. ◊

٤ - ٢. حقول التفريق.

تعريف.

ليكن الحقل E تمديداً ما للحقل F و $f(x) \in F[x]$.
 - نقول عن الحدودية $f(x)$ إنها تتفرق فوق الحقل E إذا أمكن كتابة الحدودية $f(x)$ على شكل جداء لمضاريب خطية في $E[x]$. أي إذا أمكن كتابة $f(x)$ في $E[x]$ على الشكل الآتي:

$$f(x) = \lambda(x - a_1)(x - a_2) \cdots (x - a_n)$$

حيث $\lambda \in F$ و $a_1, a_2, \dots, a_n \in E$.

- نقول عن الحقل E إنه حقل التفريق للحدودية $f(x)$ فوق F إذا كانت الحدودية $f(x)$ تتفرق في الحقل E ولا تتفرق في أي حقل آخر K يحقق $F \subseteq K \subsetneq E$.

ينتج من التعريف مباشرة أن حقل التفريق لحدودية ما لا يعتمد فقط على الحدودية ذاتها ولكن يعتمد أيضاً على الحقل الذي تتفرق فيها الحدودية نفسها. بالاعتماد على ما سبق يمكننا صياغة التمهيدية الآتية:

تمهيدية ٤-٢-١.

ليكن الحقل K تمديداً ما للحقل F و $f(x) \in F[x]$. الشروط الآتية متكافئة:

- ١ - الحقل K هو حقل التفريق للحدودية $f(x)$ فوق F .
- ٢ - الحدودية $f(x)$ تتفرق فوق K إلى مضاريب خطية والحقل K مولد فوق F بجميع أصفار الحدودية $f(x)$.

البرهان.

(1) $\Leftrightarrow$ (2) . لنفرض أن K هو حقل التفريق للحدودية $f(x)$ فوق F . حسب التعريف فإن $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية على الشكل الآتي:

$$f(x) = \lambda(x - a_1)(x - a_2) \cdots (x - a_n)$$

حيث $\lambda \in F$ و $a_1, a_2, \dots, a_n \in K$. ومنه نجد أن $F(a_1, a_2, \dots, a_n) \subseteq K$.

من جهة أخرى، أصبح لدينا أن الحدودية $f(x)$ تتفرق فوق $F(a_1, a_2, \dots, a_n)$ إلى

مضاريب خطية وحسب التعريف نجد أن $K = F(a_1, a_2, \dots, a_n)$.
 (2) $\Leftarrow$ (1). لنفرض أن $K = F(a_1, a_2, \dots, a_n)$ وأن $f(x)$ تتفرق فوق K إلى مضاريب خطية. ليكن L حقلاً جزئياً في K ويحوي F . إذا كانت $f(x)$ تتفرق فوق L إلى مضاريب خطية عندئذ فإن $a_1, a_2, \dots, a_n \in L$ ومنه نجد أن:
 $\diamond . K = F(a_1, a_2, \dots, a_n) \subseteq L \subseteq K$

نتيجة.

ليكن F حقلاً و $f(x) \in F[x]$. إن حقل التفريق للحدودية $f(x)$ فوق الحقل F هو أصغر حقل تتفرق فيه الحدودية $f(x)$ فوق F .
 لنورد الآن عدداً من الأمثلة:

أمثلة.

١ - لنأخذ الحدودية $f(x) = x^2 - 2 \in Q[x]$ فنجد أن الحدودية $f(x)$ تتفرق في حقل الأعداد الحقيقية R والذي يحوي الحقل Q على الشكل:

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})$$

بينما حقل التفريق للحدودية $f(x)$ فوق الحقل Q هو الحقل:

$$Q(\sqrt{2}) = \{a + b\sqrt{2}; a, b \in Q\}$$

وذلك لأن $f(x) = (x - \sqrt{2})(x + \sqrt{2}) \in Q(\sqrt{2})[x]$.

٢ - لنأخذ الحدودية $f(x) = x^2 + 2 \in Q[x]$ فنجد أن الحدودية $f(x)$ تتفرق في حقل الأعداد العقدية (المركبة) C والذي يحوي الحقل Q على الشكل:

$$f(x) = (x - \sqrt{-1})(x + \sqrt{-1})$$

بينما حقل التفريق للحدودية $f(x)$ فوق الحقل Q هو الحقل:

$$Q(i) = \{a + bi; a, b \in Q; i^2 = -1\}$$

وذلك لأن $f(x) = (x - \sqrt{-1})(x + \sqrt{-1}) \in Q(i)[x]$.

لندرس الآن ومن خلال المبرهنة الآتية أي الحدوديات التي تملك حقل تفريق.

مبرهنة ٢-٢-٤.

ليكن F حقلاً و $f(x) \in F[x]$. إذا كانت $\partial f(x) = n \geq 1$ عندئذ يوجد حقل تفريق K للحدودية $f(x)$ فوق الحقل F يحقق $[K:F] \leq n!$.
البرهان.

سوف نورد البرهان بطريقة الاستقراء الرياضي بحسب درجة الحدودية $f(x)$.
- إذا كانت $\partial f(x) = 1$ عندئذ $f(x) = a_1x + a_0$ حيث $a_1, a_0 \in F$ وأن $a_1 \neq 0$ ،
وبما أن F حقل فإن $a_1^{-1} \in F$. لنضع $x_0 = -a_1^{-1}a_0$ فنجد أن $f(x) = a_1(x - x_0)$ وهنا نجد أن الحقل $f(x_0)$ هو حقل التفريق للحدودية $f(x)$ فوق الحقل F وبما أن $x_0 \in F$ نجد أن $F(x_0) = F$ أي أن F هو حقل التفريق للحدودية $f(x)$ كما أن $[K:F] = 1 = n!$.

- لنفرض أن $\partial f(x) > 1$ وأن المبرهنة صحيحة لأجل جميع الحقول وجميع الحدوديات التي درجة كل منها أصغر من درجة $f(x)$. عندئذ حسب المبرهنة (٣-١-٥) فإنه يوجد تمديد E للحقل F يحوي صفراً للحدودية $f(x)$ وليكن a_1 ، وحسب التمهيدية (١-٧-١) فإن الحدودية $x - a_1 \in E[x]$ تقسم $f(x)$ في $E[x]$ وبالتالي يوجد $g(x) \in E[x]$ بحيث يكون $f(x) = (x - a_1) \cdot g(x)$ وبما أن

$$\partial f(x) = \partial(x - a_1) + \partial g(x)$$

وأن $\partial(x - a_1) = 1$ نجد أن $\partial g(x) < \partial f(x)$ وحسب الفرض الاستقرائي فإنه يوجد حقل تفريق K للحدودية $g(x)$ فوق الحقل E .

وهذا يبين لنا أن الحقل K يحوي الحقل E وجميع أصفار الحدودية $f(x)$ ولتكن $a_1, a_2, a_3, \dots, a_n$. وهكذا نجد أن الحقل $F(a_1, a_2, \dots, a_n)$ هو حقل تفريق للحدودية $f(x)$ فوق الحقل F .

أمثلة.

١ - لنأخذ الحدودية $f(x) = x^4 - x^2 - 2 \in Q[x]$ فنجد أن

$$f(x) = (x^2 - 2) \cdot (x^2 + 1)$$

وهذا يبين لنا أن جميع أصفار الحدودية $f(x)$ والتي عددها يساوي 4 هي $\pm \sqrt{2}, \pm i$

وبالتالي يكون حقل التفريق للحدودية $f(x)$ فوق الحقل Q هو $Q(\sqrt{2}, i)$ وحسب المبرهنة (٣-١-٢) فإن:

$$\begin{aligned} Q(\sqrt{2}, i) &= Q(\sqrt{2})(i) = \{a + bi; a, b \in Q(\sqrt{2})\} = \\ &= \{a_1 + a_2\sqrt{2} + (b_1 + b_2i); a_1, a_2, b_1, b_2 \in Q\} = \\ &= \{a_1 + b_1i + (a_2 + b_2i)\sqrt{2}; a_1, a_2, b_1, b_2 \in Q\} \end{aligned}$$

٢ - أوجد حقل التفريق للحدودية $f(x) = x^3 - 1 \in Q[x]$ فوق الحقل Q .
نلاحظ أولاً أن جميع أصفار الحدودية $x^3 - 1$ البالغ عددها 3 هي $1, -1/2 \pm i\sqrt{3}/2$ وبالتالي يكون أصغر حقل يحوي الحقل Q وجميع أصفار الحدودية $x^3 - 1$ هو الحقل $Q(\sqrt{3}, i)$. مما سبق نجد أن $Q(\sqrt{3}, i)$ هو حقل التفريق للحدودية $x^3 - 1$.

٣ - أوجد حقل التفريق للحدودية $f(x) = x^2 + x + 2 \in Z_3[x]$ فوق الحقل $Z_3 = \{0, 1, 2\}$.

بما أن $f(x) = [x - (1 + i)] \cdot [x - (1 - i)]$ وبالتالي فإن جميع أصفار الحدودية $f(x)$ البالغ عددها 2 هي $1 \pm i$. ومنه نجد أن أصغر حقل يحوي الحقل Z_3 وجميع أصفار الحدودية $f(x)$ هو الحقل $Z_3(i)$ ، انظر التمرين المحلول (٣-٦).

سوف نعالج الآن المسألة الآتية:

ليكن F حقلاً و $f(x) \in F[x]$ ، عندئذ أي حقل تفريق للحدودية $f(x)$ فوق الحقل F يكونان متماثلين. لأجل ذلك نحن بحاجة أولاً إلى التمهيدية الآتية:

تمهيدية ٤-٢-٣.

ليكن الحقل K تمديداً للحقل F و $a \in K$. عندئذ يوجد تشاكل $\varphi: F[x] \rightarrow F(a)$ من أجله $\varphi(F[x]) = F(a)$.
البرهان.

بالعودة إلى التمرين المحلول (٣-٤) وجدنا أن التطبيق $\varphi: F[x] \rightarrow F(a)$ المعروف بالشكل الآتي: أيأ كان $f(x) \in F[x]$ فإن $\varphi(f(x)) = f(a)$ هو تشاكل.
بما أن $\varphi(F[x]) \subseteq F(a)$ نجد أن $\varphi(F[x])$ هو حقل جزئي في $F(a)$ يحوي كلاً من

الحقل F والعنصر a ، وذلك لأنه أياً كان $b \in F$ فإن $g(x) = ba^{-1}x \in F[x]$ وأن $\varphi(g(x)) = g(a) = ba^{-1}a = b \in \varphi(F[x])$.
كما أن $\lambda(x) = x \in F[x]$ وأن $\varphi(\lambda(x)) = \lambda(a) = a \in \varphi(F[x])$. بما أن $F(a) \subseteq \varphi(F[x])$ فإن a والعنصر F يحوي كلاً من $F(a) \subseteq \varphi(F[x])$.
مما سبق نجد أن $\varphi(F[x]) = F(a)$. ♦

تمهيدية ٤-٢-٤.

ليكن الحقل K تمديداً للحقل F وليكن $a \in K$ عنصراً جبرياً فوق الحقل F . عندئذ التشاكل $\varphi: F[x] \rightarrow F(a)$ المعرفة بالشكل الآتي: أياً كان $f(x) \in F[x]$ فإن $\varphi(f(x)) = f(a)$ ، غامر.
البرهان.

حسب التمرين المحلول (٣-٤) فإن φ هو تشاكل حلقي. بما أن العنصر $a \in K$ جبري فوق الحقل F ، لنفرض أن $p(x) \in F[x]$ هي الحدودية الأصغرية للعنصر a فوق F وأن $\partial p(x) = n$ وليكن $b \in F(a)$ عندئذ حسب المبرهنة (٣-١-٦) فإن $b = \sum_{i=0}^{n-1} c_i a^i$ حيث $c_i \in F$ وذلك أياً كان $0 \leq i \leq n-1$. ومنه فإن $h(x) = \sum_{i=0}^{n-1} c_i x^i \in F[x]$ وأن:

$$\varphi(h(x)) = h(a) = \sum_{i=0}^{n-1} c_i a^i = b$$

وهكذا نجد أن التشاكل φ غامر. ♦

تمهيدية ٤-٢-٥.

ليكن الحقل K تمديداً للحقل F وليكن $p(x) \in F[x]$ حدودية أولية. لنفرض أن $a \in K$ صفر للحدودية $p(x)$ عندئذ يوجد تماثل $\alpha: F(a) \rightarrow F[x]/\langle p(x) \rangle$ من أجله $\alpha(a) = x + \langle p(x) \rangle$.
البرهان.

وجدنا حسب التمرين المحلول (٣-٤) أن العلاقة $\varphi: F[x] \rightarrow F(a)$ المعرفة بالشكل الآتي: أياً كان $f(x) \in F[x]$ فإن $\varphi(f(x)) = f(a)$ هي تشاكل حلقي. ولما كان

العنصر a جبرياً فوق F فإنه حسب التمهيدية (٤-٢-٤) فإن التشاكل φ غامر. بما أن a صفر للحدودية $p(x)$ فإن $p(a) = 0$ و $\varphi(p(x)) = 0$ وهذا يبين أن $p(x) \in \text{Ker } \varphi$ وبالتالي فإن $\langle p(x) \rangle \subseteq \text{Ker } \varphi$. من جهة أخرى، بما أن الحدودية $p(x)$ أولية فوق F فإن المثالي $\langle p(x) \rangle$ يكون أعظمية في $F[x]$ ومنه نجد أن $\text{Ker } \varphi = \langle p(x) \rangle$ ، وحسب مبرهنة التماثل الأولى فإن $F[x]/\text{Ker } \varphi \cong \text{Im } \varphi$ ، أي أن:

$$F[x]/\langle p(x) \rangle \cong F(a)$$

لنفرض أن هذا التماثل $\bar{\varphi}: F[x]/\langle p(x) \rangle \rightarrow F(a)$ المعرف بالشكل الآتي: أيًا كان $x + \langle p(x) \rangle \in F[x]/\langle p(x) \rangle$ ولما كان $\bar{\varphi}(f(x)) = \varphi(f(x))$ فإن $f(x) \in F[x]$ فإن $\bar{\varphi}(x) = \varphi(x) = a$. لنفرض أن $\alpha: F(a) \rightarrow F[x]/\langle p(x) \rangle$ هو التماثل العكسي، عندئذ يكون $\alpha \cdot \bar{\varphi} = I_{F[x]/\langle p(x) \rangle}$ ومنه نجد أن:

$$\alpha \cdot \bar{\varphi}(x + \langle p(x) \rangle) = x + \langle p(x) \rangle$$

أي أن $\alpha(\bar{\varphi}(x + \langle p(x) \rangle)) = x + \langle p(x) \rangle$ ، وبالتالي يكون $\alpha(\varphi(x)) = x + \langle p(x) \rangle$ وهكذا نجد أن $\alpha(a) = x + \langle p(x) \rangle$.

مبرهنة ٤-٢-٦.

ليكن F, K حقليين و $\varphi: F \rightarrow K$ تماثلاً. لنفرض أن $p(x) \in F[x]$ حدودية أولية فوق الحقل F وأن a صفرًا للحدودية $p(x)$ في تمديد ما للحقل F . إذا كان b صفر للحدودية $\varphi(p(x)) \in K[x]$ في تمديد ما للحقل K ، عندئذ: يوجد تماثل $\mu: F(a) \rightarrow K(b)$ من أجله $\mu(a) = b$.

البرهان.

لنفرض أن $p(x) \in F[x]$ حدودية أولية فوق الحقل F وأن a صفر للحدودية $p(x)$ في تمديد ما للحقل F . عندئذ حسب التمهيدية (٤-٢-٤) يوجد تماثل:

$$\alpha: F(a) \rightarrow F[x]/\langle p(x) \rangle$$

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

من جهة أخرى، بما أن $\varphi: F \rightarrow K$ تماثل حقلي فإنه حسب التمرين المحلول (١-٤)

يمكن تمديد هذا التماثل إلى التماثل الحلقي $\varphi: F[x] \rightarrow K[x]$ ، وبما أن الحدودية $p(x)$ أولية فوق الحقل F فإنه حسب التمرين المحلول (٦-١) تكون الحدودية $\varphi(p(x))$ حدودية أولية فوق الحقل K وبما أن العنصر b هو صفر للحدودية $\varphi(p(x)) \in K[x]$ في تمديد ما للحقل K فإنه حسب التمهيدية (٤-٢-٤) يوجد تماثل $\beta: K(b) \rightarrow K[x]/\langle \varphi(p(x)) \rangle$ من أجله:

$$\beta(b) = x + \langle \varphi(p(x)) \rangle$$

لنبرهن على أن التطبيق $\theta: F[x]/\langle p(x) \rangle \rightarrow K[x]/\langle \varphi(p(x)) \rangle$ المعرف بالشكل التالي: أيأ كان $f(x) + \langle p(x) \rangle \in F[x]/\langle p(x) \rangle$ فإن:

$$\theta(f(x) + \langle p(x) \rangle) = \varphi(f(x)) + \langle \varphi(p(x)) \rangle$$

هو تماثل حقلي. إن التطبيق θ هو تشاكل، لأنه أيأ كان:

$$\lambda(x) + \langle p(x) \rangle, \psi(x) + \langle p(x) \rangle \in F[x]/\langle p(x) \rangle$$

$$\begin{aligned} \theta[(\lambda(x) + \langle p(x) \rangle) + (\psi(x) + \langle p(x) \rangle)] &= \theta[(\lambda(x) + \psi(x)) + \langle p(x) \rangle] = \\ &= \varphi(\lambda(x) + \psi(x)) + \langle \varphi(p(x)) \rangle = [\varphi(\lambda(x)) + \varphi(\psi(x))] + \langle \varphi(p(x)) \rangle = \\ &= (\varphi(\lambda(x)) + \langle \varphi(p(x)) \rangle) + (\varphi(\psi(x)) + \langle \varphi(p(x)) \rangle) = \\ &= \theta(\lambda(x) + \langle p(x) \rangle) + \theta(\psi(x) + \langle p(x) \rangle) \end{aligned}$$

كما أن

$$\begin{aligned} \theta[(\lambda(x) + \langle p(x) \rangle) \cdot (\psi(x) + \langle p(x) \rangle)] &= \theta(\lambda(x) \cdot \psi(x) + \langle p(x) \rangle) = \\ &= \varphi(\lambda(x) \cdot \psi(x)) + \langle \varphi(p(x)) \rangle = \varphi(\lambda(x)) \cdot \varphi(\psi(x)) + \langle \varphi(p(x)) \rangle = \\ &= \varphi(\lambda(x)) \cdot \varphi(\psi(x)) + \langle \varphi(p(x)) \rangle = \varphi(\lambda(x)) \cdot \varphi(\psi(x)) + \langle \varphi(p(x)) \rangle = \\ &= [\varphi(\lambda(x)) + \langle \varphi(p(x)) \rangle] \cdot [\varphi(\psi(x)) + \langle \varphi(p(x)) \rangle] = \\ &= \theta((\lambda(x) + \langle p(x) \rangle) \cdot \theta(\psi(x) + \langle p(x) \rangle)) \end{aligned}$$

مما سبق نجد أن θ تشاكل. كما أن التطبيق θ متباين لأنه إذا كان $\lambda(x) + \langle p(x) \rangle \in \text{Ker } \theta$ فإن $\theta(\lambda(x) + \langle p(x) \rangle) = 0 = \langle \varphi(p(x)) \rangle$ وبالتالي يكون $\varphi(\lambda(x)) \in \langle \varphi(p(x)) \rangle$ وبما أن التشاكل $\varphi(\lambda(x)) = \varphi(p(x)) \cdot q_0(x)$ بحيث $q_0(x) \in K[x]$ ومنه توجد

$\varphi: F[x] \rightarrow K[x]$ تماثل فإنه توجد $q(x) \in F[x]$ بحيث $\varphi(q(x)) = q_0(x)$ ومنه

يكون $\varphi(\lambda(x)) = \varphi(p(x)) \cdot \varphi(q(x)) = \varphi(p(x) \cdot q(x))$ وبالتالي يكون:

$$\lambda(x) = p(x) \cdot \varphi(q(x)) \in \langle p(x) \rangle$$

وهذا يبين لنا أن $\lambda(x) + \langle p(x) \rangle = \langle p(x) \rangle$ أي أن التشاكل θ متباين.

كما أن التطبيق θ غامر لأنه إذا كان $\langle \varphi(p(x)) \rangle \in F[x] / \langle \varphi(p(x)) \rangle$ فإن

$\eta_0(x) \in K[x]$ ولكون التشاكل $\varphi: F[x] \rightarrow K[x]$ تماثلاً فإنه يوجد $\eta(x) \in F[x]$

بحيث يكون $\varphi(\eta(x)) = \eta_0(x)$ ومنه نجد أن $\eta(x) + \langle p(x) \rangle$ هو عنصر من $F[x] / \langle p(x) \rangle$ وأن:

$$\theta(\eta(x) + \langle p(x) \rangle) = \varphi(\eta(x)) + \langle \varphi(p(x)) \rangle = \eta_0(x) + \langle \varphi(p(x)) \rangle$$

وهذا يبين لنا أن التشاكل θ غامر. مما سبق نجد أن التطبيق θ تماثل.

لنفرض أن $\mu = \beta^{-1} \cdot \theta \cdot \alpha: F(a) \rightarrow K(b)$ فنجد أن μ تماثلاً بالإضافة لذلك فإن:

$$\begin{aligned} \mu(a) &= \beta^{-1} \cdot \theta \cdot \alpha(a) = \beta^{-1} \cdot \theta(\alpha(a)) = \beta^{-1} \cdot \theta(x + \langle p(x) \rangle) = \\ &= \beta^{-1} \cdot \theta(x + \langle p(x) \rangle) = \beta^{-1}(\varphi(x) + \langle \varphi(p(x)) \rangle) = \\ &= \beta^{-1}(x + \langle \varphi(p(x)) \rangle) = b \end{aligned}$$

نأتي الآن إلى دراسة المبرهنة الآتية والتي سوف نثبت من خلالها أن أي حقلي تفريق لحدودية ما فوق حقل معين، هما حقلان متماثلان.

مبرهنة ٧-٢-٤.

ليكن F, K حقلين و $\varphi: F \rightarrow K$ تماثلاً حقيقياً، وليكن $f(x) \in F[x]$. إذا كان

E هو حقل التفريق للحدودية $f(x)$ فوق الحقل F و E' هو حقل التفريق للحدودية

$\varphi(f(x))$ فوق الحقل K ، عندئذ فإن $E \cong E'$.

البرهان.

سوف نورد البرهان بالاستقراء حسب درجة الحدودية $f(x)$.

- إذا كان $\partial f(x) = 1$ عندئذ $f(x) = a_1x + a_0$ حيث $a_1, a_0 \in F$ وأن $a_1 \neq 0$ ، وبما

أن F حقل فإن $x_0 = -a_1^{-1}a_0 \in F$ ومنه $f(x) = a_1(x - x_0) \in F[x]$ وهذا يبين لنا

أن $F = E$.

من جهة أخرى، ليكن $\varphi: F[x] \rightarrow K[x]$ التماثل الموافق للتماثل $\varphi: F \rightarrow K$ عندئذ
 $\varphi(a_1), \varphi(a_0) \in K$ ، وأن $\varphi(a_1) \neq 0$ وأن $\varphi(f(x)) = \varphi(a_1)x + \varphi(a_0)$ وذلك لكون φ
تماثلاً، وبما أن K حقل فإن $y_0 = -(\varphi(a_1))^{-1} \cdot \varphi(a_0) \in K$ وأن
 $\varphi(f(x)) = \varphi(a_1)(x - y_0) \in K[x]$

وهذا يبين لنا أن $E' = K$. مما سبق نجد أن $E = F \cong K = E'$.

- لنفرض الآن أن $\partial f(x) > 1$ وأن المبرهنة صحيحة لأجل جميع الحدوديات التي
درجة كل منها أصغر من $\partial f(x)$.

بما أن F حقلاً وأن $\partial f(x) > 1$ فإنه حسب المبرهنة (٢-٢-١) فإن $f(x)$ غير قابلة
للقلب في $F[x]$ وبالتالي فإن $f(x)$ يمكن كتابتها على شكل جداء منته لحدوديات أولية
في $F[x]$.

ليكن $p(x) \in F[x]$ أحد العوامل الأولية للحدودية $f(x)$ وليكن a صفراً للحدودية
 $p(x)$ في الحقل E و b صفراً للحدودية $\varphi(p(x))$ في الحقل E' ، عندئذ حسب
المبرهنة (٦-٢-٤) فإنه يوجد تماثل حقلي $\alpha: F(a) \rightarrow K(b)$ من أجله $\alpha(a) = b$.

من جهة أخرى، بما أن a صفر للحدودية $f(x)$ في الحقل $F(a)$ فإن
 $f(x) = (x - a) \cdot g(x)$ حيث $g(x) \in F(a)[x]$ ، عندئذ يكون E هو حقل التفريق
للحدودية $g(x)$ فوق الحقل $F(a)$. كما أن E' هو حقل التفريق للحدودية $\alpha(g(x))$
فوق الحقل $K(b)$ وبما أن $\partial g(x) < \partial f(x)$ فإنه حسب الفرض الاستقرائي يوجد
تماثل $\mu: E \rightarrow E'$ موافق للتماثل α على $F(a)$ وبالتالي موافق للتماثل φ على F .

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة النتيجة التالية والتي تثبت وحدانية حقل

التفريق:

نتيجة.

ليكن F حقلاً و $f(x) \in F[x]$. عندئذ أي حقلي تفريق للحدودية $f(x)$ فوق

الحقل F متماثلان.

البرهان.

لنفرض أن E و E' حقلًا تفريق للحدودية $f(x)$ فوق الحقل F عندئذٍ بالاعتماد على المبرهنة (٦-٢-٤) وبفرض أن $I_F : F \rightarrow F$ هو التماثل المطابق نجد أن $E \cong E'$.

لندرس الآن واحداً من الشروط التي من أجلها يكون حقل ما مغلقاً جبرياً وذلك من خلال المبرهنة الآتية:

مبرهنة ٨-٢-٤.

ليكن الحقل E تمديداً جبرياً للحقل F . إذا كانت كل حدودية $f(x) \in F[x]$ تتفارق فوق الحقل E ، عندئذٍ يكون الحقل E مغلقاً جبرياً.

البرهان.

نعلم أن $E \subseteq \bar{E}$. ليكن $a \in \bar{E}$ عندئذٍ يكون العنصر a جبرياً فوق الحقل E وحسب المبرهنة (٧-٣-٣) يكون الحقل $E(a)$ تمديداً منتهياً للحقل E وحسب المبرهنة (٣-٣-٦) يكون الحقل $E(a)$ تمديداً جبرياً للحقل E ، وبما أن الحقل E تمديد جبري للحقل F فإنه حسب المبرهنة (٨-٣-٣) يكون الحقل $E(a)$ تمديداً جبرياً للحقل F وبالتالي يكون العنصر a عنصراً جبرياً فوق الحقل F ، ومنه توجد $h(x) \in F[x]$ بحيث $h(x) \neq 0$ وأن $h(a) = 0$. وحسب الفرض فإن الحدودية $h(x)$ تتفارق فوق الحقل E ، وهذا يبين لنا أن جميع أصفار الحدودية $h(x)$ تنتمي إلى الحقل E وبشكل خاص العنصر a ، ومنه $a \in E$ وهكذا نجد أن $\bar{E} \subseteq E$. مما سبق نجد أن $E = \bar{E}$ أي أن الحقل E مغلق جبرياً.

تمهيدية ٩-٢-٤.

ليكن F حقلًا مميزه يساوي الصفر وأن الحقل K تمديد منته للحقل F . لنفرض أن E حقل جزئي في K يحوي F . إذا كان K حقل تفريق فوق F عندئذٍ يكون K حقل تفريق فوق E .

البرهان.

لنفرض أن K حقل تفريق فوق F عندئذٍ توجد حدودية $h(x) \in F[x]$ بحيث $\partial h(x) \geq 1$ وأن $K = F(a_1, a_2, \dots, a_n)$ حيث $a_i \in K$ هي جميع أصفار الحدودية

$h(x)$ في K ومنه يكون:

$$K = F(a_1, a_2, \dots, a_n) \subseteq L(a_1, a_2, \dots, a_n) \subseteq K$$

وهذا يبين أن $K = L(a_1, a_2, \dots, a_n)$ ولما كانت $h(x) \in F[x] \subseteq L[x]$ نجد أن K حقل تفريق فوق E .

مثال.

أثبت أن الحدودية $h(x) = x^4 - 3 \in Q[x]$ أولية فوق الحقل Q ثم أوجد حقل التفريق لها فوق Q .

الحل.

نلاحظ أن الحدودية $h(x)$ غير قابلة للقلب فوق Q ، لأن $\partial h(x) > 0$. حسب معيار أيزنشتاين ولأجل $p = 2$ نجد أن الحدودية $h(x)$ أولية فوق Q . كما أن :

$$h(x) = x^4 - 3 = (x^2 - \sqrt{3})(x^2 + \sqrt{3})$$

وهذا يبين أن أصفار الحدودية $h(x)$ هي $\pm \sqrt[4]{3}$ ، $\pm i \cdot \sqrt[4]{3}$ والتي يمكن التعبير عنها بالشكل الآتي $i^j \cdot \sqrt[4]{3}$ حيث $j = 0, 1, 2, 3$.

ومنه فإن حقل التفريق للحدودية $h(x)$ فوق Q هو:

$$Q(\sqrt[4]{3}, i \cdot \sqrt[4]{3}) = Q(\sqrt[4]{3}, i)$$

تمارين محلولة (٤)

١ - أوجد حقل تفريق الحدودية $f(x) = x^4 + 1 \in Q[x]$ فوق الحقل Q .
الحل.

نلاحظ أن جميع أصفار الحدودية $x^4 + 1$ هي:

$$\pm \sqrt{2}/2, \pm i \cdot \sqrt{2}/2$$

وهي جميعها تنتمي إلى الحقل $Q(\sqrt{2}, i)$. وبالتالي فإن أصغر حقل يحوي الحقل Q و أصفار الحدودية $f(x)$ هو الحقل $Q(\sqrt{2}, i)$ والذي يعد حقل التفريق للحدودية $f(x)$.

٢ - ليكن $a \in Q$ عدداً موجباً ولنأخذ الحدودية $f(x) = x^n - a \in Q[x]$. أوجد جميع أصفار الحدودية $f(x)$ فوق الحقل Q .
الحل.

بفرض أن y هو صفر للحدودية $f(x)$ فوق الحقل Q ، عندئذ $f(y) = 0$ ومنه $y^n = a$ أي أن $y = \sqrt[n]{a} = \sqrt[n]{a} \cdot \sqrt[n]{1}$.
لنفرض أن $w = \sqrt[n]{1}$ فنجد أن:

$$w^n = 1 = \cos 360 + i \sin 360$$

وحسب قانون دومافر فإن:

$$w = \sqrt[n]{1} = \cos 360/n + i \sin 360/n$$

حيث $n = 1, 2, \dots$ وأن $w^k \neq 1$ أيًا كان $1 \leq k \leq n$ وبالتالي يكون:

$$a^{1/n}, wa^{1/n}, w^2 a^{1/n}, \dots, w^{n-1} a^{1/n}$$

هي جميع أصفار الحدودية $f(x)$ فوق الحقل Q أو في الحقل $Q(\sqrt[n]{a}, w)$.

من أجل $n = 6, a = 3$ نجد أن $f(x) = x^6 - 3 \in Q[x]$ وأن:

$$w = \sqrt[6]{1} = 1/2 + i \sqrt{3}/2, \quad w^2 = -1/2 + i \sqrt{3}/2, \quad w^3 = -1$$

$$w^4 = -1/2 - i \sqrt{3}/2, \quad w^5 = 1/2 - i \sqrt{3}/2$$

وهكذا نجد أن أصفار الحدودية $f(x)$ فوق الحقل Q هي:

$$\sqrt[6]{3}, (1/2 + i\sqrt{3}/2)\sqrt[6]{3}, (-1/2 + i\sqrt{3}/2)\sqrt[6]{3}, -\sqrt[6]{3} \\ (-1/2 - i\sqrt{3}/2)\sqrt[6]{3}, (1/2 - i\sqrt{3}/2)\sqrt[6]{3},$$

٣ - ليكن F حقلاً و $a \in F$. إذا كانت $f(x) \in F[x]$ ، أثبت أن الحدوديتين $f(x)$ و $f(x+a)$ لهما حقل تفريق واحد.

الحل.

نفرض أن $a_1, a_2, \dots, a_n$ هي جميع أصفار الحدودية $f(x)$ في تمديد ما للحقل F ، عندئذ يكون الحقل $F(a_1, a_2, \dots, a_n)$ هو حقل تفريق الحدودية $f(x)$ فوق الحقل F . من جهة أخرى، إذا كان a_j صفراً للحدودية $f(x)$ فإن $x = a_j - a$ هو صفر للحدودية $f(x+a)$ لأن:

$$f(x+a) = f(a_j - a + a) = f(a_j) = 0$$

ومنه نجد أن جميع أصفار الحدودية $f(x+a)$ هي:

$$a_1 - a, a_2 - a, \dots, a_n - a$$

وبالتالي فإن حقل تفريق الحدودية $f(x+a)$ فوق F هو:

$$F(a_1 - a, a_2 - a, \dots, a_n - a)$$

لنبرهن الآن على أن:

$$F(a_1 - a, a_2 - a, \dots, a_n - a) = F(a_1, a_2, \dots, a_n)$$

نلاحظ أنه أياً كان $1 \leq j \leq n$ فإنه حسب المبرهنة (٣-١-٢) فإن:

$$F(a_j) = F(1 \cdot a_j - a) = F(a_j - a)$$

$$\text{ومنه نجد أن } F(a_1 - a, a_2 - a, \dots, a_n - a) = F(a_1, a_2, \dots, a_n)$$

٤ - ليكن F حقلاً و $p(x) \in F[x]$ حدودية أولية فوق F . ليكن الحقل K تمديداً للحقل

F و $a, b \in K$ أصفاراً للحدودية $p(x)$. أثبت أنه يوجد تماثل $\mu: F(a) \rightarrow F(b)$ من أجله $\mu(a) = b$.

الحل.

بما أن الحدودية $p(x)$ أولية فوق F ، فإن المثالي $A = \langle p(x) \rangle$ يكون أعظمية في $F[x]$ وبالتالي تكون حلقة الخارج $F[x]/A$ حقلاً. بما أن العنصر a هو صفر للحدودية $p(x)$ فإنه حسب التمهيدية (٥-٢-٤) يوجد تماثل $\alpha: F(a) \rightarrow F[x]/A$ من أجله $\alpha(a) = x + A$.

أيضاً بما أن العنصر b هو صفر للحدودية $p(x)$ فإنه حسب التمهيدية (٥-٢-٤) يوجد تماثل:

$$\beta: F(b) \rightarrow F[x]/A$$

من أجله $\beta(b) = x + A$. لنضع $\mu = \beta^{-1}\alpha$ فنجد أن $\mu: F(a) \rightarrow F(b)$ وأن:

$$\mu(a) = \beta^{-1}\alpha(a) = \beta^{-1}(x + A) = b$$

$$٥ - \text{ أثبت أن } Q(1 + \sqrt{2}) = Q(\sqrt{2}).$$

الحل.

بما أن $Q(\sqrt{2})$ حقلاً وأن $1, \sqrt{2} \in Q(\sqrt{2})$ نجد أن $1 + \sqrt{2} \in Q(\sqrt{2})$ ومنه فإن $Q(1 + \sqrt{2}) \subseteq Q(\sqrt{2})$.

من جهة أخرى، لدينا $-1, 1 + \sqrt{2} \in Q(1 + \sqrt{2})$ وبالتالي فإن:

$$\sqrt{2} = -1 + (1 + \sqrt{2}) \in Q(1 + \sqrt{2})$$

ومنه فإن $Q(1 + \sqrt{2}) = Q(\sqrt{2})$ ، وهكذا نجد أن $Q(1 + \sqrt{2}) = Q(\sqrt{2})$.

٦ - ليكن الحقل E تمديداً للحقل F . ولتكن B, D حقولاً جزئية في E كل منها تمديد للحقل F . عندئذ فإن $B \cap D$ هو حقل جزئي في E وهو تمديد للحقل F .

الحل.

نعلم أن تقاطع حقلين جزئيين هو حقل جزئي، ومنه فإن $B \cap D$ هو حقل جزئي في E . بما أن كلا من B و D هو تمديد للحقل F فإن $F \subseteq B$ و $F \subseteq D$ ومنه $F \subseteq B \cap D$ أي أن $B \cap D$ هو تمديد للحقل F .

٧ - ليكن الحقل E تمديداً للحقل F . ولتكن B, D حقولاً جزئية في E كل منها تمديد للحقل F . عندئذ يوجد في E حقل جزئي أصغري يحوي B و D نرمز له $B.D$ وهو

تمديد للحقل F .

الحل.

لنأخذ المجموعة $\mathfrak{L}$ المؤلف من جميع الحقول الجزئية في E والتي كل منها يحوي B و D . لنضع $BD = \bigcap_{L \in \mathfrak{L}} L$. إن BD هو حقل جزئي في E . بما أنه أي $L \in \mathfrak{L}$ فإن $B \subseteq L$ و $D \subseteq L$ نجد أن $B \subseteq BD$ وأيضاً $D \subseteq BD$. أي أن BD هو حقل جزئي في E يحوي كلا من B و D . من جهة أخرى، بما أن $F \subseteq B \subseteq BD$ نجد أن B, D هو تمديد للحقل F .

ليكن K حقل جزئي آخر يحوي B و D عندئذ فإن $K \in \mathfrak{L}$ ومنه فإن $B, D \subseteq K$ وهذا يبين لنا أن BD هو أصغر حقل جزئي في E يحوي B و D .

٨ - ليكن الحقل K تمديداً للحقل F وليكن $a \in K$. إذا كانت $f(x) \in F[x]$ وكان العنصر $f(a)$ جبرياً فوق F ، أثبت أن العنصر a هو أيضاً جبرياً فوق F .

الحل.

لنفرض أن العنصر $f(a)$ جبري فوق F ، عندئذ توجد $g(x) \in F[x]$ $0 \neq g(x)$ بحيث $g(f(a)) = 0$. بما أن $g(x) \in F[x]$ فإن $g(f(x)) \in F[x]$ و $0 \neq g(f(x))$ وأن $g(f(a)) = 0$ وهذا يبين لنا أن العنصر a هو عنصر جبري فوق F .

٩ - لتكن E هي الغلاقة الجبرية للحقل F . أثبت أن كل حدودية في $F[x]$ تتفرق في $E[x]$.

الحل.

لنفرض أن E هي الغلاقة الجبرية للحقل F وأن $0 \neq f(x) \in F[x]$. بما أن كل صفر للحدودية $f(x)$ يحقق $f(a) = 0$ نجد أن كل صفر للحدودية $f(x)$ هو عنصر جبري فوق F . وبما أن E هي الغلاقة الجبرية للحقل F فإن $a \in E$. وهذا يبين أن جميع أصفار الحدودية $f(x)$ تنتمي للحقل E ومنه فإن الحدودية $f(x)$ تتفرق فوق E .

١٠ - أوجد حقل التفريق للحدودية $f(x) = (x^2 - 3)(x^3 + 1) \in Q[x]$.

الحل.

بما أن $f(x) = (x - \sqrt{3})(x + \sqrt{3})(x - 1)(x^2 + x + 1) \in Q[x]$ نجد أن حقل التفريق للحدودية $f(x)$ يجب أن يحوي $\sqrt{3}$ و i ومنه نجد أن حقل التفريق هو $Q(\sqrt{3}, i)$.

١١ - ليكن F حقلاً مميزه $p \neq 0$ ولتكن $f(x) = x^p - a \in F[x]$. أثبت أنه إما $f(x)$ أولية فوق F أو أن $f(x)$ تتفارق فوق F .

الحل.

بما أن $f(x) = x^p - a \in F[x]$ ، عندئذ فإن $a \in F$. وهنا نميز حالتين:
- الأولى. $a \notin F^p$ وحسب المبرهنة (٤-٢-١) فإن الحدودية $f(x)$ تكون أولية في $F[x]$.

- الثانية. $a \in F^p$ عندئذ يوجد $b \in F$ بحيث $a = b^p$ ومنه نجد أن:

$$f(x) = x^p - a = x^p - b^p = (x - b)^p$$

ومنه نجد أن $f(x)$ تتفارق في $F[x]$.

١٢ - ليكن الحقل E تمديداً جبرياً للحقل F . إذا كانت كل حدودية في $F[x]$ تتفارق في E ، أثبت أن الحقل E مغلق جبرياً.

الحل.

لتكن $\bar{E}$ الغلافة الجبرية للحقل E فوق F . بما أن الحقل E هو تمديد جبري للحقل F فإن $F \subseteq E \subseteq \bar{E}$.

ليكن $a \in \bar{E}$ عندئذ فإن a هو عنصر جبري فوق F ومنه توجد $h(x) \in F[x]$ بحيث $h(a) = 0$ وحسب الفرض فإن $h(x)$ تتفارق في E وبالتالي فإن E يحوي جميع أصفار الحدودية $h(x)$ بما فيها a ، أي أن $a \in E$. ومنه نجد أن $E = \bar{E}$ وبالتالي الحقل E مغلق جبرياً.

١٣ - ليكن الحقل K تمديداً للحقل F . إذا كان $[K : F] = 2$ أثبت أن الحقل K هو حقل تفريق مجموعة من الحدوديات فوق F .

الحل.

لنفرض أن $[K:F] = 2$ عندئذ فإن الحقل K هو تمديد منته للحقل F وبالتالي هو تمديد جبري للحقل F . من جهة أخرى، يوجد $a, b \in K$ بحيث يكون $K = F(a, b)$. ومنه فإن $x - a, x - b \in K[x]$ كما أن:

$$x^2 - (a+b)x + ab = (x-a)(x-b) \in K[x]$$

وهذا يبين أن الحقل K هو حقل تفريق للحدوديات:

$$x^2 - (a+b)x + ab, (x-a), (x-b)$$

١٤ - لنفرض أن R هو حقل الأعداد الحقيقية. ليكن $\sigma: R \rightarrow R$ تماثلاً ذاتياً للحقل R وليكن $a, b \in R$ والمطلوب:

١ - إذا كان $a > 0$ أثبت أن $\sigma(a) > 0$.

٢ - إذا كان $a > b$ أثبت أن $\sigma(a) > \sigma(b)$.

الحل.

١ - لنفرض أن $a > 0$ ، عندئذ فإن $\sqrt{a} \in R$ ومنه فإن $a = \sqrt{a} \cdot \sqrt{a}$ وبالتالي يكون:

$$\sigma(a) = \sigma(\sqrt{a} \cdot \sqrt{a}) = \sigma(\sqrt{a}) \cdot \sigma(\sqrt{a}) = (\sigma(\sqrt{a}))^2 > 0$$

٢ - لنفرض أن $a > b$ ، عندئذ فإن $a - b > 0$ وحسب (١) نجد أن $\sigma(a - b) > 0$ وأن $\sigma(a - b) = \sigma(a) - \sigma(b) > 0$ وهذا يبين أن $\sigma(a) > \sigma(b)$.

تمارين (٤)

- ١ - أوجد حقل التفريق للحدودية $x^4 - 1$ فوق الحقل Q .
- ٢ - أوجد حقل التفريق للحدودية $x^3 - 1$ فوق الحقل Q .
- ٣ - أوجد حقل التفريق للحدودية $(x^2 - x + 1)(x^2 + x + 1) = x^4 + x^2 + 1$ فوق الحقل Q .
- ٤ - أوجد حقل تفريق للحدودية $x^4 - x^2 - 2$ فوق الحقل Z_3 .
- ٥ - أوجد الحدودية $p(x)$ في $Q[x]$ التي تحقق أن $\langle p(x) \rangle \cong Q(\sqrt{1+\sqrt{5}})$.
- ٦ - اكتب الحدودية $x^3 + 2x + 1$ على شكل جداء لمضاريب خطية في تمديد ما للحقل Z_3 .
- ٧ - اكتب الحدودية $x^8 - x$ على شكل جداء مضاريب لحدوديات أولية فوق Z_2 .
- ٨ - أوجد حقل التفريق للحدودية $f(x) = x^2 - 4x + 4$ فوق الحقل Q .
- ٩ - أوجد حقل التفريق للحدودية $x^3 + x + 1$ فوق الحقل Z_2 ثم اكتب الحدودية $x^3 + x + 1$ على شكل جداء لمضاريب خطية فوق حقل التفريق هذا.
- ١٠ - أثبت أن أي حقل منته مرتبته p^n حيث p عدد أولي و n عدد صحيح موجب.
- ١١ - أوجد حقل التفريق K للحدودية $f(x) = x^2 - 2x + 4$ فوق الحقل Q ، ثم أوجد $[K : Q]$.
- ١٢ - أوجد حقل التفريق K للحدودية $f(x) = x^2 - 2x - 1$ فوق الحقل Q ، ثم أوجد $[K : Q]$.
- ١٣ - أوجد حقل التفريق K للحدودية $f(x) = x^4 - 2$ فوق الحقل Q ، ثم أوجد $[K : Q]$.
- ١٤ - ليكن F حقل منته مرتبته n . أثبت أنه أياً كان $x \in F$ بحيث $x \neq 0$ فإن $x^{n-1} = 1$.

١٥ - ليكن F حقلاً منتهياً مرتبته 32. أثبت أن الحقول الجزئية في F هي فقط F و $\{0,1\}$.

١٦ - ليكن F حقلاً منتهياً مرتبته أكبر من 2. أثبت أن مجموع عناصر هذا الحقل تساوي $\{0\}$.

١٧ - ليكن n عدداً صحيحاً موجباً. أثبت أن $(n-1)! \equiv (n-1) \pmod{-n}$ عندما وفقط عندما يكون العدد n أولياً.

١٨ - لأجل أي عدد أولي p ، أثبت أن $(p-2)! \equiv 1 \pmod{-p}$.

١٩ - ليكن F حقلاً ولتكن $I = \{f(x) : f(x) \in F[x]; f(a) = 0 \forall a \in F\}$.

١. أثبت أن المجموعة I تشكل مثاليًا في $F[x]$.

٢. إذا كان الحقل F منته، أثبت أن المثالي I غير منته.

٣. إذا كان الحقل F غير منته، أثبت أن المثالي $I = \{0\}$.

٢٠ - لأجل أي عدد أولي p ، أثبت أن:

$$x^{p-1} - 1 = (x-1)(x-2) \cdots [x-(p-1)]$$

في الحقل $Z_p[x]$.

٢١ - لنأخذ الحقل Z_{13} بالنسبة لعمليتي الجمع والضرب بالمقاس 13. ولنأخذ المجموعة

$$Z_{13}(i) = \{a + bi : a, b \in Z_{13} : i^2 = -1\}$$

والمطلوب:

١. أوجد جميع عناصر المجموعة $Z_{13}(i)$.

٢. أثبت أن المجموعة $Z_{13}(i)$ لا تشكل حقلاً.

٢٢ - أوجد حقل التفريق للحدوديات الآتية:

$$(x^2 - 1)(x^3 - 3), \quad (x^2 - 1)(x^3 - 2)$$

فوق الحقل Q .

الفصل الخامس

التمديدات المنفصلة

٥ - ١. المشتق والأصفار.

نعلم حتى الآن أن كل حدودية فوق حقل ما، درجتها أكبر من الصفر يمكن أن تتفريق في تمديد ما لهذا الحقل، وذلك حسب المبرهنة (٤-٢-٢). السؤال الذي يتبادر إلى الذهن هو التالي، هل توجد طرق خاصة لتفريق الحدوديات الأولية؟. الإجابة نعم توجد طرق خاصة لأجل تفريق الحدوديات الأولية. ولدراسة هذه الطرق نحن بحاجة إلى مفهوم جديد وهو مشتق الحدودية، الذي سوف نورده من خلال التعريف الآتي:

تعريف.

ليكن F حقلاً و $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in F[x]$. إن مشتق الحدودية $f(x)$ هو حدودية في $F[x]$ نرمز لها $f'(x)$ وتساوي:

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1 \in F[x]$$

لنورد الآن بعضاً من خواص المشتق للحدوديات وذلك من خلال التمهيدية الآتية:

تمهيدية ٥-١-١.

ليكن F حقلاً و $f(x), g(x) \in F[x]$ وليكن $a \in F$. عندئذ:

$$1. (f(x) + g(x))' = f'(x) + g'(x)$$

$$2. (a \cdot f(x))' = a \cdot f'(x)$$

$$3. (f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$$

البرهان.

نتركه للقارئ. ♦

لندرس الآن ومن خلال التمهيدية التالية، متى يكون مشتق حدودية ما يساوي الصفر وذلك في حالة كون مميز الحقل يساوي الصفر.

تمهيدية ٥-١-٢.

ليكن F حقلاً مميزه يساوي الصفر و $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ بحيث $f(x) \in F[x]$ و $f(x) \neq 0$. عندئذ:

١ - الشرط اللازم والكافي كي يكون $f'(x) = 0$ هو أن يكون $a_j = 0$ وذلك أيّاً كان $j = 1, 2, \dots, n$.

٢ - إذا كان $\partial f(x) > 0$ فإن $f'(x) \neq 0$.

البرهان.

١ - لزوم الشرط. لنفرض أن $f'(x) = 0$ عندئذ:

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1 = 0$$

ومنه يكون $a_j = 0$ وذلك أيّاً كان $j = 1, 2, \dots, n$.

كفاية الشرط. لنفرض أن $a_j = 0$ وذلك أيّاً كان $j = 1, 2, \dots, n$. عندئذ يكون:

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1 = 0$$

٢ - لنفرض أن $\partial f(x) > 0$ عندئذ يكون $f'(x) \neq 0$ ، لأنه إذا كان $f'(x) = 0$ عندئذ

حسب (١) يكون $f(x) = a_0 \in F$ وهذا يبين لنا أن $\partial f(x) = 0$ وهذا غير ممكن، وبالتالي فإن $f'(x) \neq 0$.

أما الآن فسوف ندرس ومن خلال المبرهنة الآتية، متى يكون مشتق حدودية ما يساوي الصفر وذلك في حالة كون مميز الحقل لا يساوي الصفر.

مبرهنة ٥-١-٣.

ليكن F حقلاً مميزه يساوي $p \neq 0$ و $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ بحيث $f(x) \in F[x]$ و $f(x) \neq 0$. الشرط اللازم والكافي كي يكون $f'(x) = 0$ هو أن يكون $f(x) = g(x^p)$ ، حيث $g(x) \in F[x]$.

البرهان.

لزوم الشرط. لنفرض أن $f'(x) = 0$ ، عندئذ يكون:

$$n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1 = 0$$

ومنه نجد أن $m \cdot a_m = 0$ حيث $1 \leq m \leq n$. بما أن:

$$m \cdot a_m = m \cdot (1_F \cdot a_m) = (m \cdot 1_F) \cdot a_m = 0$$

نجد أنه إما $a_m = 0$ أو $(m \cdot 1_F) = 0$.

- إذا كان $a_m = 0$ فإن $a_m x^m = 0$.

- إذا كان $(m \cdot 1_F) = 0$ ، عندئذٍ وحسب خوارزمية القسمة لأجل العددين p, m يوجد $q, r \in \mathbb{Z}$ بحيث $m = qp + r$ حيث $0 \leq r < p$. إن $r = 0$ لأنه إذا كان $r \neq 0$ عندئذٍ يكون $m \cdot 1_F = (q \cdot 1_F) \cdot (p \cdot 1_F) + r \cdot 1_F$ ومنه يكون $r \cdot 1_F = 0$ حيث $0 < r < p$ وهذا يناقض كون p مميزاً للحقل F . ومنه نجد أن $r = 0$ وبالتالي يكون $m = q \cdot p$ وهذا يبين لنا أن $a_m x^m = a_m x^{qp}$. مما سبق نجد أنه أيأ كان $1 \leq m \leq n$ فإن $a_m x^m = a_m x^{qp}$.

بهذا الشكل نجد أن كل حد من الحدود $a_0, a_1 x, \dots, a_{n-1} x^{n-1}, a_n x^n$ إما أن يساوي الصفر أو أن درجته هي من مضاعفات العدد p ، ومنه نجد أن $f(x) = g(x^p)$ حيث $g(x) \in F[x]$.

كفاية الشرط. لنفرض أن $f(x) = g(x^p)$ حيث $g(x) \in F[x]$ عندئذٍ بالإمكان كتابة $f(x)$ بالشكل الآتي $f(x) = b_n x^{np} + b_{n-1} x^{(n-1)p} + \dots + b_1 x^p + b_0$ حيث $b_i \in F$ وذلك أيأ كان $0 \leq i \leq n$ ، ومنه فإن:

$$f'(x) = n \cdot p \cdot b_n x^{(np)-1} + (n-1) \cdot p \cdot b_{n-1} x^{[(n-1)p]-1} + \dots + p \cdot b_1 x^{p-1}$$

وبما أن p مميز الحقل F فإن $p \cdot b_j = 0$ وذلك أيأ كان $1 \leq j \leq n$ وهذا يبين لنا أن $f'(x) = 0$.

تعريف.

ليكن F حقلاً و $f(x) \in F[x]$ ، وليكن a صفراً للحدودية $f(x)$ في تمديد ما E للحقل F .

١. نقول إن a صفر بسيط للحدودية $f(x)$ إذا كانت $(x-a)$ تقسم $f(x)$ في $E[x]$.

بالشكل $f(x) = (x-a) \cdot g(x)$ حيث $g(x) \in E[x]$ وأن $g(a) \neq 0$.

٢. نقول إن a صفر مضاعف للحدودية $f(x)$ من المرتبة k إذا كانت $(x-a)^k$ تقسم

$f(x)$ في $E[x]$ بالشكل $f(x) = (x-a)^k \cdot g(x)$ حيث $g(x) \in E[x]$ وأن

$g(a) \neq 0$ ، وحيث $k \geq 2$ عدد صحيح.

لندرس الآن الشرط اللازم والكافي كي تملك حدودية ما جذراً بسيطاً وذلك من خلال التمهيدية الآتية:

تمهيدية ٥-١-٤.

ليكن F حقلاً و $f(x) \in F[x]$ وليكن a صفراً للحدودية $f(x)$ في تمديد ما E للحقل F . الشرط اللازم والكافي كي يكون a صفراً بسيطاً للحدودية $f(x)$ هو أن يكون $f'(a) \neq 0$.

البرهان.

لزوم الشرط. لنفرض أن a صفر بسيط للحدودية $f(x)$ في تمديد ما E للحقل F عندئذ $f(x) = (x-a) \cdot g(x)$ حيث $g(x) \in E[x]$ وأن $g(a) \neq 0$. ومنه نجد أن $f'(x) = g(x) + (x-a) \cdot g'(x)$ وبالتالي يكون $f'(a) = g(a) \neq 0$.

كفاية الشرط. لنفرض أن $f'(a) \neq 0$. بما أن a صفر للحدودية $f(x)$ في تمديد ما E للحقل F فإن $(x-a)^k$ تقسم $f(x)$ في $E[x]$ حيث $k \geq 1$ عدد صحيح. ومنه توجد $g(x) \in E[x]$ بحيث $f(x) = (x-a)^k \cdot g(x)$ إذا كان $k > 1$ عندئذ يكون:

$$f'(x) = k \cdot (x-a)^{k-1} \cdot g(x) + (x-a)^k \cdot g'(x)$$

ومنه يكون $f'(a) = 0$ ، وهذا غير ممكن. مما سبق نجد أن $k = 1$ وهذا يبين أن a هو صفر بسيط للحدودية $f(x)$.

لندرس الآن الشرط اللازم والكافي كي تملك حدودية ما صفراً مضاعفاً وذلك من خلال المبرهنة الآتية:

مبرهنة ٥-١-٥.

ليكن F حقلاً و $f(x) \in F[x]$. عندئذ الحدودية $f(x)$ تملك صفراً مضاعفاً في تمديد ما E للحقل F عندما وفقط عندما، كل من $f(x)$ و $f'(x)$ يملكان قاسماً مشتركاً في $F[x]$ درجته موجبة.

البرهان.

لنزم الشرط. لنفرض أن الحدودية $f(x)$ تملك صفراً مضاعفاً a في تمديد ما E للحقل F ، عندئذ يوجد عدد صحيح $k > 1$ بحيث $(x-a)^k$ تقسم $f(x)$ في $E[x]$ ومنه يوجد $g(x) \in E[x]$ بحيث $f(x) = (x-a)^k \cdot g(x)$ وبالتالي يكون:

$$f'(x) = k \cdot (x-a)^{k-1} \cdot g(x) + (x-a)^k \cdot g'(x)$$

وهنا نجد أن $(x-a)$ هو قاسم مشترك لكل من $f(x)$ و $f'(x)$ في $E[x]$. لنفرض جـداً أنه لا توجد قواسم مشتركة بين $f(x)$ و $f'(x)$ في $F[x]$ وبما أن $f(x), f'(x) \in F[x]$ ينتج أن العنصرين $f(x)$ و $f'(x)$ أوليان فيما بينهما في $F[x]$ وبالتالي يوجد $h(x), \mu(x) \in F[x]$ بحيث أن $f(x) \cdot h(x) + f'(x) \cdot \mu(x) = 1$. وبالنظر إلى $f(x) \cdot h(x) + f'(x) \cdot \mu(x)$ على أنه عنصر في $E[x]$ نجد أن:

$$\begin{aligned} f(x) \cdot h(x) + f'(x) \cdot \mu(x) &= (x-a)^k \cdot g(x) \cdot h(x) + \\ &+ k \cdot (x-a)^{k-1} \cdot g(x) \cdot \mu(x) + (x-a)^k \cdot g'(x) \cdot \mu(x) \end{aligned}$$

ومنه نجد أن:

$$\begin{aligned} 1 &= (x-a) \cdot [(x-a)^{k-1} \cdot g(x) \cdot h(x) + k \cdot (x-a)^{k-2} \cdot g(x) \cdot \mu(x) + \\ &+ (x-a)^{k-1} \cdot g'(x) \cdot \mu(x)] \end{aligned}$$

بفرض أن:

$$\begin{aligned} \theta(x) &= (x-a)^{k-1} \cdot g(x) \cdot h(x) + k \cdot (x-a)^{k-2} \cdot g(x) \cdot \mu(x) + \\ &+ (x-a)^{k-1} \cdot g'(x) \cdot \mu(x) \end{aligned}$$

نجد أن $1 = (x-a) \cdot \theta(x)$ حيث $\theta(x) \in E[x]$ وهذا يبين لنا أن $(x-a)$ يقسم الواحد في $E[x]$ وهذا غير ممكن، ومنه نجد أن كلاً من $f(x)$ و $f'(x)$ يملك قاسماً مشتركاً في $F[x]$ درجته موجبة.

كفاية الشرط. لنفرض أن كلاً من $f(x)$ و $f'(x)$ يملكان قاسماً مشتركاً في $F[x]$ درجته موجبة. لنفرض جـداً أن $f(x)$ لا يملك صفراً مضاعفاً. وليكن a صفراً للقاسم المشترك، ومنه يكون a صفراً لكل من $f(x)$ و $f'(x)$. وبالتالي يوجد $q(x) \in F[x]$ بحيث أن $f(x) = (x-a) \cdot q(x)$ وأن $q(a) \neq 0$ ، ومنه نجد أن:

$$f'(x) = q(x) + (x-a) \cdot q'(x)$$

وهكذا نجد أن $f'(a) = q(a) = 0$ ، وهذا غير ممكن. مما سبق نجد أن الحدودية $f(x)$ تملك صفراً مضاعفاً.

لندرس الآن الشرط اللازم كي تملك الحدودية الأولية صفراً مضاعفاً وذلك حسب حالة مميز للحقل، من خلال المبرهنة الآتية:

مبرهنة ٥-١-٦.

ليكن F حقلاً و $f(x) \in F[x]$ حدودية أولية في $F[x]$. عندئذ:

١ - إذا كان مميز الحقل F يساوي الصفر عندئذ الحدودية $f(x)$ لا تملك أصفاراً مضاعفة في أي تمديد للحقل F .

٢ - إذا كان مميز الحقل F يساوي $p \neq 0$ ، وكانت الحدودية $f(x)$ تملك صفراً مضاعفاً في تمديد ما للحقل F ، عندئذ $f(x) = g(x^p)$ ، حيث $g(x) \in F[x]$.

البرهان.

١ - لنفرض أن مميز الحقل F يساوي الصفر. لنفرض جداً أن الحدودية $f(x)$ تملك صفراً مضاعفاً في تمديد ما للحقل F عندئذ حسب المبرهنة (٥-١-٥) فإن $f(x)$ و $f'(x)$ يملكان قاسماً مشتركاً في $F[x]$ درجته موجبة وليكن $g(x)$. ومنه فإن $g(x) \in F[x]$ وأن $\partial g(x) > 0$. وبالتالي يوجد $q(x), r(x) \in F[x]$ بحيث $f(x) = g(x) \cdot q(x)$ و $f'(x) = g(x) \cdot r(x)$. وبما أن الحدودية $f(x)$ أولية في $F[x]$ عندئذ إما $g(x)$ قابلة للقلب أو $q(x)$ قابلة للقلب في $F[x]$. بما أن $\partial g(x) > 0$ فإن $g(x)$ غير قابل للقلب في $F[x]$ ، ومنه نجد أن $q(x)$ قابل للقلب في $F[x]$ وبالتالي يكون $q(x) = b$ حيث $b \in F$ و $b \neq 0$. وهكذا نجد أن $f(x) = b^{-1} \cdot f(x)$ وبالتالي يكون $f'(x) = b^{-1} \cdot f(x) \cdot r(x)$ وهذا يبين لنا أن $\partial f'(x) \geq \partial f(x)$ وهذا غير ممكن.

مما سبق نجد أن الحدودية $f(x)$ لا تملك أصفاراً مضاعفة في أي تمديد للحقل F .

٢ - لنفرض أن مميز الحقل F يساوي $p \neq 0$. ولنفرض أن الحدودية $f(x)$ تملك صفراً مضاعفاً في تمديد ما للحقل F عندئذ حسب المبرهنة (٥-١-٥) فإن $f(x)$ و $f'(x)$ يملكان قاسماً مشتركاً في $F[x]$ درجته موجبة وليكن $g(x)$ ، ومنه $g(x) \in F[x]$ وأن $\partial g(x) > 0$. وبالتالي يوجد $q(x), r(x) \in F[x]$ بحيث

فإن $f(x) = g(x) \cdot q(x)$ و $f'(x) = g(x) \cdot r(x)$. وبما أن الحدودية $f(x)$ أولية في $F[x]$ عندئذ إما $g(x)$ قابلة للقلب أو $q(x)$ قابلة للقلب في $F[x]$. بما أن $\partial g(x) > 0$ فإن $g(x)$ غير قابلة للقلب في $F[x]$ ، ومنه نجد أن $q(x)$ قابلة للقلب في $F[x]$ وبالتالي يكون $q(x) = b$ حيث $b \in F$ و $b \neq 0$. وهكذا نجد أن $g(x) = b^{-1} \cdot f(x)$ وبالتالي يكون $f'(x) = b^{-1} \cdot f(x) \cdot r(x)$ وهذا يبين لنا أن $f'(x) = 0$ وحسب المبرهنة (٣-١-٤) فإن $f(x) = g(x^p)$ ، حيث $g(x) \in F[x]$.

وجدنا من خلال التمرين المحلول (١-٣) أن بعض الحقول المولدة بعنصرين يمكن أن تكون تمديدات بسيطة، المبرهنة التالية تثبت لنا أنه ضمن شروط محددة فإن هذا الأمر محقق دوماً:

مبرهنة ٧-١-٥

ليكن F حقلاً مميزه يساوي الصفر، وليكن الحقل K تمديداً ما للحقل F وليكن $a, b \in K$ عنصرين جبريين فوق F . عندئذ يوجد $c \in F(a, b)$ بحيث $F(c) = F(a, b)$.

البرهان.

لتكن $p(x) \in F[x]$ الحدودية الأصغرية للعنصر الجبري a فوق F و $g(x) \in F[x]$ الحدودية الأصغرية للعنصر الجبري b فوق F . لنفرض أن $a = a_1, a_2, \dots, a_n$ هي جميع الأصفار المختلفة للحدودية $p(x)$ في K وأن $b = b_1, b_2, \dots, b_m$ هي جميع الأصفار المختلفة للحدودية $g(x)$ في K .

نختار العنصر $d \in F$ بحيث $d \neq (a_i - a)(b - b_j)^{-1}$ وذلك لأجل جميع قيم $i \geq 1$ و $j > 1$. بمعنى آخر، نختار العنصر d بحيث $a_i \neq a + d(b - b_j)$ وذلك أيأ كان $j > 1$. لنضع $c = a + db$ ولنبرهن على أن $F(c) = F(a, b)$.

بما أن $a, b \in F(a, b)$ وأن $d \in F$ فإن $c = a + db \in F(a, b)$ ومنه نجد أن $F(c) \subseteq F(a, b)$. لنبرهن الآن على أن $b \in F(c)$.

لنأخذ الحدوديات $g(x)$ و $r(x) = p(c - dx)$ فنجد أن $g(x) \in F(c)[x]$ وأيضاً: $r(x) = p(c - dx) = p(a) = 0$ كما أن $r(b) = p(c - db) = p(a) = 0$ و $g(b) = 0$.

لنفرض أن $h(x) \in F(c)[x]$ الحدودية الأصغرية للعنصر b فوق $F(c)$. عندئذ حسب المبرهنة (٣-٣-٤) فإن $h(x)$ تقسم كلاً من $g(x)$ و $r(x)$ في $F(c)[x]$. وبالتالي توجد $\alpha(x), \lambda(x) \in F(c)[x]$ بحيث $g(x) = h(x) \cdot \lambda(x)$ و $r(x) = h(x) \cdot \alpha(x)$ وبما أن كل صفر للحدودية $h(x)$ في K هو صفر لكل من الحدوديتين $g(x)$ و $r(x)$ نجد أن جميع الأصفار الممكنة للحدودية $h(x)$ في K تنتمي للمجموعة:

$$\{a_1, \dots, a_n, b_1, b_2, \dots, b_m\}$$

بما أن $r(b_j) = p(c - db_j) = p(a + db - db_j) = p(a + d(b - b_j)) \neq 0$ وذلك حسب اختيارنا للعنصر $d \neq (a_i - a)(b - b_j)^{-1}$ لأجل جميع القيم $j > 1$. وهذا يبين لنا أن b هو الصفر الوحيد للحدودية $h(x)$ في K ، ومنه نجد أن $h(x) = (x - b)^t$. وبما أن مميز الحقل F يساوي الصفر فإنه حسب المبرهنة (٥-١-٦) الحدودية $h(x)$ لا تملك أصفاراً مضاعفة وبالتالي فإن $t = 1$. وهكذا نجد أن $h(x) = (x - b) \in F(c)[x]$ وهذا يبين لنا أن $b \in F(c)$ ، وبما أن $c = a + db$ نجد أن $a = c - db \in F(c)$ لأن $d \in F$ ، أصبح لدينا $a, b \in F(c)$ ، ومنه يكون $F(a, b) \subseteq F(c)$. مما سبق نجد أن $F(c) = F(a, b)$.

مبرهنة ٥-١-٨.

ليكن F حقلاً و $f(x) \in F[x]$ حدودية أولية فوق F . عندئذ الشروط الآتية متكافئة:

- ١ - الحدودية $f(x)$ تملك صفراً مضاعفاً في تمديد ما للحقل F .
 - ٢ - توجد $g(x) \in F[x]$ بحيث $\partial g(x) > 0$ وتقسم كل من $f(x), f'(x)$ في $F[x]$.
 - ٣ - جميع أصفار الحدودية $f(x)$ مضاعفة.
- البرهان.

(١) $\Leftrightarrow$ (٢). لنفرض جديلاً أن درجة أي حدودية في $F[x]$ تقسم كل من $f(x), f'(x)$ تساوي الصفر. حسب الفرض يوجد $a \in K$ صفر مضاعف للحدودية $f(x)$ حيث K تمديد ما للحقل F وأن مرتبة a تساوي k عندئذ $k \neq 1$ ومنه توجد $h(x) \in F[x]$ بحيث

$$f(x) = (x - a)^k \cdot h(x)$$

وأن $h(a) \neq 0$ وبالتالي يكون:

$$\begin{aligned} f'(x) &= k(x-a)^{k-1} \cdot h(x) + (x-a)^k \cdot h'(x) = \\ &= (x-a)^{k-1} \cdot [k \cdot h(x) + (x-a) \cdot h'(x)] \end{aligned}$$

ولما كانت $(x-a)^{k-1} \in F[x]$ وتنقسم كلا من $f(x), f'(x)$ فإنه حسب الفرض يكون:

$$k = \partial(x-a)^{k-1} = 0$$

ومنه يكون $k=1$ وهذا غير ممكن.

(٢) $\Leftarrow$ (٣). لنبرهن أولاً على أن $f'(x) = 0$. لنفرض جدلاً أن $f'(x) \neq 0$. حسب الفرض فإنه توجد $g(x) \in F[x]$ بحيث $\partial g(x) > 0$ وأن $g(x)$ تنقسم كلا من $f(x)$ و $f'(x)$ ومنه فإن:

$$f(x) = (x-a)^k \cdot h(x), \quad f'(x) = g(x) \cdot \beta(x)$$

حيث $\alpha(x), \beta(x) \in F[x]$.

لما كانت الحدودية $f(x)$ أولية في $F[x]$ وأن $\partial g(x) > 0$ نجد أن $\partial \alpha(x) = 0$ ومنه يكون:

$$\partial f(x) = \partial g(x) \leq \partial g(x) + \partial \beta(x) = \partial f'(x)$$

وهذا يناقض كون $\partial f'(x) < \partial f(x)$ ومنه يكون $f'(x) = 0$.

لنفرض أن $f(x)$ تملك صفراً بسيطاً $b \in K$ حيث K تمديد ما للحقل F . عندئذ فإن:

$$f(x) = (x-a) \cdot g(x)$$

حيث $g(x) \in F[x]$ وأن $g(b) \neq 0$. ولما كانت الحدودية $f(x)$ أولية وأن:

$$\partial(x-a) = 1 \neq 0$$

نجد أن $\partial g(x) = 0$ ومنه فإن $g(x) = b \in F$ وأن $b \neq 0$ ومنه يكون:

$$f(x) = b(x-a)$$

وبالتالي فإن $f'(x) = b = 0$ وهذا غير ممكن، وهكذا نجد أن جميع أصفار الحدودية $f(x)$ مضاعفة. ♦

٥ - ٢. التمديدات الجبرية المنفصلة.

سوف ندرس في هذه الفقرة نوعاً جديداً من الحدوديات وهي الحدوديات المنفصلة التي لها أهمية خاصة في دراستنا المقبلة. البداية سوف تكون مع المبرهنة الآتية:

مبرهنة ١-٢-٥.

ليكن F حقلاً مميزه يساوي $p \neq 0$ وليكن $a \in F$ بحيث $a \notin F^p$. عندئذ أياً كان العدد الصحيح غير السالب $m \in \mathbb{Z}$ ، فإن الحدودية $x^{p^m} - a \in F[x]$ هي حدودية أولية في $F[x]$.

البرهان.

واضح أن $x^{p^m} - a \in F[x]$ وأن $x^{p^m} - a \neq 0$ كما أن $\partial(x^{p^m} - a) = p^m \geq 1$ وهذا يبين لنا أن الحدودية $x^{p^m} - a$ غير قابلة للقلب في $F[x]$. وبما أن F حقل فإن الحلقة $F[x]$ هي حلقة تحليل وحيد، وبالتالي توجد في $F[x]$ حدودية أولية آخر معاملاتها يساوي الواحد وتقسم $x^{p^m} - a$ في $F[x]$ ولتكن $\varphi(x)$. لنفرض أن h أكبر عدد صحيح من أجله $[\varphi(x)]^h$ يقسم $x^{p^m} - a$ في $F[x]$ ، ولنبرهن على أن $h = 1$. لنفرض جذاً أن $x^{p^m} - a \neq [\varphi(x)]^h$ عندئذ توجد $\lambda(x) \in F[x]$ بحيث $x^{p^m} - a = [\varphi(x)]^h \cdot \lambda(x)$ وأن $\lambda(x) \neq 0$ و $\lambda(x) \neq 1$. بما أن الحدودية $\varphi(x)$ أولية في $F[x]$ عندئذ حسب المبرهنة (٣-١-٤) يوجد تمديد بسيط $F(c)$ للحقل F من أجله $\varphi(c) = 0$. ومنه:

$$c^{p^m} - a = [\varphi(c)]^h \cdot \lambda(c) = 0$$

وهذا يبين لنا أن $c^{p^m} = a$ وهكذا نجد أن $x^{p^m} - a = x^{p^m} - c^{p^m} = (x - c)^{p^m}$ حيث $\lambda(x) = b$ فإن $\partial \lambda(x) = 0$ إذا كانت $b \in F$ من جهة أخرى، إن $\partial \lambda(x) \geq 1$ لأنه إذا كانت $\partial \lambda(x) = 0$ فإن $\lambda(x) = b$ حيث $b \neq 0$ و $b \neq 1$. وبما أن آخر معاملات الحدودية $\varphi(x)$ يساوي الواحد فإن آخر معاملات الحدودية $[\varphi(x)]^h$ يساوي الواحد وبالتالي يكون آخر معاملات الحدودية $[\varphi(x)]^h \cdot \lambda(x)$ يساوي b وهذا يبين لنا أن آخر معاملات الحدودية $x^{p^m} - a$ يساوي $b \neq 1$ وهذا غير ممكن، مما سبق نجد أن $\partial \lambda(x) \geq 1$. ومنه نجد أن:

$$p^m = \partial(x - c)^{p^m} = \partial[\varphi(x)]^h + \partial \lambda(x) > \partial[\varphi(x)]^h$$

من جهة ثالثة، إن $\lambda(c) = 0$ لأنه إذا كان $\lambda(c) \neq 0$ وبما أن:

$$(x-c)^{p^m} = [\varphi(x)]^h \cdot \lambda(x)$$

نجد أن $0 = (c-c)^{p^m} = [\varphi(c)]^h \cdot \lambda(c) \neq 0$ ولكون $\lambda(c) \neq 0$ نجد أن $[\varphi(c)]^h = 0$.

وبما أن $F(c)$ حقل فإن الحدودية $x-c$ تقسم $[\varphi(x)]^h$ في $F(c)[x]$.

لنفرض أن d أكبر عدد صحيح موجب من أجله $(x-c)^d$ يقسم $[\varphi(x)]^h$ في $F(c)[x]$ ، عندئذ يوجد $q(x) \in F(c)[x]$ بحيث:

$$[\varphi(x)]^h = (x-c)^d \cdot q(x)$$

وأن $q(c) \neq 0$ ومنه نجد أن:

$$\partial [\varphi(x)]^h = \partial (x-c)^d + \partial q(x) \geq \partial (x-c)^d = d$$

مما سبق نجد أن $d \leq \partial [\varphi(x)]^h \leq p^m$ أي أن $p^m > d$ وأخيراً نجد أن:

$$(x-c)^{p^m} = (x-c)^d \cdot q(x) \cdot \lambda(x)$$

ومنه نجد أن $(x-c)^{p^m-d} = q(x) \cdot \lambda(x)$ وبالتالي يكون $q(c) \cdot \lambda(c) = 0$ وبما أن

$\lambda(c) \neq 0$ نجد أن $q(c) = 0$ وهذا غير ممكن، مما سبق نجد أن $\lambda(c) = 0$. أصبح

لدينا $\lambda(x) \cdot [\varphi(x)]^h = x^{p^m} - a$ وأن $\lambda(x) \neq 0$ و $\lambda(x) \neq 1$ و $\lambda(c) = 0$. بما أن

$\varphi(x)$ أولية في $F[x]$ وأن $\varphi(x)$ لا تقسم $\lambda(x)$ في $F[x]$ نجد أن الحدوديتين $\varphi(x)$

و $\lambda(x)$ أوليتان فيما بينهما في $F[x]$ وبالتالي يوجد $\mu(x), \beta(x) \in F[x]$ بحيث:

$$1 = \beta(x) \cdot \varphi(x) + \mu(x) \cdot \lambda(x)$$

ومنه نجد أن $0 = \lambda(c) \cdot \mu(c) + \varphi(c) \cdot \beta(c) = 1$ وهذا غير ممكن. وهكذا نجد أن

$$x^{p^m} - a = [\varphi(x)]^h, \text{ ومنه فإن:}$$

$$p^m = \partial (x^{p^m} - a) = \partial [\varphi(x)]^h = h \cdot \partial \varphi(x)$$

وهذا يبين لنا أن h يقسم p^m وبالتالي فإن $h = p^s$ حيث $s \in \mathbb{Z}$. إن $s = 0$ لأنه إذا كان

$s > 0$ فإن $s^{p^m} - a = [\varphi(x)]^{h^s}$ وهذا يبين لنا أن معاملات الحدودية $\varphi(x)$ تنتمي

للحقل F^p أي أن معاملات الحدودية $x^{p^m} - a$ تنتمي للحقل F^p وبالتالي فإن $a \in F^p$

وهذا غير ممكن، إذن $s = 0$ وبالتالي فإن $h = p^s = 1$. مما سبق نجد أن

$$x^{p^m} - a = \varphi(x) \text{ وهذا يبين لنا أن الحدودية } x^{p^m} - a \text{ هي حدودية أولية في } F[x]. \diamond$$

تعريف.

ليكن F حقلاً و $f(x) \in F[x]$ حدودية أولية في $F[x]$. عندئذ:

- نقول عن الحدودية $f(x)$ إنها حدودية منفصلة في $F[x]$ إذا كان $f'(x) \neq 0$.
- نقول عن الحدودية $f(x)$ إنها حدودية غير منفصلة في $F[x]$ إذا كان $f'(x) = 0$.

أما الشرط اللازم والكافي الذي من أجله تكون حدودية ما منفصلة نرده من خلال التعريف الآتي:

تعريف.

ليكن F حقلاً و $g(x) \in F[x]$ بحيث $g(x) \neq 0$. نقول عن الحدودية $g(x)$ إنها منفصلة في $F[x]$ إذا حققت الشرط: إذا كانت $f(x) \in F[x]$ حدودية أولية في $F[x]$ وكانت $f(x)$ تقسم $g(x)$ في $F[x]$ فإن الحدودية $f(x)$ هي حدودية منفصلة في $F[x]$.
نأتي الآن لدراسة التمهيدية الآتية والتي تبين لنا أي الحدوديات تكون منفصلة فوق الحقول التي مميزها يساوي الصفر:

تمهيدية ٥-٢-٢.

ليكن F حقلاً مميزه يساوي الصفر. عندئذ أياً كانت $g(x) \in F[x]$ بحيث $\partial g(x) > 0$ فإن الحدودية $g(x)$ تكون منفصلة فوق F .

البرهان.

لتكن $f(x) \in F[x]$ حدودية أولية في $F[x]$ وتقسم $g(x)$ في $F[x]$. بما أن الحدودية $f(x)$ أولية في $F[x]$ فإن $\partial f(x) > 0$ وبما أن مميز الحقل F يساوي الصفر فإنه حسب التمهيدية (٥-١-٢) يكون $f'(x) = 0$ وحسب التعريف تكون الحدودية $f(x)$ منفصلة في $F[x]$ وبالتالي تكون الحدودية $g(x)$ تكون منفصلة في $F[x]$.

مبرهنة ٥-٢-٣.

ليكن F حقلاً مميزه $p \neq 0$. الشرط اللازم والكافي كي يكون الحقل F حقلاً كاملاً هو أن يتحقق الشرط:

أياً كانت $g(x) \in F[x]$ بحيث $\partial g(x) > 0$ فإن الحدودية $g(x)$ تكون منفصلة فوق F .

البرهان.

لزوم الشرط. لنفرض أن الحقل F هو حقل كامل عندئذ يكون $F = F^p$.

لتكن $g(x) \in F[x]$ بحيث $\partial g(x) > 0$ ولتكن $f(x) \in F[x]$ حدودية أولية في $F[x]$ وتقسم $g(x)$ في $F[x]$. لنفرض جـداً أن الحدودية $f(x)$ غير منفصلة فوق F عندئذ يكون $f'(x) = 0$ وحسب المبرهنة (٣-١-٥) فإن $f(x) = \varphi(x^p)$ حيث $\varphi(x) \in F[x]$. ومنه فإن $f(x) = m \cdot p$ حيث m عدد صحيح موجب. وبالتالي يكون $f(x) = \sum_{j=0}^m b_j x^{j \cdot p}$ حيث $b_j \in F$ وذلك أيّاً كان $0 \leq j \leq m$ كما أن $b_m \neq 0$. وبما أن الحقل F هو حقل كامل فإن $F = F^p$ وبالتالي يوجد $d_j \in F$ بحيث $b_j = d_j^p$ وذلك أيّاً كان $0 \leq j \leq m$. ومنه يكون:

$$f(x) = \sum_{j=0}^m b_j x^{j \cdot p} = \sum_{j=0}^m d_j^p x^{j \cdot p} = \sum_{j=0}^m (d_j x^j)^p = \left(\sum_{j=0}^m d_j x^j \right)^p$$

وبما أن $b_m \neq 0$ فإن $d_m \neq 0$ ومنه $\sum_{j=0}^m d_j x^j \in F[x]$ وأن $\partial \left(\sum_{j=0}^m d_j x^j \right) = m > 0$ وبالتالي فإن الحدودية $\sum_{j=0}^m d_j x^j$ غير قابلة للقلب في $F[x]$ وأن $f(x) = \left(\sum_{j=0}^m d_j x^j \right)^p$ وهذا يناقض كون الحدودية $f(x)$ أولية في $F[x]$. مما سبق نجد أن الحدودية $f(x)$ منفصلة في $F[x]$.

كفاية الشرط. واضح أن $F^p \subseteq F$. لنفرض جـداً أن $F \neq F^p$ عندئذ يوجد $a \in F$ بحيث $a \notin F^p$ وحسب المبرهنة (١-٢-٥) تكون الحدودية $x^p - a \in F[x]$ أولية في $F[x]$. بما أن $\partial(x^p - a) = p > 0$ فإنه حسب الفرض تكون الحدودية $x^p - a$ منفصلة فوق F وبالتالي يكون $(x^p - a)' \neq 0$. من جهة أخرى، إن $(x^p - a)' = p \cdot x^{p-1} = 0$ وهذا تناقض، مما سبق نجد أن $F = F^p$ وبالتالي يكون الحقل F هو حقل كامل. ◊

بالاعتماد على التمهيدية (٢-٢-٥) والمبرهنة (٣-٢-٥) يمكننا صياغة النتيجة الآتية:

نتيجة.

كل حدودية درجتها أكبر من الصفر فوق حقل كامل هي حدودية منفصلة. ◊

نأتي الآن إلى دراسة نوع جديد من العناصر الجبرية فوق حقل ما وذلك من خلال التعريف الآتي:

تعريف.

- ليكن الحقل K تمديداً للحقل F وليكن $a \in K$ عنصراً جبرياً فوق F .
- نقول عن العنصر a إنه عنصر منفصل فوق الحقل F إذا كانت الحدودية الأصغرية للعنصر a في $F[x]$ هي حدودية منفصلة في $F[x]$.
 - نقول عن العنصر a إنه عنصر غير منفصل فوق الحقل F إذا كانت الحدودية الأصغرية للعنصر a في $F[x]$ هي حدودية غير منفصلة في $F[x]$.
- بالاعتماد على التعريف الأخير يمكننا صياغة التمهيدية الهامة الآتية:

تمهيدية ٥-٢-٤.

- ليكن الحقل K تمديداً للحقل F وليكن $a \in K$ عنصراً جبرياً فوق F . عندئذ:
- إذا كان للحقل F مميز يساوي الصفر فإن العنصر a يكون عنصراً منفصلاً فوق F .
 - إذا كان للحقل F مميز يساوي $p \neq 0$ وكان $F = F^p$ فإن العنصر a يكون عنصراً منفصلاً فوق F .

البرهان.

- لنفرض أن مميز الحقل F يساوي الصفر. لتكن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a في $F[x]$ عندئذ حسب التمهيدية (٥-٢-٢) تكون الحدودية $f(x)$ منفصلة في $F[x]$ وبالتالي يكون العنصر a منفصلاً فوق F .
- لنفرض أن مميز الحقل F يساوي $p \neq 0$ وأن $F = F^p$ ولتكن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a في $F[x]$ عندئذ حسب المبرهنة (٥-٢-٣) تكون الحدودية $f(x)$ منفصلة في $F[x]$ وبالتالي يكون العنصر a منفصلاً فوق F .

بالاعتماد على التمهيدية الأخيرة يمكننا صياغة النتيجة الآتية:

نتيجة.

كل عنصر جبري فوق حقل كامل هو عنصر منفصل. ◊
نأتي الآن إلى دراسة المبرهنة الآتية:

مبرهنة ٥-٢-٥.

ليكن الحقل K تمديداً للحقل F وليكن $a \in K$ عنصراً جبرياً فوق F . ولتكن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a في $F[x]$ عندئذ:

١. الشرط اللازم والكافي كي يكون العنصر a عنصراً غير منفصل فوق F هو أن يكون $f'(a) = 0$.

٢. إذا كان العنصر a عنصراً غير منفصل فوق F وكانت $g(x) \in F[x]$ بحيث $g(a) = 0$ فإن $g'(a) = 0$.

البرهان.

١ - لزوم الشرط. لنفرض أن العنصر a عنصر غير منفصل فوق F عندئذ حسب التعريف تكون الحدودية $f(x)$ غير منفصلة في $F[x]$ وبالتالي يكون $f'(x) = 0$ ومنه نجد أن $f'(a) = 0$.

كفاية الشرط. لنفرض أن $f'(a) = 0$. لنفرض جـداً أن $f'(x) \neq 0$ عندئذ بما أن الحدودية $f(x)$ أولية في $F[x]$ وأن $f(x)$ لا تقسم $f'(x)$ في $F[x]$ فإن الحدوديتين $f(x)$ و $f'(x)$ أوليتان فيما بينهما وبالتالي توجد $q(x), r(x) \in F[x]$ بحيث:

$$1 = q(x) \cdot f(x) + f'(x) \cdot r(x)$$

ومنه يكون $0 = q(a) \cdot f(a) + f'(a) \cdot r(a) = 1$ ، وهذا غير ممكن.

مما سبق نجد أن $f'(x) = 0$ وبالتالي تكون الحدودية $f(x)$ غير منفصلة في $F[x]$ وحسب التعريف يكون العنصر a عنصراً غير منفصل فوق F .

٢ - لنفرض أن العنصر a غير منفصل فوق F ولتكن $g(x) \in F[x]$ بحيث $g(a) = 0$ عندئذ حسب المبرهنة (٣-٣-٤) فإن الحدودية $f(x)$ تقسم $g(x)$ في $F[x]$ وبالتالي توجد $\lambda(x) \in F[x]$ بحيث $g(x) = f(x) \cdot \lambda(x)$ ومنه يكون:

$$g'(x) = f'(x) \cdot \lambda(x) + f(x) \cdot \lambda'(x)$$

أي أن $g'(a) = f'(a) \cdot \lambda(a) + f(a) \cdot \lambda'(a) = 0$ وهو المطلوب. ◊

ملاحظة.

ليكن الحقل K تمديداً للحقل F و $a \in K$. ولتكن $g(x) \in F[x]$ بحيث $g(x) \neq 0$. إذا كان $g(a) = 0$ عندئذ حسب التمهيدية (٧-١-١) فإن $x - a$ تقسم $g(x)$ في $F[x]$. لنفرض أن n هو أكبر عدد صحيح موجب من أجله $(x - a)^n$ يقسم $g(x)$ في $F[x]$ ، عندئذ توجد $\lambda(x) \in F[x]$ بحيث $g(x) = (x - a)^n \cdot \lambda(x)$ وأن $\lambda(a) \neq 0$. لدينا أيضاً $x - a$ تقسم $g(x)$ في $F(a)[x]$. لنفرض أن m هو أكبر عدد صحيح موجب من أجله $(x - a)^m$ يقسم $g(x)$ في $F(a)[x]$ ، عندئذ توجد $h(x) \in F(a)[x]$ بحيث $g(x) = (x - a)^m \cdot h(x)$ وأن $h(a) \neq 0$. إن $n = m$ لأنه إذا كان $n \neq m$ ويفرض أن $n > m$ نجد أن:

$$(x - a)^n \cdot \lambda(x) = (x - a)^m \cdot h(x)$$

ومنه يكون $(x - a)^{n-m} \cdot \lambda(x) = h(x)$ وبالتالي فإن $h(a) = (a - a)^{n-m} \cdot \lambda(a) = 0$ وهذا غير ممكن. مما سبق نجد أن $n = m$ وبالتالي يكون $h(x) = \lambda(x)$. بهذا الشكل نكون قد بينا أن مرتبة أي صفر لحدودية ما لا تتعلق باختيار التمديد الذي ينتمي إليه صفر الحدودية.

نأتي الآن إلى دراسة المبرهنة الآتية:

مبرهنة ٥-٢-٦.

ليكن الحقل K تمديداً للحقل F وليكن $a \in K$ عنصراً جبرياً فوق F . ولتكن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a في $F[x]$. عندئذ:

- ١ - الشرط اللازم والكافي كي يكون العنصر a غير منفصل فوق F هو أن يكون a صفراً مضاعفاً للحدودية $f(x)$.
- ٢ - إذا كان العنصر a غير منفصل فوق F وكانت $g(x) \in F[x]$ بحيث $g(a) = 0$ فإن a يكون صفراً مضاعفاً للحدودية $g(x)$.

البرهان.

بما أن $f(a) = 0$ فإن $x - a$ يقسم $f(x)$ في $F[x]$. لنفرض أن m هو أكبر عدد صحيح موجب من أجله $(x - a)^m$ يقسم $f(x)$ في $F[x]$. عندئذ توجد $\lambda(x) \in F[x]$ بحيث $f(x) = (x - a)^m \cdot \lambda(x)$ وأن $\lambda(a) \neq 0$.

١ - لزوم الشرط. لنفرض أن العنصر a غير منفصل فوق F عندئذ حسب التعريف يكون $f'(x) = 0$. من جهة أخرى، إن $m > 1$ لأنه إذا كان $m = 1$ نجد أن:

$$f'(x) = \lambda(x) + (x - a) \cdot \lambda'(x)$$

ومنه يكون $f'(a) = \lambda(a) + (a - a) \cdot \lambda'(a) = \lambda(a)$ وبالتالي فإن $\lambda(a) = 0$ وهذا غير ممكن. ومنه نجد أن a هو صفر مضاعف للحدودية $f(x)$.

كفاية الشرط. لنفرض أن العنصر a هو صفر مضاعف للحدودية $f(x)$ عندئذ يكون $m > 1$ وبالتالي يكون $m - 1 > 0$ ومنه نجد أن:

$$f'(x) = m \cdot (x - a)^{m-1} \cdot \lambda(x) + (x - a)^m \cdot \lambda'(x)$$

وهكذا نجد أن $f'(a) = 0$ وحسب المبرهنة (٥-٢-٥) نجد أن العنصر a غير منفصل فوق F .

٢ - لنفرض أن العنصر a غير منفصل فوق F ولتكن $g(x) \in F[x]$ بحيث $g(a) = 0$. بما أن $g(a) = 0$ فإن $x - a$ يقسم $g(x)$ في $F[x]$. لنفرض أن n هو أكبر عدد صحيح موجب من أجله $(x - a)^n$ يقسم $g(x)$ في $F[x]$ ، عندئذ توجد $\mu(x) \in F[x]$ بحيث $g(x) = (x - a)^n \cdot \mu(x)$ وأن $\mu(a) \neq 0$. من جهة أخرى، بما أن العنصر a غير منفصل فوق F فإنه حسب المبرهنة (٥-٢-٥) يكون $g'(a) = 0$. ومنه نجد أن a هو صفر مضاعف للحدودية $g(x)$ ، لأنه إذا كان a صفرًا بسيطاً للحدودية $g(x)$ فإن $n = 1$ ومنه يكون $g(x) = (x - a) \cdot \mu(x)$ وبالتالي:

$$g'(x) = \mu(x) + (x - a) \cdot \mu'(x)$$

ومنه يكون $\mu(a) = 0$ وهذا مناقض لكون $\mu(a) \neq 0$. مما سبق نجد أن $n > 1$ وبالتالي يكون العنصر a صفرًا مضاعفًا للحدودية $g(x)$.

تعريف.

ليكن F حقلًا مميزه $p \neq 0$. ولتكن $g(x) \in F[x]$ بحيث $g(x) \neq 0$. وجدنا سابقاً أنه

إذا كانت $g(x) \in F[x^p]$ فإن $g(x) = \lambda(x^p)$ حيث $\lambda(x) \in F[x]$ لنفرض أن m أكبر عدد صحيح موجب من أجله $g(x) \in F[x^{p^m}]$ عندئذ $g(x) \notin F[x^{p^{m+1}}]$ ومنه فإن $g(x) = h(x^{p^m})$ حيث $h(x) \in F[x]$ وأن $h(x) \notin F[x^p]$ وهنا نجد أن $\partial g(x) = \partial h(x) \cdot p^m$ بفرض $\partial g(x) = n$ و $\partial h(x) = n_0$ عندئذ يكون $n = n_0 \cdot p^m$. نسمي n_0 درجة انفصالية الحدودية $g(x)$ ، و نسمي p^m درجة عدم انفصالية الحدودية $g(x)$.

نأتي الآن لدراسة العلاقة بين درجة انفصالية الحدودية والحدودية المنفصلة وذلك من خلال المبرهنة الآتية:

مبرهنة ٧-٢-٥

ليكن F حقلاً مميزه $p \neq 0$ ولتكن $f(x) \neq 0$ حدودية أولية في $F[x]$. لنفرض أن $\partial f(x) = n$ وأن n_0 درجة انفصالية الحدودية $f(x)$. الشرط اللازم والكافي كي تكون الحدودية $f(x)$ منفصلة في $F[x]$ هو أن يكون $n = n_0$.

البرهان.

لنفرض أن p^m درجة عدم انفصالية الحدودية $f(x)$ ، عندئذ يكون $n = n_0 \cdot p^m$. لزوم الشرط. لنفرض أن الحدودية $f(x)$ منفصلة في $F[x]$ عندئذ حسب التعريف يكون $f'(x) \neq 0$ ، وحسب المبرهنة (٣-١-٥) نجد أن $f(x) \notin F[x^p]$. أصبح لدينا $f(x) \in F[x^{p^0}]$ وأن $f(x) \notin F[x^{p^{0+1}}]$ وهذا يبين لنا أن $m = 0$ وبالتالي فإن $n = n_0$. كفاية الشرط. لنفرض أن $n = n_0$ عندئذ يكون $n = n \cdot p^m$ ومنه نجد أن $p^m = 1$ أي أن $m = 0$ وهذا يبين لنا أن $f(x) \in F[x^{p^0}]$ وأن $f(x) \notin F[x^{p^{0+1}}]$ وبالتالي يكون $f'(x) \neq 0$ أي أن الحدودية $f(x)$ منفصلة فوق F .

مبرهنة ٨-٢-٥

ليكن F حقلاً و $f(x) \in F[x]$ حدودية منفصلة فوق F . لنفرض أن E هو حقل تفريق الحدودية $f(x)$ فوق F . عندئذ:

١ - أي صفر $a \in E$ الحدودية $f(x)$ هو صفر بسيط.

٢ - درجة الحدودية $f(x)$ تساوي إلى عدد الأصفار المختلفة للحدودية $f(x)$ في E .
البرهان.

١ - لنفرض أن $a \in E$ صفر للحدودية $f(x)$. سوف نميز حالتين:
- إذا كانت الحدودية $f(x)$ أولية في $F[x]$ عندئذ تكون $f(x)$ الحدودية الأصغرية للعنصر a فوق F ولما كانت الحدودية $f(x)$ منفصلة فإن العنصر a يكون منفصلاً فوق F وحسب المبرهنة (٥-٢-٦) (١) يكون a صفرًا بسيطاً للحدودية $f(x)$.
- لنفرض أن الحدودية $f(x)$ ليست أولية في $F[x]$ ولما كان العنصر a جبرياً فوق F لنفرض أن $p(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F ولما كان $f(a) = 0$ فإن $p(x)$ تقسم $f(x)$ في $F[x]$ ولما كانت الحدودية $f(x)$ منفصلة فإن الحدودية $g(x)$ تكون منفصلة ومنه يكون العنصر a منفصلاً فوق F وحسب المبرهنة (٥-٢-٦) (٢) يكون a صفرًا بسيطاً للحدودية $f(x)$.

٢ - لما كان E هو حقل تفريق الحدودية $f(x)$ فوق F لنفرض أن $a_1, a_2, \dots, a_n$ هي جميع الأصفار المختلفة للحدودية $f(x)$ في E وحسب (١) فإن هذه الأصفار هي أصفار بسيطة للحدودية $f(x)$ ولما كان E هو حقل تفريق الحدودية $f(x)$ نجد أن:

$$f(x) = b(x - a_1)(x - a_2) \cdots (x - a_n)$$

حيث $0 \neq b \in F$ وهذا يبين أن $\partial f(x) = n$ وأن n هو عدد الأصفار المختلفة للحدودية $f(x)$ في E .

٥ - ٣. التمديدات المنفصلة.

في هذه الفقرة سوف ندرس التمديدات الجبرية المنفصلة لحقل ما والبداية ستكون مع التعريف الآتي:

تعريف.

- ليكن الحقل K تمديداً جبرياً للحقل F .
- نقول عن الحقل K إنه تمديد جبري منفصل للحقل F إذا كان كل عنصر من K هو عنصراً منفصلاً فوق F .
 - نقول عن الحقل K إنه تمديد جبري غير منفصل للحقل F إذا لم يكن التمديد K للحقل F تمديداً منفصلاً.
- بالاعتماد على التعريف الأخير والتمهيدية (٤-٢-٤) يمكننا صياغة التمهيدية الآتية:

تمهيدية ٥-٣-١.

ليكن F حقلاً. عندئذ:

- ١ - إذا كان مميز الحقل F يساوي الصفر فإن أي تمديد جبري للحقل F هو تمديد منفصل.
- ٢ - إذا كان للحقل F مميز يساوي $p \neq 0$ وكان $F = F^p$ فإن أي تمديد جبري للحقل F هو تمديد منفصل.

البرهان.

ليكن الحقل K تمديداً جبرياً للحقل F .

- ١ - لنفرض أن للحقل F مميزاً يساوي الصفر. وليكن $a \in K$ عندئذ يكون العنصر a جبرياً فوق F وحسب التمهيدية (٤-٢-٤) يكون العنصر a منفصلاً فوق F وبالتالي يكون الحقل K تمديداً منفصلاً للحقل F .
- ٢ - لنفرض أن مميز الحقل F يساوي $p \neq 0$ وأن $F = F^p$. وليكن $a \in K$ عندئذ يكون العنصر a جبرياً فوق F وحسب التمهيدية (٤-٢-٤) يكون العنصر a منفصلاً فوق F وبالتالي يكون الحقل K تمديداً منفصلاً للحقل F . ◊

بالاعتماد على التمهيدية الأخيرة يمكننا صياغة النتيجة الآتية:

نتيجة.

كل تمديد جبري لحقل كامل هو تمديد منفصل. ◊

تعريف.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً للحقل F . نقول عن العنصر $a \in K$ إنه عنصر غير منفصل تماماً فوق الحقل F إذا وجد عدد صحيح غير سالب r بحيث $a^{p^r} \in F$.

نقول عن التمديد K للحقل F إنه تمديد غير منفصل تماماً للحقل F إذا كان كل عنصر من K هو عنصر غير منفصل تماماً فوق الحقل F .

بالاعتماد على التعريف الأخير يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن F حقلاً مميزه $p \neq 0$. إن كل عنصر من الحقل F هو عنصر غير منفصل تماماً فوق الحقل F . ◊

لندرس الآن درجة التمديد غير المنفصل لحقل ما وذلك من خلال المبرهنة الآتية:

مبرهنة ٢-٣-٥.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً بسيطاً وغير منفصل تماماً للحقل F . عندئذ يكون $[K : F] = p^n$ حيث n عدد صحيح غير سالب.

البرهان.

لنفرض أن الحقل K هو تمديد بسيط وغير منفصل تماماً للحقل F ، عندئذ يوجد $a \in K$ بحيث $K = F(a)$. وبما أن الحقل K تمديد غير منفصل تماماً للحقل F فإن العنصر a غير منفصل تماماً فوق الحقل F وبالتالي يوجد عدد صحيح غير سالب r بحيث $a^{p^r} \in F$. لنفرض أن n هو أصغر عدد صحيح غير سالب من أجله $a^{p^n} \in F$.

- إذا كان $n = 0$ عندئذ يكون $a = a^{p^n} \in F$ والتالي يكون $K = F(a) = F$ وهنا نجد أن $[K : F] = [F : F] = 1 = p^n$.

- إذا كان $n > 0$ ، لنفرض أن $b = a^{p^n} \in F$ ، عندئذ فإن $b \notin F^p$ لأنه إذا كان $b \in F^p$ فإنه يوجد $d \in F$ بحيث $b = d^p$ ومنه يكون $a^{p^n} - d^p = 0$ أي أن $(a^{p^{n-1}} - d)^p = 0$ وهكذا نجد أن $a^{p^{n-1}} - d = 0$ ومنه $a^{p^{n-1}} = d \in F$ وهذا يناقض كون n هو أصغر عدد صحيح غير سالب من أجله $a^{p^n} \in F$. مما سبق نجد أن $b \notin F^p$ وحسب المبرهنة (١-٢-٥) تكون الحدودية $x^{p^n} - b$ أولية في $F[x]$. وبما أن $a^{p^n} - b = 0$ نجد أن $x^{p^n} - b$ هي الحدودية الأصغرية للعنصر الجبري a فوق F . وحسب المبرهنة (٣-٣-٥) يكون $[K : F] = [F(a) : F] = \partial(x^{p^n} - b) = p^n$.

المبرهنة الأخيرة صحيحة لأجل التمديدات المنتهية وهذا ما تبينه المبرهنة الآتية:

مبرهنة ٣-٣-٥.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً منتهياً وغير منفصل تماماً للحقل F . عندئذ يكون $[K : F] = p^n$ حيث n عدد صحيح غير سالب. البرهان.

لنفرض أن الحقل K تمديد منته للحقل F وأن $[K : F] = m$. عندئذ توجد مجموعة من عناصر الحقل K مؤلفة من m عنصر ولتكن $\{a_1, a_2, \dots, a_m\} \subset K$ تولد الحقل K فوق F . ومنه يكون $K = F(a_1, a_2, \dots, a_m)$. لنضع $K_0 = F$ و

$$K_1 = K_0(a_1) = F(a_1)$$

$$K_2 = K_1(a_2) = K_0(a_1)(a_2) = F(a_1, a_2)$$

وهكذا نجد أن:

$$K_m = K_{m-1}(a_m) = K_0(a_1, a_2, \dots, a_{m-1})(a_m) = F(a_1, a_2, \dots, a_m)$$

نلاحظ أن الحقل K_i هو تمديد بسيط للحقل K_{i-1} وذلك لأجل جميع القيم $0 \leq i \leq m$. من جهة أخرى، ليكن $b \in K_i$ عندئذ يكون $b \in K$ وبما أن الحقل K هو تمديد غير منفصل تماماً للحقل F فإن b هو عنصر غير منفصل تماماً فوق F وبالتالي يوجد

عدد صحيح غير سالب s بحيث $b^{p^s} \in F$ وبما أن $F \subseteq K_{i-1}$ نجد أن $b^{p^s} \in K_{i-1}$ أي أن العنصر b غير منفصل تماماً فوق الحقل K_{i-1} . وهذا يبين لنا أن الحقل K_i هو تمديد غير منفصل تماماً للحقل K_{i-1} وذلك أيّاً كان $0 \leq i \leq m$. أصبح لدينا الحقل K_i هو تمديد بسيط وغير منفصل تماماً للحقل K_{i-1} وذلك أيّاً كان $0 \leq i \leq m$ وحسب المبرهنة (٥-٣-٢) فإن $[K_i : K_{i-1}] = p^{n_i}$ ، حيث n_i هو عدد صحيح غير سالب. من جهة ثالثة، بما أن الحقل K تمديد منته للحقل F وأن:

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{m-1} \subseteq K_m = K$$

نجد أن:

$$\begin{aligned} [K : F] &= [K_m : K_{m-1}] \cdot [K_{m-1} : K_{m-2}] \cdots [K_2 : K_1] \cdot [K_1 : F] = \\ &= p^{n_m} \cdot p^{n_{m-1}} \cdots p^{n_2} \cdot p^{n_1} = p^{n_m + n_{m-1} + \cdots + n_2 + n_1} = p^n \end{aligned}$$

$$\diamond \cdot n = n_m + n_{m-1} + \cdots + n_2 + n_1$$

لندرس الآن العناصر المنفصلة وغير المنفصل تماماً في آن واحد وذلك من خلال المبرهنة الآتية:

مبرهنة ٥-٣-٤.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً للحقل F و $a \in K$. إذا كان العنصر a منفصلاً فوق F وغير منفصل تماماً فوق F ، عندئذ يكون $a \in F$. البرهان.

بما أن العنصر a غير منفصل تماماً فوق F فإنه يوجد عدد صحيح غير سالب r بحيث $a^{p^r} \in F$. لنفرض أن n أصغر عدد صحيح غير سالب من أجله $a^{p^n} \in F$. لنفرض جلاً أن $n \neq 0$ ، عندئذ يكون $n > 0$ وبفرض أن $a^{p^n} = b \in F$ نجد أن الحدودية $f(x) = x^{p^n} - b \in F[x]$ هي الحدودية الأصغرية للعنصر a فوق F . لما كان العنصر a منفصل فوق F فإن الحدودية $f(x)$ تكون منفصلة فوق F وبالتالي يكون $f'(x) \neq 0$. من جهة أخرى، إن:

$$f'(x) = p^n \cdot x^{p^n-1} = p^n \cdot (1 \cdot x^{p^n-1}) = (p^n \cdot 1) \cdot x^{p^n-1} = 0$$

وهذا يتناقض مع كون $f'(x) \neq 0$. مما سبق نجد أن $n = 0$ ومنه يكون $a \in F$.

تمهيدية ٥-٣-٥ .

ليكن الحقل K تمديداً جبرياً منفصلاً للحقل F وليكن E حقلاً جزئياً في K يحوي F . عندئذ يكون الحقل K تمديداً جبرياً منفصلاً للحقل E .
البرهان.

بما أن K تمديد جبري للحقل F و E حقل جزئي في K يحوي F فإن K تمديد جبري للحقل E . ليكن $a \in K$ عندئذ فإن a هو عنصر جبري منفصل فوق F . بفرض أن $f(x) \in F[x]$ $0 \neq f(x)$ الحدودية الأصغرية للعنصر a فوق F عندئذ حسب المبرهنة (٥-٢-٦) فإن a هو صفر بسيط للحدودية $f(x)$ فوق F . من جهة أخرى، لنفرض جـداً أن العنصر a غير منفصل فوق الحقل E ، عندئذ وبما أن $f(x) \in E[x]$ وأن $f(a) = 0$ فإنه حسب المبرهنة (٥-٢-٦) فإن a هو صفر مضاعف للحدودية $f(x)$ وهذا غير ممكن، مما سبق نجد أن العنصر a منفصل فوق الحقل E وبالتالي يكون الحقل K تمديداً جبرياً منفصلاً للحقل E .

إن للتمديدات الجبرية المنفصلة لحقل ما F تأثيراً على هذا الحقل سندرسه من خلال المبرهنة الآتية:

مبرهنة ٥-٣-٦ .

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً للحقل F . عندئذ:
١ . إذا كان K تمديداً جبرياً منفصلاً للحقل F فإن $F.K^p = K$.
٢ . إذا كان الحقل K تمديداً منتهياً للحقل F وكان $F.K^p = K$ فإن K يكون تمديداً جبرياً منفصلاً للحقل F .

البرهان.

١ - بما أن كلا من F و K^p حقول جزئية في K فإنه حسب التمرين المحلول (٣-١٠) الجداء $F.K^p$ هو حقل جزئي في K يحوي كلا من F و K^p أي أن $F.K^p \subseteq K$. من جهة ثانية، ليكن $a \in K$ عندئذ فإن $a^p \in K^p \subseteq F.K^p$ وهذا

يبين لنا أن العنصر a غير منفصل تماماً فوق الحقل $F \cdot K^p$. أيضاً بما أن الحقل K تمديد جبري منفصل للحقل F وأن $F \subseteq F.K^p \subseteq K$ وحسب التمهيدية (٥-٣-٥) فإن K هو تمديد جبري منفصل للحقل $F \cdot K^p$ وبالتالي يكون العنصر a منفصلاً فوق الحقل $F \cdot K^p$ وحسب المبرهنة (٤-٣-٥) فإن $a \in F.K^p$. مما سبق نجد أن $K \subseteq F.K^p$ ومنه يكون $F.K^p = K$.

٢ - لنفرض أن الحقل K تمديد منته للحقل F وأن $F.K^p = K$. بما أن الحقل K تمديد منتهي للحقل F فإنه حسب المبرهنة (٦-٣-٣) يكون K تمديداً جبرياً للحقل F بالإضافة لذلك لنفرض أن $[K : F] = n$. لنبرهن أولاً على أنه إذا كانت $\{v_1, v_2, \dots, v_t : t \leq n\}$ مجموعة جزئية من K مستقلة خطياً فوق F فإن المجموعة $\{v_1^p, v_2^p, \dots, v_t^p\}$ تكون مستقلة خطياً فوق F .

لنفرض أن $\{v_1, v_2, \dots, v_t : t \leq n\}$ مجموعة جزئية من K مستقلة خطياً فوق F ، عندئذ يوجد في K عناصر $v_{t+1}, v_{t+2}, \dots, v_n$ بحيث تشكل المجموعة $\{v_1, v_2, \dots, v_n\}$ قاعدة للحقل K فوق F . ليكن $y \in K$ بما أن $F.K^p = K$ فإن $y \in F.K^p$ ومنه $y = \sum_{i=1}^h b_i c_i$ حيث $b_i \in F, c_i \in K^p$ وبالتالي فإن $c_i = d_i^p$ حيث $d_i \in K$. بما أن المجموعة $\{v_1, v_2, \dots, v_n\}$ تشكل قاعدة للحقل K فوق F فإن $d_i = \sum_{j=1}^n a_{i,j} v_j$ حيث $a_{i,j} \in F$ ومنه فإن:

$$\begin{aligned} y &= \sum_{i=1}^h b_i \cdot c_i = \sum_{i=1}^h b_i \cdot d_i^p = \sum_{i=1}^h b_i \cdot \left(\sum_{j=1}^n a_{i,j} v_j \right)^p = \sum_{i=1}^h b_i \cdot \sum_{j=1}^n (a_{i,j} v_j)^p = \\ &= \sum_{i=1}^h b_i \cdot \sum_{j=1}^n a_{i,j}^p \cdot v_j^p = \sum_{j=1}^n \sum_{i=1}^h (b_i \cdot a_{i,j}^p) \cdot v_j^p = \sum_{j=1}^n \left(\sum_{i=1}^h (b_i \cdot a_{i,j}^p) \right) \cdot v_j^p \end{aligned}$$

وهذا يبين لنا أن المجموعة $\{v_1^p, v_2^p, \dots, v_n^p\}$ تولد الحقل K فوق F وبما أن $[K : F] = n$ نجد أن المجموعة $\{v_1^p, v_2^p, \dots, v_n^p\}$ تشكل قاعدة للحقل K فوق F وبالتالي تكون المجموعة $\{v_1^p, v_2^p, \dots, v_t^p\}$ مستقلة خطياً فوق F .

ليكن $a \in K$ ولنفرض جديلاً أن العنصر a غير منفصل فوق F ، بفرض أن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F ، عندئذ حسب التعريف تكون

الحدودية $f(x)$ غير منفصلة في $F[x]$ وبفرض أن $\partial f(x) = m$ وأن m_0 درجة انفصالية الحدودية $f(x)$ فوق F وأن p^r درجة عدم انفصالية الحدودية $f(x)$ فوق F ، عندئذ فإن $m = m_0 \cdot p^r$ وبما أن الحدودية $f(x)$ غير منفصلة في $F[x]$ فإنه حسب المبرهنة (٧-٢-٥) يكون $m \neq m_0$ ومنه نجد أن $m > m_0$. وبما أن $\partial f(x) = m$ فإنه حسب المبرهنة (٥-١-٣) فإن المجموعة $\{1, a, a^2, \dots, a^{m-1}\}$ تشكل قاعدة للحقل $F(a)$ فوق F وبالتالي تكون المجموعة $\{1, a, a^2, \dots, a^{m-1}\}$ مستقلة خطياً فوق F ومنه فإن المجموعة $\{1, a, a^2, \dots, a^{m_0}\}$ تكون مستقلة خطياً فوق F وهكذا نجد أن المجموعة $\{1, a^{p^r}, a^{2p^r}, \dots, a^{m_0 p^r}\}$ مستقلة خطياً فوق F .

من جهة أخرى، إن $f(x) = \sum_{i=0}^{m_0} q_i x^{i \cdot p^r}$ حيث $q_i \in F$ وبما أن $f(x) \neq 0$ وأن $f(a) = 0$ نجد أن $\sum_{i=0}^{m_0} q_i a^{i \cdot p^r} = 0$ وهذا يبين لنا أن المجموعة:

$$\{1, a^{p^r}, a^{2p^r}, \dots, a^{m_0 p^r}\}$$

مرتبطة خطياً فوق F ، وهذا تناقض. مما سبق نجد أن العنصر a منفصل فوق F وبالتالي يكون الحقل K تمديداً جبرياً منفصلاً للحقل F .

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً منتهياً للحقل F . الشرط اللازم والكافي كي يكون الحقل K تمديداً منفصلاً للحقل F هو أن يكون $F.K^p = K$.

تأثير آخر للعناصر المنفصلة ندرسه من خلال المبرهنة الآتية:

مبرهنة ٧-٣-٥.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل E تمديداً للحقل F و $a \in E$ عنصراً جبرياً فوق F . عندئذ:

١ - إذا كان $F(a) = F(a^p)$ فإن العنصر a هو عنصر منفصل فوق F .

٢ - إذا كان العنصر a منفصلاً فوق الحقل F فإن $F(a) = F(a^p)$ بالإضافة لذلك،

فإن الحقل $F(a)$ يكون تمديداً جبرياً منفصلاً للحقل F .
البرهان.

١ - لنفرض أن $F(a) = F(a^p)$. بما أن $a \in F(a^p)$ فإن $a^p \in (F(a^p))^p$ أيضاً بما أن $F \subseteq F(a^p)$ فإن $F^p \subseteq (F(a^p))^p$ ومنه نجد أن $F^p(a^p) \subseteq (F(a^p))^p$.
من جهة أخرى، ليكن $y \in (F(a^p))^p$ عندئذ يوجد $z \in F(a^p)$ بحيث $y = z^p$. من جهة ثانية، بما أن $z \in F(a)$ وأن العنصر a جبري فوق الحقل F فإنه حسب المبرهنة (٦-١-٣) يكون $z = \sum_{i=0}^{n-1} b_i a^i$ حيث $b_i \in F$ وأن n هي درجة الحدودية الأصغرية للعنصر a فوق F . ومنه نجد أن:

$$y = z^p = \left(\sum_{i=0}^{n-1} b_i a^i \right)^p = \sum_{i=0}^{n-1} (b_i a^i)^p = \sum_{i=0}^{n-1} b_i^p a^{i \cdot p} \in F^p(a^p)$$

وهكذا نجد أن $(F(a^p))^p \subseteq F^p$ ، مما سبق نجد أن $(F(a^p))^p = F^p(a^p)$.
بفرض أن $K = F(a)$ عندئذ يكون:

$$\begin{aligned} F.K^p &= F.(F(a))^p = F.(F(a^p))^p = F.F^p(a^p) = \\ &= F(a^p) = F(a) = K \end{aligned}$$

وبما أن العنصر a جبري فوق الحقل F فإنه حسب المبرهنة (٥-٣-٣) يكون الحقل $K = F(a)$ تمديداً منتهياً للحقل F . وبما أن $F.K^p = K$ فإنه حسب المبرهنة (٥-٣-٣) يكون الحقل $K = F(a)$ تمديداً منفصلاً للحقل F وبالتالي يكون العنصر a منفصلاً فوق F .

٢ - لنفرض أن العنصر a منفصل فوق الحقل F عندئذ يكون العنصر a منفصلاً فوق الحقل $F(a^p)$. من جهة أخرى، بما أن $a^p \in F(a^p)$ فإن العنصر a غير منفصل تماماً فوق الحقل $F(a^p)$ وحسب المبرهنة (٤-٣-٥) فإن $a \in F(a^p)$ ومنه يكون $F(a) \subseteq F(a^p)$. أيضاً بما أن $a^p \in F(a)$ فإن $F(a^p) \subseteq F(a)$ وهكذا نجد أن $F(a) = F(a^p)$. وحسب (١) يكون الحقل $F(a)$ تمديداً جبرياً منفصلاً للحقل F .

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً للحقل F و $a \in K$. الشرط اللازم والكافي كي يكون الحقل $F(a)$ تمديداً منفصلاً للحقل F هو أن يكون $F(a) = F(a^p)$.

سوف ندرس الآن علاقة التعدي بين التمديدات الجبرية المنفصلة في حالة كون هذه التمديدات منتهية وذلك من خلال المبرهنة الآتية:

مبرهنة ٥-٣-٨.

ليكن الحقل E تمديداً منتهياً للحقل K وليكن الحقل K تمديد منته للحقل F . إذا كان الحقل E تمديداً جبرياً منفصلاً للحقل K وكان الحقل K تمديداً جبرياً منفصلاً للحقل F ، عندئذ يكون الحقل E تمديداً جبرياً منفصلاً للحقل F .

البرهان.

بما أن الحقل E تمديداً منتهياً للحقل K وأن الحقل K تمديداً منتهياً للحقل F فإنه حسب المبرهنة (٣-٢-١) يكون الحقل E تمديداً منتهياً للحقل F . وحسب المبرهنة (٣-٣-٦) يكون الحقل E تمديداً جبرياً للحقل F . سوف نميز حالتين:

- الحالة الأولى: إذا كان مميز الحقل F يساوي الصفر، عندئذ حسب التمهيدية (٥-٢-٤) يكون كل عنصر جبري فوق F منفصلاً وبالتالي يكون التمديد E تمديداً جبرياً منفصلاً للحقل F .

- الحالة الثانية: إذا كان مميز الحقل F هو $p \neq 0$. بما أن E تمديد جبري منفصل للحقل K ، عندئذ حسب المبرهنة (٥-٣-٦) فإن $K \cdot E^p = E$. أيضاً بما أن K تمديد جبري منفصل للحقل F ، عندئذ حسب المبرهنة (٥-٣-٦) فإن $F \cdot K^p = K$. ومنه نجد:

$$E = K \cdot E^p = F \cdot K^p \cdot E^p = F \cdot E^p$$

وبما أن الحقل E تمديد منته للحقل F فإنه حسب المبرهنة (٤-٣-٦) يكون الحقل E تمديد جبري منفصل للحقل F .

لندرس الآن الحقل الممدد بعدد منته من العناصر الجبرية المنفصلة فوق حقل ما وذلك من خلال المبرهنة الآتية:

مبرهنة ٩-٣-٥.

ليكن الحقل K تمديداً للحقل F ولتكن $a_1, a_2, \dots, a_n \in K$ عناصر جبرية منفصلة فوق F عندئذ يكون الحقل $F(a_1, a_2, \dots, a_n)$ تمديداً جبرياً منفصلاً للحقل F .
البرهان.

بما أن العناصر $a_1, a_2, \dots, a_n \in K$ جبرية فوق F فإنه حسب المبرهنة (٩-٣-٣) يكون الحقل $F(a_1, a_2, \dots, a_n)$ تمديداً منتهياً للحقل F وحسب المبرهنة (٦-٣-٣) يكون الحقل $F(a_1, a_2, \dots, a_n)$ تمديداً جبرياً للحقل F . نميز حالتين:

- الحالة الأولى: إذا كان مميز الحقل F يساوي الصفر، عندئذ حسب التمهيدية (٥-٢-٢) (٤) يكون كل عنصر جبري فوق F منفصلاً وبالتالي يكون التمديد $F(a_1, a_2, \dots, a_n)$ تمديداً جبرياً منفصلاً للحقل F .

- الحالة الثانية: إذا كان مميز الحقل F هو $p \neq 0$. سوف نورد البرهان بالاستقراء حسب n . من أجل $n=1$. بما أن العنصر $a_1 \in K$ جبري منفصل فوق F فإنه حسب المبرهنة (٥-٣-٧) يكون الحقل $F(a_1)$ تمديداً جبرياً منفصلاً للحقل F . لنفرض أن المبرهنة صحيحة لأجل $n-1$. لنضع $F_i = F(a_1, a_2, \dots, a_i)$ حيث $1 \leq i \leq n$. أصبح لدينا $F_{n-1} = F(a_1, a_2, \dots, a_{n-1})$ تمديداً جبرياً منفصلاً للحقل F وأن:

$$F_n = F(a_1, a_2, \dots, a_n) = F(a_1, a_2, \dots, a_{n-1})(a_n) = F_{n-1}(a_n)$$

وبما أن العنصر $a_n \in K$ جبري منفصل فوق F فإن العنصر $a_n \in K$ جبري منفصل فوق F_{n-1} وحسب المبرهنة (٥-٣-٧) يكون الحقل $F_n = F_{n-1}(a_n)$ تمديداً جبرياً منفصلاً للحقل F_{n-1} . أصبح لدينا $F_n = F_{n-1}(a_n)$ تمديداً منتهياً للحقل F_{n-1} وأن الحقل $F_{n-1} = F(a_1, a_2, \dots, a_{n-1})$ تمديد منته للحقل F ، أيضاً بما أن $F_n = F_{n-1}(a_n)$ تمديد منفصل للحقل F_{n-1} وأن الحقل $F_{n-1} = F(a_1, a_2, \dots, a_{n-1})$ تمديد منفصل للحقل F فإنه حسب المبرهنة (٥-٣-٨) يكون الحقل $F_n = F(a_1, a_2, \dots, a_n)$ تمديداً جبرياً منفصلاً للحقل F . ◊

سوف ندرس الآن علاقة التعدي بين التمديدات الجبرية المنفصلة وذلك من خلال المبرهنة الآتية:

مبرهنة ١٠-٣-٥

ليكن الحقل E تمديداً جبرياً منفصلاً للحقل K و K تمديداً جبرياً منفصلاً للحقل F ، عندئذ يكون الحقل E تمديداً جبرياً منفصلاً للحقل F .
البرهان.

بما أن الحقل E تمديد جبري للحقل K و K تمديد جبري للحقل F ، عندئذ حسب المبرهنة (٨-٣-٣) يكون الحقل E تمديداً جبرياً للحقل F . سوف نميز حالتين:
- الحالة الأولى: إذا كان مميز الحقل F يساوي الصفر، عندئذ حسب التمهيدية (٥-٢-٤) يكون كل عنصر جبري فوق F منفصلاً وبالتالي يكون التمديد E تمديداً جبرياً منفصلاً للحقل F .

- الحالة الثانية: إذا كان مميز الحقل F هو $p \neq 0$.
ليكن $a \in E$ عندئذ بما أن الحقل E تمديد جبري للحقل K فإن العنصر a هو عنصر جبري فوق K ، لنفرض أن $f(x) \in K[x]$ الحدودية الأصغرية للعنصر a فوق K وأن $\partial f(x) = n$ عندئذ يكون $f(x) = \sum_{i=0}^n b_i x^i$ حيث $b_i \in K$ لأجل جميع القيم $0 \leq i \leq n$.

لنضع $F_n = F(b_0, b_1, \dots, b_n)$ فنجد أن $f(x) \in F_n[x]$ وأن $f(a) = 0$ وهذا يبين لنا أن العنصر a هو عنصر جبري فوق F_n وحسب المبرهنة (٧-٣-٣) يكون $F_n(a)$ تمديداً منتهياً للحقل F_n . من جهة أخرى، بما أن الحقل K تمديد جبري للحقل F وأن $b_0, b_1, \dots, b_n \in K$ فإن العناصر $b_0, b_1, \dots, b_n$ هي عناصر جبرية فوق F وحسب المبرهنة (٩-٣-٣) يكون الحقل F_n تمديداً منتهياً للحقل F .

من جهة ثالثة، بما أن الحقل K تمديد جبري منفصل للحقل F وأن $b_0, b_1, \dots, b_n \in K$ فإن العناصر $b_0, b_1, \dots, b_n$ هي عناصر جبرية منفصلة فوق F وحسب المبرهنة (٥-٩-٣) يكون الحقل F_n تمديداً منفصلاً للحقل F . أيضاً، بما أن $f(x)$ الحدودية

الأصغرية للعنصر a فوق الحقل F_n لأن $F_n \subseteq K$ وبما أن العنصر a منفصل فوق K فإن الحدودية $f(x)$ منفصلة فوق K وبالتالي فإن $f'(x) \neq 0$ وهذا يبين لنا أن $f'(x) \neq 0$ فوق F_n ومنه فإن الحدودية $f(x)$ منفصلة فوق F_n وبالتالي العنصر a منفصل فوق F_n وحسب المبرهنة (٥-٣-٧) نجد أن $F_n(a)$ هو تمديد جبري منفصل للحقل F_n . أصبح لدينا $F_n(a)$ تمديد منته ومنفصل للحقل F_n و F_n تمديد منته ومنفصل للحقل F وحسب المبرهنة (٥-٢-١٥) نجد أن الحقل $F_n(a)$ هو تمديد جبري منفصل للحقل F وبالتالي يكون العنصر a منفصلاً فوق الحقل F . مما سبق نجد أن الحقل E تمديد جبري منفصل للحقل F .

سوف ندرس الآن البنية الجبرية لمجموعة العناصر المنفصلة فوق حقل ما وذلك من خلال المبرهنة الآتية:

مبرهنة ٥-٣-١١.

ليكن الحقل K تمديداً للحقل F و $\bar{F}$ الغلافة الجبرية للحقل F في K . إن المجموعة:

$$F_0 = \{a : a \in K; F \text{ عنصر جبري منفصل فوق } F\}$$

تشكل حقلاً جزئياً في K يحوي الحقل F ومحتوى في $\bar{F}$.

البرهان.

واضح من خلال تعريف المجموعة F_0 أن $F_0 \subseteq \bar{F}$. إن $0 \in F_0$ لأن الحدودية $f(x) = x \in F[x]$ أولية فوق F وأن $f(0) = 0$ وبالتالي الحدودية $f(x)$ هي الحدودية الأصغرية للعنصر 0 فوق F وأن $f'(x) = 1 \neq 0$ ، أي أن الحدودية $f(x)$ منفصلة فوق F وبالتالي العنصر 0 منفصل فوق F .

أيضاً $1 \in F_0$ لأن الحدودية $g(x) = x - 1 \in F[x]$ أولية فوق F وأن $g(1) = 0$ وبالتالي الحدودية $g(x)$ هي الحدودية الأصغرية للعنصر 1 فوق F وأن $g'(x) = 1 \neq 0$ ، أي أن الحدودية $g(x)$ منفصلة فوق F وبالتالي العنصر 1 منفصل فوق F ، كما أن $1 \neq 0$.

ليكن $a_1, a_2 \in F_0$ عندئذ $a_1, a_2 \in K$ وأن هذه العناصر منفصلة فوق F وحسب المبرهنة (٥-٣-٩) يكون الحقل $F(a_1, a_2)$ تمديداً جبرياً منفصلاً للحقل F ، وبما أن

$a_1 - a_2 \in F(a_1, a_2)$ نجد أن العنصر $a_1 - a_2$ منفصل فوق F وبالتالي يكون $a_1 - a_2 \in F_0$. إذا كان $a_2 \neq 0$ فإن $a_1.a_2^{-1} \in F(a_1, a_2)$ وبالتالي يكون العنصر $a_1.a_2^{-1}$ منفصلاً فوق F ومنه فإن $a_1.a_2^{-1} \in F_0$. ما سبق نجد أن F_0 حقل جزئي في K . لنبرهن على أن $F \subseteq F_0$. ليكن $b \in F$ عندئذ الحدودية $h(x) = x - b \in F[x]$ هي الحدودية الأصغرية للعنصر b فوق F وأن $h'(x) = 1 \neq 0$ أي أن $h(x)$ منفصلة فوق F وبالتالي يكون العنصر b منفصلاً فوق F ، أي أن $b \in F_0$ ومنه نجد أن $F \subseteq F_0$.

تعريف.

ليكن الحقل K تمديداً للحقل F . نسمي الحقل:

$$F_0 = \{a : a \in K; \text{ عنصر جبري منفصل فوق } F\}$$

التمديد الجبري المنفصل الأعظمي للحقل F في K .

ونقول عن الحقل F إنه مغلق انفصالياً في K إذا كان $F_0 = F$.

لندرس الآن العلاقة بين الغلاقة الجبرية لحقل ما والتمديد الجبري المنفصل الأعظمي لهذا الحقل وذلك من خلال المبرهنة الآتية:

مبرهنة ١٢-٣-٥.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً للحقل F و $\bar{F}$ الغلاقة الجبرية للحقل F في K و F_0 التمديد الجبري المنفصل الأعظمي للحقل F في K . إن الحقل $\bar{F}$ هو تمديد جبري غير منفصل تماماً للحقل F_0 .

البرهان.

بما أن الحقل $\bar{F}$ تمديد جبري للحقل F وأن $F \subseteq F_0 \subseteq \bar{F}$ فإن الحقل $\bar{F}$ هو تمديد جبري للحقل F_0 . ليكن $a \in \bar{F}$ عندئذ العنصر a جبري فوق F . لنفرض أن $f(x)$ الحدودية الأصغرية للعنصر a فوق F وأن p^m درجة عدم انفصالية $f(x)$ فوق F ، عندئذ فإن $f(x) \in F[x^{p^m}]$ وأن $f(x) \notin F[x^{p^{m+1}}]$ ومنه $f(x) = \varphi(x^{p^m})$ حيث $\varphi(x) \in F[x]$ وأن $\varphi(x) \notin F[x^p]$. بما أن $f(x) \neq 0$ فإن $\varphi(x) \neq 0$. كما أن $\varphi(x)$

غير قابلة للقلب في $F[x]$. لأنه إذا كانت $\varphi(x)$ قابلة للقلب في $F[x]$ فإنه توجد $\psi(x) \in F[x]$ بحيث $\varphi(x).\psi(x) = 1$ ومنه يكون $\varphi(x^{p^m}).\psi(x^{p^m}) = 1$ أي أن $\varphi(x^{p^m}).\psi(x^{p^m}) = 1$ وبالتالي يكون $f(x)$ قابلاً للقلب في $F[x]$ وهذا غير ممكن. بالإضافة لذلك، الحدودية $f(x)$ أولية في $F[x]$ لأنه إذا كانت $\varphi_1(x), \varphi_2(x) \in F[x]$ بحيث $\varphi(x) = \varphi_1(x).\varphi_2(x)$ عندئذ يكون $\varphi(x) = \varphi_1(x^{p^m}).\varphi_2(x^{p^m})$ وبما أن الحدودية $f(x)$ أولية في $F[x]$ عندئذ إما $\varphi_1(x^{p^m})$ أو $\varphi_2(x^{p^m})$ تكون قابلة للقلب في $F[x]$.

إذا كانت $\varphi_1(x^{p^m})$ قابلة للقلب في $F[x]$ عندئذ تكون $\partial \varphi_1(x^{p^m}) = \partial \varphi_1(x).p^m = 0$ ومنه فإن $\partial \varphi_1(x) = 0$ أي أن $\varphi_1(x)$ قابلة للقلب في $F[x]$. أيضاً إذا كانت $\varphi_2(x^{p^m})$ قابلة للقلب في $F[x]$ تكون $\varphi_2(x)$ قابلة للقلب في $F[x]$ ، وهذا يبين لنا أن الحدودية $\varphi(x)$ أولية في $F[x]$.

كما أن $\varphi(a^{p^m}) = 0$ أي أن $\varphi(x)$ هي الحدودية الأصغرية للعنصر a^{p^m} فوق F وبما أن $\varphi(x) \notin F[x^p]$ فإنه حسب المبرهنة (٥-١-٣) يكون $\varphi'(x) \neq 0$ ومنه تكون الحدودية $\varphi(x)$ منفصلة فوق F وبالتالي يكون العنصر a^{p^m} منفصلاً فوق F أي أن $a^{p^m} \in F_0$ ، وهذا يبين لنا أن العنصر a غير منفصل تماماً فوق F . مما سبق نجد أن الحقل $\bar{F}$ تمديد جبري غير منفصل تماماً للحقل F_0 .

تعريف.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً منتهياً للحقل F و $\bar{F}$ الغلاقة الجبرية للحقل F في K و F_0 التمديد الجبري المنفصل الأعظمي للحقل F في K . بما أن K تمديد منته للحقل F فإنه حسب المبرهنة (٣-٣-٦) فإن K تمديد جبري للحقل F وبالتالي فإن $\bar{F} = K$. أصبح لدينا $\bar{F} = K \subseteq F_0 \subseteq F$. بما أن K تمديد منته للحقل F فإنه حسب المبرهنة (٣-٢-٢) يكون $\bar{F} = K$ تمديداً منتهياً للحقل F_0 ، من جهة أخرى، بما أن $\bar{F}$ تمديد جبري غير منفصل تماماً للحقل F_0 وذلك حسب المبرهنة (٥-٣-٣) (١٢) فإنه حسب المبرهنة (٥-٣-٣) يكون $[K : F_0] = p^m$ حيث m عدد صحيح غير سالب. لنفرض أن $[F_0 : F] = n_0$ نجد أن:

$$.[K : F] = [K : F_0].[F_0 : F] = p^m.n_0$$

نسمي n_0 درجة انفصالية الحقل K فوق F ونرمز لها $[K : F]_s$ ونسمي p^m درجة عدم

انفصالية الحقل K فوق F ونرمز لها $[K : F]_i$.

باستخدام الرموز السابقة نجد أن:

$$[K : F] = [K : F]_s.[K : F]_i$$

$$.[K : F]_i = p^m = [K : F_0] \text{ وأن } [K : F]_s = n_0 = [F_0 : F]$$

لندرس الآن العلاقة بين درجة انفصالية الحدودية الأصغرية لعنصر جبري ودرجة انفصالية التمديد المولد بعنصر جبري وذلك من خلال المبرهنة الآتية:

مبرهنة ١٣-٣-٥.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً للحقل F و $a \in K$ عنصراً جبرياً فوق F . إذا كانت $f(x)$ الحدودية الأصغرية للعنصر a فوق F وكانت n_0 درجة انفصالية $f(x)$ فوق F و p^m درجة عدم انفصالية $f(x)$ فوق F . عندئذ يكون:

$$[F(a) : F]_s = n_0, \quad [F(a) : F]_i = p^m$$

البرهان.

بما أن p^m درجة عدم انفصالية $f(x)$ فوق F ، عندئذ فإن $f(x) \in F[x^{p^m}]$ وأن $f(x) \notin F[x^{p^{m+1}}]$ ومنه $f(x) = \varphi(x^{p^m})$ حيث $\varphi(x) \in F[x]$ وأن $\varphi(x) \notin F[x^p]$. بفرض أن $y = a^{p^m} \in F$ ، عندئذ بما أن $f(x)$ الحدودية الأصغرية للعنصر a فوق F فإن $\varphi(x)$ هي الحدودية الأصغرية للعنصر a^{p^m} فوق F . وبما أن $\varphi(x) \notin F[x^p]$ فإنه حسب المبرهنة (٣-١-٥) يكون $\varphi'(x) \neq 0$ ومنه تكون الحدودية $\varphi(x)$ منفصلة فوق F وبالتالي يكون العنصر $y = a^{p^m}$ منفصلاً فوق F وحسب المبرهنة (٧-٣-٥) يكون الحقل $F(y)$ تمديداً جبرياً منفصلاً للحقل F . وبما أن $y = a^{p^m} \in F(a)$ فإن $F(y) \subseteq F(a)$ ، بفرض أن F_0 التمديد الجبري المنفصل الأعظمي للحقل F في $F(a)$ عندئذ يكون $F(y) \subseteq F_0$.

من جهة أخرى، بما أن $\partial f(x) = n_0.p^m$ وأن $\partial f(x) = \partial \varphi(x).p^m$ نجد أن

$\partial \varphi(x) = n_0$ وبالتالي يكون $[F(y):F] = n_0$. بفرض أن $\partial f(x) = n$ عندئذ تكون المجموعة $\{1, a, a^2, \dots, a^{n-1}\}$ قاعدة للحقل $F(a)$ فوق F وبالتالي أياً كان $z \in F(a)$ فإن z يكتب بصورة وحيدة على الشكل $z = \sum_{i=0}^{n-1} b_i \cdot a^i$ حيث $b_i \in F$ لأجل جميع القيم $0 \leq i \leq n-1$ ، ومنه يكون:

$$z^{p^m} = \left(\sum_{i=0}^{n-1} b_i \cdot a^i \right)^{p^m} = \sum_{i=0}^{n-1} (b_i \cdot a^i)^{p^m} = \sum_{i=0}^{n-1} b_i^{p^m} \cdot a^{i \cdot p^m} \in F(a^{p^m})$$

وهذا يبين لنا أنه أياً كان $z \in F(a)$ فإن العنصر z غير منفصل تماماً فوق $F(y)$ ومنه فإن $F(a)$ تمديد غير منفصل تماماً للحقل $F(y)$. لنبرهن على أن $F_0 \subseteq F(y)$. ليكن $d \in F_0$ عندئذ d عنصر منفصل فوق F وبما أن $F \subseteq F(y) \subseteq F_0$ نجد أن d عنصر منفصل فوق $F(y)$ ، كما أن $d \in F_0 \subseteq F(a)$ وبالتالي فإن d غير منفصل تماماً فوق $F(y)$ وحسب المبرهنة (٥-٣-٤) نجد أن $d \in F(y)$ وهكذا فإن $F_0 \subseteq F(y)$ ، مما سبق نجد أن $F_0 = F(y)$ وبالتالي يكون:

$$[F(a):F]_s = [F_0:F] = [F(y):F] = n_0$$

وبما أن $[F(a):F] = n = n_0 \cdot p^m$ وأن:

$$[F(a):F] = [F(a):F]_s \cdot [F(a):F]_i = n_0 \cdot [F(a):F]_i$$

نجد أن $[F(a):F]_i = p^m$ ◊

مبرهنة ١٤-٣-٥

ليكن F حقلاً مميزه يساوي الصفر. إذا كان الحقل K تمديداً منتهياً ومنفصلاً للحقل

F ، عندئذ يوجد $\alpha \in K$ بحيث $K = F(\alpha)$.

البرهان.

لنفرض أن الحقل K تمديد منته ومنفصل للحقل F ولنفرض أيضاً أن $[K:F] = n$. سوف نورد البرهان بالاستقراء حسب n .

- من أجل $n = 1$ في هذه الحالة يكون $K = F(\alpha)$ حيث $\alpha \in K$.

- من أجل $n = 2$. في هذه الحالة يوجد $\beta, \gamma \in K$ بحيث $K = F(\beta, \gamma)$.

لنفرض أن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر β وأن $g(x) \in F[x]$ الحدودية

الأصغرية للعنصر γ . ولما كان الحقل K تمديداً منفصلاً للحقل F فإن العنصرين β, γ منفصلان فوق F وحسب التعريف تكون كل من $f(x), g(x)$ حدودية منفصلة فوق F . وحسب المبرهنة (٤-٢-٦) تكون جميع أصفار الحدوديتين $f(x)$ و $g(x)$ هي أصفاراً بسيطة فوق F . لنفرض أن $\beta = \beta_1, \beta_2, \dots, \beta_n \in \bar{F}$ هي جميع الأصفار الحدودية $f(x)$ فوق F والتي جميعها أصفار بسيطة فوق F ، وأن $\gamma = \gamma_1, \gamma_2, \dots, \gamma_m \in \bar{F}$ هي جميع الأصفار الحدودية $g(x)$ فوق F والتي جميعها أصفار بسيطة فوق F . وبما أن الحقل F غير منته فإنه يوجد $a \in F$ بحيث $a \neq \beta_i - \beta / \gamma - \gamma_j$ وذلك لأجل كل i, j و $j \neq 1$. ومنه يكون $a(\gamma - \gamma_j) \neq \beta_i - \beta$ وبالتالي يكون:

$$\beta + a\gamma \neq \beta_i + a\gamma_j$$

لنضع $\alpha = \beta + a\gamma$ فيكون $\alpha \neq \beta_i + a\gamma_j$ ومنه نجد أن $\alpha - a\gamma_j \neq \beta_i$ وذلك لأجل كل i, j و $j \neq 1$. لنأخذ الحدودية $h(x) = f(\alpha - ax) \in F(\alpha)[x]$ فنجد أن:

$$h(\gamma) = f(\alpha - a\gamma) = f(\beta) = 0$$

فضلاً عن ذلك، فإن $h(\gamma_j) \neq 0$ لأجل $j \neq 1$ ، لأنه إذا كان $h(\gamma_j) = 0$ حيث $j \neq 1$ نجد أن $h(\gamma_j) = f(\alpha - a\gamma_j) = 0$ وهذا يبين أن $\alpha - a\gamma_j \in \{\beta_1, \beta_2, \dots, \beta_n\}$ لنفرض أن $\alpha - a\gamma_j = \beta_i$ حيث $1 \leq i \leq n$ فيكون $\beta + a\gamma - a\gamma_j = \beta_i$ وهذا يبين أن $a(\gamma - \gamma_j) = \beta_i - \beta$ وهذا غير ممكن.

من جهة أخرى، بما أن $h(\gamma) = 0$ نجد أن $x - \gamma$ يقسم $h(x)$ في $F(\alpha)[x]$ لأن $h(x) \in F(\alpha)[x]$ ، كما أن $x - \gamma$ يقسم $g(x)$ في $F(\alpha)[x]$ وهذا يبين أن كلا من $g(x)$ و $h(x)$ يملكان عاملاً مشتركاً هو $x - \gamma$ والذي هو الحدودية الأصغرية للعنصر γ فوق $F(\alpha)$ ومنه يكون $\gamma \in F(\alpha)$ وبالتالي يكون $\beta = \alpha - a\gamma \in F(\alpha)$. مما سبق نجد أن $F(\beta, \gamma) = F(\alpha)$ وبحسب مبدأ الاستقرار نحصل على المطلوب. ◊

اعتماداً على المبرهنة الأخيرة يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن F حقلاً مميزه يساوي الصفر. عندئذ أي تمديد منته للحقل F هو تمديد بسيط.

البرهان.

لنفرض أن K هو تمديد منته للحقل F ، عندئذ يكون K تمديداً جبرياً للحقل F ، لما كان مميز الحقل F يساوي الصفر، فإنه حسب التمهيدية (١-٣-٥) يكون الحقل K تمديداً منفصلاً للحقل F . أصبح لدينا K هو تمديد منته ومنفصل للحقل F وحسب المبرهنة (١٤-٣-٥) يكون الحقل K تمديداً بسيطاً للحقل F . ◊

مبرهنة ١٥-٣-٥.

ليكن F حقلاً مميزه $p \neq 0$. لنفرض أن الحقل K تمديد للحقل F وأن الحقل E تمديد للحقل K . عندئذ الشروط الآتية متكافئة:

- ١ - الحقل E تمديد غير منفصل تماماً للحقل F .
- ٢ - الحقل E تمديد غير منفصل تماماً للحقل K والحقل K تمديد غير منفصل تماماً للحقل F .

البرهان.

لدينا حسب الفرض $F \subseteq K \subseteq E$.

(1) $\Leftrightarrow$ (2). لنفرض أن الحقل E تمديد غير منفصل تماماً للحقل F وليكن $a \in E$

وحسب التعريف يوجد عدد صحيح $n \geq 0$ بحيث $a^{p^n} \in F$ ولما كان $F \subseteq K$ نجد أن $a^{p^n} \in K$ وهذا يبين أن الحقل E تمديد غير منفصل تماماً للحقل K .

ليكن $b \in K$ عندئذ يكون $b \in E$ وحسب التعريف يوجد عدد صحيح $m \geq 0$ بحيث $b^{p^m} \in F$ وهذا يبين أن الحقل K تمديد غير منفصل تماماً للحقل F .

(2) $\Leftrightarrow$ (1). ليكن $a \in E$ وحسب الفرض يوجد عدد صحيح $n \geq 0$ بحيث $a^{p^n} \in K$

وأيضاً حسب الفرض يوجد عدد صحيح $m \geq 0$ بحيث $(a^{p^n})^{p^m} \in F$ ومنه نجد أن $a^{p^{n+m}} \in F$ وهذا يبين أن الحقل E تمديد غير منفصل تماماً للحقل F . ◊

تمارين محلولة (٥)

١ - ليكن F حقلاً مميزه $p \neq 0$ ولتكن $f(x) = x^p - a \in F[x]$. أثبت أنه إما $f(x)$ أولية، أو أن $f(x)$ تتفرق فوق F .

الحل.

بما أن $f(x) = x^p - a \in F[x]$ ، عندئذ فإن $a \in F$. نميز حالتين:
 - $a \notin F^p$ وحسب المبرهنة (٥-٢-١) فإن الحدودية $f(x)$ أولية في $F[x]$.
 - $a \in F^p$ عندئذ يوجد $b \in F$ بحيث $a = b^p$. ومنه نجد أن

$$f(x) = x^p - a = x^p - b^p = (x - a)^p \in F[x]$$
 وهذا يبين أن $f(x)$ تتفرق في $F[x]$.

٢ - ليكن F حقلاً . لنأخذ التطبيق $D: F[x] \rightarrow F[x]$ المعروف بالشكل الآتي: أيأ كان $f(x) \in F[x]$ فإن $D(f(x)) = f'(x)$. والمطلوب:

- أ- أثبت أن التطبيق D هو تشكل للزمرة $(F[x], +)$.
- ب- إذا كان مميز الحقل F يساوي الصفر ، أوجد نواة التشاكل D .
- ت- إذا كان مميز الحقل F يساوي $p \neq 0$ ، أوجد نواة التشاكل D .

الحل.

أ - ليكن $f(x), g(x) \in F[x]$ ، بالاعتماد على التمهيدية (٥-١-١) نجد أن:

$$\begin{aligned} D(f(x) + g(x)) &= (f(x) + g(x))' = f'(x) + g'(x) = \\ &= D(f(x)) + D(g(x)) \end{aligned}$$

وهذا يبين أن D هو تشكل للزمرة $(F[x], +)$.

ب - لنفرض أن مميز الحقل F يساوي الصفر .

ليكن $f(x) \in \text{Ker } D$ عندئذ $f(x) \in F[x]$ وأن $f'(x) = 0$ وحسب التمهيدية (٥-١-٢) نجد أن $\partial f(x) = 0$ ومنه نجد أن:

$$\text{Ker } D = \{f(x) : f(x) \in F[x]; \partial f(x) = 0\}$$

ت - لنفرض أن مميز الحقل F يساوي $p \neq 0$.
 ليكن $f(x) \in \text{Ker } D$ عندئذ $f(x) \in F[x]$ وأن $D(f(x)) = f'(x) = 0$ وحسب
 التمهيدية (٥-١-٣) نجد أن $f(x) = g(x^p)$ حيث $g(x) \in F[x]$ ومنه نجد أن:
 $\text{Ker } D = \{f(x) : f(x) \in F[x]; f(x) = g(x^p) : g(x) \in F[x]\}$

٣ - بالعودة إلى التمرين (٢)، أثبت أنه لأجل كل عدد صحيح $m > 1$ فإن:

$$D((f(x))^m) = m \cdot (f(x))^{m-1} \cdot f'(x)$$

وذلك أياً كان $f(x) \in F[x]$.

الحل.

نلاحظ أنه لأجل $m = 2$ فإنه حسب التمهيدية (٥-١-١) نجد أن:

$$\begin{aligned} D((f(x))^2) &= (f(x) \cdot f(x))' = f'(x) \cdot f(x) + f(x) \cdot f'(x) = \\ &= 2 \cdot f(x) \cdot f'(x) \end{aligned}$$

لنفرض أن المساواة صحيحة لأجل العدد $m-1$ عندئذ يكون:

$$D((f(x))^{m-1}) = (m-1) \cdot (f(x))^{m-2} \cdot f'(x)$$

ومنه نجد أن:

$$\begin{aligned} D((f(x))^m) &= ((f(x))^m)' = ((f(x))^{m-1} \cdot f(x))' = \\ &= (f(x))^{m-1} \cdot f'(x) + (f(x))^{m-1} \cdot f'(x) = (m-1) \cdot (f(x))^{m-2} \cdot f'(x) \cdot f(x) + \\ &+ (f(x))^{m-1} \cdot f'(x) = (m-1) \cdot (f(x))^{m-1} \cdot f'(x) + (f(x))^{m-1} \cdot f'(x) = \\ &= m \cdot (f(x))^{m-1} \cdot f'(x) \end{aligned}$$

٤ - ليكن $F = Q(i, -i, \sqrt{5}, \sqrt{-5})$ و $K = Q(i, \sqrt{5})$. أثبت أن كلا من F, K هو

تمديد بسيط للحقل Q .

الحل.

بما أن $i, \sqrt{5} \in F$ نجد أن $K = Q(i, \sqrt{5}) \subseteq F$.

من جهة أخرى، لما كان K حقلاً وأن $i, \sqrt{5} \in K$ نجد أن $-i, -\sqrt{5} \in K$ ، أصبح لدينا
 $i, -i, \sqrt{5}, \sqrt{-5} \in K$ ومنه فإن $F = Q(i, -i, \sqrt{5}, \sqrt{-5}) \subseteq K$ وهكذا نجد أن
 $F = K$. كي يتم المطلوب لنبرهن على أن $K = Q(i, \sqrt{5}) = Q(i + \sqrt{5})$.

لما كان $i, \sqrt{5} \in K$ فإن $i + \sqrt{5} \in K$ ومنه فإن $Q(i, \sqrt{5}) = K$ و $Q(i + \sqrt{5}) \subseteq Q(i, \sqrt{5})$.
من جهة ثالثة، لما كان $i + \sqrt{5} \in Q(i + \sqrt{5})$ نجد أن:

$$(i + \sqrt{5})^2 = 4 + 2i\sqrt{5} \in Q(i + \sqrt{5})$$

ومنه فإن $(i + \sqrt{5}) \cdot (4 + 2i\sqrt{5}) = 12i \in Q(i + \sqrt{5})$ وبالتالي فإن $i \in Q(i + \sqrt{5})$ ومنه نجد أن $\sqrt{5} = (i + \sqrt{5}) - i \in Q(i + \sqrt{5})$ وهكذا فإن $i, \sqrt{5} \in Q(i + \sqrt{5})$ وهذا يبين أن $Q(i, \sqrt{5}) \subseteq Q(i + \sqrt{5})$ وبالتالي فإن $K = Q(i, \sqrt{5}) = Q(i + \sqrt{5})$.
مما سبق نجد أن $F = K = Q(i + \sqrt{5})$ وهذا يبين أن كلاً من F, K هو تمديد بسيط للحقل Q . ◊

٥ - أثبت أن كل حدودية أولية فوق حقل غير منته تكون منفصلة.

الحل.

لنفرض أن F حقلاً غير منته، عندئذ يكون مميز F يساوي الصفر.
لتكن $f(x) \in F[x]$ حدودية أولية فوق الحقل F ، لما كان $\partial f(x) > 0$ فإنه حسب التمهيدية (٥-٢-٢) تكون الحدودية $f(x)$ منفصلة فوق F . ◊

٦ - ليكن F, L حقليْن و $\sigma: F \rightarrow L$ تشاكلاً حلقياً. إذا كان $d \in L$ عندئذ التطبيق

$$\sigma_d: F[x] \rightarrow L \text{ المعرفة بالشكل الآتي: أيًا كان } q(x) \in F[x] \text{ فإن:}$$

$$\sigma_d q(x) = (\sigma(q(x)))(d)$$

تشاكل حلقى.

الحل.

ليكن $q(x), \mu(x) \in F[x]$ ولنفرض أن $q(x) = \sum_{i=0}^n a_i x^i$, $\mu(x) = \sum_{i=0}^m b_i x^i$ حيث $a_i, b_j \in F$ أيًا كان i, j . لنفرض أن $n \geq m$ نجد أن:

$$q(x) + \mu(x) = \sum_{i=0}^n (a_i + b_i) x^i$$

ومنه يكون:

$$\sigma(q(x) + \mu(x)) = \sum_{i=0}^n \sigma(a_i + b_i) x^i \in L[x]$$

وبالتالي فإن:

$$\begin{aligned}\sigma(q(x) + \mu(x))(d) &= \sum_{i=0}^n \sigma(a_i + b_i)d^i = \sum_{i=0}^n (\sigma(a_i) + \sigma(b_i))d^i = \\ &= \sum_{i=0}^n (\sigma(a_i) + \sum_{i=0}^n \sigma(b_i))d^i = (\sigma(q(x)))(d) + (\sigma(\mu(x)))(d)\end{aligned}$$

ومنه نجد أن:

$$\begin{aligned}\sigma_d(q(x) + \mu(x)) &= (\sigma(q(x) + \mu(x)))(d) = \\ &= (\sigma(q(x)))(d) + (\sigma(\mu(x)))(d) = \sigma_d(q(x)) + \sigma_d(\mu(x))\end{aligned}$$

كما أن $q(x) \cdot \mu(x) = \sum_{k=0}^{n+m} c_k x^k \in F$ حيث $c_k = \sum_{i+j=k} a_i \cdot b_j$ ومنه نجد أن:

$$\begin{aligned}\sigma(q(x) \cdot \mu(x)) &= \sum_{k=0}^{n+m} \sigma(c_k) x^k \in L[x] \\ \sigma(c_k) &= \sigma(\sum_{i+j=k} a_i \cdot b_j) = \sum_{i+j=k} \sigma(a_i \cdot b_j) = \sum_{i+j=k} \sigma(a_i) \cdot \sigma(b_j)\end{aligned}$$

ومنه يكون:

$$\begin{aligned}(\sigma(q(x) \cdot \mu(x)))(d) &= \sum_{k=0}^{n+m} \sigma(c_k) d^k = \sum_{i=0}^n (\sigma(a_i) d^i \cdot \sum_{i=0}^m \sigma(b_i)) d^i = \\ &= (\sigma(q(x)))(d) \cdot (\sigma(\mu(x)))(d)\end{aligned}$$

وهذا يبين أن $\sigma_d(q(x) \cdot \mu(x)) = \sigma_d(q(x)) \cdot \sigma_d(\mu(x))(d)$ أي أن التطبيق σ_d هو تشاكل حلقي. ♦

٧ - ليكن الحقل E تمديداً للحقل F وأن $a, b \in K$. أثبت أن:

$$F(a, b) = F(a)(b) = F(a) \cdot F(b)$$

الحل.

لدينا حسب المبرهنة (٣-١-٢) أن $F(a, b) = F(a)(b)$.

من جهة أخرى، لما كان:

$$a \in F(a) \subseteq F(a) \cdot F(b), \quad b \in F(b) \subseteq F(a) \cdot F(b)$$

نجد أن $F(a, b) \subseteq F(a) \cdot F(b)$. أيضاً لما كان:

$$F(a) \subseteq F(a, b), \quad F(b) \subseteq F(a, b)$$

فإن $F(a, b) = F(a) \cdot F(b)$ ، مما سبق نجد أن $F(a, b) = F(a) \cdot F(b)$.

٨ - ليكن الحقل K تمديداً للحقل F ولنفرض أن الحدودية:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

إذا كان $b \in K$ $0 \neq b$ صفراً للحدودية $f(x)$ ، أثبت أن العنصر b^{-1} هو صفر للحدودية:

$$g(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in F[x]$$

الحل.

لنفرض أن العنصر $0 \neq b \in K$ هو صفر للحدودية $f(x)$ ، عندئذ يكون:

$$a_nb^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$$

لنضرب طرفي المساواة السابقة بالعنصر $(b^{-1})^n$ فنجد أن:

$$a_0(b^{-1})^n + a_1(b^{-1})^{n-1} + \dots + a_{n-1}b^{-1} + a_n = 0$$

وهذا يبين أن العنصر b^{-1} هو صفر للحدودية $g(x)$.

٩ - اكتب الحدودية $4x^2 - 4x + 8$ على جداء لحدوديات أولية في كل من الحلقات

الآتية $Z[x], Q[x], Z_{11}[x]$.

الحل.

في الحلقة $Z[x]$ إن $4x^2 - 4x + 8 = (2)(2)(x^2 - x + 2)$ حيث أن كلاً من:

$$(2), (x^2 - x + 2) \in Z[x]$$

هي حدودية أولية.

في الحلقة $Q[x]$ إن $4x^2 - 4x + 8$ هي حدودية أولية.

في الحلقة $Z_{11}[x]$ إن $4x^2 - 4x + 8 = (4x + 2)(x + 4)$ حيث أن كلاً من:

$$(4x + 2), (x + 4) \in Z_{11}[x]$$

هي حدودية أولية.

تمارين (٥)

١ - أثبت أن المجموعة $F = \{0,2,4,6,8\}$ بالنسبة لعمليتي الجمع والضرب بالمقاس 10 تشكل حقلاً.

٢ - لنأخذ المجموعة $Z_n[i] = \{a+bi : a,b \in Z_n; i^2 = -1\}$ والمطلوب:

أ - أثبت أنه لأجل $n = 3,7,11$ فإن $Z_n[i]$ تشكل حقلاً.

ب - أثبت أنه لأجل $n = 2,5,13$ فإن $Z_n[i]$ لا تشكل حقلاً.

٣ - أوجد جميع أصفار الحدودية $f(x) = x^2 - x + 2 \in Z_3[x]$.

٤ - ليكن F حقلاً منتهياً مرتبته n . أثبت أنه أياً كان $a \in F$ فإن $a^{n-1} = 1$.

٥ - ليكن F حقلاً منتهياً مرتبته 8. وليكن $a, b \in F$ بحيث $a^2 + ab + b^2 = 0$. أثبت أن $a = b = 0$.

٦ - لتكن $Z_2[x]$ حلقة الحدوديات فوق الحقل Z_2 ولتكن $x^2 + x + 1 \in Z_2[x]$. أثبت أن حلقة الخارج $Z_2[x]/\langle x^2 + x + 1 \rangle$ تشكل حقلاً.

٧ - أثبت أن الحقلين $Q(\sqrt{2})$ و $Q(\sqrt{5})$ متماثلان.

٨ - أثبت أن $(50!)^2 = -1 \pmod{101}$.

٩ - أثبت أن الحقل $Q(\sqrt{2})$ يماثل الحقل $Q[x]/\langle x^2 - 2 \rangle$.

١٠ - أثبت أنه لأجل أي عدد أولي p يوجد حقل مرتبته p^2 .

١١ - ليكن F حقلاً مميزه $p \neq 0$ و $f(x) = x^p - a \in F[x]$. أثبت أن الحدودية $f(x)$ إما أولية في $F[x]$ أو تتفرق فوق F .

١٢ - أوجد الحدودية الأصغرية للعنصر $\sqrt{-3} + \sqrt{2}$ فوق Q .

١٣ - أوجد الحدودية الأصغرية للعنصر $\sqrt[3]{-3} + \sqrt[3]{4}$ فوق Q .

١٤ - أوجد حقل التفريق للحدودية $x^4 - x^2 - 2$ فوق الحقل Z_3 .

١٥ - أثبت أن الحدودية $x^{50} - 1$ لا تملك أصفاراً مضاعفة في أي تمديد للحقل Z_3 .

١٦ - أثبت أن الحقل $Q(\sqrt[4]{2})$ هو تمديد للحقل $Q(\sqrt{2})$ وحدد عناصره.

١٧ - ليكن F حقلاً و $f(x) \in F[x]$. إذا كانت $\partial f(x) = 2$ ، وإذا كان a صفراً للحدودية $f(x)$ في تمديد ما للحقل F . أثبت أن $F(a)$ هو حقل التفريق للحدودية $f(x)$ فوق F .

١٨ - ليكن F حقلاً و a عنصراً جبرياً فوق F درجته n . أثبت أن العنصر a^{-1} جبري فوق F ودرجته n .

١٩ - ليكن F حقلاً و a, b عنصراً جبرياً فوق F . أثبت أن العنصر b جبري فوق $F(a)$.

٢٠ - ليكن F و $p(x) \in F[x]$. إذا كانت $\partial p(x) = n$ وكان الحقل K هو حقل التفريق للحدودية $p(x)$ فوق F . أثبت أن $[K : F] \leq n!$.

الفصل السادس

الحقول المنتهية

٦ - ١. الحقول المنتهية .

في هذه الفقرة سوف ندرس الحقول المنتهية والتي تعد واحداً من أهم فروع الجبر المجرد والأكثر متعة ويعد Galois أول من أدخل مفهوم الحقول المنتهية وذلك عام 1830. سنبدأ أولاً بدراسة مسألة وجود الحقول المنتهية.

نعلم سابقاً من خلال دراستنا لنظرية الحلقات أنه لأجل أي عدد أولي p يوجد حقل منته مرتبته p وهو الحقل Z_p وهذا الحقل وحيد، بمعنى أن أي حقل آخر مرتبته p يماثل Z_p وهذا ما سوف تثبته لنا المبرهنة الآتية:

مبرهنة ٦-١-١.

لأجل أي عدد أولي p يوجد حقل منته مرتبته p وهو الحقل Z_p وهذا الحقل وحيد، بمعنى أنه إذا وجد حقل آخر F مرتبته p فإن F يماثل Z_p أي $F \cong Z_p$.
البرهان.

نعلم أنه لأجل أي عدد أولي p فإن مجموعة الأعداد الصحيحة:

$$Z_p = \{0, 1, 2, \dots, p-1\}$$

بالنسبة لعمليتي الجمع والضرب بالمقاس p تشكل حقلاً والذي يسمى حقل الأعداد الصحيحة بالمقاس p .

ليكن F حقلاً آخر مرتبته p ، عندئذ حسب التمهيدية (٤-١-٢) فإن مميز الحقل F لا يساوي الصفر. بما أن الزمرة الجمعية $(F, +)$ مرتبتها p فإن $p \cdot 1_F = 0$.

لنعرف العلاقة $\tau: Z_p \rightarrow F$ بالشكل الآتي: أيّاً كان $n \in Z_p$ فإن $\tau(n) = n \cdot 1_F$ فنجد أن τ تطبيق، لأنه إذا كان $n, m \in Z_p$ بحيث $n = m$ فإن $n \cdot 1_F = m \cdot 1_F$ ومنه $\tau(n) = \tau(m)$. كما أن τ تشاكل، لأنه إذا كان $n, m \in Z_p$ فإن:

$$\tau(n+m) = (n+m) \cdot 1_F = n \cdot 1_F + m \cdot 1_F = \tau(n) + \tau(m)$$

$\tau(n \cdot m) = (n \cdot m) \cdot 1_F = (n \cdot m)(1_F \cdot 1_F) = (n \cdot 1_F) \cdot (m \cdot 1_F) = \tau(n) \cdot \tau(m)$
 كما أن $\tau(1) = 1$ ، ومنه حسب التمهيدية (٣-١-٣) فإن τ متباين. لنضع:

$$K = \text{Im}(\tau) = \{0, 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, (p-1) \cdot 1_F\}$$

ف نجد أن K حقل جزئي في F مرتبته p ومنه فإن $F = \text{Im}(\tau)$ وهذا يبين لنا أن τ تماثل وبالتالي فإن $F \cong Z_p$.

المبرهنة الآتية تعد تعميماً للمبرهنة السابقة، وهي تعد من المبرهنات الأساسية في دراسة الحقول المنتهية:

مبرهنة ٢-١-٦.

لأجل أي عدد أولي p ولأجل أي عدد صحيح موجب n يوجد حقل منته مرتبته p^n وهذا الحقل وحيد، بمعنى أنه إذا وجد حقلان F و K مرتبة كل منهما تساوي p^n فإن $F \cong K$ أي $F \cong K$.

البرهان.

ليكن p عدداً أولياً و $n \geq 1$ عدداً صحيحاً. لنأخذ الحقل Z_p والحدودية:

$$f(x) = x^{p^n} - x \in Z_p[x]$$

ف نجد أن $f(x) \neq 0$ كما أن $\partial f(x) = p^n$. وحسب المبرهنة (٢-٢-٤) يوجد حقل تفريق للحدودية $f(x)$ فوق Z_p وليكن E . لنبرهن على أن الحقل E منته ومرتبته p^n . نلاحظ أولاً أن مميز الحقل E يساوي p وذلك لأن مميز الحقل Z_p يساوي p وبالتالي فإن الحقل E هو حقل منته. من جهة أخرى، بما أن $\partial f(x) = p^n$ فإنه حسب المبرهنة (٨-١-١) فإن الحدودية تملك بالتحديد p^n صفراً بما فيها الأصفار المضاعفة.

بما أن $f'(x) = p^n x^{p^n-1} - 1 = -1$ نجد أن كلاً من $f(x)$ و $f'(x)$ لا تملك عوامل مشتركة في $Z_p[x]$ درجته موجبة وحسب المبرهنة (٥-١-٥) فإن $f(x)$ لا تملك أصفاراً مضاعفة في أي تمديد للحقل Z_p وبالتالي فإن الحدودية $f(x)$ تملك بالتحديد p^n صفراً بسيطاً وهذه الأصفار مختلفة متتى متتى.

لنفرض أن K هي مجموعة جميع أصفار الحدودية $f(x)$ في E . إن K تشكل حقلاً

جزئياً في E لأن $0,1 \in K$ وبالتالي فإن K مجموعة جزئية في E غير خالية وأن $0 \neq 1$. ليكن $a, b \in K$ عندئذ فإن $a^{p^n} = a$ وأن $b^{p^n} = b$ ومنه فإن:

$$\begin{aligned} f(a-b) &= (a-b)^{p^n} - (a-b) = (a^{p^n} - b^{p^n}) - (a-b) = \\ &= (a-b) - (a-b) = 0 \end{aligned}$$

ومنه فإن $a-b \in K$ ، كما أنه إذا كان $b \neq 0$ فإن:

$$\begin{aligned} f(ab^{-1}) &= (ab^{-1})^{p^n} - (ab^{-1}) = (a^{p^n} (b^{p^n})^{-1}) - (ab^{-1}) = \\ &= (ab^{-1}) - (ab^{-1}) = 0 \end{aligned}$$

ومنه فإن $ab^{-1} \in K$. وهذا يبين أن K تشكل حقلاً جزئياً في E مرتبته p^n .

بما أن K تشكل حقلاً جزئياً في E يحوي جميع أصفار الحدودية $f(x)$ فإن الحدودية $f(x)$ تتفرد في $K[x]$ إلى مضارب خطية، ومنه فإن K هو حقل تفريق الحدودية $f(x)$. من جهة أخرى، بما أن E هو حقل تفريق الحدودية $f(x)$ نجد أن $K = E$ ومنه فإن E هو حقل التفريق للحدودية $f(x)$ فوق Z_p ومؤلف من p^n عنصر.

الوحدانية. لنفرض أن F حقل آخر مرتبته p^n ، عندئذ فإن F يحوي حقلاً جزئياً يماثل Z_p وذلك من خلال التشاكل $\tau: Z_p \rightarrow F$ المعرف بالشكل الآتي: أيًا كان $n \in Z_p$ فإن $\tau(n) = n.1_F$. ولأن كل عنصر $a \in F^*$ يحقق $a^{p^n-1} = 1$ نجد أن $a^{p^n} = a$ وبالتالي فإن كل عنصر $a \in F^*$ هو صفر للحدودية $f(x) = x^{p^n} - x$ ومنه نجد أن F هو حقل تفريق الحدودية $f(x)$ فوق Z_p . أصبح لدينا كل من F و E هو حقل تفريق الحدودية $f(x)$ فوق Z_p وحسب المبرهنة (٤-٢-٦) فإن $F \cong E$.

بالاعتماد على المبرهنة الأخيرة، أصبح بالإمكان القول إنه يوجد حقل منته وحيد مرتبته p^n . بالاعتماد على هذه الحقيقة يمكننا صياغة التعريف الآتي:

تعريف.

نسمي كل حقل منته F مرتبته p^n حقل غالوا من المرتبة p^n ونرمز له $GF(p^n)$. لنورد الآن المبرهنة المهمة الآتية والتي تنص على أن التمديد المنتهي لحقل منته هو حقل منته.

مبرهنة ٣-١-٦.

ليكن الحقل E تمديداً منتهياً للحقل F وأن $[E : F] = n$. إذا كان الحقل F منتهياً ومرتبته تساوي q ، عندئذ يكون الحقل E منتهياً ومرتبته تساوي q^n .

البرهان.

لنفرض أن $[E : F] = n$ عندئذ توجد قاعدة $\{a_1, a_2, \dots, a_n\} \subseteq E$ للحقل E فوق F ، ومنه أياً كان $y \in E$ فإن $y = \beta_1 a_1 + \beta_2 a_2 + \dots + \beta_n a_n$ حيث $\beta_i \in F$ وذلك لأجل كل $1 \leq i \leq n$. وبما أن مرتبة الحقل F تساوي q فإن كل عنصر $\beta_j \in F$ يأخذ q قيمة، وهكذا نجد أن الحقل E يتألف من q^n عنصر. ◊

نتيجة.

كل حقل منته F مميزه يساوي $p \neq 0$ يتألف فقط يتألف من p^n عنصر، حيث $n \geq 1$ عدد صحيح.

البرهان.

لنفرض أن F حقلاً منتهياً مميزه $p \neq 0$ حسب المبرهنة (٤-١-٤) فإن الحقل F يحوي حقلاً جزئياً مرتبته p وليكن F_p . ولكون الحقل F منتهياً فإن $[E : F_p] = n$ حيث $n \geq 1$ عدد صحيح، وحسب المبرهنة (٣-١-٦) فإن مرتبة الحقل F تساوي p^n . ◊

المبرهنة الآتية تبين لنا طبيعة الزمرة الضربية لحقول غالوا:

مبرهنة ٤-١-٦.

ليكن $F = GF(p^n)$ حقل غالوا. عندئذ الزمر الضربية F^* للحقل F هي زمرة دوارة (دائرية).

البرهان.

بما أن $F = GF(p^n)$ فإن مرتبة الحقل F تساوي p^n . لنأخذ الزمرة الضربية F^* للحقل F بالنسبة لعملية الضرب المعرفة على الحقل F . لنفرض أن $(F^* : 1) = m \geq 1$.

- إذا كان $m = 1$ عندئذ فإن الزمرة F^* دوارة.
- إذا كان $m \neq 1$ عندئذ فإن m غير قابل للقلب في Z ، وبما أن حلقة الأعداد الصحيحة

Z هي حلقة تحليل وحيد فإن العنصر m يمكن كتابته بصورة وحيدة على الشكل:

$$m = p_1^{r_1} \cdot p_2^{r_2} \cdots p_t^{r_t}$$

حيث $p_1, p_2, \dots, p_t$ أعداد أولية مختلفة مثلى مثلى و $r_1, r_2, \dots, r_t$ أعداد صحيحة موجبة.

لنضع $k_i = m/p_i$ حيث $i = 1, 2, \dots, t$ فنجد أن $k_i < m$. لأنه إذا وجد $j \in \{1, 2, \dots, t\}$ من أجله $k_j \geq m$ فإن $m/p_j \geq m$ ومنه $m \geq mp_j$ وهذا غير ممكن لأن $p_j > 1$.

لنأخذ الحدودية $f(x) = x^{k_i} - 1 \in F[x]$ فنجد أن $f(x) \neq 0$ وأن $f(x) = k_i$ و $\partial f(x) = k_i$ ومنه فإن عدد جميع أصفار الحدودية $f(x)$ يساوي k_i بما فيها الأصفار المضاعفة. وبما أن $k_i < m = (F^*: 1)$ فإنه توجد عناصر $b_i \in F^*$ ليست أصفاراً للحدودية $f(x)$ حيث

$i = 1, 2, \dots, s$. لنضع $y_i = b_i^{m/p_i^{r_i}}$ فنجد أن:

$$y_i^{p_i^{r_i}} = (b_i^{m/p_i^{r_i}})^{p_i^{r_i}} = b_i^m = 1$$

وهذا يبين أن مرتبة العنصر y_i تقسم $p_i^{r_i}$ ومنه فإن $o(y_i) = p_i^{s_i}$ حيث $0 \leq s_i \leq r_i$ من جهة أخرى، إن:

$$y_i^{p_i^{r_i-1}} = (b_i^{m/p_i^{r_i}})^{p_i^{r_i-1}} = b_i^{m/p_i} = b_i^{k_i}$$

وبما أن b_i ليس صفراً للحدودية $f(x)$ ، فإن $b_i^{k_i} - 1 \neq 0$ أي أن $b_i^{k_i} \neq 1$ وبالتالي يكون

$y_i^{p_i^{r_i-1}} \neq 1$ ومنه نجد أن $s_i = r_i$. لأنه إذا وجد دليل j لأجله $s_j < r_j$ فإن $s_j < r_j$ وبالتالي يكون $r_j - s_j > 0$ ومنه نجد أن

$$y_j^{p_j^{r_j-1}} = y_j^{p_j^{r_j+s_j-s_j-1}} = (y_j^{p_j^{s_j}})^{p_j^{r_j-s_j-1}} = (1)^{p_j^{r_j-s_j-1}} = 1$$

وهذا يناقض كون $y_i^{p_i^{r_i-1}} \neq 1$ ومنه يكون $s_i = r_i$ وبالتالي فإن $o(y_i) = p_i^{r_i}$.

لنضع $y = y_1 \cdot y_2 \cdots y_s$ فنجد أن $y \in F^*$. لنبرهن على أن $o(y) = m$. لنفرض جلاً أن $o(y) \neq m$. عندئذ فإن $o(y)$ تقسم m وبالتالي فإن $o(y)$ تقسم $\prod_{i=1}^t p_i^{r_i}$ ومنه فإن

$o(y)$ تقسم على الأقل واحداً من المضاريب $p_i^{r_i}$ وليكن $p_l^{r_l}$ حيث $l \in \{1, 2, \dots, s\}$.

ومنه نجد أن $o(y)$ تقسم m/p_l ومنه يكون $y^{m/p_l} = 1$ وبالتالي $(y_1 \cdot y_2 \cdots y_s)^{m/p_l} = 1$ ومنه فإن

$$y_1^{m/p_l} \cdot y_2^{m/p_l} \cdots y_s^{m/p_l} = 1$$

بما أن $o(y_i) = p_i^{r_i}$ حيث $i \in \{1, 2, \dots, s\} \setminus \{l\}$ تقسم m/p_l نجد أن $y_i^{m/p_l} = 1$ حيث $p_l^{r_l}$ تقسم m/p_l ومنه فإن $y_l^{m/p_l} = 1$ وبالتالي $i \in \{1, 2, \dots, s\} \setminus \{l\}$ تقسم m/p_l ومنه فإن $p_l^{r_l+1}$ يقسم m وهذا غير ممكن.

مما سبق نجد أن $o(y) = m$. وهكذا نجد أن $\langle y \rangle$ زمرة جزئية في F^* وأن $m = (1: \langle y \rangle)$ وهذا يبين لنا أن $F^* = \langle y \rangle$ أي أن الزمرة F^* دوارة. ◊

المبرهنة الآتية تبين لنا طبيعة كل من الزمرة الجمعية والزمرة الضربية لحقل غالوا مرتبته p^n :

مبرهنة ٥-١-٦

ليكن $F = GF(p^n)$ حقل غالوا مرتبته p^n . عندئذ:

١ - الزمرة الجمعية للحقل $F = GF(p^n)$ تماثل

$$\underbrace{Z_p \oplus Z_p \oplus \dots \oplus Z_p}_{n \text{ factors}}$$

٢ - الزمرة الضربية للحقل $F = GF(p^n)$ هي زمرة دوارة مرتبتها $p^n - 1$ وتماثل Z_{p^n-1} .

البرهان.

١ - بما أن الحقل F منته وأن العلاقة $\varphi: Z \rightarrow F$ المعرفة بالشكل $\varphi(n) = n.1$ وذلك أيضاً كان $n \in Z$ ، هي تشاكل وأن $\text{Ker } \varphi \neq 0$ لأن الحقل F منته فإن $\text{Ker } \varphi$ تشكل مثالياً رئيسياً في Z ، ومنه فإن $\langle p \rangle = \text{Ker } \varphi$ حيث p عدد أولي. ومنه فإن:

$$Z / \text{Ker } \varphi = Z / pZ \cong Z_p$$

وهذا يبين أن F يحوي حقلاً جزئياً يماثل Z_p ومنه فإن مميز الحقل F يساوي p . وبالتالي أياً كان $a \in F$ فإن $a^p = a$. وهكذا نجد أن كل عنصر مغاير للصفر في F له مرتبة جمعية تساوي p . مما سبق نجد أن F يشكل فضاء شعاعياً فوق Z_p وهو منتهي البعد لأن الحقل F منته. لنفرض أن بعد F فوق Z_p يساوي n عندئذ كل عنصر $a \in F$ يكتب بصورة وحيدة على النحو $\alpha_1 w_1 + \alpha_2 w_2 + \dots + \alpha_n w_n$ حيث $\alpha_1, \alpha_2, \dots, \alpha_n \in Z_p$ وهذا يبين أن $F \cong Z_p \oplus Z_p \oplus \dots \oplus Z_p$.

٢ - وجدنا حسب المبرهنة (٦-١-٤) أن الزمرة الضربية F^* للحقل F هي زمرة دوارة ومرتبته تساوي $p^n - 1$ ولذلك فهي تماثل الزمرة Z_{p^n-1} .

لما كان الحقل $GF(p)$ حقلاً جزئياً من الحقل المنتهي $GF(p^n)$ ، فإن الحقل $GF(p^n)$ هو تمديد منته للحقل $GF(p)$. التمهيدية الآتية تحدد لنا درجة تمديد الحقل $GF(p^n)$ فوق $GF(p)$:

تمهيدية ٦-١-٦.

لأجل أي عدد أولي p ولأجل أي عدد صحيح $n \geq 1$ فإن:

$$[GF(p^n) : GF(p)] = p^n$$

البرهان.

وجدنا حسب المبرهنة (٦-١-٥) أن $GF(p^n) \cong \underbrace{Z_p \oplus Z_p \oplus \dots \oplus Z_p}_{n \text{ factors}}$ ولما كان

$Z_p \oplus Z_p \oplus \dots \oplus Z_p$ فضاءً متجهياً فوق الحقل Z_p قاعدته هي:

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

المؤلفة من n عنصراً نجد أن $[GF(p^n) : GF(p)] = p^n$.

تعد الحدودية $x^{p^n} - x \in Z_p[x]$ واحدة من الحدوديات المهمة، المبرهنة الآتية تحدد لنا حقاً تفريق هذه الحدودية:

مبرهنة ٦-١-٧.

الحقل $GF(p^n)$ هو حقل تفريق الحدودية $x^{p^n} - x$ فوق الحقل Z_p .

البرهان.

واضح أن الحقل $GF(p) \cong Z_p$ حقل جزئي في الحقل $GF(p^n)$ وذلك حسب التمهيدية (٦-١-٦)، ومنه فإن مميز الحقل $GF(p^n)$ يساوي p . لنفرض أن F الزمرة الضربية للحقل $GF(p^n)$ ، إن مرتبة الزمرة F تساوي $p^n - 1$ ، ومنه أيّاً كان $a \in F$ فإن $a^{p^n-1} = 1$ أي أنه أيّاً كان $a \in F$ فإن $a^{p^n} - a = 0$ وهذا يبين لنا أن كل عنصر $a \in F$ هو صفر للحدودية $x^{p^n} - x \in Z_p[x]$ ، ومنه فإن كل عنصر من الحقل

$GF(p^n)$ هو صفر للحدودية $x^{p^n} - x$ فوق الحقل Z_p . ولما كانت الحدودية تملك على الأكثر p^n صفرًا نجد أن $GF(p^n)$ هو حقل تفريق الحدودية $x^{p^n} - x$ فوق الحقل Z_p .

وجدنا سابقاً أن الزمرة الضربية لحقل منته هي زمرة دوارة، التمهيدية الآتية تبين لنا طبيعة المولدات لهذه الزمرة:

تمهيدية ٦-١-٨.

إذا كان العنصر a مولداً للزمرة الضربية للحقل $GF(p^n)$ ، عندئذ فإن a هو عنصر جبري فوق الحقل $GF(p)$ درجته n .
البرهان.

وجدنا حسب التمهيدية (٦-١-٦) أن $[GF(p^n) : GF(p)] = p^n$ وهذا يبين أن الحقل $GF(p^n)$ هو تمديد منته للحقل $GF(p)$ وبالتالي يكون الحقل $GF(p^n)$ تمديداً جبرياً للحقل $GF(p)$. لنفرض أن F الزمرة الضربية للحقل $GF(p^n)$ ، عندئذ فإن $GF(p^n) = \{0\} \cup F$. لنفرض أن a مولد للزمرة F عندئذ فإن $a \in GF(p^n)$ يكون a عنصراً جبرياً فوق الحقل $GF(p)$ ، وأن $F = \langle a \rangle$ ومنه فإن:

$$GF(p^n) = \{0\} \cup F = GF(p)(a)$$

وهكذا نجد أن $[GF(p)(a) : GF(p)] = [GF(p^n) : GF(p)] = p^n$.

المبرهنة الآتية تحدد لنا طبيعة الحقول الجزئية في الحقل $GF(p^n)$ وشكل هذه الحقول ومتى تكون موجودة:

مبرهنة ٦-١-٩.

ليكن $n \geq 1$ عدداً صحيحاً. عندئذ:

١ - لأجل أي عدد صحيح موجب m يقسم n فإن الحقل $GF(p^n)$ يحوي حقلاً جزئياً واحداً فقط من الشكل $GF(p^m)$.

٢ - كل حقل جزئي في $GF(p^n)$ هو من الشكل $GF(p^m)$ ، حيث m عدد صحيح موجب يقسم n .

البرهان.

١ - لنفرض أن m عدد صحيح موجب يقسم n . عندئذ فإن:

$$p^n - 1 = (p^m - 1)(p^{n-m} + p^{n-2m} + \dots + p^m + 1)$$

وهذا يبين أن $p^m - 1$ يقسم $p^n - 1$ ، وحسب التمرين المحلول (٦-١) فإن الحدودية $x^{p^m-1} - 1$ تقسم الحدودية $x^{p^n-1} - 1$ في $Z_p[x]$. وبالتالي فإن كل صفر للحدودية $x(x^{p^m-1} - 1)$ هو صفر للحدودية $x(x^{p^n-1} - 1)$ ، وحسب التمرين المحلول (٦-٢) فإن مجموعة أصفار الحدودية $x(x^{p^m-1} - 1)$ هي $GF(p^m)$ وأن مجموعة أصفار الحدودية $x(x^{p^n-1} - 1)$ هي $GF(p^n)$ وأن $GF(p^m) \subseteq GF(p^n)$ وهذا يبين أن $GF(p^m)$ هو حقل جزئي في الحقل $GF(p^n)$.

الوحدانية. لنفرض أن الحقل $GF(p^n)$ يحوي حقلين جزئيين مختلفين مرتبة كل منهما p^m عندئذ فإن الحدودية $x(x^{p^m-1} - 1)$ تملك أكثر من p^m صفراً وهذا غير ممكن.

٢ - لنفرض أن F حقل جزئي في الحقل $GF(p^n)$ مرتبته p^m حيث m عدد صحيح موجب. عندئذ حسب المبرهنة (٦-١-٢) فإن F يماثل الحقل $GF(p^m)$ ، وحسب التمهيدية (٦-١-٦) نجد أن:

$$\begin{aligned} n = [GF(p^n) : GF(p)] &= [GF(p^n) : GF(p^m)] \cdot [GF(p^m) : GF(p)] = \\ &= [GF(p^n) : GF(p^m)] \cdot m \end{aligned}$$

وهذا يبين أن m يقسم n .

مثال.

أوجد حقل تفريق الحدودية $x^4 - x \in Z_2[x]$ فوق الحقل Z_2 .

لما كان في الحقل Z_2 نظير الواحد هو الواحد نجد أن:

$$x^4 - x = x^4 + x = x(x^3 + 1)$$

ولما كان $1 \in Z_2$ صفراً للحدودية $x^3 + 1$ نجد أن:

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

لنفرض أن $h(x) = x^2 + x + 1 \in Z_2[x]$. نلاحظ أن الحدودية $h(x)$ لا تملك أصفاراً

في الحقل Z_2 ومنه فإن الحدودية $h(x)$ أولية فوق الحقل Z_2 .

لما كانت درجة الحدودية $h(x)$ تساوي 2 فإن الحدودية $h(x)$ تملك صفرين في تمديد ما للحقل Z_2 ، لنفرض أنهما w_1, w_2 فيكون $w_1 + w_2 = 1$ لأن مجموع صفري الحدودية $h(x)$ يساوي أمثال x وهذا يبين أن صفري الحدودية $h(x)$ هما $w_1, w_1 + 1$ في تمديد ما للحقل Z_2 . لنأخذ الحقل $Z_2(w_1)$ فنجد أن $w_1, w_1 + 1 \in Z_2(w_1)$ وهذا يبين أن الحقل $Z_2(w_1)$ هو حقل تفريق الحدودية $h(x)$ فوق الحقل Z_2 وذلك لأن:

$$Z_2(w_1, w_1 + 1) = Z_2(w_1)$$

وحسب المبرهنة (٦-١-٩) فإن أي تمديد للحقل Z_2 هو من الشكل Z_{2^n} وهذا يبين أن:

$$Z_2(w_1) = Z_4$$

ولما كانت الحدودية $h(x)$ هي الحدودية الأصغرية للعنصر w_1 فوق الحقل Z_2 نجد أن:

$$[Z_2(w_1) : Z_2] = \partial h(x) = 2$$

وهذا يبين أن المجموعة $\{1, w_1\}$ تشكل قاعدة للحقل $Z_2(w_1)$ فوق Z_2 أي أن كل عنصر من الحقل $Z_2(w_1)$ يكتب بصورة وحيدة على الشكل $a + bw_1$ حيث $a, b \in Z_2$. مما سبق نجد أن حقل تفريق الحدودية $x^4 - x$ فوق الحقل Z_2 هو $Z_2(w_1) = Z_4$.

تمارين محلولة (٦)

١ - ليكن n, m عددين صحيحين موجبين. إذا كان m يقسم n ، عندئذ فإنه لأجل أي حقل F فإن الحدودية $x^m - 1$ تقسم الحدودية $x^n - 1$ في $F[x]$.
الحل.

بما أن m يقسم n فإنه يوجد $q \in \mathbb{Z}$ بحيث $n = qm$ ومنه فإن:

$$\begin{aligned} x^n - 1 &= (x^m - 1)(x^{n-m} + x^{n-2m} + \dots + x^{n-qm}) = \\ &= (x^m - 1)(x^{n-m} + x^{n-2m} + \dots + x^{n-qm-1} + 1) \end{aligned}$$

وهذا يبين أن الحدودية $x^m - 1$ تقسم الحدودية $x^n - 1$ في $F[x]$. ◊

٢ - ليكن p عدداً أولياً و $n \geq 1$ عدداً صحيحاً. إن مجموعة أصفار الحدودية $x^{p^n} - x$ تشكل حقلاً مرتبته p^n هو $GF(p^n)$.
الحل.

لنأخذ الحقل Z_p ، إن $x^n - 1 \in Z_p$ وحسب المبرهنة (١-١-٧) فإن الحدودية $x^{p^n} - x$ تملك p^n صفراً بما فيها الأصفار المضاعفة. لنفرض أن K هي مجموعة أصفار الحدودية $x^{p^n} - x$ في حقل التقريب E فوق Z_p ، فنجد أن $0, 1 \in K$. ليكن $a, b \in K$ عندئذ يكون $a^{p^n} - a = b^{p^n} - b = 0$ وبالتالي فإن:

$$(a - b)^{p^n} - (a - b) = (a^{p^n} - a) - (b^{p^n} - b) = 0$$

وهذا يبين أن $a - b$ هو صفر للحدودية $x^{p^n} - x$ وبالتالي فإن $a - b \in K$. بفرض أن $b \neq 0$ فنجد أن:

$$(a \cdot b^{-1})^{p^n} - a \cdot b^{-1} = a^{p^n} \cdot b^{-p^n} - ab^{-1} = ab^{-1} - ab^{-1} = 0$$

وهذا يبين أن $a \cdot b^{-1}$ هو صفر للحدودية $x^{p^n} - x$ وبالتالي فإن $a \cdot b^{-1} \in K$ ، ومنه نجد أن K حقلاً مرتبته p^n وبالتالي $K = GF(p^n)$. ◊

٣ - ليكن n, m عددين صحيحين موجبين. إذا كان m يقسم n ، عندئذ فإنه لأجل أي عدد أولي p فإن $[GF(p^n) : GF(p^m)] = n/m$.

الحل.

بما أن m يقسم n فإنه حسب المبرهنة (٦-١-٨) يكون $GF(p^m)$ حقلاً جزئياً في الحقل $GF(p^n)$ وبما أن:

$$GF(p) \subseteq GF(p^m) \subseteq GF(p^n)$$

وأن الحقل $GF(p^n)$ هو حقل منتهي فإن الحقل $GF(p^n)$ هو تمديد منتهي للحقل $GF(p)$ ، ومنه فإن:

$$[GF(p^n) : GF(p)] = [GF(p^n) : GF(p^m)] \cdot [GF(p^m) : GF(p)]$$

وحسب التمهيدية (٦-١-٦) نجد أن $n = [GF(p^n) : GF(p^m)] \cdot m$ وهذا يبين أن $[GF(p^n) : GF(p^m)] = n/m$.

$$٤ - \text{أوجد كلاً من } [GF(64) : GF(8)], [GF(729) : GF(9)].$$

الحل.

$$[GF(729) : GF(9)] = [GF(3^6) : GF(3^2)] = 6/2 = 3$$

$$[GF(64) : GF(8)] = [GF(2^6) : GF(2^3)] = 6/3 = 2$$

٥ - ليكن p عدداً أولياً وأن $GF(p^n)$ حقل غالوا مرتبته p^n . أثبت أن:

أ - العلاقة $\varphi : GF(p^n) \rightarrow GF(p^n)$ المعرفة بالشكل الآتي: أيّاً كان $a \in GF(p^n)$ فإن $\varphi(a) = a^p$ هي تماثل للحقل $GF(p^n)$.

ب - أثبت أن $\varphi^n = I_{GF(p^n)}$. نسمي التابع φ تابع فريبنوس.

الحل.

أ - لنبرهن أولاً أن مميز الحقل $GF(p^n)$ يساوي p . بما أن مرتبة الزمرة الجمعية $(GF(p^n), +)$ تساوي p^n نجد أنه أيّاً كان $a \in GF(p^n)$ فإن $p^n \cdot a = 0$ وأن $p^{n-1} \cdot a \neq 0$ ، ومنه فإن:

$$p^n \cdot a = (p \cdot 1) \cdot (p^{n-1} \cdot a) = 0$$

ولما كان $GF(p^n)$ حقلاً فإن $p \cdot 1 = 0$. واضح أن العلاقة φ هي تطبيق، وهي أيضاً تشاكل، لأنه إذا كان $a, b \in GF(p^n)$ فإن:

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

$$\varphi(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = \varphi(a) \cdot \varphi(b)$$

وهو أيضاً متباين، لأنه إذا كان $\varphi(a) = \varphi(b)$ فإن $a^p = b^p$ وبالتالي يكون:

$$(a-b)^p = a^p - b^p = 0$$

ومنه فإن $a-b=0$ أي أن $a=b$.

وهكذا نجد أن $GF(p^n) \cong Im \varphi$ وبالتالي يكون φ تماثلاً.

٢ - لنبرهن بالاستقراء حسب n أن $\varphi^n(a) = a^{p^n}$ وذلك أياً كان $a \in GF(p^n)$.

- من أجل $n=1$ نجد أن $\varphi(a) = a^p$.

- من أجل $n=2$ نجد أن $\varphi^2(a) = \varphi(\varphi(a)) = \varphi(a^p) = (a^p)^p = a^{p^2}$.

- لنفرض أن المساواة صحيحة لأجل $n-1$ أي لنفرض أن $\varphi^{n-1}(a) = a^{p^{n-1}}$ فنجد أن:

$$\varphi^n(a) = \varphi(\varphi^{n-1}(a)) = \varphi(a^{p^{n-1}}) = (a^{p^{n-1}})^p = a^{p^n}$$

ولما كانت الزمرة الضربية للحقل $GF(p^n)$ مرتبتها تساوي $p^n - 1$ نجد أن:

$$a^{p^n} = a^{p^n-1} \cdot a = a$$

وهكذا نجد أن $\varphi^n(a) = a^{p^n} = a$ وهذا يبين أن $\varphi^n = I_{GF(p^n)}$.

٦ - أثبت أن كل عنصر من الحقل $GF(p^n)$ يكتب بصورة وحيدة على الشكل a^p

حيث $a \in GF(p^n)$.

الحل.

لما كانت الزمرة الضربية للحقل $GF(p^n)$ مرتبتها تساوي $p^n - 1$ عندئذ أياً كان

$b \in GF(p^n)$ فإن $b^{p^n-1} = 1$ ومنه فإن $b^{p^n} = b$ ومنه نجد أن:

$$b = b^{p^n} = (b^{p^{n-1}})^p$$

لنفرض أن $a = b^{p^{n-1}}$ نجد أن $a \in GF(p^n)$ وأن $b = a^p$.

الوحدانية. لنفرض أن $b = a^p = a_1^p$ حيث $a, a_1 \in GF(p^n)$ عندئذ يكون:

$$0 = a^p - a_1^p = (a - a_1)^p$$

وهذا يبين أن $a - a_1 = 0$ أي أن $a = a_1$.

تمارين (٦)

- ١ - أوجد جميع الحقول الجزئية في كل من الحقول الآتية: $GF(2^{30})$, $GF(3^{18})$.
- ٢ - ليكن L حقلاً جزئياً في الحقل $GF(p^n)$ مرتبته p^s و K حقلاً جزئياً في الحقل $GF(p^n)$ مرتبته p^t . أوجد مرتبة الحقل $K \cap L$.
- ٣ - ليكن F حقلاً منتهياً مرتبته 1024 ولنفرض أن $F^* = \langle a \rangle$. أوجد جميع الحقول الجزئية في F وعناصرها.
- ٤ - ليكن F حقلاً منتهياً مرتبته 185 ولنفرض أن $F^* = \langle a \rangle$. أثبت أن $a^{62} = -1$.
- ٥ - لتكن $g(x)$ حدودية أولية فوق الحقل $GF(p)$ ، ولنفرض أن $g(x)$ تقسم الحدودية $x^{p^n} - x$. أثبت أن $\partial g(x)$ تقسم n .
- ٦ - ليكن α, β عنصرين من الزمرة الضربية للحقل $GF(81)$ وأن مرتبة α تساوي 5 ومرتبة β تساوي 16. أثبت أن العنصر $\alpha \cdot \beta$ يولد الزمرة الضربية للحقل $GF(81)$.
- ٧ - لنفرض أن الحقل E تمديد جبري للحقل F وأن R حلقة تحقق $F \subseteq R \subseteq E$. أثبت أن R حقل.
- ٨ - ليكن الحقل K تمديداً للحقل F وأن $a, b \in K$. إذا كان العنصر $a \cdot b$ جبرياً فوق F أثبت أن العنصر a يكون جبرياً فوق الحقل $F(b)$.
- ٩ - ليكن الحقل K تمديداً للحقل F وأن $a \in K$. إذا كان العنصر a جبرياً فوق F وكانت درجته تساوي n أثبت أن العنصر a^{-1} يكون جبرياً فوق الحقل F ودرجته n .
- ١٠ - أوجد درجة تمديد كل من الحقول الآتية:
 - الحقل $Q(\sqrt{2}, \sqrt[4]{2})$ فوق الحقل Q .
 - الحقل $Q(\sqrt{2}, \sqrt[4]{26})$ فوق الحقل $Q(\sqrt{3})$.
 - الحقل $Q(\sqrt[3]{2}, \sqrt[4]{6}, \sqrt[4]{24})$ فوق الحقل Q .
 - الحقل $Q(\sqrt{2}, \sqrt{3})$ فوق الحقل $Q(\sqrt{2} + \sqrt{3})$.
 - الحقل $Q(\sqrt{2}, \sqrt{6} + \sqrt{10})$ فوق الحقل $Q(\sqrt{3} + \sqrt{5})$.

الفصل السابع

التماثلات الذاتية للحقول

٧ - ١. العناصر المترافقة .

تعد أصفار الحدوديات الأولية فوق أي حقل من العناصر المهمة، ولأجل ذلك سوف ندرس هذه العناصر بشيء من التفصيل، والبداية ستكون مع التعريف الآتي:

تعريف.

ليكن الحقل K تمديداً جبرياً للحقل F وليكن $a, b \in K$ عنصرين جبريين فوق الحقل F . نقول عن العنصرين a, b إنهما مترافقان فوق الحقل F إذا كانت الحدودية الأصغرية للعنصر a فوق F هي ذاتها الحدودية الأصغرية للعنصر b فوق F .

بالاعتماد على التعريف السابق يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن الحقل K تمديداً للحقل F و $p(x) \in F[x]$ و $p(x) \neq 0$. إذا كانت الحدودية $p(x)$ أولية في $F[x]$ وكانت $p(x)$ تملك أصفاراً في الحقل K ، فإن جميع تلك الأصفار هي عناصر مترافقة مثلي مثلي فوق الحقل F .

مثال.

العنصران $\sqrt{2}, -\sqrt{2}$ مترافقان فوق الحقل Q .

وذلك لأنه توجد حدودية $p(x) = x^2 - 2 \in Q[x]$ وتحقق $p(\sqrt{2}) = p(-\sqrt{2}) = 0$ ولما كانت الحدودية $p(x)$ أولية في Q فإن الحدودية $p(x) = x^2 - 2 \in Q[x]$ هي الحدودية الأصغرية للعنصرين $\sqrt{2}, -\sqrt{2}$. بينما مرافق العنصر الجبري $\sqrt{2}$ فوق الحقل R هو نفسه $\sqrt{2}$ ، لأن $x - \sqrt{2} \in R[x]$ هي الحدودية الأصغرية للعنصر $\sqrt{2}$ وهي تملك صفراً واحداً فقط.

لمتابعة دراستنا للعناصر المترافقة نحن بحاجة إلى التمهيدية الآتية والتي تحدد لنا

العلاقة بين العناصر الجبرية فوق حقل ما والتشاكلات بين الحقول:

تمهيدية ٧-١-١.

ليكن الحقل K تمديداً للحقل F وليكن $a, b \in K$ عنصرين جبريين فوق الحقل F .

عندئذ يوجد تشاكل $\psi_{a,b}: F(a) \rightarrow F(b)$ معرفاً بالشكل الآتي:

$$\psi_{a,b}\left(\sum_{i=0}^{n-1} c_i a^i\right) = \sum_{i=0}^{n-1} c_i b^i$$

وذلك أيّاً كان $\sum_{i=0}^{n-1} c_i a^i \in F(a)$.

البرهان.

لنفرض أن العنصرين $a, b \in K$ جبريان فوق F ولنفرض أن $p(x) \in F[x]$ الحدودية

الأصغرية للعنصر a فوق F وأن $\partial p(x) = n$ ، عندئذ حسب المبرهنة (٣-٣-٥) فإن

$[F(a): F] = n$ وأن المجموعة $\{1, a, a^2, \dots, a^{n-1}\} \subseteq F(a)$ تشكل قاعدة للحقل

$F(a)$ فوق F . لنعرف $\psi_{a,b}: F(a) \rightarrow F(b)$ بالشكل: أيّاً كان $\sum_{i=0}^{n-1} c_i a^i \in F(a)$ فإن

$\sum_{i=0}^{n-1} c_i a^i \in F(a)$ فنجد أن $\psi_{a,b}\left(\sum_{i=0}^{n-1} c_i a^i\right) = \sum_{i=0}^{n-1} c_i b^i$ و

$\sum_{i=0}^{n-1} c_i a^i = \sum_{i=0}^{n-1} d_i a^i$ حيث $c_i, d_i \in F$ أيّاً كان $0 \leq i \leq n-1$ ، بحيث $\sum_{i=0}^{n-1} d_i a^i \in F(a)$

نجد أن $\sum_{i=0}^{n-1} (c_i - d_i) a^i = 0$ ولما كانت المجموعة $\{1, a, a^2, \dots, a^{n-1}\}$ تشكل قاعدة

للحقل $F(a)$ فوق F ينتج أن $c_i - d_i = 0$ وبالتالي $c_i = d_i$ أيّاً كان $0 \leq i \leq n-1$

ومنه يكون $\sum_{i=0}^{n-1} c_i b^i = \sum_{i=0}^{n-1} d_i b^i$ أي أن $\psi_{a,b}\left(\sum_{i=0}^{n-1} c_i a^i\right) = \psi_{a,b}\left(\sum_{i=0}^{n-1} d_i a^i\right)$.

كما أن $\psi_{a,b}$ تشاكل لأن:

$$\begin{aligned} \psi_{a,b}\left(\sum_{i=0}^{n-1} c_i a^i + \sum_{i=0}^{n-1} d_i a^i\right) &= \psi_{a,b}\left(\sum_{i=0}^{n-1} (c_i + d_i) a^i\right) = \sum_{i=0}^{n-1} (c_i + d_i) b^i = \\ &= \sum_{i=0}^{n-1} (c_i + d_i) b^i = \sum_{i=0}^{n-1} c_i b^i + \sum_{i=0}^{n-1} d_i b^i = \psi_{a,b}\left(\sum_{i=0}^{n-1} c_i a^i\right) + \psi_{a,b}\left(\sum_{i=0}^{n-1} d_i a^i\right) \\ \psi_{a,b}\left[\left(\sum_{i=0}^{n-1} c_i a^i\right) \cdot \left(\sum_{i=0}^{n-1} d_i a^i\right)\right] &= \psi_{a,b}\left(\sum_{k=0}^{2(n-1)} \alpha_k a^k\right) = \sum_{k=0}^{2(n-1)} \alpha_k b^k = \end{aligned}$$

$$= (\sum_{i=0}^{n-1} c_i b^i) \cdot (\sum_{i=0}^{n-1} d_i b^i) = \psi_{a,b}(\sum_{i=0}^{n-1} c_i a^i) \cdot \psi_{a,b}(\sum_{i=0}^{n-1} d_i a^i)$$

مما سبق نجد أن التطبيق $\psi_{a,b}$ هو تشاكل. ◊

المبرهنة الآتية تعطينا الشرط اللازم والكافي لترافق عنصرين جبريين فوق حقل ما:

مبرهنة ٧-١-٢.

ليكن الحقل K تمديداً للحقل F وليكن $a, b \in K$ عنصرين جبريين فوق الحقل F .
الشروط الآتية متكافئة:

١ - العنصران a, b مترافقان فوق الحقل F .

٢ - التشاكل $\psi_{a,b} : F(a) \rightarrow F(b)$ هو تماثل.

البرهان.

(1) $\Leftrightarrow$ (2). لنفرض أن العنصرين a, b مترافقان فوق الحقل F وأن $p(x) \in F[x]$ الحدودية الأصغرية للعنصرين a, b فوق F وأن $\partial p(x) = n$. لما كان العنصر a جبرياً فوق F فإنه حسب التمهيدية (٤-٢-٤) يكون التشاكل $\varphi_a : F[x] \rightarrow F(a)$ المعروف بالشكل الآتي: أيّاً كان $f(x) \in F[x]$ فإن $\varphi_a(f(x)) = f(a)$ ، غامر. وبما أن الحدودية $p(x)$ أولية فوق F فإن المثالي $\langle p(x) \rangle$ أعظمي في $F[x]$.

من جهة أخرى، بما أن $p(x)$ هي الحدودية الأصغرية للعنصر a فوق F فإن:
 $\varphi_a(p(x)) = p(a) = 0$ وهذا يبين أن $p(x) \in \text{Ker } \varphi_a$ ومنه فإن $\langle p(x) \rangle \in \text{Ker } \varphi_a$.
لتكن $\lambda(x) \in \text{Ker } \varphi_a$ عندئذ $\varphi_a(\lambda(x)) = 0 = \lambda(a)$ وحسب خوارزمية القسمة لأجل $p(x), \lambda(x)$ ، يوجد $q(x), r(x) \in F[x]$ بحيث $\lambda(x) = q(x) \cdot p(x) + r(x)$ وأنه إما $r(x) = 0$ أو $\partial r(x) < \partial p(x)$. لنفرض جلاً أن $r(x) \neq 0$ عندئذ يكون:

$$\varphi_a(\lambda(x)) = \varphi_a(q(x)) \cdot \varphi_a(p(x)) + \varphi_a(r(x))$$

$$\lambda(a) = q(a) \cdot p(a) + r(a)$$

ومنه نجد أن $r(a) = 0$ ، كما أن $\partial r(x) < \partial p(x)$ وهذا يناقض كون الحدودية $p(x)$ هي الحدودية الأصغرية للعنصر a فوق F ، ومنه فإن $r(x) = 0$ وبالتالي يكون:

$$\lambda(x) = q(x) \cdot p(x) \in p(x) \cdot F[x] = \langle p(x) \rangle$$

ومنه نجد أن $\langle p(x) \rangle \subseteq \text{Ker } \varphi_a$ ، وهكذا فإن $\text{Ker } \varphi_a = \langle p(x) \rangle$. بشكل مشابهة نجد أن $\text{Ker } \varphi_b = \langle p(x) \rangle$. وحسب مبرهنة التماثل الأولى نجد أن:

$$F[x]/\langle p(x) \rangle = F[x]/\text{Ker } \varphi_a \cong F(a)$$

$$F[x]/\langle p(x) \rangle = F[x]/\text{Ker } \varphi_b \cong F(b)$$

لنرمز للتماثل الأول $\overline{\varphi_a}$ وللتماثل الثاني $\overline{\varphi_b}$ ، عندئذ:

$$\overline{\varphi_a}(\mu(x) + \langle p(x) \rangle) = \varphi_a(\mu(x)) = \mu(a)$$

$$\overline{\varphi_b}(\mu(x) + \langle p(x) \rangle) = \varphi_b(\mu(x)) = \mu(b)$$

وذلك أي أن $\mu(x) + \langle p(x) \rangle \in F[x]/\langle p(x) \rangle$ كان

لنبرهن الآن على أن $\overline{\varphi_a} \cdot \overline{\varphi_b}^{-1} = \psi_{a,b}$. أي أن كان $\sum_{i=0}^{n-1} c_i a^i \in F(a)$ فإن:

$$\begin{aligned} \overline{\varphi_b} \cdot \overline{\varphi_a}^{-1} \left(\sum_{i=0}^{n-1} c_i a^i \right) &= \overline{\varphi_b} \left(\overline{\varphi_a}^{-1} \left(\sum_{i=0}^{n-1} c_i a^i \right) \right) = \overline{\varphi_b} \left(\sum_{i=0}^{n-1} c_i a^i + \langle p(x) \rangle \right) = \\ &= \left(\sum_{i=0}^{n-1} c_i b^i \right) = \psi_{a,b} \left(\sum_{i=0}^{n-1} c_i a^i \right) \end{aligned}$$

وهذا يبين لنا أن $\psi_{a,b} = \overline{\varphi_b} \cdot \overline{\varphi_a}^{-1}$ وبالتالي فإن $\psi_{a,b}$ تماثل.

(2) $\Leftarrow$ (1) . لنفرض أن $\psi_{a,b}$ تماثل وأن $p(x)$ هي الحدودية الأصغرية للعنصر a فوق

F وأن $\partial p(x) = n$ ، ولنفرض أيضاً أن $h(x)$ هي الحدودية الأصغرية للعنصر b فوق

F وأن $\partial h(x) = m$. لنبرهن أولاً أن $\psi_{b,a}^{-1} = \psi_{a,b}$. لما كان $\psi_{a,b}$ تماثلاً فإن $\psi_{a,b}^{-1}$

موجود وأن $\psi_{a,b}^{-1} : F(b) \rightarrow F(a)$ ، كما أن $\psi_{b,a} : F(b) \rightarrow F(a)$.

من جهة أخرى، أي أن كان $\sum_{i=0}^{m-1} c_i b^i \in F(b)$ فإن:

$$\psi_{a,b}^{-1} \left(\sum_{i=0}^{m-1} c_i b^i \right) = \sum_{i=0}^{m-1} c_i a^i = \psi_{b,a} \left(\sum_{i=0}^{m-1} c_i b^i \right)$$

وهذا يبين لنا أن $\psi_{a,b}^{-1} = \psi_{b,a}$ ، ومنه $\psi_{a,b}^{-1} = \psi_{b,a}$.

لنفرض أن $p(x) = \sum_{i=0}^{n-1} c_i x^i$ ، $h(x) = \sum_{i=0}^{m-1} d_i x^i$ حيث $c_i, d_j \in F$ وذلك لأجل جميع

القيم $0 \leq i \leq n, 0 \leq j \leq m$. بما أن $0 = p(a) = \sum_{i=0}^n c_i a^i \in F(a)$ نجد أن:

$$\psi_{a,b}(\sum_{i=0}^n c_i a^i) = \psi_{a,b}(0) = 0$$

ومنه يكون $\sum_{i=0}^n c_i b^i = 0$ ، وهذا يبين لنا أن $p(b) = 0$ وحسب المبرهنة (٣-٣-٤) نجد

أن $h(x)$ تقسم $p(x)$ في $F[x]$ ، ومنه يوجد $\alpha(x) \in F[x]$ بحيث:

$$p(x) = \alpha(x) \cdot h(x)$$

أيضاً لما كان $0 = h(b) = \sum_{i=0}^m d_i b^i \in F(b)$ نجد أن:

$$\psi_{b,a}(\sum_{i=0}^m d_i b^i) = \psi_{b,a}(0) = 0$$

ومنه يكون $\sum_{i=0}^m d_i a^i = 0$ ، وهذا يبين لنا أن $h(a) = 0$ وحسب المبرهنة (٣-٣-٤) نجد

أن $p(x)$ تقسم $h(x)$ في $F[x]$ ، ومنه يوجد $\beta(x) \in F[x]$ بحيث:

$$h(x) = \beta(x) \cdot p(x)$$

مما سبق نجد أن $\partial h(x) \leq \partial p(x)$ ، ومنه فإن $\partial h(x) = \partial p(x)$.

أي أن $n = m$. لنفرض أن $a_n = b_m = 1$ فنجد أن $\alpha(x)$ ومنه يكون $h(x) = p(x)$ وهذا يبين أن العنصرين a, b مترافقان. ◊

مثال.

وجدنا أن العنصرين $\sqrt{2}, -\sqrt{2}$ مترافقان فوق الحقل Q وحسب المبرهنة (٧-١-١) فإنه يوجد تماثل $\psi: Q(\sqrt{2}) \rightarrow Q(-\sqrt{2})$ يحقق $\psi(\sqrt{2}) = -\sqrt{2}$. بما أن $Q(\sqrt{2}) = Q(-\sqrt{2})$ وحقل وأن $\sqrt{2} \in Q(\sqrt{2})$ نجد أن $-\sqrt{2} \in Q(\sqrt{2})$ ومنه فإن $Q(\sqrt{2}) = Q(-\sqrt{2})$ وبالتالي يكون $\psi: Q(\sqrt{2}) \rightarrow Q(\sqrt{2})$ ويحقق $\psi(\sqrt{2}) = -\sqrt{2}$. إن التماثل ψ معرف بالشكل الآتي: أيأ كان $a + b\sqrt{2} \in Q(\sqrt{2})$ فإن $\psi(a + b\sqrt{2}) = a - b\sqrt{2}$ (تأكد من ذلك).

اعتماداً على المبرهنة الأخيرة يمكننا صياغة التمهيدية الآتية:

تمهيدية ٧-١-٣.

ليكن الحقل K تمديداً للحقل F وليكن $a \in K$ عنصراً جبرياً فوق الحقل F . عندئذ

لأجل أي تشاكل متباين $\bar{F} \rightarrow F(a) : \psi$ لأجله $\psi(c) = c$ وذلك أيّاً كان $c \in F$ ، يكون العنصر $\psi(a)$ مرافقاً للعنصر a فوق F ، حيث $\bar{F}$ الغلاقة الجبرية للحقل F .
البرهان.

لنفرض أن $\bar{F} \rightarrow F(a) : \psi$ تشاكل متباين لأجله $\psi(c) = c$ وذلك أيّاً كان $c \in F$. نلاحظ أولاً أن $\psi(a) \in \bar{F}$ وهذا يبين أن العنصر $\psi(a)$ جبري فوق F . من جهة أخرى، لنفرض أن $p(x) = \sum_{i=0}^n d_i x^i \in F[x]$ الحدودية الأصغرية للعنصر a فوق F ، عندئذ يكون $\sum_{i=0}^n d_i a^i = 0$ ومنه فإن:

$$\begin{aligned} 0 &= \psi\left(\sum_{i=0}^n d_i a^i\right) = \sum_{i=0}^n \psi(d_i a^i) = \sum_{i=0}^n \psi(d_i) \psi(a^i) = \\ &= \sum_{i=0}^n d_i (\psi(a))^i = p(\psi(a)) \end{aligned}$$

وهذا يبين أن $\psi(a)$ صفر للحدودية $p(x)$ وبالتالي فإن العنصرين $a, \psi(a)$ مترافقان. ◊

تمهيدية ٧-١-٤.

ليكن F حقلاً و a, b عنصرين مترافقين فوق F . عندئذ يوجد تشاكل متباين $\bar{F} \rightarrow F(a) : \psi_{a,b}$ من أجله $\psi_{a,b}(c) = c$ وذلك أيّاً كان $c \in F$ ، حيث $\bar{F}$ الغلاقة الجبرية للحقل F .
البرهان.

لنفرض أن العنصرين a, b مترافقان فوق F وأن $p(x) \in F[x]$ الحدودية الأصغرية للعنصرين a, b ، ولنفرض أيضاً أن $\partial p(x) = n$. عندئذ حسب المبرهنة (٧-١-٣) يوجد تماثل $\bar{F}(b) \rightarrow F(a) : \psi_{a,b}$ معرف بالشكل الآتي: أيّاً كان $\sum_{i=0}^{n-1} c_i a^i \in F(a)$ فإن:

$$\psi_{a,b}\left(\sum_{i=0}^{n-1} c_i a^i\right) = \sum_{i=0}^{n-1} c_i b^i$$

ومنه فإن $\psi_{a,b}(a) = b$ ، كما أن $\psi_{a,b}(c) = c$ وذلك أيّاً كان $c \in F$. بما أن العنصر b جبري فوق F فإن $F(b)$ هو تمديد جبري للحقل F ومنه فإن $F(b) \subseteq \bar{F}$ ، وهكذا نجد أن $\bar{F} \rightarrow F(a) : \psi_{a,b}$ هو تشاكل متباين يحقق الشروط الواردة في النص. ◊

التمهيدية الآتية تحدد لنا الحد الأعلى لعدد العناصر المترافقة مع عنصر ما فوق
حقل مميزه لا يساوي الصفر:

تمهيدية ٧-١-٥.

ليكن الحقل K تمديداً للحقل F الذي مميزه $p \neq 0$ ، ولتكن $f(x) \in F[x]$ حدودية
أولية فوق F ، ولنفرض أن n_0 درجة انفصالية $f(x)$. إذا كان $a \in K$ صفراً للحدودية
 $f(x)$ ، عندئذ عدد جميع عناصر K المختلفة مثلي مثلي والمترافقة مع a فوق F بما
فيها a أصغر أو يساوي n_0 .

البرهان.

لنفرض أن $\partial f(x) = n$ وأن p^n هي درجة عدم انفصالية $f(x)$ فوق F ، عندئذ
 $n = n_0 p^n$. سوف نميز حالتين:

- إذا كانت الحدودية $f(x)$ منفصلة فوق F عندئذ حسب المبرهنة (٥-٢-٧) فإن
 $n = n_0$. ومنه فإن عدد جميع الأصفار المختلفة مثلي مثلي للحدودية $f(x)$ بما فيها
 a أصغر أو يساوي n_0 وبالتالي فإن عدد جميع عناصر الحقل K المختلفة مثلي مثلي
والمترافقة مع a بما فيها a أصغر أو يساوي n_0 .

- إذا كانت الحدودية $f(x)$ غير منفصلة فوق F عندئذ فإن كل صفر للحدودية $f(x)$
هو صفر مضاعف من المرتبة p^m ومنه فإن عدد جميع الأصفار المختلفة مثلي مثلي
للحدودية $f(x)$ بما فيها a أصغر أو يساوي $n_0 = n/m$. وبالتالي فإن عدد جميع
عناصر الحقل K المختلفة مثلي مثلي والمترافقة مع a فوق F بما فيها a أصغر أو
يساوي n_0 .

المبرهنة الآتية تحدد لنا بالتحديد عدد العناصر المترافقة مع عنصر ما فوق حقل
مميزه لا يساوي الصفر:

مبرهنة ٧-١-٦.

ليكن الحقل K تمديداً للحقل F الذي مميزه $p \neq 0$ ، ولتكن $f(x) \in F[x]$ حدودية
أولية فوق F . لنفرض أن n_0 درجة انفصالية $f(x)$ وأن $a_1 \in K$ صفر للحدودية

$f(x)$. الشرط اللازم والكافي كي تتفرق الحدودية $f(x)$ في $K[x]$ إلى مضارب خطية هو أن يكون عدد جميع عناصر K المختلفة مثني ومتني والمترافقة مع a_1 فوق F بما فيها a_1 يساوي n_0 .

البرهان.

لنفرض أن $\partial f(x) = n$ وأن p^n هي درجة عدم انفصالية $f(x)$ فوق F ، عندئذ $n = n_0 p^n$. سوف نميز حالتين:

لزوم الشرط. لنفرض أن الحدودية $f(x)$ تتفرق في $K[x]$ إلى مضارب خطية. سوف نميز حالتين:

- إذا كانت الحدودية $f(x)$ منفصلة فوق F عندئذ حسب المبرهنة (٥-٢-٧) فإن $n = n_0$. ومنه بالإمكان كتابة $f(x)$ على الشكل الآتي:

$$f(x) = b \cdot (x - a_1) \cdot (x - a_2) \cdot \dots \cdot (x - a_{n_0}) = b \cdot \prod_{i=1}^{n_0} (x - a_i)$$

حيث $b \in F$ وأن $a_1, a_2, \dots, a_{n_0} \in K$ ، ومنه فإن العناصر $a_1, a_2, \dots, a_{n_0}$ مترافقة مع a_1 فوق F ، ولما كانت الحدودية $f(x)$ منفصلة وأن a_i حيث $1 \leq i \leq n_0$ أصفار للحدودية $f(x)$ فإن العناصر a_i مختلفة مثني وعددها يساوي n_0 .

- إذا كانت الحدودية $f(x)$ غير منفصلة فوق F عندئذ بالإمكان كتابة $f(x)$ على الشكل الآتي:

$$f(x) = b \cdot (x - a_1)^{p^n} \cdot (x - a_2)^{p^n} \cdot \dots \cdot (x - a_{n_0})^{p^n} = b \cdot \prod_{i=1}^{n_0} (x - a_i)^{p^n}$$

حيث $b \in F$ وأن $a_1, a_2, \dots, a_{n_0} \in K$ ، ومنه فإن العناصر $a_1, a_2, \dots, a_{n_0}$ مختلفة مثني ومترافقة مع a_1 فوق F وعددها يساوي n_0 .

كفاية الشرط. لنفرض أن $a_1, a_2, \dots, a_{n_0} \in K$ هي جميع عناصر الحقل K المختلفة مثني ومتني والمترافقة مع a_1 فوق F بما فيها a_1 .

- إذا كانت الحدودية $f(x)$ منفصلة فوق F فإن $n = n_0$. ومنه فإن $f(x)$ تتفرق في $K[x]$ إلى مضارب خطية وذلك لأن الحقل K يحوي جميع أصفار الحدودية $f(x)$.

- إذا كانت الحدودية $f(x)$ غير منفصلة فوق F عندئذ $n = n_0 p^n$ ومنه بالإمكان كتابة $f(x)$ على الشكل الآتي:

$$f(x) = b \cdot (x - a_1)^{p^1} \cdot (x - a_2)^{p^2} \cdot \dots \cdot (x - a_{n_0})^{p^{n_0}} = b \cdot \prod_{i=1}^{n_0} (x - a_i)^{p^i}$$
 حيث $b \in F$ وأن $a_1, a_2, \dots, a_{n_0} \in K$ ، وهذا يبين أن $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية. ◊

مبرهنة ٧-١-٧.

ليكن الحقل K تمديداً للحقل F الذي مميزه يساوي الصفر، ولتكن $f(x) \in F[x]$ حدودية أولية فوق F وأن $\partial f(x) = n$ وليكن $a_1 \in K$ صفراً للحدودية $f(x)$. الشرط اللازم والكافي كي تتفرق الحدودية $f(x)$ في $K[x]$ إلى مضاريب خطية هو أن يكون عدد جميع عناصر K المختلفة مثني مثني والمترافقة مع a_1 فوق F بما فيها a_1 يساوي n .

البرهان.

لزوم الشرط. لنفرض أن الحدودية $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية عندئذ بالإمكان كتابة $f(x)$ على الشكل الآتي:

$$f(x) = b \cdot (x - a_1) \cdot (x - a_2) \cdot \dots \cdot (x - a_n) = b \cdot \prod_{i=1}^n (x - a_i)$$

حيث $b \in F$ وأن $a_1, a_2, \dots, a_n \in K$ ، ولما كانت الحدودية $f(x)$ أولية فوق F فإن العناصر $a_1, a_2, \dots, a_n$ تكون مترافقة مع a_1 فوق F ولما كانت $\partial f(x) = n \geq 1$ فإنه حسب التمهيدية (٥-٢-٢) تكون الحدودية $f(x)$ منفصلة فوق F ، أي أن أي صفر للحدودية $f(x)$ هو صفر بسيط وهذا يبين أن العناصر $a_1, a_2, \dots, a_n$ مختلفة مثني مثني وعددها n ومترافقة مع a_1 .

كفاية الشرط. بما أن $\partial f(x) = n$ فإن $f(x)$ تملك n صفراً على الأكثر.

من جهة أخرى، بما أن $a_1, a_2, \dots, a_n \in K$ هي جميع عناصر الحقل K المختلفة مثني مثني والمترافقة مع a_1 فوق F وبما أن كل عنصر مترافق مع a_1 فوق F هو صفر للحدودية $f(x)$ نجد أن الحقل K يحوي جميع أصفار الحدودية $f(x)$ وبالتالي فإن $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية. ◊

٧ - ٢. التماثلات الذاتية.

في هذه الفقرة سوف ندرس التماثلات المتباينة والغامرة بين الحقول والتي سوف ندعوها تماثلات، والبداية ستكون مع التعريف الآتي:

تعريف.

ليكن F حقلاً. نسمي كل تماثل متباين وغامر (تماثل) $\alpha: F \rightarrow F$ تماثلاً ذاتياً للحقل F .

ينتج من التعريف مباشرة التمهيدية الآتية:

تمهيدية ٧-٢-١.

إن مجموعة التماثلات الذاتية لحقل ما F تشكل زمرة بالنسبة لعملية تركيب التطبيقات، نرمز لها $Aut(F)$.

البرهان.

نتركه للقارئ. ◊

تعريف.

ليكن $\sigma: F \rightarrow F$ تماثلاً ذاتياً للحقل F . نقول عن العنصر $a \in F$ إنه مثبت وفق σ إذا كان $\sigma(a) = a$. نرمز لمجموعة العناصر المثبتة وفق σ بالشكل:

$$F_\sigma = \{a : a \in F; \sigma(a) = a\}$$

التمهيدية الآتية تبين لنا البنية الجبرية للمجموعة F_σ :

تمهيدية ٧-٢-٢.

ليكن $\sigma: F \rightarrow F$ تماثلاً ذاتياً للحقل F . إن المجموعة F_σ تشكل حقلاً جزئياً من الحقل F .

البرهان.

واضح من خلال تعريف المجموعة F_σ إنها مجموعة جزئية في F وغير خالية، حيث أن $0, 1 \in F_\sigma$ ، لأن $\sigma(1) = 1$ ، $\sigma(0) = 0$. ليكن $a, b \in F_\sigma$ عندئذ فإن:

$$\sigma(a-b) = \sigma(a) + \sigma(-b) = \sigma(a) - \sigma(b) = a-b$$

بفرض أن $b \neq 0$ ، عندئذ:

$$\sigma(a \cdot b^{-1}) = \sigma(a) \cdot \sigma(b^{-1}) = \sigma(a) \cdot (\sigma(b))^{-1} = a \cdot b^{-1}$$

ومنه نجد أن $a-b, a \cdot b^{-1} \in F_\sigma$ ، وهذا يبين لنا أن المجموعة F_σ تشكل حقلاً جزئياً في الحقل F . ♦

تعريف.

ليكن الحقل E تمديداً للحقل F . نسمي كل تماثل ذاتي $\sigma: E \rightarrow E$ للحقل E من أجله $\sigma(a) = a$ أيّاً كان $a \in F$ ، F -تماثل ذاتي للحقل E . نرمز لمجموعة كل الـ F -تماثلات الذاتية للحقل E بالشكل $G(E/F)$.

اعتماداً على التعريف السابق يمكننا صياغة التمهيدية الآتية:

تمهيدية ٧-٢-٣.

ليكن الحقل E تمديداً للحقل F . إن المجموعة $G(E/F)$ تشكل زمرة جزئية من الزمرة $Aut(E)$.

البرهان.

واضح أن المجموعة $G(E/F)$ ليست خالية لأن التطبيق المطابق $I_E: E \rightarrow E$ هو تماثل ذاتي للحقل E ويحقق $I_E(a) = a$ وذلك أيّاً كان $a \in F$ وهذا يبين أن $I_E \in G(E/F)$.

ليكن $\tau, \sigma \in G(E/F)$ عندئذ $\tau, \sigma^{-1} \in Aut(E)$ وبالتالي يكون $\tau \cdot \sigma^{-1} \in Aut(E)$ وبما أنه أيّاً كان $a \in F$ فإن:

$$a = I_E(a) = (\sigma^{-1} \cdot \tau)(a) = \sigma^{-1}(\tau(a)) = \sigma^{-1}(a)$$

ومنه نجد أن:

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

وهذا يبين أن $\tau \cdot \sigma^{-1} \in G(E/F)$ ، ومنه فإن $G(E/F)$ زمرة جزئية من الزمرة $Aut(E)$. ♦

ملاحظة.

ليكن الحقل E تمديداً للحقل F ، وجدنا حسب التمهيدية (٧-٢-٣) أن مجموعة F - تماثلات الذاتية للحقل E تشكل زمرة جزئية من الزمرة $Aut(E)$ ، وهذا يقودنا إلى التعريف الآتي:

تعريف.

ليكن الحقل E تمديداً للحقل F . نسمي الزمرة $G(E/F)$ زمرة غالوا للحقل E فوق F .

أمثلة.

١ - إذا كان الحقل E تمديداً للحقل F وكان $E = F$ ، عندها $G(E/F) = \{I_F\}$ حيث I_F هو التطبيق المطابق على F .

٢ - أوجد زمرة غالوا للحقل $Q(\sqrt{2})$ فوق الحقل Q ، أي $G(Q(\sqrt{2})/Q)$.
وجدنا سابقاً أن العنصرين $\sqrt{2}, -\sqrt{2}$ مترافقان فوق الحقل Q وحسب المبرهنة (٧-١-٢) فإنه يوجد تماثل $Q(\sqrt{2}) \rightarrow Q(-\sqrt{2})$ معرف بالشكل الآتي: أي كان $a + b\sqrt{2} \in Q(\sqrt{2})$ فإن $a - b\sqrt{2}$ $\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$.
للسهولة لنضع $\tau = \psi_{\sqrt{2}, -\sqrt{2}}$. فنجد أنه أيّاً كان $a \in Q$ فإن $\tau(a) = a$ وأن $\tau(\sqrt{2}) = -\sqrt{2}$. ومنه نجد أن $\tau \in G(Q(\sqrt{2})/Q)$ فضلاً عن التماثل المطابق.
لنبرهن على أن $G(Q(\sqrt{2})/Q) = \{1, \tau\}$.

ليكن $\lambda \in G(Q(\sqrt{2})/Q)$ عندئذ بما أن $2 \in Q$ فإن $\lambda(2) = 2$ ومنه نجد أن:

$$2 = \lambda(2) = \lambda(\sqrt{2} \cdot \sqrt{2}) = \lambda(\sqrt{2}) \cdot \lambda(\sqrt{2}) = (\lambda(\sqrt{2}))^2$$

وهكذا نجد أن $\lambda(\sqrt{2}) = \pm\sqrt{2}$.

- إذا كان $\lambda(\sqrt{2}) = +\sqrt{2}$ نجد أن $\lambda = I_{Q(\sqrt{2})}$.

- إذا كان $\lambda(\sqrt{2}) = -\sqrt{2}$ نجد أن $\lambda = \tau$. وهكذا فإن $G(Q(\sqrt{2})/Q) = \{1, \tau\}$.

نأتي الآن إلى صياغة المبرهنة المهمة الآتية:

مبرهنة ٧-٢-٤.

ليكن F, F' حقلين و $\tau: F \rightarrow F'$ تماثلاً. لنفرض أن $f(x) \in F[x]$ حدودية أولية فوق F وأن $\overline{f(x)} \in F'[x]$ الحدودية المقابلة للحدودية $f(x)$ وفق التماثل τ . إذا كان α صفراً للحدودية $f(x)$ في تمديد ما للحقل F وكان β صفراً للحدودية $\overline{f(x)}$ في تمديد ما للحقل F' ، عندئذ يوجد تماثل $\sigma: F(\alpha) \rightarrow F'(\beta)$ امتداداً للتماثل τ من أجله $\sigma(\alpha) = \beta$.

البرهان.

لنفرض أن $\partial f(x) = n \geq 1$ وأن $f(x) = \sum_{i=0}^n c_i x^i$ حيث $c_i \in F, 0 \leq i \leq n$ ، عندئذ يكون $\overline{f(x)} = \sum_{i=0}^n \tau(c_i) x^i$ ولما كان τ تماثلاً وأن $c_n \neq 0$ نجد أن $\tau(c_n) \neq 0$ وهذا يبين أن $\partial \overline{f(x)} = n$ ، ولكون الحدودية $f(x)$ أولية فوق الحقل F فإنه حسب التمرين المحلول (٦-١) تكون الحدودية $\overline{f(x)}$ أولية فوق الحقل F' . أيضاً لما كانت الحدودية $f(x)$ هي الحدودية الأصغرية للعنصر α وأن $\partial f(x) = n$ فإن كل عنصر $y \in F(\alpha)$ يكتب بصورة وحيدة على الشكل $y = \sum_{i=0}^{n-1} d_i \alpha^i$ حيث $d_i \in F$. لنعرف التطبيق $\sigma: F(\alpha) \rightarrow F'(\beta)$ بالشكل الآتي: أيّاً كان $\sum_{i=0}^{n-1} d_i \alpha^i \in F(\alpha)$ فإن:

$$\sigma(\sum_{i=0}^{n-1} d_i \alpha^i) = \sum_{i=0}^{n-1} \tau(d_i) \beta^i \in F(\beta)$$

ف نجد أن σ تشاكل، لأنه إذا كان $\sum_{i=0}^{n-1} d_i \alpha^i, \sum_{i=0}^{n-1} b_i \alpha^i \in F(\alpha)$ فإن:

$$\begin{aligned} \sigma(\sum_{i=0}^{n-1} d_i \alpha^i + \sum_{i=0}^{n-1} b_i \alpha^i) &= \sigma(\sum_{i=0}^{n-1} (d_i + b_i) \alpha^i) = \sum_{i=0}^{n-1} \tau(d_i + b_i) \beta^i = \\ &= \sum_{i=0}^{n-1} (\tau(d_i) + \tau(b_i)) \beta^i = \sum_{i=0}^{n-1} \tau(d_i) \beta^i + \sum_{i=0}^{n-1} \tau(b_i) \beta^i = \\ &= \sigma(\sum_{i=0}^{n-1} d_i \alpha^i) + \sigma(\sum_{i=0}^{n-1} b_i \alpha^i) \end{aligned}$$

لنفرض أن:

$$(\sum_{i=0}^{n-1} d_i \alpha^i) \cdot (\sum_{i=0}^{n-1} b_i \alpha^i) = \sum_{i=0}^{2(n-1)} k_i \alpha^i$$

حيث $k_s = \sum_{s=i+j} d_i b_j$ فنجد أن:

$$\tau(k_s) = \tau(\sum_{s=i+j} d_i b_j) = \sum_{s=i+j} \tau(d_i b_j) = \sum_{s=i+j} \tau(d_i) \cdot \tau(b_j)$$

وهذا يبين أن:

$$\sigma((\sum_{i=0}^{n-1} d_i \alpha^i) \cdot (\sum_{i=0}^{n-1} b_i \alpha^i)) = \sigma(\sum_{i=0}^{2(n-1)} k_i \alpha^i) = \sum_{i=0}^{2(n-1)} \tau(k_i) \beta^i =$$

$$= (\sum_{i=0}^{n-1} \tau(d_i) \beta^i) \cdot (\sum_{i=0}^{n-1} \tau(b_i) \beta^i) = \sigma(\sum_{i=0}^{n-1} d_i \alpha^i) \cdot \sigma(\sum_{i=0}^{n-1} b_i \alpha^i)$$

وهكذا نجد أن σ تشاكل، وهو أيضاً متباين، لأنه إذا كان:

$$\sigma(\sum_{i=0}^{n-1} d_i \alpha^i) = \sigma(\sum_{i=0}^{n-1} b_i \alpha^i)$$

$$\text{نجد أن } \sum_{i=0}^{n-1} \tau(d_i) \beta^i = \sum_{i=0}^{n-1} \tau(b_i) \beta^i \text{ ومنه فإن:}$$

$$\sum_{i=0}^{n-1} (\tau(d_i) - \tau(b_i)) \beta^i = 0$$

أي أن $\sum_{i=0}^{n-1} \tau(d_i - b_i) \beta^i = 0$ ، ولما كانت المجموعة $\{1, \beta, \beta^2, \dots, \beta^{n-1}\}$ تشكل قاعدة للحقل $F'(\beta)$ فوق F' نجد أن $\tau(d_i - b_i) = 0$ حيث $0 \leq i \leq n-1$ ولما كان τ متبايناً نجد أن $d_i = b_i$ أيّاً كان $0 \leq i \leq n-1$ وهذا يبين أن $\sum_{i=0}^{n-1} d_i \alpha^i = \sum_{i=0}^{n-1} b_i \alpha^i$ وهكذا نجد أن σ متباين. لنبرهن على أن σ غامر. بما أن $\overline{f(x)}$ الحدودية الأصغرية للعنصر β فوق F' وأن $\partial \overline{f(x)} = n$ فإن كل عنصر $y' \in F'(\beta)$ يكتب بصورة وحيدة على الشكل $y' = \sum_{i=0}^{n-1} v_i \beta^i$ حيث $v_i \in F'$ لأجل $0 \leq i \leq n-1$.

ليكن $\sum_{i=0}^{n-1} v_i \beta^i \in F'(\beta)$ ، بما أن $v_i \in F'$ وأن τ غامر فإنه يوجد $u_i \in F$ بحيث يكون $v_i = \tau(u_i)$ ومنه نجد أن $\sum_{i=0}^{n-1} u_i \alpha^i \in F(\alpha)$ وأن:

$$\sigma(\sum_{i=0}^{n-1} u_i \alpha^i) = \sum_{i=0}^{n-1} \tau(u_i) \beta^i = \sum_{i=0}^{n-1} v_i \beta^i$$

مما سبق نجد أن σ تماثل. لنبرهن الآن على أن التماثل σ امتداد للتماثل τ .

ليكن $a \in F$ عندئذ فإن $a = a \alpha^0 \in F(\alpha)$ وأن $a = a \alpha^0$ و $\sigma(a) = \tau(a) \beta^0 = \tau(a)$ وهذا يبين أن التماثل σ امتداد للتماثل τ ، كما أن $\sigma(\alpha) = \tau(1 \cdot \alpha) = \tau(1) \cdot \beta = \beta$.

مبرهنة ٧-٢-٥.

ليكن F, F' حقليين و $\tau: F \rightarrow F'$ تماثلاً. لنفرض أن $f(x) \in F[x]$ وأن $\partial f(x) \geq 1$ وأن $\overline{f(x)} \in F'[x]$ الحدودية المقابلة للحدودية $f(x)$ وفق التماثل τ . إذا كان K حقل تفريق الحدودية $f(x)$ فوق F وكان K' حقل تفريق الحدودية $\overline{f(x)}$ فوق F' ، عندئذ يوجد تماثل $\sigma: K \rightarrow K'$ امتداداً للتماثل τ يحقق الشرط: إذا كان $\alpha \in K$ صفراً للحدودية $f(x)$ عندئذ يكون $\sigma(\alpha) \in K'$ صفراً للحدودية $\overline{f(x)}$.

البرهان.

لنفرض أن $\partial f(x) = n \geq 1$. سوف نورد البرهان بالاستقراء حسب n .
 من أجل $n = 1$ ، في هذه الحالة تكون الحدودية $f(x)$ أولية في $F[x]$ ولما كان K حقل
 تفريق الحدودية $f(x)$ فوق F فإنه يوجد $\alpha \in K$ بحيث $f(\alpha) = 0$ وأن $K = F(\alpha)$.
 من جهة أخرى، تكون $\partial \overline{f(x)} = 1$ وبالتالي فإن الحدودية $\overline{f(x)}$ تكون أولية فوق F'
 ولما كان K' حقل تفريق الحدودية $\overline{f(x)}$ فوق F' ، عندئذ يوجد $\beta \in K'$ بحيث
 $\overline{f(\beta)} = 0$ وأن $K' = F'(\beta)$. وحسب المبرهنة (٧-٢-٤) يوجد تماثل $\sigma: K \rightarrow K'$
 امتداداً للتماثل τ لأجله $\sigma(\alpha) = \beta$.

لنفرض أن $n > 1$ وأن المبرهنة صحيحة لأجل كل حدودية درجتها أصغر من n فوق F .
 بما أن $\partial f(x) = n > 1$ فإن الحدودية $f(x)$ غير قابلة للقلب فوق F ومنه توجد حدودية
 أولية $\varphi(x) \in F[x]$ تقسم $f(x)$ في $F[x]$ ، ولما كان K حقل تفريق الحدودية $f(x)$
 فوق F فإنه يوجد $\alpha \in K$ بحيث $\varphi(\alpha) = 0$.

لنفرض أن $\overline{\varphi(x)} \in F'[x]$ الحدودية المقابلة للحدودية $\varphi(x)$ وفق التماثل τ . بما أن
 الحدودية $\varphi(x)$ أولية فوق F وتقسم $f(x)$ في $F[x]$ فإن الحدودية $\overline{\varphi(x)}$ تكون أولية
 في $F'[x]$ وتقسم $\overline{f(x)}$ في $F'[x]$ ، ولما كان K' حقل تفريق الحدودية $\overline{f(x)}$ فوق F'
 فإنه يوجد $\beta \in K'$ بحيث $\overline{\varphi(\beta)} = 0$ ، وحسب المبرهنة (٧-٢-٤) يوجد تماثل
 $\sigma_1: F(\alpha) \rightarrow F'(\beta)$ امتداداً للتماثل τ من أجله $\sigma_1(\alpha) = \beta$.

بما أن $\varphi(\alpha) = 0$ فإن $f(\alpha) = 0$ ومنه فإن $x - \alpha \in F(\alpha)[x]$ وتقسم $f(x)$ في
 $F(\alpha)[x]$ ومنه توجد $f_1(x) \in F(\alpha)[x]$ بحيث $f(x) = (x - \alpha) \cdot f_1(x)$ ومنه فإن

$$\overline{f(x)} = (x - \sigma_1(\alpha)) \cdot \overline{f_1(x)} = (x - \beta) \cdot \overline{f_1(x)}$$

حيث $\overline{f_1(x)}$ هي الحدودية المقابلة للحدودية $f_1(x)$ وفق التماثل σ_1 ، مما سبق نجد أن
 $\partial \overline{f_1(x)} = \partial \overline{f(x)} - 1 = n - 1 < n$.

من جهة أخرى، بما أن K حقل تفريق الحدودية $f(x)$ فوق F فإن K حقل تفريق
 الحدودية $f_1(x)$ فوق $F(\alpha)$. أيضاً بما أن K' حقل تفريق الحدودية $\overline{f(x)}$ فوق F'
 فإن K' هو حقل تفريق الحدودية $\overline{f_1(x)}$ فوق $F'(\beta)$ ، وحسب الفرض الاستقرائي يوجد
 تماثل $\sigma: K \rightarrow K'$ امتداداً للتماثل σ_1 ، لأجله صورة كل صفر للحدودية $f_1(x)$ في K

هو صفر للحدودية $\overline{f_1(x)}$ في K' وأن $\sigma(\alpha) = \sigma_1(\alpha) = \beta$ ، ولما كان σ_1 امتداداً للتماثل τ فإن σ امتداد للتماثل τ لأجله صورة كل صفر للحدودية $f(x)$ في K هو صفر للحدودية $\overline{f(x)}$ في K' . ◊

بالاعتماد على المبرهنة الأخيرة يمكننا صياغة المبرهنة المهمة الآتية:

مبرهنة ٧-٢-٦.

ليكن الحقل K تمديداً للحقل F . إذا كانت $f(x) \in F[x]$ بحيث $\partial f(x) \geq 1$ وإذا كان K هو حقل تقريب الحدودية $f(x)$ فوق F عندئذ يوجد F - تماثل ذاتي للحقل K .
البرهان.

ينتج مباشرة من المبرهنة (٧-٢-٥) من أجل $I_F = \tau \cdot \circ$. ◊

٧ - ٣. تمديد التشاكلات.

تعريف.

ليكن F, K حقلين ولنفرض أن $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in F[x]$.
إذا كان $\sigma : F \rightarrow K$ تشاكلاً حلقياً، في هذه الحالة نسمي الحدودية:
$$\sigma(f(x)) = \sigma(a_n)x^n + \sigma(a_{n-1})x^{n-1} + \dots + \sigma(a_1)x + \sigma(a_0) \in K[x]$$

صورة الحدودية $f(x)$ وفق التشاكل σ .

تعريف.

ليكن الحقل K تمديداً للحقل F و L حقلاً ما. لنفرض أن $\sigma_0 : F \rightarrow L$ و $\sigma : K \rightarrow L$ تشاكلان حلقيان. نقول إن التشاكل σ ممدد للتشاكل σ_0 إذا كان $\sigma(a) = \sigma_0(a)$ وذلك أيّاً كان $a \in F$ ، أي أن $\sigma = \sigma_0$ على F .

مبرهنة ٧-٣-١.

ليكن الحقل $F(\alpha)$ تمديداً بسيطاً للحقل F و K حقلاً آخر يحوي الحقل F . عندئذ:
١ - إذا كان العنصر α جبرياً فوق F وكانت $p(x) \in F[x]$ الحدودية الأصغرية للعنصر α فوق F فإنه لأجل أي F -تشاكل $\varphi : F(\alpha) \rightarrow K$ يكون العنصر $\varphi(\alpha)$ صفراً للحدودية $p(x)$ في الحقل K .
٢ - إذا كانت $\mathfrak{T}$ هي مجموعة كل الـ F -تشاكلات من الشكل $\varphi : F(\alpha) \rightarrow K$ وكانت $\mathfrak{T}_0$ مجموعة كل أصفار الحدودية $p(x)$ في الحقل K فإنه يوجد تطبيق متباين وغامر (تقابل) $f : \mathfrak{T} \rightarrow \mathfrak{T}_0$.
البرهان.

لنفرض أن $p(x) = \sum_{i=0}^n b_i x^i$ حيث $b_i \in F$ وذلك أيّاً كان $0 \leq i \leq n$. لما كان α صفراً للحدودية $p(x)$ نجد أن $0 = p(\alpha) = \sum_{i=0}^n b_i \alpha^i$.
ليكن $\varphi : F(\alpha) \rightarrow K$ هو F -تشاكل ولما كان $\sum_{i=0}^n b_i \alpha^i \in F(\alpha)$ نجد أن:
$$\varphi(\sum_{i=0}^n b_i \alpha^i) = \varphi(0) = 0$$

ومنه يكون $\sum_{i=0}^n b_i \varphi(\alpha^i) = 0$ وبالتالي نجد أن $\sum_{i=0}^n b_i (\varphi(\alpha))^i = 0$
وهذا يبين أن العنصر $\varphi(\alpha)$ صفر للحدودية $p(x)$ في الحقل K .

٢ - لنعرف العلاقة $f: \mathfrak{S} \rightarrow \mathfrak{S}_0$ بالشكل الآتي: أيّاً كان $\varphi \in \mathfrak{S}$ فإن $f(\varphi) = \varphi(\alpha)$ فنجد أن f تطبيق، لأنه إذا كان $\varphi_1, \varphi_2 \in \mathfrak{S}$ فإن كلاً من φ_1, φ_2 هو F -تشاكل من الشكل $\varphi: F(\alpha) \rightarrow K$. إذا كان $\varphi_1 = \varphi_2$ ، ولما كان $\alpha \in F(\alpha)$ نجد أن $\varphi_1(\alpha) = \varphi_2(\alpha)$ وهذا يبين أن $f(\varphi_1) = f(\varphi_2)$ ، أي أن f تطبيق. كما أن f متباين، لأنه إذا كان $f(\varphi_1) = f(\varphi_2)$ نجد أن $\varphi_1(\alpha) = \varphi_2(\alpha)$ ولما كان كل من φ_1, φ_2 هو F -تشاكل فإنه أيّاً كان $\beta \in F$ فإن $\varphi_1(\beta) = \beta = \varphi_2(\beta)$ وهذا يبين أن $\varphi_1 = \varphi_2$. لنبرهن على أن f غامر.

ليكن $\gamma \in \mathfrak{S}_0$ عندئذ فإن γ هو صفر للحدودية $p(x)$ ، ولما كانت الحدودية $p(x)$ أولية في $F[x]$ فإن المثالي $\langle p(x) \rangle$ يكون أعظمية في $F[x]$ وبالتالي تكون حلقة الخارج $F[x]/\langle p(x) \rangle$ حقلاً.

لنأخذ التشاكل $\lambda: F[x] \rightarrow K$ المعرفة بالشكل الآتي: أيّاً كان $g(x) \in F[x]$ فإن $\lambda(g(x)) = g(\gamma)$. نلاحظ أن $\text{Ker}(\lambda) = \langle p(x) \rangle$ لأنه إذا كان $g(x) \in \text{Ker}(\lambda)$ فإن $\lambda(g(x)) = 0$ ومنه يكون $g(\gamma) = 0$ ولما كانت $p(x)$ الحدودية الأصغرية للعنصر γ فوق F نجد أن $p(x)$ تقسم $g(x)$ في $F[x]$ وهذا يبين أن $g(x) \in \langle p(x) \rangle$ أي $\text{Ker}(\lambda) \subseteq \langle p(x) \rangle$. من جهة أخرى، ليكن $\mu(x) \in \langle p(x) \rangle$ ولما كانت $F[x]$ حلقة مثاليات رئيسية نجد أن $\mu(x) = p(x)u(x)$ حيث $u(x) \in F[x]$ ، ولما كان $p(\gamma) = 0$ نجد أن $\mu(\gamma) = 0$ وهذا يبين أن $\lambda(\mu(x)) = 0$ وبالتالي يكون $\mu(x) \in \text{Ker}(\lambda)$ ، أي أن $\langle p(x) \rangle \subseteq \text{Ker}(\lambda)$ وهكذا نجد أن $\text{Ker}(\lambda) = \langle p(x) \rangle$ وحسب مبرهنة التماثل الأولى يكون:

$$F[x]/\langle p(x) \rangle = F[x]/\text{Ker}(\lambda) \cong \text{Im}(\lambda)$$

لنفرض أن هذا التماثل هو ψ فيكون $\psi: F[x]/\langle p(x) \rangle \rightarrow K$ تشاكلاً حلقياً معرّفاً بالشكل الآتي: أيّاً كان $h(x) \in F[x]$ فإن:

$$\psi(h(x) + \langle p(x) \rangle) = \lambda(h(x)) = h(\gamma)$$

من جهة ثالثة، وحسب المبرهنة (٣-١-٦) فإن $f(\alpha) \cong F[x]/\langle p(x) \rangle$ لنرمز لهذا التماثل $\theta: f(\alpha) \rightarrow F[x]/\langle p(x) \rangle$.

لنضع $\varphi_0 = \psi\theta$ فنجد أن $\varphi_0 : F(\alpha) \rightarrow K$ تشاكل حلقي ويحقق:

$$\varphi_0(\alpha) = \psi\theta(\alpha) = \psi(x + \langle p(x) \rangle) = \lambda(x) = \gamma$$
فضلاً عن ذلك، فإنه أيّاً كان $b \in F$ فإن:

$$\varphi_0(b) = \psi\theta(b) = \psi(b + \langle p(x) \rangle) = b$$

وهذا يبين أن $\varphi_0 = \psi\theta : F(\alpha) \rightarrow K$ هو F -تشاكل ومنه فإن $\varphi_0 \in \mathfrak{I}$ كما أن
 $f(\varphi_0) = \varphi_0(\alpha) = \gamma$ ، مما سبق نجد أن التطبيق f غامر. ◊

اعتماداً على المبرهنة الأخيرة يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن الحقل $F(\alpha)$ تمديداً بسيطاً للحقل F و K حقلاً آخر يحوي الحقل F . إذا كان
العنصر α جبرياً فوق F وكانت $p(x) \in F[x]$ الحدودية الأصغرية للعنصر α فوق
 F فإن عدد الـ F -تشاكلات $\varphi : F(\alpha) \rightarrow K$ يساوي إلى عدد الأصفار المختلفة
للحدودية $p(x)$ في الحقل K .

مبرهنة ٧-٣-٢.

ليكن الحقل $F(\alpha)$ تمديداً بسيطاً للحقل F و K حقلاً ما. لنفرض أن $\varphi_0 : F \rightarrow K$
تشاكل حلقي، عندئذ:

١ - إذا كان العنصر α جبرياً فوق F وكانت $p(x) \in F[x]$ الحدودية الأصغرية
للعنصر α فوق F فإنه لأجل أي تمديد للتشاكل φ_0 من الشكل $\varphi : F(\alpha) \rightarrow K$ يكون
العنصر $\varphi(\alpha)$ صفراً للحدودية $\varphi_0(p(x))$ في الحقل K .

٢ - إذا كانت $\mathfrak{I}'$ هي مجموعة كل التمديدات للتشاكل φ_0 من الشكل $\varphi : F(\alpha) \rightarrow K$
وكانت $\mathfrak{I}'_0$ مجموعة كل أصفار الحدودية $\varphi_0(p(x))$ في الحقل K فإنه يجد تطبيقاً
متبايناً وغامراً (تقابلاً) $f : \mathfrak{I}' \rightarrow \mathfrak{I}'_0$.

البرهان.

لنفرض أن $p(x) = \sum_{i=0}^n b_i x^i$ حيث $b_i \in F$ وذلك أيّاً كان $0 \leq i \leq n$. لدينا أيضاً
لأجل كل $b \in F$ فإن $\varphi(b) = \varphi_0(b)$.

١ - لما كان α صفراً للحدودية $p(x)$ نجد أن $p(\alpha) = \sum_{i=0}^n b_i \alpha^i = 0$ ، ومنه يكون:

$$\begin{aligned} 0 &= \varphi(0) = \varphi(\alpha) = \varphi(\sum_{i=0}^n b_i \alpha^i) \\ &= \sum_{i=0}^n \varphi(b_i) \varphi(\alpha^i) = \sum_{i=0}^n \varphi_0(b_i) \varphi(\alpha)^i \end{aligned}$$

وهذا يبين أن العنصر $\varphi(\alpha)$ صفر للحدودية $\varphi_0(p(x))$ في الحقل K .

٢ - لنعرف العلاقة $\mathfrak{T}'_0 \rightarrow \mathfrak{T}' : f$ بالشكل الآتي: أيّاً كان $\varphi \in \mathfrak{T}'$ فإن $f(\varphi) = \varphi(\alpha)$

ف نجد أن f تطبيق، لأنه إذا كان $\varphi_1, \varphi_2 \in \mathfrak{T}'$ فإن كل من φ_1, φ_2 هو تمديد للتشاكل φ_0 من الشكل $\varphi_1, \varphi_2 : F(\alpha) \rightarrow K$. فإذا كان $\varphi_1 = \varphi_2$ ، ولما كان $\alpha \in F(\alpha)$ نجد أن

$$\varphi_1(\alpha) = \varphi_2(\alpha) \text{ وهذا يبين أن } f(\varphi_1) = f(\varphi_2), \text{ أي أن } f \text{ تطبيق.}$$

كما أن f متباين، لأنه إذا كان $f(\varphi_1) = f(\varphi_2)$ نجد أن $\varphi_1(\alpha) = \varphi_2(\alpha)$ ولما كان كل من φ_1, φ_2 تمديداً للتشاكل φ_0 فإنه أيّاً كان $\beta \in F$ فإن:

$$\varphi_1(\beta) = \varphi_0(\beta) = \varphi_2(\beta)$$

وهذا يبين أن $\varphi_1 = \varphi_2$. لنبرهن على أن التطبيق f غامر.

ليكن $\gamma \in \mathfrak{T}'_0$ عندئذ فإن $\gamma \in K$ هو صفر للحدودية $\varphi_0(p(x))$ ، ولما كانت الحدودية $p(x)$ أولية في $F[x]$ نجد أن المثالي $\langle p(x) \rangle$ يكون أعظماً في $F[x]$ وبالتالي تكون حلقة الخارج $F[x]/\langle p(x) \rangle$ حقلاً.

لنأخذ التشاكل $\lambda : F[x] \rightarrow K$ المعرفة بالشكل الآتي: أيّاً كان $g(x) \in F[x]$ فإن $\lambda(g(x)) = \varphi_0(g(\gamma))$. لنبرهن على أن $\text{Ker}(\lambda) = \langle p(x) \rangle$.

لما كان $\varphi_0 : F \rightarrow K$ تشاكلاً حلقياً فإنه حسب التمهيدية (٣-١-٣) يكون φ_0 متبايناً ومنه يكون التشاكل $\varphi_0 : F \rightarrow \text{Im}(\varphi_0)$ تماثلاً. من جهة أخرى، وحسب التمرين المحلول (٥-١) يكون التشاكل $\varphi_0 : F[x] \rightarrow \text{Im}(\varphi_0)[x]$ تماثلاً أيضاً ولما كانت الحدودية $p(x)$ أولية في $F[x]$ فإن الحدودية $\varphi_0(p(x))$ تكون أولية في $\text{Im}(\varphi_0)[x]$. أيضاً لما كان $\gamma \in \mathfrak{T}'_0$ العنصر $\gamma \in K$ هو صفر للحدودية $\varphi_0(p(x))$ وهذا يبين أن $\varphi_0(p(x))$ هي الحدودية الأصغرية للعنصر γ فوق الحقل $\text{Im}(\varphi_0)$.

ليكن $g(x) \in \text{Ker}(\lambda)$ عندئذ فإن $g(x) \in F[x]$ وأن $\lambda(g(x)) = 0$ أي أن $\varphi_0(g(\gamma)) = 0$ ومنه فإن الحدودية $\varphi_0(p(x))$ تقسم $\varphi_0(g(x))$ في $\text{Im}(\varphi_0)[x]$ ولما

كان $\varphi_0 : F[x] \rightarrow Im(\varphi_0)[x]$ تماثلاً نجد أن الحدودية $p(x)$ تقسم $g(x)$ في $F[x]$ وهذا يبين أن $g(x) \in \langle p(x) \rangle$ أي أن $g(x) \in \langle p(x) \rangle$ وبالتالي يكون $Ker(\lambda) \subseteq \langle p(x) \rangle$.

الاحتواء المعاكس. ليكن $\mu(x) \in \langle p(x) \rangle$ ولما كانت $F[x]$ حلقة مثاليات رئيسية نجد أن $\mu(x) = p(x)v(x)$ حيث $v(x) \in F[x]$ وأن:

$$\lambda(\mu(x)) = \lambda(p(x)v(x)) = \lambda(p(x))\lambda(v(x))$$

وبالتالي يكون $\varphi_0(\mu(\gamma)) = \varphi_0(p(\gamma)) \cdot \varphi_0(v(\gamma))$ ولما كان $\gamma \in \mathfrak{I}'_0$ هو صفر للحدودية $\varphi_0(p(x))$ نجد أن $\varphi_0(\mu(\gamma)) = 0$ أي أن $\lambda(\mu(x)) = 0$ وهذا يبين أن $\mu(x) \in Ker(\lambda)$ ، أي أن $\langle p(x) \rangle \subseteq Ker(\lambda)$ مما سبق نجد $Ker(\lambda) = \langle p(x) \rangle$ وحسب مبرهنة التماثل الأولى يكون:

$$F[x]/\langle p(x) \rangle = F[x]/Ker(\lambda) \cong Im(\lambda)$$

لنفرض أن هذا التماثل هو ψ فيكون $\psi : F[x]/\langle p(x) \rangle \rightarrow K$ تشاكلاً حلقياً معرّفًا بالشكل الآتي: أيًا كان $h(x) \in F[x]$ فإن:

$$\psi(h(x) + \langle p(x) \rangle) = \lambda(h(x)) = \varphi_0(h(\gamma))$$

من جهة ثالثة، وحسب المبرهنة (٣-١-٦) فإن $f(\alpha) \cong F[x]/\langle p(x) \rangle$ لنرمز لهذا التماثل $\theta : f(\alpha) \rightarrow F[x]/\langle p(x) \rangle$. لنضع $\psi_0 = \psi\theta$ فنجد أن $\psi_0 : F(\alpha) \rightarrow K$ تشاكل حلقى ويحقق:

$$\psi_0(\alpha) = \psi\theta(\alpha) = \psi(x + \langle p(x) \rangle) = \lambda(x) = \varphi_0(1 \cdot \gamma) = \varphi_0(1) \cdot \gamma = \gamma$$

فضلاً عن ذلك، فإنه أيًا كان $b \in F$ فإن:

$$\psi_0(b) = \psi\theta(b) = \psi(b + \langle p(x) \rangle) = \lambda(b) = \varphi_0(b)$$

وهذا يبين أن $\psi_0 = \psi\theta : F(\alpha) \rightarrow K$ هو تمديد للتشاكل φ_0 ومنه فإن $\psi_0 \in \mathfrak{I}'_0$ كما أن $f(\psi_0) = \psi_0(\alpha) = \gamma$ ، مما سبق نجد أن التطبيق f غامر.

اعتماداً على المبرهنة الأخيرة يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن الحقل $F(\alpha)$ تمديداً بسيطاً للحقل F و K حقلاً ما. إذا كان العنصر α جبرياً فوق F وكانت $p(x) \in F[x]$ الحدودية الأصغرية للعنصر α فوق F وإذا كان $\varphi_0 : F \rightarrow K$ تشاكلاً حلقياً فإن عدد التمديدات للتشاكل φ_0 يساوي إلى عدد الأصفار المختلفة للحدودية $\varphi_0(p(x))$ في الحقل K .

لنورد عدداً من الأمثلة على المبرهنة الأخيرة:

أمثلة.

١ - لنفرض أن $F = Q$ وأن $K = C$ حقل الأعداد المركبة وأن $\alpha = \sqrt{2}$. لنفرض أن $i_0 : Q \rightarrow C$ تشاكل الاحتواء القانوني. لما كانت $p(x) = x^2 - 2 \in Q[x]$ هي الحدودية الأصغرية للعنصر $\sqrt{2}$ وأن لهذه الحدودية صفرين مختلفين هما $\sqrt{2}, -\sqrt{2}$ فإنه حسب المبرهنة (٧-٣-٢) يوجد تمديدان مختلفان للتشاكل i_0 هما:

$$\sigma_1 : Q(\sqrt{2}) \rightarrow K, \quad \sigma_1(\sqrt{2}) = \sqrt{2}$$

$$\sigma_2 : Q(\sqrt{2}) \rightarrow K, \quad \sigma_2(\sqrt{2}) = -\sqrt{2}$$

ويحققان $\sigma_1(a) = a = \sigma_2(a)$ وذلك أيّاً كان $a \in Q$.

٢ - لنفرض أن $F = Q$ وأن $K = C$ حقل الأعداد المركبة وأن $\alpha = i$. لنفرض أن $i_0 : Q \rightarrow C$ تشاكل الاحتواء القانوني. لما كانت $p(x) = x^2 + 1 \in Q[x]$ هي الحدودية الأصغرية للعنصر i وأن لهذه الحدودية صفرين مختلفين هما $i, -i$ فإنه حسب المبرهنة (٧-٣-٢) يوجد تمديدان مختلفان للتشاكل i_0 هما:

$$\sigma_1 : Q(i) \rightarrow K, \quad \sigma_1(i) = i$$

$$\sigma_2 : Q(i) \rightarrow K, \quad \sigma_2(i) = -i$$

ويحققان $\sigma_1(a) = a = \sigma_2(a)$ وذلك أيّاً كان $a \in Q$.

٣ - بالعودة إلى المثال (٢) نجد أنه من أجل $K = R$ فإن تشاكل الاحتواء القانوني $i_0 : Q \rightarrow R$ لا يوجد له أي تمديد حسب المبرهنة (٧-٣-٢) وذلك لأن الحدودية $x^2 + 1 \in R[x]$ لا تملك أصفاراً في الحقل R .

٤ - لنفرض أن $F = Q$ وأن $K = C$ حقل الأعداد المركبة وأن $\alpha = \sqrt[3]{2}$.

لنفرض أن $i_0 : Q \rightarrow C$ تشاكل الاحتواء القانوني. واضح أن العنصر α جبري فوق Q لأنه صفر للحدودية $x^3 + 2 \in Q[x]$. إن الحدودية $x^3 + 2$ تملك ثلاثة أصفار في C

هي: $\sqrt[3]{2}, \sqrt[3]{2} \frac{-1+i\sqrt{3}}{2}, \sqrt[3]{2} \frac{-1-i\sqrt{3}}{2}$. بفرض أن:

$$j_1 = \frac{-1+i\sqrt{3}}{2}, \quad j_2 = \frac{-1-i\sqrt{3}}{2}$$

فتكون أصفار الحدودية $x^3 - 2$ في C هي $\sqrt[3]{2}, \sqrt[3]{2} \cdot j_1, \sqrt[3]{2} \cdot j_2$. وحسب المبرهنة (٧-٣-٢) فإنه يوجد ثلاثة تمديدات للتشاكل i_0 وهي:

$$\begin{aligned} \sigma_1 : Q(\sqrt[3]{2}) &\rightarrow C, & \sigma_1(\sqrt[3]{2}) &= \sqrt[3]{2} \\ \sigma_2 : Q(\sqrt[3]{2}) &\rightarrow C, & \sigma_2(\sqrt[3]{2}) &= \sqrt[3]{2} \cdot j_1 \\ \sigma_3 : Q(\sqrt[3]{2}) &\rightarrow C, & \sigma_3(\sqrt[3]{2}) &= \sqrt[3]{2} \cdot j_2 \end{aligned}$$

٥ - بالعودة إلى المثال (٤) نجد أنه من أجل $K = R$ فإن تشاكل الاحتواء القانوني

$i_0 : Q \rightarrow R$ يملك تمديداً واحداً فقط وذلك لأن الحدودية $x^3 + 2 \in R[x]$ تملك صفرًا واحداً في الحقل R هو $\sqrt[3]{2}$ ، وهذا التمديد هو:

$$\sigma : Q(\sqrt[3]{2}) \rightarrow R, \quad \sigma(\sqrt[3]{2}) = \sqrt[3]{2}$$

مبرهنة ٧-٣-٣.

ليكن F حقلاً و $f(x) \in F[x]$ و $0 \neq f(x)$ ولنفرض أن E هو الحقل المولد فوق F بجميع أصفار الحدودية $f(x)$. ليكن K حقلاً آخر يحوي F ويحوي حقل تقرييق الحدودية $f(x)$ ، عندئذ:

١ - يوجد F - تشاكل حقيقي $\varphi : E \rightarrow K$.

٢ - إن عدد جميع الـ F - تشاكلات $\varphi : E \rightarrow K$ أصغر أو يساوي $[E : F]$ وهذا العدد يساوي $[E : F]$ إذا كانت جميع أصفار الحدودية $f(x)$ مختلفة مثلي مثلي.

البرهان.

لنفرض أن $\alpha_1, \alpha_2, \dots, \alpha_n$ هي جميع أصفار الحدودية $f(x)$ عندئذ حسب الفرض

يكون $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$. لما كانت العناصر $\alpha_1, \alpha_2, \dots, \alpha_n$ جبرية فوق F لنفرض أن $p_i(x) \in F[x]$ هي الحدودية الأصغرية للعنصر α_i فوق F لأجل جميع القيم $1 \leq i \leq n$. لما كان $f(\alpha_i) = 0$ نجد أن الحدودية $p_i(x)$ تقسم $f(x)$ في $F[x]$ وذلك أيأ كان $1 \leq i \leq n$ وحسب المبرهنة (٣-٣-٥) فإن $\partial p_i(x) = [F(\alpha_i) : F]$.
لنأخذ تشاكل الاحتواء القانوني $i_0 : F \rightarrow K$. لما كنت الحدودية $p_1(x)$ تقسم $f(x)$ في $F[x]$ فإن كل صفر للحدودية $p_1(x)$ هو صفر للحدودية $f(x)$ ولما كان الحقل K يحوي حقل تقرييق الحدودية $f(x)$ فإن K يحوي جميع أصفار الحدودية $p_1(x)$ ومنه فإن $\alpha_1 \in K$ وهذا يبين أن الحدودية $i_0(p_1(x))$ تملك صفراً في K ، لأن:

$$i_0(p_1(x)) = p_1(x)$$

وحسب المبرهنة (٧-٣-٢) يوجد F -تشاكل $i_1 : F(\alpha_1) \rightarrow K$ تمديداً للتشاكل i_0 وأن عدد هذه التمديدات يساوي إلى عدد الأصفار المختلفة للحدودية $p_1(x)$ وبالتالي فهي أصغر أو تساوي $\partial p_i(x)$ التي تساوي $[F(\alpha_i) : F]$.

لنفرض أن $\sigma_1 : F(\alpha_1) \rightarrow K$ هو أحد التمديدات للتشاكل i_0 التي تم الحصول عليها. لما كان العنصر α_2 جبرياً فوق F فإن العنصر α_2 يكون جبرياً فوق $F(\alpha_1)$.

لنفرض أن $q_2(x) \in F(\alpha_1)[x]$ الحدودية الأصغرية للعنصر α_2 فوق $F(\alpha_1)$ ، لما كانت $p_2(x) \in F(\alpha_1)[x]$ وأن $p_2(\alpha_2) = 0$ نجد أن $q_2(x)$ تقسم $p_2(x)$ في $F(\alpha_1)[x]$ ، ولما كان كل صفر للحدودية $q_2(x)$ هو صفر للحدودية $p_2(x)$ وأن كل صفر للحدودية $p_2(x)$ هو صفر للحدودية $f(x)$ وإن جميع أصفار الحدودية $f(x)$ تقع في K نجد أن جميع أصفار الحدودية $q_2(x)$ موجودة في K ومنه فإن الحدودية $\sigma_1(q_2(x))$ تملك صفراً في الحقل K وبالتالي يوجد تمديد $\sigma_2 : F(\alpha_1)(\alpha_2) \rightarrow K$

للتشاكل σ_1 وهذا التمديد من الشكل $\sigma_2 : F(\alpha_1, \alpha_2) \rightarrow K$.

بالطريقة نفسها يتم إثبات أن عدد تمديدات التشاكل i_0 من الشكل:

$$\sigma : E = F(\alpha_1, \alpha_2, \dots, \alpha_n) \rightarrow K$$

أصغر أو يساوي درجة التمديد $[E : F]$ وفي حالة كون جميع أصفار الحدودية $f(x)$ مختلفة مثتى مثتى نحصل على المساواة. ◊

اعتماداً على المبرهنة الأخيرة يمكننا صياغة النتيجة الآتيتين:

نتيجة ١.

ليكن F حقلاً و $p(x) \in F[x]$. إذا كان كل من K, E حقل تفريق للحدودية $p(x)$ فوق F ، عندئذ يكون $K \cong E$.

البرهان.

لما كان E حقل تفريق للحدودية $p(x)$ فوق F فإن E يكون مولداً فوق F بجميع أصفار الحدودية $p(x)$ وحسب المبرهنة (٧-٣-٣) فإنه يوجد F -تشاكل $\varphi: E \rightarrow K$ أيضاً لما كان K حقل تفريق للحدودية $p(x)$ فوق F فإن K يكون مولداً فوق F بجميع أصفار الحدودية $p(x)$ وحسب المبرهنة (٧-٣-٣) فإنه يوجد F -تشاكل $\psi: K \rightarrow E$ ولما كان كل من φ, ψ تشاكلاً متبايناً وأن كلا من K, E فضاء متجهي فوق F منتهي البعد نجد أن:

$$[K:F] \leq [E:F], \quad [E:F] \leq [K:F]$$

ومنه نجد أن $[K:F] = [E:F]$ وهذا يبين أن $K \cong E$. ◊

نتيجة ٢.

ليكن F حقلاً و K, E تمديدين للحقل F . إذا كان التمديد E للحقل F منتهياً، عندئذ:

١ - يوجد تمديد منته L للحقل K و F -تشاكل $\tau: E \rightarrow L$.

٢ - عدد جميع الـ F -تشاكلات $\sigma: E \rightarrow K$ أصغر أو يساوي $[E:F]$.

البرهان.

١ - لما كان E تمديداً منتهياً للحقل F فإنه توجد عناصر $\alpha_1, \alpha_2, \dots, \alpha_n \in E$ بحيث يكون $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ ولما كان كل تمديد منته هو تمديداً جبرياً نجد أن العناصر $\alpha_1, \alpha_2, \dots, \alpha_n$ جبرية فوق F . لنفرض أن $p_i(x) \in F[x]$ هي الحدودية الأصغرية للعنصر α_i فوق F لأجل جميع القيم $1 \leq i \leq n$. لنفرض أيضاً أن:

$$f(x) = \prod_{i=1}^n p_i(x) \in F[x]$$

لنفرض أن L حقل تفريق للحدودية $f(x)$ فوق K حيث $f(x) \in F[x] \subseteq K[x]$ عندئذ حسب المبرهنة (٧-٣-٣) يوجد F -تشاكل $\tau: E \rightarrow L$ واضح أن L هو تمديد

منته للحقل K .

٢ - إن عدد جميع الـ F -تشاكلات $\sigma: E \rightarrow K$ أصغر أو يساوي درجة تمديد الحقل E فوق F .

مثال.

لنفرض أن $F = Q$ وأن $K = C$ حقل الأعداد المركبة وأن $K = Q(j, \sqrt[3]{2})$ حيث $j = \frac{-1 - i\sqrt{3}}{2}$. أوجد جميع الـ F -تشاكلات من الشكل $\sigma: K \rightarrow C$.

الحل.

لدينا الحقول الثلاثة $Q, Q(j), Q(j, \sqrt[3]{2})$ التي تحقق $Q \subseteq Q(j) \subseteq Q(j, \sqrt[3]{2})$.
- من أجل $Q \subseteq Q(j)$ لنأخذ تشاكل الاحتواء القانوني $i_0: Q \rightarrow C$. إن الحدودية $x^2 + x + 1 \in Q[x]$ هي الحدودية الأصغرية للعنصر j فوق Q وأن أصفار هذه الحدودية هي j, j^2 ، ومنه يوجد تمديدان للتشاكل i_0 هما:

$$\begin{aligned}\sigma_1: Q(j) &\rightarrow C, & \sigma_1(j) &= j \\ \sigma_2: Q(j) &\rightarrow C, & \sigma_2(j) &= j^2\end{aligned}$$

وأن كلا منهما هو F -تشاكل لأنهما تمديدان للتشاكل i_0 .

- من أجل $Q(j) \subseteq Q(j, \sqrt[3]{2})$ لنفرض أن $K = Q(j, \sqrt[3]{2})$ ، لنأخذ الـ F -تشاكل:

$$\sigma_1: Q(j) \rightarrow C, \quad \sigma_1(j) = j$$

لما كانت الحدودية $x^3 - 2 \in Q(j)[x]$ هي الحدودية الأصغرية للعنصر $\sqrt[3]{2}$ فوق $Q(j)$ والتي أصفارها هي $\sqrt[3]{2}, \sqrt[3]{2}j, \sqrt[3]{2}j^2$ وأن جميع هذه الأصفار تنتمي إلى الحقل C فإنه يوجد ثلاثة تمديدات للتشاكل σ_1 هي:

$$\begin{aligned}\tau_1: K = Q(j, \sqrt[3]{2}) &\rightarrow C, & \tau_1(\sqrt[3]{2}) &= \sqrt[3]{2} \\ \tau_2: K = Q(j, \sqrt[3]{2}) &\rightarrow C, & \tau_2(\sqrt[3]{2}) &= \sqrt[3]{2} \cdot j \\ \tau_3: K = Q(j, \sqrt[3]{2}) &\rightarrow C, & \tau_3(\sqrt[3]{2}) &= \sqrt[3]{2} \cdot j^2\end{aligned}$$

بالمثل يمكن إيجاد التمديدات الثلاثة للتشاكل σ_2 على الحقل $K = Q(j, \sqrt[3]{2})$.

مما سبق نجد أنه يوجد لتشاكل الاحتواء القانوني i_0 ستة تمديدات على الحقل $Q(j, \sqrt[3]{2})$

وهي:

$$\begin{aligned}
 \tau_1 : K = Q(j, \sqrt[3]{2}) &\rightarrow C, & \tau_1(\sqrt[3]{2}) &= \sqrt[3]{2} \\
 \tau_2 : K = Q(j, \sqrt[3]{2}) &\rightarrow C, & \tau_2(\sqrt[3]{2}) &= \sqrt[3]{2} \cdot j \\
 \tau_3 : K = Q(j, \sqrt[3]{2}) &\rightarrow C, & \tau_3(\sqrt[3]{2}) &= \sqrt[3]{2} \cdot j^2 \\
 \psi_1 : K = Q(j, \sqrt[3]{2}) &\rightarrow C, & \psi_1(\sqrt[3]{2}) &= \sqrt[3]{2} \\
 \psi_2 : K = Q(j, \sqrt[3]{2}) &\rightarrow C, & \psi_2(\sqrt[3]{2}) &= \sqrt[3]{2} \cdot j \\
 \psi_3 : K = Q(j, \sqrt[3]{2}) &\rightarrow C, & \psi_3(\sqrt[3]{2}) &= \sqrt[3]{2} \cdot j^2
 \end{aligned}$$

وهذه التمديدات يمكن وضعها في جدول كالآتي:

	τ_1	τ_2	τ_3	ψ_1	ψ_2	ψ_3
$j \rightarrow$	j	j	j	j^2	j^2	j^2
$\sqrt[3]{2} \rightarrow$	$\sqrt[3]{2}$	$\sqrt[3]{2}j$	$\sqrt[3]{2}j^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}j$	$\sqrt[3]{2}j^2$

مبرهنة ٧-٣-٤.

ليكن F حقلاً و E, K تمديدين للحقل F . إذا كان E تمديداً جبرياً للحقل F وكان الحقل K مغلقاً جبرياً عندئذ يوجد F - تشاكل $\sigma : E \rightarrow K$.
البرهان.

سوف نميز حالتين:

- الحالة الأولى. إذا كان الحقل E تمديداً منتهياً للحقل F عندئذ حسب المبرهنة (٧-٣-٣) يوجد F - تشاكل $\sigma : E \rightarrow K$.

- إذا كان الحقل E تمديداً جبرياً وغير منته للحقل F في هذه الحالة لنأخذ المجموعة $\mathfrak{T}$ المؤلفة من جميع الثنائيات (L', τ) حيث $F \subseteq L' \subseteq E$ وأن $\tau : L' \rightarrow K$ هو F - تشاكل، فنجد أن المجموعة $\mathfrak{T}$ ليست خالية، لأن $(F, I_F) \in \mathfrak{T}$ حيث:

$$I_F : F \rightarrow F \subseteq K$$

لنعرف على المجموعة $\mathfrak{T}$ علاقة $(\leq)$ بالشكل الآتي: أيأ كان $(L_1, \tau_1), (L_2, \tau_2) \in \mathfrak{T}$ فإن:

$$(L_1, \tau_1) \leq (L_2, \tau_2) \Leftrightarrow L_1 \subseteq L_2 \wedge \tau_2|_{L_1} = \tau_1$$

فنجذ أن الثنائية $(\mathfrak{I}, \leq)$ تشكل مجموعة مرتبة جزئياً (أثبت ذلك).

لتكن $\mathfrak{I}_0$ مجموعة جزئية وغير خالية من $\mathfrak{I}$ ومرتبة كلياً. لنفرض أن $L_0 = \cup_{(L_i, \tau_i) \in \mathfrak{I}_0} L_i$ فنجد أن L_0 حقل وأن $F \subseteq L_0 \subseteq E$ ، كما أن $L_i \subseteq L_0$ وذلك أيّاً كان $(L_i, \tau_i) \in \mathfrak{I}_0$.
لنعرف العلاقة $\tau_0 : L_0 \rightarrow K$ بالشكل الآتي: أيّاً كان $y \in L_0 = \cup_{(L_i, \tau_i) \in \mathfrak{I}_0} L_i$ فإنه يوجد $(L_j, \tau_j) \in \mathfrak{I}_0$ بحيث $y \in L_j$ ، لنضع $\tau_0(y) = \tau_j(y)$ ، فنجد أن τ_0 تطبيق، لأنه إذا كان:

$$y, z \in L_0 = \cup_{(L_i, \tau_i) \in \mathfrak{I}_0} L_i$$

بحيث $y = z$ فإنه يوجد $(L_i, \tau_i) \in \mathfrak{I}_0$ بحيث $y, z \in L_i$ ومنه يكون:

$$\tau_0(y) = \tau_i(y) = \tau_i(z) = \tau_0(z)$$

كما أن τ_0 هو تشاكل حقيقي، لأنه إذا كان $a, b \in L_0 = \cup_{(L_i, \tau_i) \in \mathfrak{I}_0} L_i$ فإنه يوجد $(L_i, \tau_i), (L_j, \tau_j) \in \mathfrak{I}_0$ بحيث $a \in L_i, b \in L_j$ ولما كانت المجموعة $\mathfrak{I}_0$ مرتبة كلياً لنفرض أن:

$$(L_i, \tau_i) \leq (L_j, \tau_j)$$

وهذا يبين أن $L_i \subseteq L_j$ وأن $\tau_j|_{L_i} = \tau_i$ ومنه فإن $a, b \in L_j$ وأن:

$$\tau_0(a+b) = \tau_j(a+b) = \tau_j(a) + \tau_j(b) =$$

$$= \tau_i(a) + \tau_j(b) = \tau_0(a) + \tau_0(b)$$

$$\tau_0(a \cdot b) = \tau_j(a \cdot b) = \tau_j(a) \cdot \tau_j(b) =$$

$$= \tau_i(a) \cdot \tau_j(b) = \tau_0(a) \cdot \tau_0(b)$$

كما أنه أيّاً كان $z \in F \subseteq L_0$ فإنه يوجد $(L_t, \tau_t) \in \mathfrak{I}_0$ بحيث $z \in L_t$ وأن:

$$\tau_0(z) = \tau_t(z) = z$$

وذلك لأن τ_t هو F -تشاكل $\tau_t : L_t \rightarrow K$ ، مما سبق نجد أن $(L_0, \tau_0) \in \mathfrak{I}$ ويحقق:

$$(L_i, \tau_i) \leq (L_0, \tau_0)$$

وذلك أيّاً كان $(L_i, \tau_i) \in \mathfrak{I}_0$ وهذا يبين أن الثنائية (L_0, τ_0) حد أعلى للمجموعة $\mathfrak{I}_0$ في

$\mathfrak{I}$ وحسب تمهيدية زورن يوجد في المجموعة $\mathfrak{I}$ عنصراً أعظماً وليكن (L, τ) .

لنبرهن على أن $L = E$ ، لنفرض جديلاً أن $L \subsetneq E$ عندئذ يوجد $a \in E$ وأن $a \notin L$ ولما كان E تمديداً جبرياً للحقل F فإن a هو عنصر جبري فوق F وبالتالي فهو عنصر جبري فوق L ومنه فإن الحقل $L(a)$ هو تمديد منته للحقل L وحسب الحالة الأولى يمكن تمديد التشاكل τ إلى التشاكل الآتي: $\tau': L(a) \rightarrow K$ بحيث أي كان $c \in L$ فإن $\tau'(c) = \tau(c)$ وهذا يبين أنه أياً كان $b \in F$ فإن $\tau'(b) = \tau(b) = b$ ومنه نجد أن τ' هو F -تشاكل وذلك لأن الحقل K مغلق جبرياً وهكذا يكون $(L(a), \tau') \in \mathfrak{S}$ وأن:

$$(L, \tau) \leq (L(a), \tau')$$

وهذا يناقض كون (L, τ) عنصراً أعظماً في $\mathfrak{S}$ ، مما سبق نجد أن $L = E$. ◊

تمارين محلولة (٧)

١ - أثبت أن مرافق العنصر $3 + \sqrt{2}$ هو $3 - \sqrt{2}$.

الحل.

نلاحظ أن الحدودية $p(x) = x^2 - 6x + 7 \in Q[x]$ هي الحدودية الأصغرية للعنصر $3 + \sqrt{2}$ فوق Q لأنها أولية فوق Q وأن $p(3 + \sqrt{2}) = 0$. وهذه الحدودية تحقق أن $p(3 - \sqrt{2}) = 0$ ، ومنه فإن العنصر $3 - \sqrt{2}$ مرافق للعنصر $3 + \sqrt{2}$.

٢ - لنفرض أن الحقل K تمديد للحقل Q وليكن $\alpha \in \text{Aut}(K)$. أثبت أنه أياً كان $a \in Q$ فإن $\alpha(a) = a$.

الحل.

لنفرض أن الحقل K تمديد للحقل Q وليكن $\alpha \in \text{Aut}(K)$. ليكن $a \in Q$ عندئذ فإن $a = n/m$ حيث $n, m \in Z$ وأن $m \neq 0$ ، ومنه فإن $a = n \cdot m^{-1}$. ولما كان $\alpha(1) = 1$ نجد أن:

$$\alpha(n) = \alpha(\underbrace{1+1+\dots+1}_{n \text{ once}}) = \underbrace{\alpha(1) + \alpha(1) + \dots + \alpha(1)}_{n \text{ once}} = n \cdot \alpha(1) = n \cdot 1 = n$$

كما أن $\alpha(m^{-1}) = \alpha(m)^{-1} = m^{-1}$ ، ومنه نجد أن:

$$\alpha(a) = \alpha(n \cdot m^{-1}) = \alpha(n) \cdot \alpha(m)^{-1} = n \cdot m^{-1} = a$$

٣ - لنأخذ الحقل $Z_2 = \{0,1\}$ والحدودية $p(x) = x^2 + x + 1 \in Z_2[x]$. والمطلوب:

أ - أثبت أن الحدودية $p(x)$ أولية في $Z_2[x]$.

بما أن $\partial p(x) = 2$ وأن $p(0) = 1, p(1) = 1$ نجد أن الحدودية $p(x)$ لا تملك أصفاراً في الحقل Z_2 وحسب المبرهنة (١-٢-٤) تكون الحدودية $p(x)$ أولية في $Z_2[x]$.

ب - أوجد حقلاً ممدداً للحقل Z_2 يحوي صفراً للحدودية $p(x)$ ، ثم شكل جدولي الجمع والضرب لهذا الحقل.

بما أن الحدودية $p(x)$ أولية في $Z_2[x]$ فإنه حسب المبرهنة (٣-١-٤) يوجد تمديد K للحقل Z_2 يحوي صفراً للحدودية $p(x)$ وليكن a ، ومنه يكون $Z_2(a)$ هو تمديد للحقل Z_2 وأن $p(a) = 0$. وحسب المبرهنة (٣-٣-٥) فإن كل عنصر $y \in Z_2(a)$ يكتب بصورة وحيدة على الشكل $y = \alpha + \beta a$ حيث $\alpha, \beta \in Z_2$ ومنه نجد أن الحقل $Z_2(a)$ يتألف من أربعة عناصر هي: $0, 1, a, 1+a$ أي أن: $Z_2(a) = \{0, 1, a, 1+a\}$ ويكون كل من جدولي الجمع والضرب على الشكل الآتي:

+	0	1	a	1+a
0	0	1	a	1+a
1	1	0	1+a	a
a	a	1+a	0	1
1+a	1+a	a	1	0

.	0	1	a	1+a
0	0	0	0	0
1	0	1	a	1+a
a	0	a	1+a	1
1+a	0	1+a	1	a

وذلك لأن $a^2 + a + 1 = 0$ ومنه فإن $a^2 = -1 - a = 1 + a$ ، كما أن:

$$(1+a)(1+a) = 1 + 2a + a^2 = 1 + 1 + a = 2 + a = a$$

ت - أوجد تابع فريبنوس على الحقل $Z_2(a)$.

حسب التمرين المحلول (٦-٤) ولما كان مميز الحقل Z_2 يساوي 2 فإن تابع فريبنوس

هو $\varphi: Z_2(a) \rightarrow Z_2(a)$ المعرفة بالشكل الآتي: أيًا كان $y \in Z_2(a)$ فإن $\varphi(y) = y^2$

ومنه فإن:

$$\varphi(0) = 0, \quad \varphi(1) = 1, \quad \varphi(a) = a^2 = 1 + a, \quad \varphi(1+a) = (1+a)^2 = a$$

ج - أوجد الحقل المثبت من خلال تابع فريبنوس.
لما كان $\varphi(0)=0$, $\varphi(1)=1$ فإن Z_2 هو الحقل المثبت من خلال تابع فريبنوس،
وهذا يبين أن تابع فريبنوس هو Z_2 - تماثل ذاتي للحقل $Z_2(a)$.
ح - أوجد مرتبة تابع فريبنوس.
نلاحظ أن:

$$\varphi^4(0)=0, \quad \varphi^4(1)=1, \quad \varphi^4(a)=a^4=(a^2)^2=(1+a)^2=a$$

$$\varphi^4(1+a)=(1+a)^4=((1+a)^2)^2=(a)^2=1+a$$

وهذا يبين أن مرتبة تابع فريبنوس تساوي 4.

٤ - أوجد $G(Q(\sqrt{2}, \sqrt{3})/Q)$.

الحل.

نلاحظ أولاً أن $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2})(\sqrt{3}) = Q(\sqrt{3})(\sqrt{2})$ وأن $\sqrt{2}, -\sqrt{2}$ عنصران مترافقان فوق الحقل $Q(\sqrt{3})$ ، لأن $x^2 - 2 \in Q(\sqrt{3})[x]$ هي الحدودية الأصغرية للعنصرين $\sqrt{2}, -\sqrt{2}$ فوق الحقل $Q(\sqrt{3})$. كما أن العنصرين $\sqrt{3}, -\sqrt{3}$ مترافقان فوق الحقل $Q(\sqrt{2})$ ، لأن $x^2 - 3 \in Q(\sqrt{2})[x]$ هي الحدودية الأصغرية للعنصرين $\sqrt{3}, -\sqrt{3}$ فوق الحقل $Q(\sqrt{2})$. حسب المبرهنة (٦-١-٢) يوجد تماثل:

$$\psi_{\sqrt{2}, -\sqrt{2}} : Q(\sqrt{3})(\sqrt{2}) \rightarrow Q(\sqrt{3})(-\sqrt{2})$$

يحقق $\psi_{\sqrt{2}, -\sqrt{2}}(\sqrt{2}) = -\sqrt{2}$ وأن $\psi_{\sqrt{2}, -\sqrt{2}}(c) = c$ أيًا كان $c \in Q(\sqrt{3})$. أيضاً يوجد تماثل:

$$\psi_{\sqrt{3}, -\sqrt{3}} : Q(\sqrt{2})(\sqrt{3}) \rightarrow Q(\sqrt{2})(-\sqrt{3})$$

يحقق $\psi_{\sqrt{3}, -\sqrt{3}}(\sqrt{3}) = -\sqrt{3}$ وأن $\psi_{\sqrt{3}, -\sqrt{3}}(c) = c$ أيًا كان $c \in Q(\sqrt{2})$.

للسهولة، لنضع $\psi_{\sqrt{2}, -\sqrt{2}} = \tau_1$, $\psi_{\sqrt{3}, -\sqrt{3}} = \tau_2$ فنجد أن τ_1, τ_2 تماثلات للحقل $Q(\sqrt{2}, \sqrt{3})$ وأن $\tau_1(c) = \tau_2(c) = c$ وذلك أيًا كان $c \in Q$. ومنه فإن $\tau_1 \cdot \tau_2$ هو تماثل للحقل $Q(\sqrt{2}, \sqrt{3})$ يحقق $\tau_1 \cdot \tau_2(c) = c$ وذلك أيًا كان $c \in Q$. كما أن:

$$\tau_1 \cdot \tau_2(\sqrt{2}) = \tau_1(\tau_2(\sqrt{2})) = \tau_1(-\sqrt{2}) = -\sqrt{2}$$

$$\tau_1 \cdot \tau_2(\sqrt{3}) = \tau_1(\tau_2(\sqrt{3})) = \tau_1(\sqrt{3}) = -\sqrt{3}$$

أي أن:

$$\tau_1 \cdot \tau_2(a) = \begin{cases} a & a \in Q \\ -\sqrt{2} & a = -\sqrt{2} \\ -\sqrt{3} & a = -\sqrt{3} \end{cases}$$

ومنه نجد أن $\{1, \tau_1, \tau_2, \tau_1 \cdot \tau_2\} \subseteq G(Q(\sqrt{2}, \sqrt{3})/Q)$

ليكن $\sigma \in G(Q(\sqrt{2}, \sqrt{3})/Q)$ ، بما أن $2, 3 \in Q$ نجد أن:

$$2 = \sigma(2) = \sigma(\sqrt{2} \cdot \sqrt{2}) = \sigma(\sqrt{2}) \cdot \sigma(\sqrt{2}) = (\sigma(\sqrt{2}))^2$$

ومنه فإن $\sigma(\sqrt{2}) = \pm\sqrt{2}$

$$3 = \sigma(3) = \sigma(\sqrt{3} \cdot \sqrt{3}) = \sigma(\sqrt{3}) \cdot \sigma(\sqrt{3}) = (\sigma(\sqrt{3}))^2$$

ومنه فإن $\sigma(\sqrt{3}) = \pm\sqrt{3}$ وهنا يكون لدينا الحالات الآتية:

- إذا كان $\sigma(\sqrt{2}) = \sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$ نجد أن $\sigma = 1$.

- إذا كان $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$ نجد أن $\sigma = \tau_1$.

- إذا كان $\sigma(\sqrt{2}) = \sqrt{2}$, $\sigma(\sqrt{3}) = -\sqrt{3}$ نجد أن $\sigma = \tau_2$.

- إذا كان $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = -\sqrt{3}$ نجد أن $\sigma = \tau_1 \cdot \tau_2$.

وهكذا نجد أن:

$$G(Q(\sqrt{2}, \sqrt{3})/Q) = \{1, \tau_1, \tau_2, \tau_1 \cdot \tau_2\}$$

ويمكننا تشكيل جدول الضرب للزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q)$ الآتي:

	1	τ_1	τ_2	$\tau_1 \cdot \tau_2$
1	1	τ_1	τ_2	$\tau_1 \cdot \tau_2$
τ_1	τ_1	1	$\tau_1 \cdot \tau_2$	τ_2
τ_2	τ_2	$\tau_1 \cdot \tau_2$	1	τ_1
$\tau_1 \cdot \tau_2$	$\tau_1 \cdot \tau_2$	τ_2	τ_1	1

للتأكد من صحة الجدول السابق، نلاحظ أن:

$\tau_1^2(\sqrt{2}) = \tau_1(\tau_1(\sqrt{2})) = \tau_1(-\sqrt{2}) = \tau_1(-1) \cdot \tau_1(\sqrt{2}) = (-1) \cdot (-\sqrt{2}) = \sqrt{2}$
 وذلك لأن $-1 \in Q$ ، ومنه فإن $\tau_1^2 = 1$. بالمثل نجد أن $\tau_2^2 = 1$.
 كما أن:

$$\tau_1 \cdot (\tau_1 \cdot \tau_2) = (\tau_1 \cdot \tau_1) \cdot \tau_2 = 1 \cdot \tau_2 = \tau_2$$

وأنه أيًا كان $c \in Q$ فإن:

$$\tau_2 \cdot \tau_1(c) = \tau_2(\tau_1(c)) = \tau_2(c) = c$$

$$\tau_2 \cdot \tau_1(\sqrt{2}) = \tau_2(\tau_1(\sqrt{2})) = \tau_2(-\sqrt{2}) = -\sqrt{2}$$

$$\tau_2 \cdot \tau_1(\sqrt{3}) = \tau_2(\tau_1(\sqrt{3})) = \tau_2(\sqrt{3}) = -\sqrt{3}$$

وهكذا نجد أن $\tau_2 \cdot \tau_1 = \tau_1 \cdot \tau_2$.

كما أن $\tau_2 \cdot (\tau_1 \cdot \tau_2) = \tau_2 \cdot (\tau_2 \cdot \tau_1) = \tau_2^2 \cdot \tau_1 = 1 \cdot \tau_1 = \tau_1$ وأن:

$$(\tau_1 \cdot \tau_2) \cdot (\tau_1 \cdot \tau_2) = \tau_1 \cdot (\tau_2 \cdot \tau_2) \cdot \tau_1 = \tau_1 \cdot \tau_2^2 \cdot \tau_1 = \tau_1^2 = 1$$

٥ - لنفرض أن $F = \mathbb{R}$ حقل الأعداد الحقيقية وأن $K = \mathbb{C}$ حقل الأعداد العقدية (المركبة). أثبت أن التطبيق $\sigma: K \rightarrow K$ المعرف بالشكل الآتي: أيًا كان $a + ib \in K$ حيث $a, b \in F$ ، فإن $\sigma(a + ib) = a - ib$ هو F -تماثل ذاتي للحقل K .
 الحل.

واضح أن الحقل K هو تمديد للحقل F . ليكن $a_1 + ib_1, a_2 + ib_2 \in K$ عندئذ فإن:

$$\begin{aligned} \sigma((a_1 + ib_1) + (a_2 + ib_2)) &= \sigma((a_1 + a_2) + i(b_1 + b_2)) = \\ &= (a_1 + a_2) - i(b_1 + b_2) = (a_1 - ib_1) + (a_2 - ib_2) = \\ &= \sigma(a_1 + ib_1) + \sigma(a_2 + ib_2) \end{aligned}$$

$$\begin{aligned} \sigma((a_1 + ib_1) \cdot (a_2 + ib_2)) &= \sigma((a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2)) = \\ &= (a_1 a_2 - b_1 b_2) - i(a_1 b_2 + b_1 a_2) = (a_1 - ib_1) \cdot (a_2 - ib_2) = \\ &= \sigma(a_1 + ib_1) \cdot \sigma(a_2 + ib_2) \end{aligned}$$

كما أن σ متباين، لأنه إذا كان $\sigma(a_1 + ib_1) = \sigma(a_2 + ib_2)$ ينتج أن:

$$a_1 - ib_1 = a_2 - ib_2$$

ومنه فإن $a_1 = a_2, b_1 = b_2$ وبالتالي يكون $a_1 + ib_1 = a_2 + ib_2$.

وأن σ غامر، لأنه أياً كان $a+ib \in K$ فإن $a, b \in F$ وبالتالي يكون $a-ib \in K$ ومنه فإن $\sigma(a-ib) = a - (-i)b = a+ib$ مما سبق نجد أن σ هو تماثل ذاتي للحقل K .

فضلاً عن ذلك، أياً كان $a \in F$ فإن $a \in K$ وأن $\sigma(a) = a$ وهذا يبين أن σ هو F -تماثل ذاتي للحقل K .

٦ - لنفرض أن $F = \mathbb{R}$ حقل الأعداد الحقيقية وأن $K = \mathbb{C}$ حقل الأعداد العقدية (المركبة). والمطلوب:

أ - أوجد الزمرة $G(K/F)$.

ب - أثبت أن $G(K/F) \cong Z/2Z$.

الحل.

أ - بالعودة إلى التمرين (١) وجدنا أن التطبيق $\sigma: K \rightarrow K$ المعرف بالشكل الآتي: أياً كان $a+ib \in K$ حيث $a, b \in F$ فإن $\sigma(a+ib) = a-ib$ هو F -تماثل ذاتي للحقل K . لنبرهن على أن $\{I_K, \sigma\} = G(K/F)$.

ليكن $\tau \in G(K/F)$ عندئذ فإن $\tau: K \rightarrow K$ هو F -تماثل ذاتي للحقل K وأنه أياً كان $a+ib \in K$ حيث $a, b \in F$ فإن:

$$\tau(a+ib) = \tau(a) + \tau(i) \cdot \tau(b) = a + \tau(i) \cdot b$$

ومنه لمعرفة τ يكفي معرفة $\tau(i)$ ، ولما كان:

$$(\tau(i))^2 = \tau(i) \cdot \tau(i) = \tau(i^2) = \tau(-1) = -1$$

نجد أن $\tau(i) = \pm i$.

- إذا كان $\tau(i) = i$ نجد أن $\tau = I_K$.

- إذا كان $\tau(i) = -i$ نجد أن $\tau = \sigma$.

وهكذا نجد أن $G(K/F) = \{I_K, \sigma\}$.

ب - حسب (أ) فإن مرتبة الزمرة $G(K/F)$ تساوي 2 وبالتالي فإن الزمرة $G(K/F)$ دوارة ومرتبته تساوي 2 وبالتالي يكون $G(K/F) \cong Z_2 \cong Z/2Z$.

٧ - أوجد الزمرة $G(Q(\sqrt{3})/Q)$.

الحل.

نعلم أن $Q(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in Q\}$ حقل ومنه فإن الحقل $Q(\sqrt{3})$ هو تمديد للحقل Q .

ليكن $\sigma \in G(Q(\sqrt{3})/Q)$ عندئذ فإن $\sigma : Q(\sqrt{3}) \rightarrow Q(\sqrt{3})$ هو Q -تماثل ذاتي للحقل وأنه أياً كان $a + b\sqrt{3} \in Q(\sqrt{3})$ فإن $a, b \in Q$ وأن:

$$\sigma(a + b\sqrt{3}) = \sigma(a) + \sigma(b) \cdot \sigma(\sqrt{3}) = a + b \cdot \sigma(\sqrt{3})$$

وبالتالي لمعرفة التماثل σ يكفي معرفة $\sigma(\sqrt{3})$ ، ولما كان:

$$(\sigma(\sqrt{3}))^2 = \sigma(\sqrt{3}) \cdot \sigma(\sqrt{3}) = \sigma(\sqrt{3} \cdot \sqrt{3}) = \sigma(3) = 3$$

نجد أن $\sigma(\sqrt{3}) = \pm\sqrt{3}$.

- إذا كان $\sigma(\sqrt{3}) = \sqrt{3}$ نجد أن $\sigma = I_{Q(\sqrt{3})}$ والذي سوف نرمز له:

$$\sigma_1 : Q(\sqrt{3}) \rightarrow Q(\sqrt{3}) : \sigma_1(a + b \cdot \sqrt{3}) = a + b \cdot \sqrt{3} : a, b \in Q$$

- إذا كان $\sigma(\sqrt{3}) = -\sqrt{3}$ والذي سوف نرمز له:

$$\sigma_2 : Q(\sqrt{3}) \rightarrow Q(\sqrt{3}) : \sigma_2(a + b \cdot \sqrt{3}) = a - b \cdot \sqrt{3} : a, b \in Q$$

وهكذا نجد أن $G(Q(\sqrt{3})/Q) = \{\sigma_1, \sigma_2\}$.

٨ - أوجد الزمرة $G(Q(\sqrt[3]{2})/Q)$.

الحل.

نعلم أن $Q(\sqrt[3]{2}) = \{a + b \cdot \sqrt[3]{2} : a, b \in Q\}$ حقل ومنه فإن الحقل $Q(\sqrt[3]{2})$ هو تمديد للحقل Q .

ليكن $\sigma \in G(Q(\sqrt[3]{2})/Q)$ عندئذ فإن $\sigma : Q(\sqrt[3]{2}) \rightarrow Q(\sqrt[3]{2})$ هو Q -تماثل ذاتي للحقل $Q(\sqrt[3]{2})$ وأنه أياً كان $a + b \cdot \sqrt[3]{2} \in Q(\sqrt[3]{2})$ فإن $a, b \in Q$ وأن:

$$\sigma(a + b \cdot \sqrt[3]{2}) = \sigma(a) + \sigma(b) \cdot \sigma(\sqrt[3]{2}) = a + b \cdot \sigma(\sqrt[3]{2})$$

وبالتالي لمعرفة التماثل σ يكفي معرفة $\sigma(\sqrt[3]{2})$ ، ولما كان:

$$(\sigma(\sqrt[3]{2}))^2 = \sigma(\sqrt[3]{2}) \cdot \sigma(\sqrt[3]{2}) \cdot \sigma(\sqrt[3]{2}) = \sigma(\sqrt[3]{2} \cdot \sqrt[3]{2} \cdot \sqrt[3]{2}) = \sigma(2) = 2$$

نجد أن $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$.

لنوجد الجذور الثلاثة الأولى للعدد 2. نعلم أنه أياً كان $n \in N^*$ فإن:

$$\sqrt[n]{2} = \sqrt[n]{2} \cdot \sqrt[n]{1} = \sqrt[n]{2} \cdot (\cos(2\pi k/n) + i \sin(2\pi k/n)) = \sqrt[n]{2} \cdot e^{i2\pi k/n}$$

وأنه من أجل $n = 3$ فإن:

$$\sqrt[3]{2} = \sqrt[3]{2} \cdot \sqrt[3]{1} = \sqrt[3]{2} \cdot (\cos(2\pi k/3) + i \sin(2\pi k/3)) = \sqrt[3]{2} \cdot e^{i2\pi k/3}$$

- إذا كان $k = 0$ نجد أن $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$.
 - إذا كان $k = 1$ نجد أن $\sigma(\sqrt[3]{2}) = \sqrt[3]{2} \cdot e^{i2\pi/3} \notin Q(\sqrt[3]{2})$ وبالتالي هو مرفوض لأنه عدد عقدي.

- إذا كان $k = 2$ نجد أن $\sigma(\sqrt[3]{2}) = \sqrt[3]{2} \cdot e^{i4\pi/3} \notin Q(\sqrt[3]{2})$ وبالتالي هو مرفوض لأنه عدد عقدي.

مما سبق نجد أن $\sigma : Q(\sqrt[3]{2}) \rightarrow Q(\sqrt[3]{2})$ هو Q -تماثل ذاتي للحقل $Q(\sqrt[3]{2})$ وأنه أياً كان $a + b \cdot \sqrt[3]{2} \in Q(\sqrt[3]{2})$ فإن:

$$\sigma(a + b \cdot \sqrt[3]{2}) = a + b \cdot \sqrt[3]{2}$$

وهذا يبين أن $G(Q(\sqrt[3]{2})/Q) = \{I_{Q(\sqrt[3]{2})}\}$.

تمارين (٧)

- ١ - أوجد مرافق كل من العناصر الآتية $\sqrt{2} + i$, $\sqrt{2} - \sqrt{3}$, فوق الحقل Q .
- ٢ - أوجد مرافق العنصر الجبري $\sqrt{1+\sqrt{2}}$ فوق الحقل Q .
- ٣ - لنأخذ التمديد الآتي $E = Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$ للحقل Q ولنأخذ التماثلات الذاتية الآتية للحقل E .

$$\tau_2 = \psi_{\sqrt{2}, -\sqrt{2}} : Q(\sqrt{3}, \sqrt{5})(\sqrt{2}) \rightarrow Q(\sqrt{3}, \sqrt{5})(-\sqrt{2})$$

$$\tau_3 = \psi_{\sqrt{3}, -\sqrt{3}} : Q(\sqrt{2}, \sqrt{5})(\sqrt{3}) \rightarrow Q(\sqrt{2}, \sqrt{5})(-\sqrt{3})$$

$$\tau_5 = \psi_{\sqrt{5}, -\sqrt{5}} : Q(\sqrt{2}, \sqrt{3})(\sqrt{5}) \rightarrow Q(\sqrt{2}, \sqrt{3})(-\sqrt{5})$$

والمطلوب: أوجد كلاً مما يأتي:

$$\tau_2(\sqrt{3}), \quad \tau_2(\sqrt{2} + \sqrt{3}), \quad \tau_3 \cdot \tau_2(\sqrt{2} + 3\sqrt{5})$$

$$\tau_5 \cdot \tau_3\left(\frac{\sqrt{2} - 3\sqrt{5}}{2\sqrt{3} - \sqrt{2}}\right), \quad \tau_5^2 \cdot \tau_3 \cdot \tau_2(\sqrt{2} + \sqrt{45})$$

$$\tau_3(\tau_5(\sqrt{2} - \sqrt{3}) + \tau_2 \cdot \tau_5(\sqrt{30}))$$

- ٤ - بالعودة إلى التمرين (٣) أثبت أن مرتبة كل من τ_2, τ_3, τ_5 تساوي 2 في الزمرة $G(E/Q)$.

- ٥ - بالعودة إلى التمرين (٣) أوجد الزمرة الجزئية H من الزمرة $G(E/Q)$ المولدة بالعناصر τ_2, τ_3, τ_5 .

- ٦ - بالعودة إلى التمرين (٣) أوجد الحقل المثبت من خلال كل من التماثلات الآتية:

$$\tau_3, \quad \tau_3^2, \quad \tau_2 \cdot \tau_5, \quad \tau_2 \cdot \tau_3 \cdot \tau_5$$

الفصل الثامن

التمديدات الناعظمية

٨ - ١. التمديدات الناعظمية.

تعريف.

ليكن الحقل K تمديداً للحقل F . نقول إن K تمديد ناعظمي للحقل F إذا تحقق:

١ - الحقل K تمديد جبري للحقل F .

٢ - أيّاً كان $a \in K$ فإن K يحوي جميع العناصر المترافقة مع a فوق F .

بالاعتماد على التعريف السابق يمكننا صياغة المبرهنة الآتية:

مبرهنة ٨-١-١.

ليكن الحقل K تمديداً جبرياً للحقل F . الشروط الآتية متكافئة:

١ - الحقل K تمديد ناعظمي للحقل F .

٢ - لأجل أي حدودية أولية $f(x) \in F[x]$ تملك صفراً في K فإن K يحوي حقل التفريق للحدودية $f(x)$ فوق F .

٣ - لأجل أي حدودية أولية $f(x) \in F[x]$ تملك صفراً في K فإن $f(x)$ تتفارق في $K[x]$ إلى مضارب خطية.

البرهان.

(1) $\Leftrightarrow$ (2). لتكن $f(x) \in F[x]$ حدودية أولية ولنفرض أن $a \in K$ صفر للحدودية

$f(x)$ ، عندئذ حسب الفرض فإن K يحوي جميع أصفار الحدودية $f(x)$ لأنها

عناصر مترافقة مثتى مثتى. لنفرض أن $a_1, a_2, \dots, a_n \in K$ هي جميع أصفار الحدودية

$f(x)$ بما فيها a ، لنأخذ الحقل $F(a_1, a_2, \dots, a_n)$ الذي يمثل حقل تفريق الحدودية

$f(x)$ فنجد أن $F(a_1, a_2, \dots, a_n) \subseteq K$.

(2) $\Leftrightarrow$ (3). واضح.

(3) $\Leftrightarrow$ (1). لدينا حسب الفرض أن K تمديد جبري للحقل F . ليكن $a \in K$ ، عندئذ

فإن a هو عنصر جبري فوق F . لنفرض أن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F ، بما أن الحدودية $f(x)$ أولية في $F[x]$ وتملك صفراً $a \in K$ عندئذ حسب الفرض فإن $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية على الشكل الآتي:

$$f(x) = b(x - a_1)(x - a_2) \cdots (x - a_n) = b \prod_{i=1}^n (x - a_i)$$

حيث $a_1, a_2, \dots, a_n \in K$ و $b \in F$. وبما أن العنصر a صفر للحدودية $f(x)$ فإن $a \in \{a_1, a_2, \dots, a_n\}$ وهذا يبين أن العناصر $\{a_1, a_2, \dots, a_n\}$ هي جميع العناصر في K المترافقة مثلي مثلي مع a فوق F ، وحسب التعريف نجد أن K هو تمديد ناظمي منتهي للحقل F .

تمهيدية ٨-١-٢.

ليكن الحقل K تمديداً ناظماً منتهياً للحقل F . عندئذ توجد حدودية $f(x) \in F[x]$ بحيث $\partial f(x) \geq 1$ وأن K حقل تقريق الحدودية $f(x)$ فوق F . البرهان.

لنفرض أن الحقل K تمديد ناظمي منته للحقل F عندئذ حسب المبرهنة (٣-٣-٩) توجد عناصر $a_1, a_2, \dots, a_n \in K$ جبرية فوق F وتحقق $K = F(a_1, a_2, \dots, a_n)$. لنفرض أن $f_i(x) \in F[x]$ هي الحدوديات الأصغرية للعناصر a_i أي $1 \leq i \leq n$. لنضع $f(x) = f_1(x) \cdot f_2(x) \cdots f_n(x) = \prod_{i=1}^n f_i(x)$ فنجد أن $f(x) \in F[x]$ وأن $f(x) \neq 0$ كما أن $\partial f(x) \geq 1$ وأنه أي $1 \leq i \leq n$ فإن a_i هو صفر للحدودية، لأن $f_i(a_i) = 0$ وبالتالي يكون $f(a_i) = 0$. بما أن الحدوديات $f_i(x)$ أولية في $F[x]$ وتملك صفراً في الحقل K وأن الحقل K هو تمديد ناظمي للحقل F فإن الحدوديات $f_i(x)$ تتفرق في $K[x]$ إلى مضاريب خطية وذلك لأجل كل $1 \leq i \leq n$ ، وهذا يبين أن الحدودية $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية ومنه فإن K هو حقل تقريق الحدودية $f(x)$ فوق F .

تمهيدية ٨-١-٣.

ليكن الحقل K تمديداً ناظماً للحقل F . إذا كان L حقلاً جزئياً في K ويحوي F ، عندئذ يكون الحقل K تمديداً ناظماً للحقل L .

البرهان.

لنفرض أن الحقل K تمديد ناظمي للحقل F ، عندئذ يكون K تمديداً جبرياً للحقل F ولما كان $K \supseteq L \supseteq F$ فإنه حسب التمهيدية (٣-٣-١٤) يكون الحقل K تمديداً جبرياً للحقل L . ليكن $a \in K$ وأن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F ، لما كان K تمديداً ناظماً للحقل F فإن K يحوي جميع العناصر المترافقة مع a فوق F والتي عددها m حيث $1 \leq m \leq \partial f(x)$. بما أن كل عنصر مترافق مع a فوق F هو عنصر مترافق مع a فوق L نجد أن الحقل K يحوي جميع العناصر المترافقة مع a فوق L والتي عددها $1 \leq m \leq \partial f(x)$ ، وحسب التعريف نجد أن الحقل K هو تمديد ناظمي للحقل L . ◊

مبرهنة ٨-١-٤.

ليكن الحقل K تمديداً ناظماً منتهياً للحقل F . لنفرض أن $\alpha, \beta \in K$ عنصران مترافقان فوق F . عندئذ يوجد F -تماثل ذاتي $\sigma : K \rightarrow K$ للحقل K لأجله $\sigma(\alpha) = \beta$. البرهان.

لنفرض أن الحقل K تمديد ناظمي منتهي للحقل F ، عندئذ حسب المبرهنة (٨-١-٢) توجد $f(x) \in F[x]$ بحيث $\partial f(x) \geq 1$ وأن K هو حقل تفريق الحدودية $f(x)$ فوق F . من جهة أخرى، بما أن $\alpha, \beta \in K$ فإن K هو حقل تفريق الحدودية $f(x)$ فوق F كل من $F(\alpha), F(\beta)$ ولما كان العنصران α, β مترافقين فوق F فإنه حسب المبرهنة (٧-١-٢) يوجد F -تماثل $\tau : F(\alpha) \rightarrow F(\beta)$ لأجله $\tau(\alpha) = \beta$. بما أن τ هو F -تماثل فإن $f(x)$ هي الحدودية المقابلة للحدودية $f(x)$ وفق التماثل τ وحسب المبرهنة (٧-٢-٥) يوجد تماثل $\sigma : K \rightarrow K$ امتداد للتماثل τ ، وهذا يبين أن σ هو F -تماثل ذاتي للحقل K لأجله $\sigma(\alpha) = \tau(\alpha) = \beta$. ◊

مبرهنة ٨-١-٥.

ليكن الحقل K تمديداً ناظماً منتهياً للحقل F الذي مميزه $p \neq 0$ وليكن $a \in K$. إذا كان $\sigma(a) = a$ وفق أي F -تماثل ذاتي $\sigma : K \rightarrow K$ للحقل K فإن a هو عنصر غير منفصل تماماً فوق F .

البرهان.

ليكن $a \in K$ وأن $\sigma(a) = a$ وفق أي F -تماثل ذاتي $\sigma : K \rightarrow K$ للحقل K . بما أن العنصر a جبري فوق F ، لنفرض أن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F وأن $\partial f(x) = n$. لنفرض أيضاً أن n_0, p^m درجتا عدم انفصالية وانفصالية الحدودية $f(x)$ فوق F على الترتيب. ليكن $b \in K$ عنصراً مترافقاً مع a فوق F ، عندئذ حسب المبرهنة (٨-١-٤) يوجد F -تماثل ذاتي $\sigma : K \rightarrow K$ للحقل K من أجله $\sigma(a) = b$ وحسب الفرض فإن $\sigma(a) = a = b$ وهذا يبين أن عدد جميع عناصر الحقل K المختلفة مثلي ومثلي والمترافقة مع a فوق F يساوي الواحد وحسب المبرهنة (٧-١-٥) فإن $n_0 = 1$. سوف نميز حالتين:

- إذا كانت الحدودية $f(x)$ منفصلة فوق F عندئذ $\partial f(x) = n = n_0 = 1$ وهذا يبين أن $f(x) = x - a$ ومنه فإن $a \in F$ أي أن العنصر a غير منفصل تماماً فوق F .
 - إذا كانت الحدودية $f(x)$ غير منفصلة فوق F عندئذ $\partial f(x) = n = n_0 \cdot p^m = p^m$ وهذا يبين أن $f(x) = (x - a)^{p^m} = x^{p^m} - a^{p^m}$ ومنه فإن $a^{p^m} \in F$ أي أن العنصر a غير منفصل تماماً فوق F . ◊

تمهيدية ٨-١-٦.

ليكن الحقل K تمديداً ناظمياً منتهياً للحقل F وليكن L حقلاً جزئياً في K يحوي F . إذا كان $\tau : L \rightarrow K$ هو F -تماثل، عندئذ يوجد F -تماثل ذاتي $\sigma : K \rightarrow K$ للحقل K امتداداً للتماثل τ .

البرهان.

لنفرض أن الحقل K تمديد ناظمي منتهي للحقل F وأن $F \subseteq L \subseteq K$ ولنفرض أن $\tau : L \rightarrow K$ هو F -تماثل، عندئذ حسب التمهيدية (٨-١-٢) توجد $f(x) \in F[x]$ بحيث $\partial f(x) \geq 1$ وأن K هو حقل تفريق $f(x)$ فوق F ولما كان $F \subseteq L \subseteq K$ فإن K هو حقل تفريق $f(x)$ فوق L ، ولما كانت $f(x)$ هي الحدودية المقابلة للحدودية $f(x)$ وفق التماثل τ فإنه حسب المبرهنة (٧-٢-٥) يوجد F -تماثل ذاتي $\sigma : K \rightarrow K$ للحقل K امتداداً للتماثل τ . ◊

مبرهنة ٧-١-٨.

ليكن F حقلاً و $f(x) \in F[x]$ بحيث $\partial f(x) \geq 1$. إذا كان K هو حقل تفريق $f(x)$ فوق F عندئذ يكون الحقل K تمديداً ناظماً منتهياً للحقل F .

البرهان.

لنفرض أن K هو حقل تفريق $f(x)$ فوق F ، عندئذ فإن $K = F(a_1, a_2, \dots, a_n)$ حيث $a_i \in K$ هي جميع أصفار الحدودية $f(x)$ في K لأجل جميع القيم $1 \leq i \leq n$. ومنه فإن العناصر a_i جبرية فوق F وبالتالي فإن $K = F(a_1, a_2, \dots, a_n)$ هو تمديد منته وجبري للحقل F . لتكن $\varphi(x) \in F[x]$ حدودية أولية في $F[x]$ وأن $\varphi(x)$ تملك صفاً $\alpha \in K$ ولنبرهن على أن $\varphi(x)$ تتفرق في $K[x]$ إلى مضاريب خطية.

لنفرض أن K' هو حقل تفريق الحدودية $\varphi(x)$ فوق K وأن $\beta \in K'$ بحيث $\varphi(\beta) = 0$ ولما كان $\varphi(\alpha) = \varphi(\beta) = 0$ وأن الحدودية $\varphi(x)$ أولية فوق F فإن $\varphi(x)$ هي الحدودية الأصغرية للعنصرين α, β ومنه فإن العنصرين α, β مترافقان فوق الحقل F وحسب المبرهنة (٧-١-٢) يوجد F -تماثل $F(\alpha) \rightarrow F(\beta)$ من أجله $\tau(\alpha) = \beta$. من جهة أخرى، بما أن K هو حقل تفريق $f(x)$ فوق F فإن K هو حقل تفريق $f(x)$ فوق كل من $F(\alpha), F(\beta)$. ولما كانت الحدودية $f(x)$ هي الحدودية المقابلة للحدودية $f(x)$ وفق التماثل τ فإنه حسب المبرهنة (٧-٢-٥) يوجد تماثل $\tau: K \rightarrow K(\beta)$ امتداداً للتماثل τ . ولما كان K حقل تفريق $f(x)$ فوق F فإن $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية، وبفرض أن $\partial f(x) = n$ فإنه بالإمكان كتابة $f(x)$ على الشكل:

$$f(x) = b \cdot (x - a_1) \cdot (x - a_2) \cdot \dots \cdot (x - a_n)$$

حيث $b \in F$ وأن $a_1, a_2, \dots, a_n \in K$ ، وبفرض أن $f(x) = \sum_{i=0}^n c_i x^i$ حيث $c_i \in F$ نجد أن:

$$\sum_{i=0}^n \sigma(c_i) x^i = \sum_{i=0}^n \tau(c_i) x^i = \sum_{i=0}^n c_i x^i = f(x)$$

وهذا يبين أن الحدودية $f(x)$ هي الحدودية المقابلة للحدودية $f(x)$ وفق التماثل σ ومنه فإن:

$$f(x) = \sigma(b) \cdot (x - \sigma(a_1)) \cdot (x - \sigma(a_2)) \cdot \dots \cdot (x - \sigma(a_n)) =$$

$$= b \cdot (x - \sigma(a_1)) \cdot (x - \sigma(a_2)) \cdots (x - \sigma(a_n))$$

وهذا يبين أن $\{\sigma(a_1), \sigma(a_2), \dots, \sigma(a_n)\} = \{a_1, a_2, \dots, a_n\}$ ، ومنه نجد أن:

$$\sigma(K) = F(\sigma(a_1), \sigma(a_2), \dots, \sigma(a_n)) = F(a_1, a_2, \dots, a_n) = K$$

ولما كان $\alpha \in K$ نجد أن $\sigma(\alpha) \in \sigma(K) = K$ وبما أن التماثل σ امتداد للتماثل τ نجد أن $\beta = \tau(\alpha) = \sigma(\alpha) \in K$ ، وهكذا نجد أن صفراً للحدودية $\varphi(x)$ في K' ينتمي إلى الحقل K ولما كان K' هو حقل تفريق الحدودية $\varphi(x)$ فوق K نجد أن $K' = K$ وهذا يبين أن $\varphi(x)$ تتفرق فوق الحقل K إلى مضاريب خطية. مما سبق نجد أن الحقل K هو تمديد ناظمي منته للحقل F . ◊

مبرهنة ٨-١-٨.

ليكن الحقل K تمديداً منتهياً للحقل F . عندئذ يوجد تمديد ناظمي أصغري K' للحقل F يحوي K .
البرهان.

لنفرض أن الحقل K تمديد منته للحقل F وأن $[K:F] = n$ عندئذ توجد عناصر $a_1, a_2, \dots, a_n \in K$ بحيث $K = F(a_1, a_2, \dots, a_n)$ ، ولما كان التمديد K للحقل F منتهياً فإن K هو تمديد جبري للحقل F وبالتالي فإن العناصر $a_1, a_2, \dots, a_n$ هي عناصر جبرية فوق الحقل F . لنفرض أن $f_i(x) \in F[x]$ هي الحدوديات الأصغرية للعناصر a_i فوق F حيث $1 \leq i \leq n$ ، ولنضع:

$$f(x) = f_1(x) \cdot f_2(x) \cdots f_n(x) = \prod_{i=1}^n f_i(x)$$

ولنفرض أن K' هو حقل تفريق الحدودية $f(x)$ فوق K ، عندئذ فإن $K' \subseteq K$ ، فضلاً عن ذلك فإن $f(x)$ تتفرق في $K'[x]$ إلى مضاريب خطية فوق K ومنه فإن:

$$K' = K(b_1, b_2, \dots, b_m)$$

حيث $b_i \in K'$ ، $1 \leq i \leq m$ هي جميع أصفار الحدودية $f(x)$ في K' وبما أن $f_i(a_i) = 0$ أيأ كان $1 \leq i \leq n$ فإن $f(a_i) = 0$ ومنه يكون:

$$\{a_1, a_2, \dots, a_n\} \subseteq \{b_1, b_2, \dots, b_m\}$$

وهكذا نجد أن:

$$K' = K(b_1, b_2, \dots, b_m) = F(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_m) = \\ = F(b_1, b_2, \dots, b_m)$$

وهذا يبين لنا أن K' مولد فوق F بجميع أصفار الحدودية $f(x)$ في K' ومنه فإن K' هو حقل تفريق الحدودية $f(x)$ فوق F . مما سبق نجد أن K' تمديد ناظمي منته للحقل F وأن $K \subseteq K'$.

لنفرض أن K_1 تمديد ناظمي آخر للحقل F وأن $K_1 \subseteq K'$ ولنبرهن على أن $K_1 = K'$. بما أن $f_i(x)$ هي الحدودية الأصغرية للعنصر a_i فوق F حيث $1 \leq i \leq n$ ، عندئذ فإن $f_i(x)$ حدودية أولية في $F[x]$ وأن $f(a_i) = 0$ حيث $a_i \in K_1$ ومنه فإن $f_i(x)$ تنفرد في $K_1[x]$ إلى مضارب خطية وهكذا فإن $a_1, a_2, \dots, a_n \in K_1$ وهكذا نجد أن:

$$K' = F(a_1, a_2, \dots, a_n) \subseteq K_1$$

وبالتالي يكون $K_1 = K'$. ♦

مبرهنة ٨-١-٩.

ليكن الحقل K تمديداً منتهياً للحقل F . الشرط اللازم والكافي كي يكون الحقل K تمديداً ناظماً للحقل F هو أن يتحقق الشرط الآتي:

إذا كان الحقل K' تمديداً للحقل F فإن كل F -تماثل $\sigma: K \rightarrow K'$ يكون F -تماثلاً ذاتياً للحقل K .

البرهان.

لنؤم الشرط. لنفرض أن الحقل K تمديد ناظمي منته للحقل F ولنفرض أيضاً أن K' تمديد للحقل F وأن $\sigma: K \rightarrow K'$ هو F -تماثل. ليكن $a \in K$ ، بما أن الحقل K تمديد منته للحقل F فإن K هو تمديد جبري للحقل F وبالتالي فإن العنصر a جبري فوق F . لنفرض أن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F وأن درجة $f(x)$ تساوي $n \geq 1$ ، عندئذ $f(x) = \sum_{i=0}^n d_i x^i$ حيث $d_i \in F$ وأن $0 \leq i \leq n$. ولما كان $0 = f(a) = \sum_{i=0}^n d_i a^i$ نجد أن:

$$0 = \sigma(0) = \sigma\left(\sum_{i=0}^n d_i a^i\right) = \sum_{i=0}^n \sigma(d_i a^i) = \sum_{i=0}^n \sigma(d_i) \cdot \sigma(a^i) = \\ = \sum_{i=0}^n d_i \cdot (\sigma(a))^i$$

وهذا يبين لنا أن $f(\sigma(a)) = 0$ أي أن $f(x)$ هي أيضاً الحدودية الأصغرية للعنصر $\sigma(a)$ فوق F ، ومنه نجد أن العنصرين $a, \sigma(a)$ مترافقان فوق الحقل F ، ولما كان الحقل K تمديداً ناظماً للحقل F نجد أن $\sigma(a) \in K$ وهكذا نجد أن $\sigma(K) \subseteq K$. من جهة أخرى، بما أن $\partial f(x) = n$ فإن عدد جميع عناصر الحقل K المختلفة مثلي مثلي والمترافقة مع a فوق F بما فيها a أصغر أو يساوي n . لنفرض أن $a = a_1, a_2, \dots, a_m \in K$ حيث $m \leq n$ هي جميع العناصر في K المختلفة مثلي مثلي والمترافقة مع a فوق F عندئذ فإن:

$$\sigma\{a_1, a_2, \dots, a_m\} = \{a_1, a_2, \dots, a_m\}$$

ومنه يوجد $y \in K$ بحيث $\sigma(y) = a = a_1$ وبالتالي يكون $a = \sigma(y) \in \sigma(K)$ وهذا يبين أن $K \subseteq \sigma(K)$ وهكذا نجد أن $\sigma(K) = K$. بما أن $\sigma: K \rightarrow K'$ هو F - تماثل وأن $\sigma(K) = K$ نجد أن $\sigma: K \rightarrow K$ هو F - تماثل ذاتي للحقل K . كفاية الشرط. بما أن K هو تمديد منته للحقل F فإن K هو تمديد جبري للحقل F . لنفرض أن $\alpha \in K$ وأن β عنصر مترافق مع α فوق F . بما أن الحقل K تمديد منتهي للحقل F فإنه حسب المبرهنة (٨-١-٨) يوجد تمديد ناظمي E للحقل F يحوي K . ومنه فإن $\alpha \in E$ ولما كان β عنصراً مترافقاً مع α فوق F فإن $\beta \in E$. أصبح لدينا $\alpha, \beta \in E$ عنصرين مترافقين فوق F وحسب المبرهنة (٨-١-٤) فإنه يوجد F - تماثل ذاتي $\sigma: E \rightarrow E$ للحقل E بحيث $\sigma(\alpha) = \beta$. لنفرض أن $\sigma_1: K \rightarrow E$ هو مقصور σ على K عندئذ فإن σ_1 هو F - تماثل وحسب الفرض فإن $\sigma_1: K \rightarrow K$ يكون F - تماثلاً ذاتياً للحقل K ، ومنه نجد أن $\beta = \sigma(\alpha) = \sigma_1(\alpha) \in K$. مما سبق نجد أن الحقل K جميع العناصر المترافقة مع α فوق F وحسب التعريف يكون الحقل K تمديداً ناظماً منتهياً للحقل F . ◊

مبرهنة ٨-١-١٠.

ليكن F حقلاً مميزه $p \neq 0$ وليكن K تمديداً ناظماً منتهياً للحقل F . إذا كان L تمديداً بسيطاً ومنتهياً للحقل F وكان $F \subseteq L \subseteq K$ وإذا كانت n_0 درجة انفصالية التمديد L فوق F ، عندئذ فإن عدد جميع الـ F - تماثلات المختلفة للحقل L في K يساوي n_0 .

البرهان.

لنفرض أن الحقل L تمديد بسيط ومنته للحقل F عندئذ يوجد $a \in L$ بحيث $L = F(a)$ ، فضلاً عن ذلك فإن L تمديد منتهي للحقل F وبالتالي فإن العنصر a هو عنصر جبري فوق F . لنفرض أن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F وحسب الفرض فإن:

$$[L : F]_s = [F(a) : F]_s = n_0$$

وحسب المبرهنة (١٣-٣-٥) فإن n_0 هي درجة انفصالية $f(x)$ فوق F . من جهة أخرى، بما أن الحقل K تمديد ناظمي للحقل F وأن $f(x) \in F[x]$ حدودية أولية فوق F وتملك صفرًا $a \in K$ فإن $f(x)$ تتفكك في $K[x]$ إلى مضارب خطية وحسب المبرهنة (٦-١-٧) فإن عدد جميع عناصر الحقل K المختلفة مثلي مثلي والمترافقة مع a فوق F بما فيها a يساوي n_0 ، لنفرض أن هذه العناصر هي:

$$a = a_1, a_2, \dots, a_{n_0} \in K$$

بما أن العنصر a_i مترافق مع a فوق F فإنه حسب المبرهنة (٢-١-٧) يوجد تماثل $\tau_i : F(a) \rightarrow F(a_i)$ لأجله $\tau_i(a) = a_i$ وذلك لأجل كل $1 \leq i \leq n_0$ ، ولما كان $L = F(a)$ وأن $L \subseteq K$ فإن $\tau_i : L \rightarrow K$ هو تماثل للحقل L في K وذلك لأجل كل $1 \leq i \leq n_0$. فضلاً عن ذلك، فإن التماثلات $\tau_1, \tau_2, \dots, \tau_{n_0}$ مختلفة مثلي مثلي وذلك لأن العناصر $a_1, a_2, \dots, a_{n_0}$ مختلفة مثلي مثلي. وبما أن الصورة المباشرة للعنصر a وفق أي F -تماثل $\sigma : L \rightarrow K$ للحقل L في K هي عنصر في K ومترافق مع a فوق F أي أن $\sigma(a) \in \{a_1, a_2, \dots, a_{n_0}\}$ نجد أن أي F -تماثل σ للحقل L في K ينتمي إلى المجموعة $\{\tau_1, \tau_2, \dots, \tau_{n_0}\}$ ومنه نجد أن عدد جميع الـ F -تماثلات المختلفة للحقل L في K يساوي فقط يساوي n_0 .

مبرهنة ١١-١-٨.

ليكن F حقلاً مميزه $p \neq 0$ وليكن K تمديداً ناظماً منتهياً للحقل F . إذا كان L تمديداً منتهياً للحقل F بحيث $F \subseteq L \subseteq K$ وإذا كانت n_0 درجة انفصالية التمديد L فوق F ، عندئذ يوجد فقط يوجد n_0 F -تماثل مختلف للحقل L في الحقل K .

البرهان.

لنفرض أن F_0 هو التمديد الجبري المنفصل الأعظمي للحقل F في الحقل L وأن $\bar{F}$ الغلاقة الجبرية للحقل F في L ، عندئذ حسب التعريف يكون:

$$[L : F]_s = [F_0 : F] = n_0$$

البرهان بالاستقراء حسب n_0 .

- إذا كان $n_0 = 1$ عندئذ يكون $[F_0 : F] = 1$ ومنه فإن $F_0 = F$. من جهة أخرى، بما أن الحقل L تمديد منته للحقل F فإن L هو تمديد جبري للحقل F ومنه فإن $L = \bar{F}$ ، وحسب المبرهنة (٥-٣-١٢) بما أن الحقل $\bar{F}$ تمديد جبري غير منفصل تماماً للحقل F_0 نجد أن الحقل L هو تمديد جبري غير منفصل تماماً للحقل F .

ليكن $\sigma : L \rightarrow K$ هو F -تماثل مختلف للحقل L في الحقل K وليكن $a \in L$ ، ولما كان L تمديداً جبرياً غير منفصل تماماً للحقل F ، فإنه يوجد $m \geq 0$ عدد صحيح بحيث يكون $a^{p^m} \in F$ وبالتالي يكون $\sigma(a^{p^m}) = a^{p^m}$ ومنه فإن $(\sigma(a))^{p^m} = a^{p^m}$ أي أن $(\sigma(a))^{p^m} - a^{p^m} = 0$ وبالتالي $(\sigma(a) - a)^{p^m} = 0$ وهذا يبين أن $\sigma(a) = a$. وهكذا نجد أنه يوجد F -تماثل واحد فقط هو σ للحقل L في K معرف بالشكل الآتي: أي أن $a \in L$ فإن $\sigma(a) = a$.

- لنفرض أن $n_0 > 1$ وأن المبرهنة صحيحة لأجل أي عدد $m_0 < n_0$. بما أن $[F_0 : F] = n_0 > 1$ فإنه يوجد $\alpha \in F_0$ وأن $\alpha \notin F$ ، بما أن $\alpha \in F_0$ فإن α عنصر جبري منفصل فوق F وحسب المبرهنة (٥-٣-٧) فإن الحقل $F(\alpha)$ هو تمديد جبري منفصل للحقل F . لنفرض أن F'_0 التمديد الجبري المنفصل الأعظمي للحقل $F(\alpha)$ في L عندئذ يكون $F_0 \subseteq F(\alpha) \subseteq F'_0 \subseteq L$. بما أن F'_0 تمديد جبري منفصل للحقل $F(\alpha)$ وأن الحقل $F(\alpha)$ تمديد جبري منفصل للحقل F فإنه حسب المبرهنة (٥-٣-١٠) يكون الحقل F'_0 تمديداً جبرياً منفصلاً للحقل F ومنه فإن $F'_0 \subseteq F_0$.

من جهة أخرى، بما أن F_0 هو التمديد الجبري المنفصل الأعظمي للحقل F في L فإن الحقل F_0 هو تمديد جبري منفصل للحقل F ولما كان $F \subseteq F(\alpha) \subseteq F_0$ فإنه حسب التمهيدية (٥-٣-٥) فإن F_0 هو تمديد جبري منفصل للحقل $F(\alpha)$ وبالتالي يكون

نفرض أن $[F(\alpha):F] = s$ وأن $[L:F(\alpha)] = r$ وبما أن $F \subseteq F(\alpha) \subseteq F_0$ نجد أن

ومنه فإن $n_0 = r \cdot s$ ، ولما كان $\alpha \notin F$ فإن $r < n_0$ وحسب الفرض الاستقرائي فإنه يوجد فقط يوجد r - تماثل مختلف للحقل L في K .

لنفرض أن $\tau_1, \tau_2, \dots, \tau_r$ هي جميع الـ $F(\alpha)$ -التماثلات المختلفة للحقل L في K ولما كان $F(\alpha)$ تمديداً جبرياً منفصلاً للحقل F فإن $[F(\alpha):F]_s = s$ أي أن:

لنفرض أن $g(x) \in F[x]$ الحدودية الأصغرية للعنصر α فوق F عندئذ حسب المبرهنة (٥-٣-١٣) فإن درجة انفصالية الحدودية $g(x)$ تساوي $[F(\alpha):F]$ ، ولما كان الحقل K تمديداً نظامياً للحقل F فإن $g(x)$ تنفرق في $K[x]$ إلى مضاريب خطية وبالتالي فإن عدد جميع عناصر الحقل K المختلفة مثلي مثلي والمترافقة مع α فوق F يساوي s .

لنفرض أن $\alpha = \alpha_1, \alpha_2, \dots, \alpha_s \in K$ هي جميع عناصر الحقل K المختلفة مثلي مثلي والمترافقة مع α فوق F وحسب المبرهنة (٨-١-٤) فإنه لأجل كل $1 \leq j \leq s$ يوجد $F -$ تماثل ذاتي $\sigma_j : K \rightarrow K$ للحقل K لأجله $\sigma_j(\alpha) = \alpha_j$ ولما كانت العناصر α_j مختلفة مثلي مثلي فإن العناصر σ_j مختلفة مثلي مثلي، حيث $1 \leq j \leq s$.

ولما كان $\tau_i: L \rightarrow K$ هو $F(\alpha)$ -تماثل للحقل L في K وكان $\sigma_j: K \rightarrow K$ هو F -تماثل ذاتي للحقل K لأجل كل $1 \leq i \leq r, 1 \leq j \leq s$ نجد أن كل من التماثلات الآتية:

هو $F(\alpha)$ -تماثل للحقل L في K . فضلاً عن ذلك فإن التماثلات (*) مختلفة متى
 متى، لأنه إذا كان $\sigma_{j_1} \cdot \tau_{i_1} = \sigma_{j_2} \cdot \tau_{i_2}$ حيث $1 \leq j_1, j_2 \leq s, 1 \leq i_1, i_2 \leq r$ عندئذ

يكون $\sigma_{j_1} \cdot \tau_{i_1}(\alpha) = \sigma_{j_2} \cdot \tau_{i_2}(\alpha)$ أي أن $\sigma_{j_1}(\tau_{i_1}(\alpha)) = \sigma_{j_2}(\tau_{i_2}(\alpha))$ ولما كان τ_{i_j} هو $F(\alpha)$ -تماثل نجد أن $\sigma_{j_1}(\alpha) = \sigma_{j_2}(\alpha)$ وهذا يبين أن $\sigma_{j_1} = \sigma_{j_2}$ أي أن $j_1 = j_2$ ، ومنه يكون $\sigma_{j_1} \cdot \tau_{i_1} = \sigma_{j_1} \cdot \tau_{i_2}$ وبالتالي أيأ كان $y \in L$ فإن:

$$\sigma_{j_1} \cdot \tau_{i_1}(y) = \sigma_{j_1} \cdot \tau_{i_2}(y)$$

أي أن $\sigma_{j_1}(\tau_{i_1}(y)) = \sigma_{j_1}(\tau_{i_2}(y))$ ولما كان σ_{j_1} متبايناً نجد أن $\tau_{i_1}(y) = \tau_{i_2}(y)$ أي أن $i_1 = i_2$ ومنه يكون $\tau_{i_1} = \tau_{i_2}$.

ليكن φ هو $F(\alpha)$ -تماثلاً للحقل L في K ، عندئذ فإن $\varphi(\alpha) \in K$ هو عنصر مترافق مع α فوق F ومنه فإن $\varphi(\alpha) \in \{\alpha_1, \alpha_2, \dots, \alpha_s\}$. لنفرض أن $\varphi(\alpha) = \alpha_t$ حيث $1 \leq t \leq s$ عندئذ يكون $\sigma_t^{-1} \cdot \varphi: L \rightarrow K$ هو F -تماثلاً للحقل L في K ، ومنه فإن:

$$\sigma_t^{-1} \cdot \varphi(\alpha) = \sigma_t^{-1}(\varphi(\alpha)) = \sigma_t^{-1}(\alpha_t) = \alpha$$

وذلك لأن $\sigma_t(\alpha) = \alpha_t$ ، وهذا يبين أن $\sigma_t^{-1} \cdot \varphi$ هو $F(\alpha)$ -تماثل للحقل L في K ، ومنه فإن $\sigma_t^{-1} \cdot \varphi \in \{\tau_1, \tau_2, \dots, \tau_r\}$. لنفرض أن $\sigma_t^{-1} \cdot \varphi = \tau_q$ حيث $1 \leq q \leq r$ نجد أن $\varphi = \sigma_t \cdot \tau_q$ وهذا يبين أن $\varphi \in \{\sigma_i \cdot \tau_j : 1 \leq i \leq s, 1 \leq j \leq r\}$ وهكذا نجد أن التماثلات (*) هي جميع الـ F -تماثل المختلفة مثنى مثنى للحقل L في K وأن عددها يساوي $n_0 = r \cdot s$.

اعتماداً على المبرهنة الأخيرة يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً منتهياً للحقل F . إذا كانت n_0 درجة انفصالية التمديد K فوق F ، عندئذ فإن عدد جميع الـ F -تماثلات الذاتية المختلفة للحقل K أصغر أو يساوي n_0 .

البرهان.

بما أن الحقل K تمديد منته للحقل F عندئذ حسب المبرهنة (٨-١-٨) يوجد تمديد ناظمي منته K' للحقل F يحوي K ، أي أن $F \subseteq K \subseteq K'$ ، وحسب المبرهنة (٨-١-٨) فإنه يوجد فقط يوجد n_0 ، F -تماثل مختلف للحقل K في K' ، ولما كان كل

F - تماثل ذاتي للحقل K هو F - تماثل للحقل K في K' فإن عدد جميع الـ F - تماثلات الذاتية المختلفة للحقل K أصغر أو يساوي n_0 .

نتيجة مهمة أخرى يمكننا صياغتها اعتماداً على المبرهنة الأخيرة:

نتيجة.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل K تمديداً ناظمياً منتهياً للحقل F . إذا كانت n_0 درجة انفصالية التمديد K فوق F ، عندئذ يوجد فقط يوجد n_0 ، F - تماثل ذاتي مختلف للحقل K .

البرهان.

لما كان $F \subseteq K \subseteq K$ وأن K هو تمديد منته للحقل F ، وأيضاً K هو تمديد ناظمي منته للحقل F ، فإنه حسب المبرهنة (٨-١-١١) يوجد فقط يوجد n_0 ، F - تماثل ذاتي مختلف للحقل K .

مبرهنة ٨-١-١٢.

ليكن F حقلاً مميزه $p \neq 0$ وليكن الحقل L تمديداً منتهياً للحقل F وأن الحقل K تمديد منته للحقل L . عندئذ:

$$[K : F]_s = [K : L]_s \cdot [L : F]_s$$

$$[K : F]_i = [K : L]_i \cdot [L : F]_i$$

البرهان.

لنفرض أن F_0 التمديد الجبري المنفصل الأعظمي للحقل F في L وأن L_0 التمديد الجبري المنفصل الأعظمي للحقل L في K وأن K_0 التمديد الجبري المنفصل الأعظمي للحقل F في K ، عندئذ يكون $F \subseteq F_0 \subseteq L \subseteq L_0 \subseteq K$.

من جهة أخرى، إن $F_0 \subseteq K_0$ ، لأنه إذا كان $a \in F_0$ فإن $a \in L$ هو عنصر جبري منفصل فوق F ولما كان $L \subseteq K$ فإن $a \in K$ عنصر جبري منفصل فوق F ومنه فإن $a \in K_0$. كما أن $K_0 \subseteq L_0$ ، لأنه إذا كان $b \in K_0$ عندئذ فإن $b \in K$ عنصر جبري منفصل فوق F ومنه فإن $b \in K$ عنصر جبري منفصل فوق L ، ومنه فإن:

$$F \subseteq F_0 \subseteq K_0 \subseteq L_0 \subseteq K$$

وحسب التعريف فإن:

$$\begin{aligned} [K : F]_s &= [K_0 : F] = [K_0 : F_0] \cdot [F_0 : F] = \\ &= [K_0 : F_0] \cdot [L : F]_s \end{aligned}$$

لنبرهن على أن $[K_0 : F_0] = [L_0 : L]$.

لتكن $\{a_1, a_2, \dots, a_n\} \subseteq K_0$ مجموعة جزئية من K_0 ومستقلة خطياً فوق F_0 ، ولما كان $K_0 \subseteq L_0$ فإن $\{a_1, a_2, \dots, a_n\} \subseteq L_0$ مجموعة جزئية من L_0 ومستقلة خطياً فوق L ، لأنه إذا كانت $\{\beta_1, \beta_2, \dots, \beta_n\} \subseteq L$ تحقق $\sum_{i=1}^n \beta_i a_i = 0$ ، ولما كان الحقل L تمديداً منتهياً للحقل F فإن L هو تمديد جبري للحقل F وبالتالي يكون $L = \overline{F}$ حيث أن $\overline{F}$ هي الغلاقة الجبرية للحقل F في L . أصبح لدينا $F \subseteq F_0 \subseteq \overline{F} = L$ وحسب المبرهنة (١٢-٣-٥) فإن L هو تمديد جبري غير منفصل تماماً للحقل F_0 ومنه توجد أعداد صحيحة غير سالبة $r_1, r_2, \dots, r_n$ تحقق $\beta_i^{p^{r_i}} \in F_0$ وذلك لأجل جميع القيم $1 \leq i \leq n$. لنفرض أن $r = \max\{r_1, r_2, \dots, r_n\}$ فنجد أن $\beta_i^{p^r} \in F_0$ وذلك أيضاً كان $1 \leq i \leq n$. ومنه نجد أن $(\sum_{i=1}^n \beta_i a_i)^{p^r} = 0$ أي أن $\sum_{i=1}^n \beta_i^{p^r} a_i^{p^r} = 0$. ولما كانت $\{a_1, a_2, \dots, a_n\}$ مجموعة جزئية في K_0 ومستقلة خطياً فوق F_0 فإن المجموعة $\{a_1^{p^r}, a_2^{p^r}, \dots, a_n^{p^r}\}$ هي مجموعة جزئية في K_0 ومستقلة خطياً فوق F_0 ، وهكذا نجد أن $\beta_i^{p^r} = 0$ أيضاً كان $1 \leq i \leq n$ وبالتالي يكون $\beta_i = 0$ أيضاً كان $1 \leq i \leq n$ ، وهذا يبين أن المجموعة $\{a_1, a_2, \dots, a_n\} \subseteq K_0$ مستقلة خطياً فوق L ومنه يكون:

$$[K_0 : F_0] \leq [L_0 : L]$$

من جهة أخرى، لتكن $\{y_1, y_2, \dots, y_m\} \subseteq L_0$ مجموعة جزئية في L_0 ومستقلة خطياً فوق L ، ولما كان $F \subseteq F_0 \subseteq K_0 \subseteq L_0 \subseteq K$ نجد أن $\{y_1, y_2, \dots, y_m\} \subseteq K$ ، ولما كان الحقل K تمديداً منتهياً للحقل F فإن الحقل K تمديد جبري للحقل F ومنه فإن $K = \overline{K}$ ، حيث $\overline{K}$ الغلاقة الجبرية للحقل F في K وبما أن $F \subseteq K_0 \subseteq K = \overline{K}$ فإنه حسب المبرهنة (١٢-٣-٥) فإن K هو تمديد غير منفصل تماماً للحقل K_0 ومنه توجد أعداد صحيحة غير سالبة $s_1, s_2, \dots, s_m$ بحيث $y_i^{p^{s_i}} \in K_0$ حيث $1 \leq i \leq m$.

لنفرض أن $s = \max\{s_1, s_2, \dots, s_m\}$ فنجد أن $y_i^{p^s} \in K_0$ أيأ كان $1 \leq i \leq n$. ولما كانت $\{y_1, y_2, \dots, y_m\}$ مجموعة جزئية في L_0 ومستقلة خطياً فوق L فإن المجموعة $\{y_1^{p^s}, y_2^{p^s}, \dots, y_m^{p^s}\}$ هي مجموعة جزئية في K_0 ومستقلة خطياً فوق L ولما كان $F_0 \subseteq L$ نجد أن $\{y_1^{p^s}, y_2^{p^s}, \dots, y_m^{p^s}\}$ هي مجموعة جزئية في K_0 ومستقلة خطياً فوق F_0 ، ومنه نجد أن $[L_0 : L] \leq [K_0 : F_0]$ ، وهكذا نجد أن $[K_0 : F_0] = [L_0 : L]$.

وبالتالي يكون $[K_0 : F_0] = [L_0 : L] = [K : L]_s$ ، ومنه فإن:

$$[K : F]_s = [K : L]_s \cdot [L : F]_s$$

أخيراً، بما أن $[K : F] = [K : L] \cdot [L : F]$ نجد أن:

$$[K : F]_s \cdot [K : F]_i = [K : L]_s \cdot [K : L]_i \cdot [L : F]_s \cdot [L : F]_i$$

ومنه يكون $[K : F]_i = [K : L]_i \cdot [L : F]_i$ $\diamond$.

تعريف.

ليكن الحقل K تمديداً ناظمياً منتهياً للحقل F . نقول إن التمديد K الحقل F هو تمديد دائري إذا كانت الزمرة $G(K/F)$ دائرية (دوارة).

مبرهنة ٨-١-١٣.

ليكن الحقل K تمديداً دائرياً للحقل F ولنفرض أن L حقل جزئي في K يحوي F . إذا كان الحقل L تمديداً ناظمياً للحقل F ، عندئذ يكون:

١ - الحقل L هو تمديد دائري للحقل F .

٢ - الحقل K هو تمديد دائري للحقل L .

البرهان.

لنفرض أن الحقل K هو تمديد دائري للحقل F عندئذ يكون الحقل K تمديداً ناظمياً ومنتهياً للحقل F وأن الزمرة $G(K/F)$ تكون دوارة. فضلاً عن ذلك، بما أن L هو حقل جزئي في K يحوي F ، أي أن $F \subseteq L \subseteq K$ فإنه حسب التمهيدية (٨-١-٣) يكون الحقل K هو تمديد ناظمي ومنته للحقل L .

١ - بما أن K هو تمديد منته للحقل F وأن $F \subseteq L \subseteq K$ فإن الحقل L يكون تمديداً

منتهياً للحقل F ، ولدينا أيضاً حسب الفرض أن الحقل L تمديد ناظمي للحقل F .

لنبرهن الآن على أن الزمرة $G(L/F)$ دائرية.

نفرض أن $G(K/F) = \langle \alpha \rangle$ حيث $\alpha \in G(K/F)$ ، ولنفرض أن $\alpha_L : L \rightarrow K$ هو مقصور التماثل α على L . لما كان L هو تمديد ناظمي للحقل F فإنه حسب المبرهنة (٨-١-٩) يكون $\alpha_L : L \rightarrow L$ هو F -تماثل ذاتي للحقل L .

لنبرهن على أن $G(L/F) = \langle \alpha_L \rangle$. لما كان $\alpha_L \in G(L/F)$ نجد أن:

$$\langle \alpha_L \rangle \subseteq G(L/F)$$

ليكن $\tau \in G(L/F)$ عندئذ فإن $\tau : L \rightarrow L$ هو F -تماثل ذاتي للحقل L وبالتالي يكون $\tau : L \rightarrow K$ هو F -تماثل للحقل L في الحقل K ، ولما كان K هو تمديد ناظمي منته للحقل L فإنه حسب التمهيدية (٨-١-٦) يوجد F -تماثل ذاتي $\sigma : K \rightarrow K$ للحقل K امتداد للتماثل τ . ولما كان $G(K/F) = \langle \alpha \rangle$ فإنه يوجد عدد صحيح n بحيث $\sigma = \alpha^n$ ومنه نجد أنه أيّاً كان $y \in L$ فإن:

$$\tau(y) = \sigma(y) = \alpha^n(y) = \alpha_L^n(y)$$

وهذا يبين لنا أن $\tau = \alpha_L^n \in \langle \alpha_L \rangle$ ومنه يكون $G(L/F) \subseteq \langle \alpha_L \rangle$ مما سبق نجد أن:

$$G(L/F) = \langle \alpha_L \rangle$$

وبالتالي تكون الزمرة $G(L/F)$ دائرية. مما سبق وحسب التعريف نجد أن التمديد L للحقل F هو تمديد دائري.

٢ - وجدنا سابقاً أن الحقل K هو تمديد ناظمي ومنته للحقل L . لنبرهن الآن على أن الزمرة $G(K/L)$ دائرية.

ليكن $\tau \in G(K/L)$ عندئذ يكون $\tau : K \rightarrow K$ هو L -تماثل ذاتي للحقل K ولما كان $F \subseteq L$ نجد أن τ هو F -تماثل ذاتي للحقل K أي أن $\tau \in G(K/F)$ وهذا يبين أن $G(K/L) \subseteq G(K/F)$ أي أن الزمرة $G(K/L)$ هي زمرة جزئية من الزمرة $G(K/F)$ ولما كانت الزمرة $G(K/F)$ دائرية فإن الزمرة $G(K/L)$ تكون دائرية أيضاً، مما سبق نجد أن الحقل K هو تمديد دائري للحقل L . ◊

مبرهنة ٨-١-١٤.

ليكن F حقلاً مميزه يساوي الصفر وليكن K حقل تفريق فوق F . لنفرض أن الحقل L تمديد منتهي للحقل F . عندئذ فإن:

١ - الحقل $K \cdot L$ هو حقل تفريق فوق L .

٢ - إذا كان $a \in K$ فإن الحدودية الأصغرية للعنصر a فوق L هي ذاتها الحدودية الأصغرية للعنصر a فوق الحقل $K \cap L$.

٣ - $[K \cdot L : L] = [K : K \cap L]$.

٤ - $[K \cdot L : F] = \frac{[K : F] \cdot [K : F]}{[K \cap L : F]}$.

البرهان.

١ - لنفرض أن K حقل تفريق حدودية ما $h(x) \in F[x]$ فوق F وأن:

$$a_1, a_2, \dots, a_n \in K$$

جميع أصفار الحدودية $h(x)$ في K ، عندئذ يكون $K = F(a_1, a_2, \dots, a_n)$ ومنه نجد:

$$K \cdot L = F(a_1, a_2, \dots, a_n) \cdot L = L(a_1, a_2, \dots, a_n)$$

وأن $h(x) \in F[x] \subseteq L[x]$ ومنه نجد أن الحقل $K \cdot L$ هو حقل تفريق الحدودية $h(x) \in L[x]$ فوق L .

٢ - لما كان K حقل تفريق فوق F وأن $F \subseteq K \cap L \subseteq K$ فإنه حسب التمهيدية (٤-٢-٩) يكون K حقل تفريق فوق $K \cap L$. أيضاً لما كان مميز الحقل F يساوي الصفر وأن K تمديد جبري منته للحقل $K \cap L$ فإنه حسب المبرهنة (٨-١-٧) يكون الحقل K تمديداً ناظمياً للحقل $K \cap L$.

من جهة أخرى، لدينا حسب (١) أن $K \cdot L$ هو حقل تفريق فوق L حيث $L \subseteq K \cdot L$ وبالتالي حسب المبرهنة (٨-١-٧) فإن $K \cdot L$ هو تمديد ناظمي للحقل L .

ليكن $a \in K$ عندئذ فإن a عنصر جبري فوق $K \cap L$ ، لنفرض أن $f(x) \in (K \cap L)[x]$ الحدودية الأصغرية للعنصر a فوق الحقل $K \cap L$.

أيضاً لما كان $a \in K \subseteq K \cdot L$ وأن $K \cdot L$ تمديد جبري للحقل L فإن a عنصر جبري فوق L ، لنفرض أن $g(x) \in L[x]$ الحدودية الأصغرية للعنصر a فوق الحقل L .

ولما كان $f(x) \in (K \cap L)[x] \subseteq L[x]$ وأن $f(a) = 0$ نجد أن $g(x)$ تقسم $f(x)$ في $L[x]$.

لما كان K هو تمديد ناظمي للحقل $K \cap L$ وأن $f(x)$ حدودية أولية فوق $K \cap L$ تملك صفراً $a \in K$ فإنه حسب المبرهنة (٨-١-١) الحدودية $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية ولما كانت $g(x)$ تقسم $f(x)$ فإن $g(x)$ تتفرق في $K[x]$ إلى مضاريب خطية ومنه نجد أن $g(x) \in K[x]$ وبالتالي تكون $g(x) \in (K \cap L)[x]$. ولما كانت $f(x)$ هي الحدودية الأصغرية للعنصر a فوق الحقل $K \cap L$ وأن $g(a) = 0$ نجد أن $f(x)$ تقسم $g(x)$ في $(K \cap L)[x]$ ولما كانت كل منهما أولية نجد أن $f(x) = g(x)$.

٣ - لما كان مميز الحقل F يساوي الصفر وأن K هو حقل تفريق فوق F فإن K هو تمديد ناظمي ومنته للحقل F وحسب المبرهنة (٥-٣-١٤) فإن K هو تمديد بسيط للحقل F ، أي يوجد $\theta \in K$ بحيث $K = F(\theta)$ ومنه يكون:

$$K \cdot L = L \cdot K = L \cdot F(\theta) = L(\theta)$$

لنفرض أن $\lambda(x) \in L[x]$ الحدودية الأصغرية للعنصر θ فوق L فنجد أن:

$$[K \cdot L : L] = [L(\theta) : L] = \partial \lambda(x)$$

من جهة أخرى، لدينا $F \subseteq K \cap L \subseteq K$ ومنه فإن:

$$K = F(\theta) \subseteq (K \cap L)(\theta) \subseteq K(\theta) = K$$

وهذا يبين أن $K = (K \cap L)(\theta)$. لنفرض أن $\mu(x) \in (K \cap L)[x]$ الحدودية الأصغرية للعنصر θ فوق الحقل $K \cap L$ وحسب (٢) فإن $\mu(x) = \lambda(x)$ ومنه نجد:

$$[K \cdot L : L] = [L(\theta) : L] = \partial \lambda(x) = \partial \mu(x) =$$

$$= [(K \cap L)(\theta) : (K \cap L)] = [K : K \cap L]$$

٤ - لما كان $F \subseteq L \subseteq K \cdot L$ فإن:

$$[K \cdot L : F] = [K \cdot L : L] \cdot [L : F]$$

وحسب (٣) لدينا $[K \cdot L : L] = [K : K \cap L]$ ومنه يكون:

$$[K \cdot L : F] = [K : K \cap L] \cdot [L : F]$$

أيضاً لما كان $F \subseteq K \cap L \subseteq K$ فإن:

$$[K:F] = [K:K \cap L] \cdot [K \cap L:F]$$

ومنه فإن $[K:K \cap L] = \frac{[K:F]}{[K \cap L:F]}$ وهكذا نجد أن:

$$[K \cdot L:F] = [K:K \cap L] \cdot [L:F] = \frac{[K:F] \cdot [L:F]}{[K \cap L:F]}$$

وهو المطلوب. ◊

مبرهنة ٨-١-١٥.

ليكن الحقل K تمديداً منتهياً للحقل F . إذا كان $[K:F] = 2$ عندئذ فإن K هو تمديد ناظمي للحقل F .

البرهان.

لما كان الحقل K تمديداً منتهياً للحقل F فإن الحقل K هو تمديد جبري للحقل F . ليكن $a \in K$ ولنفرض أن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F ، عندئذ فإن $[F(a):F] = \partial f(x)$ ولما كان $F \subseteq F(a) \subseteq K$ يكون:

$$[K:F] = [K:F(a)] \cdot [F(a):F]$$

ومنه نجد أن:

$$\partial f(x) = [F(a):F] \leq [K:F] = 2$$

وهذا يبين لنا أنه إما $\partial f(x) = 1$ أو $\partial f(x) = 2$.

- إذا كانت $\partial f(x) = 1$ ولما كان $f(a) = 0$ نجد أن $f(x) = x - a$ وهذا يبين أن $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية وبالتالي الحقل K هو تمديد ناظمي للحقل F .

- لنفرض أن $\partial f(x) = 2$ عندئذ بما أن a هو صفر للحدودية $f(x)$ فإن $x - a$ تقسم $f(x)$ في $K[x]$ ومنه توجد $g(x) \in K[x]$ بحيث $f(x) = (x - a) \cdot g(x)$. وهنا نميز حالتين: $g(a) = 0$, $g(a) \neq 0$.

إذا كان $g(a) = 0$ عندئذ يكون a صفرًا مضاعفًا للحدودية $f(x)$ ، ومنه فإن K يحوي جميع أصفار الحدودية $f(x)$.

لنفرض أن $g(a) \neq 0$. لما كانت $\partial f(x) = 2$ نجد أن $\partial g(x) = 1$ ومنه فإن
 $g(x) = b_1x + b_0$ حيث $b_1, b_0 \in K$ وأن $b_1 \neq 0$. لنضع $a_0 = -b_0 \cdot b_1^{-1} \in K$ فنجد
أن $a_0 \in K$ وأن $g(a_0) = 0$ ومنه يكون $f(a_0) = 0$ وهذا يبين أن الحقل K يحوي
جميع أصفار الحدودية $f(x)$ وحسب التعريف يكون الحقل K تمديداً ناظمياً للحقل
 F . $\diamond$



٨ - ٢. تمديدات غالوا.

تعريف.

ليكن الحقل K تمديداً جبرياً للحقل F . نقول إن K هو تمديد غالوا للحقل F إذا كان الحقل K تمديداً ناظمياً ومنفصلاً للحقل F .

اعتماداً على التعريف السابق يمكننا صياغة التمهيدية الآتية:

تمهيدية ٨-٢-١.

ليكن F حقلاً مميزه $p \neq 0$. إذا كان الحقل K تمديداً ناظمياً منتهياً للحقل F ، عندئذ تكون الزمرة $G(K/F)$ منتهية.

البرهان.

لنفرض أن الحقل K تمديد ناظمي منته للحقل F وأن n_0 هي درجة انفصالية K فوق F ، عندئذ حسب النتيجة الثانية للمبرهنة (٨-١-١١) فإنه يوجد فقط يوجد n_0 - F تماثل مختلف للحقل K ، أي أن مرتبة الزمرة $G(K/F)$ يساوي n_0 وبالتالي تكون الزمرة $G(K/F)$ منتهية. ◊

تمهيدية ٨-٢-٢.

ليكن K حقلاً وأن $G = \text{Aut}(K)$ زمرة التماثلات الذاتية للحقل K . لنفرض أن H زمرة جزئية في G ، عندئذ فإن المجموعة:

$$F(H) = \{a : a \in K; \sigma(a) = a, \forall \sigma \in H\}$$

تشكل حقلاً جزئياً في K .

البرهان.

بما أنه لأجل كل $\sigma \in H$ فإن $\sigma(0) = 0$, $\sigma(1) = 1$ نجد أن $0, 1 \in F(H)$ وهذا يبين أن $F(H)$ هي مجموعة جزئية في K غير خالية.

ليكن $a, b \in F(H)$ عندئذ أياً كان $\sigma \in H$ فإن $\sigma(a) = a$, $\sigma(b) = b$ ومنه فإن:

$$\sigma(a - b) = \sigma(a) - \sigma(b) = a - b$$

ومنه فإن $a - b \in F(H)$ إذا كان $b \neq 0$ عندئذ يكون:

$$\sigma(a \cdot b^{-1}) = \sigma(a) \cdot \sigma(b^{-1}) = \sigma(a) \cdot (\sigma(b))^{-1} = a \cdot b^{-1}$$

أي أن $a \cdot b^{-1} \in F(H)$ مما سبق نستنتج أن $F(H)$ حقل جزئي في K . ◊

تعريف.

لنفرض أن K حقل وأن $G = \text{Aut}(K)$. لتكن H زمرة جزئية من الزمرة G . نسمي الحقل $F(H)$ بحقل الزمرة H غير المتغير.

تمهيدية ٨-٢-٣.

ليكن F حقلاً مميزه $p \neq 0$. إذا كان الحقل K تمديد غالوا منتهياً للحقل F ، عندئذ لأجل أي حقل جزئي L في K يحوي F يكون $L = F(G(K/L))$.

البرهان.

لنفرض أن الحقل K تمديد غالوا منتهياً للحقل F وأن L حقل جزئي في K يحوي F ، أي أن $F \subseteq L \subseteq K$. عندئذ أيّاً كان $\sigma \in G(K/L)$ فإن σ هو L -تماثل ذاتي للحقل K ومنه أيّاً كان $y \in L$ فإن $\sigma(y) = y$ وهذه تبين أن $y \in F(G(K/L))$ ، ومنه نجد أن $L \subseteq F(G(K/L))$.

ليكن $a \in F(G(K/L))$ عندئذ $a \in K$ ، لما كان الحقل K تمديداً منفصلاً للحقل F وأن $F \subseteq L \subseteq K$ ، فإنه حسب التمهيدية (٥-٣-٥) يكون K تمديداً منفصلاً للحقل L . من جهة أخرى، لما كان K تمديد غالوا منتهياً للحقل F ، فإن K تمديد ناظمي منته للحقل F ، وحسب التمهيدية (٨-١-٦) فإن K تمديد ناظمي منته للحقل L ، فضلاً عن ذلك فإن $\sigma(a) = a$ وذلك أيّاً كان $\sigma \in G(K/L)$ ، وحسب المبرهنة (٨-١-٥) فإن a هو عنصر غير منفصل تماماً فوق L ، مما سبق نجد أن $a \in L$ وبالتالي يكون $L = F(G(K/L))$ ، ومنه فإن $L = F(G(K/L))$. ◊

ليكن F حقلاً مميزه $p \neq 0$ ولنفرض أن الحقل K تمديد غالوا منته للحقل F . لنفرض أيضاً أن $\mathcal{K}'$ هي مجموعة كل الحقول الجزئية L في K التي كل منها يحوي F وأن $\mathcal{K}$ هي مجموعة كل الزمر الجزئية في الزمرة $G(K/F)$. العلاقة بين المجموعتين

$\mathfrak{I}$ و $\mathfrak{I}'$ تبينها لنا المبرهنة الآتية:

مبرهنة ٨-٢-٤.

ليكن F حقلاً مميزه $p \neq 0$ ولنفرض أن الحقل K تمديد غالوا منته للحقل F . يوجد تطبيق متباين وغامر (تقابل) $f : \mathfrak{I}' \rightarrow \mathfrak{I}$ معرف بالشكل الآتي: أيًا كان $L \in \mathfrak{I}'$ فإن:

$$f(L) = G(K/L)$$

البرهان.

لنبرهن على أن العلاقة $\mathfrak{I}' \rightarrow \mathfrak{I} : f$ المعرفة بالشكل الآتي: أيًا كان $L \in \mathfrak{I}'$ فإن $f(L) = G(K/L)$ تطبيقاً. ليكن $L_1, L_2 \in \mathfrak{I}'$ بحيث $L_1 = L_2$ عندئذ فإن:

$$G(K/L_1) = G(K/L_2)$$

أي أن $f(L_1) = f(L_2)$ ، ومنه فإن f تطبيق وهو أيضاً متباين، لأنه إذا كان $f(L_1) = f(L_2)$ فإن $G(K/L_1) = G(K/L_2)$ وحسب المبرهنة (٨-٢-٣) يكون:

$$L_1 = F(G(K/L_1)) = F(G(K/L_2)) = L_2$$

لنبرهن على أن f غامر. لنكن $H \in \mathfrak{I}$ أي أن H زمرة جزئية من الزمرة $G(K/F)$ وحسب التمهيدية (٨-٢-٢) فإن $F(H)$ هو حقل جزئي في K ، فضلاً عن ذلك فإن الحقل $F(H)$ يحوي F ، لأنه أيًا كان $a \in F$ فإن $\sigma(a) = a$ أيًا كان $\sigma \in G(K/L)$ لنضع $E = F(H)$ فنجد أن $E \in \mathfrak{I}'$.

من جهة أخرى، نلاحظ أنه أيًا كان $\tau \in H$ فإن $\tau : K \rightarrow K$ هو F -تماثل ذاتي للحقل K ويحقق أيًا كان $y \in E = F(H)$ فإن $\tau(y) = y$ وهذا يبين أن τ هو E -تماثل ذاتي للحقل K ومنه فإن $H \subseteq G(K/E)$.

من جهة ثانية، بما أن الحقل K هو تمديد غالوا منته للحقل F فإن K هو تمديد ناظمي منته للحقل F ، وحسب نتيجة المبرهنة (٨-١-١١) فإن الزمرة $G(K/F)$ منتهية وبالتالي تكون الزمرة الجزئية H منتهية. لنفرض أن $(H : 1) = n$ وأن $H = \{\tau_1, \tau_2, \dots, \tau_n\}$ ولنأخذ الحقل $K^n = (a_1, a_2, \dots, a_n)$ حيث $a_i \in K$ أيًا كان $1 \leq i \leq n$ بالنسبة لعمليتي جمع وضرب المركبات، فنجد أن K^n فضاء متجهي فوق الحقل K وأن $[K^n : K] = n$ فضلاً عن ذلك فإن المجموعة $S = \{e_1, e_2, \dots, e_n\} \subset K^n$ حيث أيًا كان $1 \leq i \leq n$ فإن:

$$e_i = (0, \dots, 0, \underset{i}{1}, 0, \dots, 0)$$

قاعدة للفضاء K^n فوق K ، ومنه فإن أي مجموعة جزئية من K^n ومؤلفة من $n+1$ عنصراً تكون مرتبطة خطياً فوق K .

لنبرهن على أن أي مجموعة جزئية من K ومؤلفة من $n+1$ عنصراً تكون مرتبطة خطياً فوق E . لتكن $S' = \{y_1, y_2, \dots, y_{n+1}\} \subset K$ مجموعة جزئية من K ومؤلفة من $n+1$ عنصر:

- إذا كان أحد عناصر المجموعة S' يساوي الصفر عندئذ تكون المجموعة S' مرتبطة خطياً فوق E .

- لنفرض أن جميع عناصر المجموعة S' مختلفة عن الصفر. لنضع:

$$v_j = (\tau_1(y_j), \tau_2(y_j), \dots, \tau_n(y_j))$$

لأجل كل $1 \leq j \leq n+1$ ، فنجد أن المجموعة:

$$S'' = \{v_1, v_2, \dots, v_n, v_{n+1}\} \subset K^n$$

مجموعة جزئية من K^n ومؤلفة من $n+1$ وبالتالي فهي مرتبطة خطياً فوق K ومنه توجد عناصر $c_1, c_2, \dots, c_n, c_{n+1} \in K$ ليست جميعها معدومة لأجلها $\sum_{i=1}^{n+1} c_i \cdot v_i = 0$ ومنه فإن:

$$c_1 \cdot v_1 + c_2 \cdot v_2 + \dots + c_n \cdot v_n + c_{n+1} \cdot v_{n+1} = 0$$

$$c_1 \cdot (\tau_1(y_1), \tau_2(y_1), \dots, \tau_n(y_1)) +$$

$$c_2 \cdot (\tau_1(y_2), \tau_2(y_2), \dots, \tau_n(y_2)) +$$

.....

$$c_{n+1} \cdot (\tau_1(y_{n+1}), \tau_2(y_{n+1}), \dots, \tau_n(y_{n+1})) = (0, 0, \dots, 0)$$

وهكذا نجد أن:

$$c_1 \cdot \tau_1(y_1) + c_2 \cdot \tau_1(y_2) + \dots + c_{n+1} \cdot \tau_1(y_{n+1}) = 0$$

$$c_1 \cdot \tau_2(y_1) + c_2 \cdot \tau_2(y_2) + \dots + c_{n+1} \cdot \tau_2(y_{n+1}) = 0$$

.....

$$c_1 \cdot \tau_n(y_1) + c_2 \cdot \tau_n(y_2) + \dots + c_{n+1} \cdot \tau_n(y_{n+1}) = 0$$

وبالتالي يكون $\sum_{j=1}^{n+1} c_j \cdot \tau_i(y_j) = 0$ وأن $1 \leq i \leq n$.

لنفرض أن M_0 هي أسرة المجموعات الجزئية $\{a_1, a_2, \dots, a_{n+1}\}$ من عناصر الحقل K غير المعدومة جميعها والتي لأجلها $\sum_{j=1}^{n+1} a_j \cdot \tau_i(y_j) = 0$ حيث $1 \leq i \leq n$. واضح أن المجموعة M_0 غير خالية، لأن $\{c_1, c_2, \dots, c_{n+1}\} \in M_0$.

لنأخذ أيضاً المجموعة M_1 المؤلفة من الأعداد الطبيعية r حيث $1 \leq r \leq n+1$ والتي لأجلها توجد مجموعة $\{b_1, b_2, \dots, b_{n+1}\} \in M_0$ بحيث يكون r هو عدد العناصر المختلفة عن الصفر في المجموعة $\{b_1, b_2, \dots, b_{n+1}\}$. واضح أن المجموعة M_1 ليست خالية لأن المجموعة M_0 ليست خالية، ولما كانت $\phi \neq M_1 \subset N$ فإن M_1 تحوي عنصراً أصغر وليكن t . بما أن $t \in M_1$ فإنه توجد مجموعة $\{d_1, d_2, \dots, d_{n+1}\} \in M_0$ بحيث أن عدد العناصر المغايرة للصفر فيها يساوي t ، لنفرض أن هذه العناصر هي $d_{l_1}, d_{l_2}, \dots, d_{l_t}$ عندئذ يكون $\sum_{j=1}^{n+1} d_j \cdot \tau_i(y_j) = 0$ حيث $1 \leq i \leq n$ ، أي أن:

$$d_1 \cdot \tau_i(y_1) + d_2 \cdot \tau_i(y_2) + \dots + d_{n+1} \cdot \tau_i(y_{n+1}) = 0 \quad \forall 1 \leq i \leq n$$

ومنه نجد أن:

$$d_{l_1} \cdot \tau_i(y_{l_1}) + d_{l_2} \cdot \tau_i(y_{l_2}) + \dots + d_{l_t} \cdot \tau_i(y_{l_t}) = 0 \quad \forall 1 \leq i \leq n$$

ولما كان $d_{l_i} \in K$ ينتج أن:

$$\tau_i(y_{l_1}) + (d_{l_1}^{-1} d_{l_2}) \cdot \tau_i(y_{l_2}) + (d_{l_1}^{-1} d_{l_3}) \cdot \tau_i(y_{l_3}) + \dots + (d_{l_1}^{-1} d_{l_t}) \cdot \tau_i(y_{l_t}) = 0$$

وذلك أيّاً كان $1 \leq i \leq n$.

لنبرهن على أن $\tau_i(d_{l_1}^{-1} d_{l_s}) = d_{l_1}^{-1} d_{l_s}$ وذلك أيّاً كان $1 \leq i \leq n$, $2 \leq s \leq t$

بالعودة إلى المساواة الأخيرة، وبأخذ الصورة المباشرة لها وفق التماثل τ_1 نجد أن:

$$\tau_1(\tau_i(y_{l_1}) + (d_{l_1}^{-1} d_{l_2}) \cdot \tau_i(y_{l_2}) + (d_{l_1}^{-1} d_{l_3}) \cdot \tau_i(y_{l_3}) + \dots + (d_{l_1}^{-1} d_{l_t}) \cdot \tau_i(y_{l_t})) = 0$$

ومنه فإن:

$$(\tau_1 \cdot \tau_i)(y_{l_1}) + \tau_1(d_{l_1}^{-1} d_{l_2}) \cdot (\tau_1 \cdot \tau_i)(y_{l_2}) + \tau_1(d_{l_1}^{-1} d_{l_3}) \cdot (\tau_1 \cdot \tau_i)(y_{l_3}) + \dots + \tau_1(d_{l_1}^{-1} d_{l_t}) \cdot (\tau_1 \cdot \tau_i)(y_{l_t}) = 0$$

ولما كان $\tau_1 \in H = \{\tau_1, \tau_2, \dots, \tau_n\}$ نجد أن:

$$\{\tau_1 \cdot \tau_1, \tau_1 \cdot \tau_2, \dots, \tau_1 \cdot \tau_n\} = \{\tau_1, \tau_2, \dots, \tau_n\}$$

لنفرض أن $\tau_1 \cdot \tau_i = \tau_\lambda$ حيث $1 \leq \lambda \leq n$ فنجد أن:

$$\begin{aligned} \tau_\lambda(y_{l_1}) + \tau_1(d_{l_1}^{-1}d_{l_2}) \cdot \tau_\lambda(y_{l_2}) + \tau_1(d_{l_1}^{-1}d_{l_3}) \cdot \tau_\lambda(y_{l_3}) + \dots + \\ + \tau_1(d_{l_1}^{-1}d_{l_t}) \cdot \tau_\lambda(y_{l_t}) = 0 \end{aligned}$$

وهكذا نجد أن:

$$\begin{aligned} \tau_\lambda(y_{l_1}) + \tau_1(d_{l_1}^{-1}d_{l_2}) \cdot \tau_\lambda(y_{l_2}) + \tau_1(d_{l_1}^{-1}d_{l_3}) \cdot \tau_\lambda(y_{l_3}) + \dots + \tau_1(d_{l_1}^{-1}d_{l_t}) \cdot \tau_\lambda(y_{l_t}) = \\ = \tau_\lambda(y_{l_1}) + (d_{l_1}^{-1}d_{l_2}) \cdot \tau_\lambda(y_{l_2}) + (d_{l_1}^{-1}d_{l_3}) \cdot \tau_\lambda(y_{l_3}) + \dots + (d_{l_1}^{-1}d_{l_t}) \cdot \tau_\lambda(y_{l_t}) \end{aligned}$$

ومنه فإن:

$$\begin{aligned} (\tau_1(d_{l_1}^{-1}d_{l_2}) - d_{l_1}^{-1}d_{l_2}) \cdot \tau_\lambda(y_{l_2}) + (\tau_1(d_{l_1}^{-1}d_{l_3}) - d_{l_1}^{-1}d_{l_3}) \cdot \tau_\lambda(y_{l_3}) + \dots + \\ + (\tau_1(d_{l_1}^{-1}d_{l_t}) - d_{l_1}^{-1}d_{l_t}) \cdot \tau_\lambda(y_{l_t}) = 0 \end{aligned}$$

ولما كان t أصغر عدد صحيح موجب في M_1 نجد أن:

$$\tau_1(d_{l_1}^{-1}d_{l_s}) - d_{l_1}^{-1}d_{l_s} = 0 \quad \forall 2 \leq s \leq t$$

$$\tau_1(d_{l_1}^{-1}d_{l_s}) = d_{l_1}^{-1}d_{l_s} \quad \forall 2 \leq s \leq t$$

بهذا الشكل نكون قد أثبتنا أن كل مجموعة جزئية من K ومؤلفة من $n+1$ عنصراً تكون مرتبطة خطياً فوق E وهذا يبين أن $[K : E] \leq n$.

لنفرض أن E_0 التمديد الجبري المنفصل الأعظمي للحقل E في K ، عندئذ يكون:

$$F \subseteq E \subseteq E_0 \subseteq K$$

بما أن K هو تمديد غالوا للحقل F فإن K هو تمديد منفصل للحقل F وحسب التمهيدية (٥-٣-٥) يكون K تمديد منفصل للحقل E وهذا يبين أن $K = E_0$. لنفرض أن n_0 هي درجة انفصالية الحقل K فوق E عندئذ يكون $[E_0 : E] = n_0$ ومنه يكون $[K : E] = n_0$ وحسب النتيجة الثانية للمبرهنة (٨-١-١١) فإنه يوجد فقط يوجد n_0 ، E -تماثل ذاتي مختلف للحقل K وبالتالي تكون مرتبة الزمرة $G(K/E)$ تساوي n_0 ، ومنه فإن:

$$(G(K/E) : 1) \leq n = (H : 1)$$

ولما كانت H زمرة جزئية من الزمرة $G(K/E)$ نجد أن:

$$(H : 1) \leq (G(K/E) : 1)$$

وهكذا نجد أن $(G(K/E) : 1) = (H : 1)$ وبالتالي تكون $G(K/E) = H$ ومنه فإن:

$$f(E) = G(K/E) = H$$

مما سبق نجد أن التطبيق f غامر. ◊

مبرهنة ٨-٢-٥.

ليكن F حقلاً مميزه $p \neq 0$ ولنفرض أن الحقل K تمديد غالوا لمنتها للحقل F . إذا كان

L حقلاً جزئياً في K يحوي F ، أي أن $F \subseteq L \subseteq K$ ، عندئذ فإن:

١ - أيأ كان $\tau \in G(K/F)$ فإن $\tau(L)$ هو حقل جزئي في K ويحقق:

$$G(K/\tau(L)) = \tau \cdot G(K/L) \cdot \tau^{-1}$$

٢ - الشرط اللازم والكافي كي يكون الحقل L تمديداً ناظمياً للحقل F هو أن تكون

الزمرة الجزئية $G(K/L)$ ناظمية في الزمرة $G(K/F)$.

٣ - إذا كانت الزمرة الجزئية $G(K/L)$ ناظمية في الزمرة $G(K/F)$ ، عندئذ فإن:

$$G(K/F)/G(K/L) \cong G(L/F)$$

البرهان.

١ - ليكن $\tau \in G(K/F)$ أي أن $\tau : K \rightarrow K$ هو F -تماثل ذاتي للحقل K وأن:

$$\tau(L) = \{\tau(y) : \forall y \in L\} \subseteq K$$

بما أن $0, 1 \in L$ نجد أن $0 = \tau(0) \in \tau(L)$ ، $1 = \tau(1) \in \tau(L)$ ، أي أن مجموعة

جزئية في K غير خالية وتحوي عنصرين مختلفين.

ليكن $a, b \in \tau(L)$ عندئذ يوجد $a_1, b_1 \in L$ بحيث $a = \tau(a_1)$ ، $b = \tau(b_1)$ ومنه فإن:

$$a - b = \tau(a_1) - \tau(b_1) = \tau(a_1 - b_1) \in \tau(L)$$

بفرض أن $b \neq 0$ عندئذ يكون $b_1 \neq 0$ وأن:

$$a \cdot b^{-1} = \tau(a_1) \cdot (\tau(b_1))^{-1} = \tau(a_1) - \tau(b_1^{-1}) = \tau(a_1 \cdot b_1^{-1}) \in \tau(L)$$

وهذا يبين أن $\tau(L)$ حقلاً جزئياً في K .

ليكن $\varphi \in G(K/\tau(L))$ عندئذ فإن $\varphi : K \rightarrow K$ هو $\tau(L)$ -تماثل ذاتي للحقل K ،

ومنه أيأ كان $y \in L$ فإن $\tau(y) \in \tau(L)$ وبالتالي يكون $\varphi(\tau(y)) = \tau(y)$ ، ومنه فإن:

$$\tau^{-1}(\varphi(\tau(y))) = \tau^{-1}(\tau(y)) = y$$

أي أن $y = \tau^{-1} \cdot \varphi \cdot \tau(y)$ وهذا يبين أن $\tau^{-1} \cdot \varphi \cdot \tau : K \rightarrow K$ هو L -تماثل ذاتي للحقل K وبالتالي فإن $\tau^{-1} \cdot \varphi \cdot \tau \in G(K/L)$. لنفرض أن $\tau^{-1} \cdot \varphi \cdot \tau = \lambda$ حيث $\lambda \in G(K/L)$ فنجد أن $\varphi = \tau \cdot \lambda \cdot \tau^{-1} \in \tau \cdot G(K/L) \cdot \tau^{-1}$ وهكذا نجد أن:

$$G(K/\tau(L)) \subseteq \tau \cdot G(K/L) \cdot \tau^{-1}$$

ليكن $\psi \in \tau \cdot G(K/L) \cdot \tau^{-1}$ عندئذ يوجد $\sigma \in G(K/L)$ بحيث $\psi = \tau \cdot \sigma \cdot \tau^{-1}$ ومنه فإن $\psi : K \rightarrow K$ هو L -تماثل ذاتي للحقل K ، فضلاً عن ذلك، أيًا كان $y \in \tau(L)$ فإنه يوجد $z \in L$ بحيث $y = \tau(z)$ ، ومنه فإن:

$$\psi(y) = \psi(\tau(z)) = \tau \cdot \sigma \cdot \tau^{-1}(\tau(z)) = \tau \cdot \sigma(\tau^{-1}(\tau(z))) = \tau \cdot \sigma(z)$$

ولما كان σ هو L -تماثلاً ذاتياً للحقل K نجد أن:

$$\psi(y) = \tau \cdot \sigma(z) = \tau(\sigma(z)) = \tau(z) = y$$

وهكذا نجد أن ψ هو $\tau(L)$ -تماثل ذاتي للحقل K ، أي أن $\psi \in G(K/\tau(L))$ ومنه $\tau \cdot G(K/L) \cdot \tau^{-1} \subseteq G(K/\tau(L))$ مما سبق نستنتج أن:

$$G(K/\tau(L)) = \tau \cdot G(K/L) \cdot \tau^{-1}$$

٢ - نعلم أن كلا من $G(K/L)$ و $G(K/F)$ هي زمرة بالنسبة لعملية تركيب التطبيقات ولما كان $F \subseteq L$ فإن كل L -تماثل ذاتي للحقل K هو F -تماثل ذاتي للحقل K أي أن $G(K/L) \subseteq G(K/F)$ وهذا يبين أن $G(K/L)$ زمرة جزئية في الزمرة $G(K/F)$. لزوم الشرط. لنفرض أن L هو تمديد ناظمي للحقل F ولنبرهن على أن:

$$G(K/L) = \mu \cdot G(K/F) \cdot \mu^{-1}$$

وذلك أيًا كان $\mu \in G(K/F)$.

ليكن $\mu \in G(K/F)$ عندئذ حسب (١) فإن:

$$G(K/\mu(L)) = \mu \cdot G(K/L) \cdot \mu^{-1} \quad (*)$$

من جهة أخرى، بما أن $\mu : K \rightarrow K$ هو F -تماثل ذاتي للحقل K ولما كان $L \subseteq K$ نجد أن $\mu : L \rightarrow K$ هو F -تماثل للحقل L في K ، ولما كان K تمديد منته للحقل F وأن $F \subseteq L \subseteq K$ فإن L هو تمديد منته للحقل F ، فضلاً عن ذلك فإن L هو

تمديد ناظمي للحقل F وحسب المبرهنة (٨-١-٩) فإن $\mu: L \rightarrow K$ يكون F -تماثلاً ذاتياً للحقل L ، أي أن $\mu: L \rightarrow L$ وبالتالي فإن $\mu(L) = L$ بالتعويض في (*) نجد:

$$G(K/L) = \mu \cdot G(K/L) \cdot \mu^{-1}$$

وهذا يبين أن الزمرة الجزئية $G(K/L)$ ناظمية في الزمرة $G(K/F)$. كفاية الشرط. لنفرض أن الزمرة الجزئية $G(K/L)$ ناظمية في الزمرة $G(K/F)$ ، عندئذ أياً كان $\varepsilon \in G(K/F)$ فإن $G(K/L) = \varepsilon \cdot G(K/L) \cdot \varepsilon^{-1}$. فضلاً عن ذلك، حسب (١) لدينا $G(K/\varepsilon(L)) = \varepsilon \cdot G(K/L) \cdot \varepsilon^{-1}$ ومنه نجد أن:

$$G(K/\varepsilon(L)) = G(K/L)$$

ولما كان K هو تمديد غالوا منته للحقل F وأن $F \subseteq L \subseteq K$ فإنه حسب المبرهنة (٨-٢-٣) يكون:

$$\varepsilon(L) = F(G(K/\varepsilon(L))) = F(G(K/L)) = L$$

أي أن $\varepsilon(L) = L$ وذلك أياً كان $\varepsilon \in G(K/F)$.

من جهة أخرى، ليكن $\varphi_1: L \rightarrow K$ هو F -تماثل للحقل L في K ، بما أن K هو تمديد غالوا منته للحقل F فإن K هو تمديد ناظمي منته للحقل F وأن $F \subseteq L \subseteq K$ وحسب التمهيدية (٨-١-٦) فإنه يوجد F -تماثل ذاتي $\varepsilon_1: K \rightarrow K$ للحقل K امتداداً للتماثل φ_1 ، وهذا يبين أن $\varepsilon_1 \in G(K/F)$ ومنه فإن $\varepsilon_1(L) = L$ وبالتالي يكون:

$$L = \varepsilon_1(L) = \varphi_1(L)$$

وهذا يبين أن $\varphi_1: L \rightarrow L$ هو F -تماثل ذاتي للحقل L وحسب المبرهنة (٨-١-٩) يكون الحقل L تمديداً ناظمياً للحقل F .

٣ - لنفرض أن الزمرة الجزئية $G(K/L)$ ناظمية في الزمرة $G(K/F)$ ، عندئذ حسب (٢) يكون الحقل L تمديداً ناظمياً للحقل F ولما كان $F \subseteq L \subseteq K$ وأن K تمديد منته للحقل F نجد أن L تمديد منته للحقل F ومنه فإن L هو تمديد ناظمي منته للحقل F . لنعرف العلاقة $f: G(K/F) \rightarrow G(L/F)$ بالشكل الآتي: ليكن $\sigma \in G(K/F)$ عندئذ فإن $\sigma: K \rightarrow K$ هو F -تماثل ذاتي للحقل K . لنفرض أن $\sigma_L: L \rightarrow K$ هو مقصور σ على L فنجد أن σ_L هو F -تماثل للحقل L في K وحسب المبرهنة (٨-١-٩)

يكون $\sigma_L \in G(L/F)$ ، F - تماثل ذاتي للحقل L وبالتالي يكون $\sigma_L \in G(L/F)$.
 لنضع $f(\sigma) = \sigma_L$ فنجد أن f تطبيقاً، لأنه إذا كان $\sigma, \tau \in G(K/F)$ بحيث
 $\sigma = \tau$ فإن $\sigma_L = \tau_L$ ومنه فإن $f(\sigma) = f(\tau)$. لنبرهن على أن f هو تشاكل زمري .
 ليكن $\sigma, \varepsilon \in G(K/F)$ ولما كانت $G(K/F)$ زمرة فإن $\sigma \cdot \varepsilon \in G(K/F)$ أي أن:
 $f(\sigma \cdot \varepsilon) = (\sigma \cdot \varepsilon)_L$ ومنه فإن للحقل K هو F - تماثل ذاتي للحقل K ومنه فإن $y \in L$ عندئذ $\varepsilon(y) = \varepsilon_L(y)$ ومنه فإن:

$$(\sigma \cdot \varepsilon)_L(y) = (\sigma \cdot \varepsilon)(y) = (\sigma(\varepsilon(y))) = (\sigma(\varepsilon_L(y)))$$

ولما كان $\varepsilon_L \in G(L/F)$ فإن $\varepsilon_L(y) \in L$ ومنه فإن $(\sigma(\varepsilon_L(y))) = (\sigma_L(\varepsilon_L(y)))$ وهكذا نجد أن:

$$(\sigma \cdot \varepsilon)_L(y) = (\sigma \cdot \varepsilon)(y) = (\sigma_L(\varepsilon_L(y))) = \sigma_L \cdot \varepsilon_L(y)$$

وبالتالي يكون $(\sigma \cdot \varepsilon)_L = \sigma_L \cdot \varepsilon_L$ وهذا يبين أن $f(\sigma \cdot \varepsilon) = f(\sigma) \cdot f(\varepsilon)$ ، أي أن f هو تشاكل زمري . لنبرهن على أن f غامر .

ليكن $\psi \in G(L/F)$ أي أن $\psi : L \rightarrow L$ هو F - تماثل ذاتي للحقل L ومنه فإن
 $\psi : L \rightarrow K$ هو F - تماثل للحقل L في K وحسب التمهيدية (٨-١-٦) يوجد F -
 تماثل ذاتي $\psi' : K \rightarrow K$ للحقل K امتداداً للتماثل ψ ومنه يكون $\psi' \in G(K/F)$ وأن

$$f(\psi') = \psi'_L = \psi$$

وهذا يبين أن f غامر ، وحسب مبرهنة التماثل الأولى فإن:

$$G(K/F)/Ker(f) \cong G(L/F)$$

لنبرهن على أن $Ker(f) = G(K/L)$. ليكن $\alpha \in Ker(f)$ عندئذ فإن $\alpha \in G(K/F)$
 أي أن $\alpha : K \rightarrow K$ هو F - تماثل ذاتي للحقل K وأن $f(\alpha) = \alpha_L$ ، أي $f(\alpha) = \alpha_L$ ،
 أن $\alpha_L = I_L$ ومنه أيأ كان $y \in L$ فإن $\alpha(y) = \alpha_L(y) = I_L(y) = y$ ومنه فإن α
 هو L - تماثل ذاتي للحقل K ، وبالتالي $\alpha \in G(K/L)$ أي أن $Ker(f) \subseteq G(K/L)$.
 ليكن $\beta \in G(K/L)$ عندئذ فإن $\beta : K \rightarrow K$ هو L - تماثل ذاتي للحقل K ولما كان
 $F \subseteq L$ فإن $\beta : K \rightarrow K$ هو F - تماثل ذاتي للحقل K ومنه يكون $\beta \in G(K/F)$
 وأن $f(\beta) = \beta_L$. فضلاً عن ذلك، أيأ كان $z \in L$ فإن $\beta_L(z) = \beta(z) = z = I_L(z)$

وهذا يبين أن $\beta_L = I_L$ أي أن $\beta_L = I_L = f(\beta) = \beta_L$ ومنه نجد أن $\beta \in \text{Ker}(f)$ ، وهكذا فإن $G(K/L) \subseteq \text{Ker}(f)$ ، مما سبق نستنتج أن $\text{Ker}(f) = G(K/L)$ ومنه يكون $\diamond . G(K/F)/G(K/L) \cong G(L/F)$

مبرهنة ٨-٢-٦.

ليكن F حقلاً منتهاً مميزه $p \neq 0$. عندئذ:

١ - مرتبة الحقل F تساوي p^n حيث $n \geq 1$ عدد صحيح.

٢ - الحقل F هو حقل تفريق الحدودية المنفصلة:

$$f(x) = x^{p^n} - x \in Z_p[x]$$

فوق الحقل Z_p .

٣ - F هو تمديد غالوا للحقل Z_p .

٤ - ومرة غالوا $G(F/Z_p)$ دوارة مولد بتابع فريبنوس .

البرهان.

١ - حسب نتيجة المبرهنة (٦-٣-١) .

٢ - لنفرض أن F^* الزمرة الضربية للحقل F ، عندئذ فإن $p^n - 1 = (F^*: 1)$ ومنه أيّاً كان $a \in F^*$ فإن $a^{p^n-1} = 1$ وبالتالي يكون $a^{p^n} - a = 0$ ومنه نجد أن كل عنصر $a \in F$ هو صفر للحدودية $f(x) = x^{p^n} - x \in Z_p[x]$ ولما كانت الحدودية $f(x)$ تملك a^{p^n} صفرًا على الأكثر نجد أن F هو حقل تفريق الحدودية $f(x)$.

من جهة أخرى، لما كان $f'(x) = -1 \neq 0$ نجد أن كل صفر للحدودية $f(x)$ هو صفر بسيط وهذا يبين أن $f(x)$ هي حدودية منفصلة فوق Z_p .

٣ - لدينا حسب (٢) أن F هو حقل تفريق حدودية منفصلة فوق الحقل Z_p ومنه فإن

F هو تمديد منفصل للحقل Z_p وناظمي أيضاً، ومنه فإن F هو تمديد غالوا للحقل Z_p .

٤ - لما كان الحقل F منتهاً مرتبته p^n فإنه حسب المبرهنة (٦-١-٣) فإن الزمرة F^* دوارة وأن $p^n - 1 = (F^*: 1)$ ، وهذا يبين أنه أيّاً كان $a \in F^*$ فإن $a^{p^n} = a$. بالعودة إلى التمرين المحلول (٦-٥) فإن تابع فريبنوس هو $\varphi: F \rightarrow F$ معرف بالشكل الآتي:

أياً كان $a \in F$ فإن $\varphi(a) = a^{p^n}$ ومنه نجد أن $\varphi(a) = a$ وهذا يبين أن φ هو F - تماثل ذاتي للحقل F وهذا يبين أن $\varphi \in G(F/Z_p)$ ، أي أن $\langle \varphi \rangle \subseteq G(F/Z_p)$.
 ليكن $a \in Z_p$ عندئذ فإن $a \in F$ ، وأنه أياً كان $n \in \mathbb{Z}$ فإن:

$$\varphi^n(a) = \varphi^{n-1}(\varphi(a)) = \varphi^{n-1}(a) = \cdots = \varphi(a) = a$$

وهذا يبين أن $a \in F(\langle \varphi \rangle)$ وبالتالي يكون $Z_p \subseteq F(\langle \varphi \rangle)$ وحسب المبرهنة (٨-٢-٤) نجد أن $G(F/Z_p) = \langle \varphi \rangle$.

تمارين محلولة (٨)

١ - أثبت أن الحقل $Q(\sqrt{3})$ هو تمديد ناظمي للحقل Q .

الحل.

لما كان العنصر $\sqrt{3}$ صفراً للحدودية $x^2 - 3 \in Q[x]$ نجد أن $\sqrt{3}$ هو عنصر جبري فوق Q وبالتالي يكون التمديد $Q(\sqrt{3})$ تمديداً منتهياً للحقل Q وبالتالي فهو تمديد جبري للحقل Q . من جهة أخرى، لما كانت الحدودية $x^2 - 3$ أولية فوق Q وأن أصفارها هي $\sqrt{3}, -\sqrt{3}$ نجد أن العنصر الوحيد المترافق مع $\sqrt{3}$ هو $-\sqrt{3} \in Q(\sqrt{3})$ وهذا يبين أنه أي $a \in Q(\sqrt{3})$ فإن الحقل $Q(\sqrt{3})$ يحوي جميع العناصر المترافقة مع a فوق Q وحسب التعريف يكون الحقل $Q(\sqrt{3})$ تمديداً ناظماً للحقل Q .

٢ - أثبت أن الحقل $Q(\sqrt[3]{2})$ ليس تمديداً ناظماً للحقل Q .

الحل.

لما كان العنصر $\sqrt[3]{2}$ صفراً للحدودية $x^3 - 2 \in Q[x]$ والتي هي حدودية أولية فوق Q ، بمعنى آخر، إن الحدودية $x^3 - 2$ هي الحدودية الأصغرية للعنصر $\sqrt[3]{2}$ فوق Q وأن أصفار هذه الحدودية هي $\sqrt[3]{2}, \sqrt[3]{2}j, \sqrt[3]{2}j^2$ حيث $j = \frac{-1-i\sqrt{3}}{2}$ وأن هذه الأصفار هي عناصر مترافقة فوق Q وأن $\sqrt[3]{2}j^2 \notin Q(\sqrt[3]{2})$ وهذا يبين أن الحقل $Q(\sqrt[3]{2})$ لا يحوي جميع العناصر المترافقة مع العنصر $\sqrt[3]{2}$ وحسب التعريف فهو ليس تمديداً ناظماً للحقل Q .

٣ - أثبت أن الحقل $Q(\sqrt[3]{2}, j)$ هو تمديد ناظمي للحقل Q ، حيث $j = \frac{-1-i\sqrt{3}}{2}$.

الحل.

لما كان العنصر $\sqrt[3]{2}$ صفراً للحدودية $x^3 - 2 \in Q[x]$ والتي هي حدودية أولية فوق Q وأن أصفار هذه الحدودية هي $\sqrt[3]{2}, \sqrt[3]{2}j, \sqrt[3]{2}j^2$ وهي تمثل جميع العناصر المترافقة مع $\sqrt[3]{2}$ فوق Q وأن هذه العناصر جميعها تنتمي للحقل $Q(\sqrt[3]{2}, j)$ وهذا يبين أن الحقل $Q(\sqrt[3]{2}, j)$ هو تمديد ناظمي للحقل Q .

٤ - لنأخذ التمددين $Q(\sqrt{2}), Q(\sqrt{3})$ للحقل Q . والمطلوب:

١ - أثبت أن كل من $Q(\sqrt{2}), Q(\sqrt{3})$ هو تمديد غالوا للحقل Q .

٢- أثبت أن الحقل $Q(\sqrt{2}, \sqrt{3})$ هو تمديد غالوا للحقل Q .

٣ - أوجد الزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q)$.

٤ - أثبت أن $G(Q(\sqrt{2}, \sqrt{3})/Q) \cong Z_2 \oplus Z_2$.

الحل.

١ - نعلم أن $Q(\sqrt{2})$ هو تمديد منته للحقل Q وأن $[Q(\sqrt{2}):Q] = 2$ ولما كانت

الحدودية الأصغرية للعنصر $\sqrt{2}$ فوق Q هي $g(x) = x^2 - 2 \in Q[x]$ وأن $Q(\sqrt{2})$ هو حقل تفريق الحدودية $g(x)$ فوق Q لأن:

$$g(x) = (x - \sqrt{2})(x + \sqrt{2}) \in Q(\sqrt{2})[x]$$

وهكذا نجد أن $Q(\sqrt{2})$ هو تمديد ناظمي للحقل Q .

من جهة أخرى، لما كان مميز الحقل Q يساوي الصفر فإنه حسب التمهيدية (٥-٣-١)

يكون $Q(\sqrt{2})$ تمديداً منفصلاً للحقل Q ، مما سبق وحسب التعريف نجد أن $Q(\sqrt{2})$

هو تمديد غالوا للحقل Q .

بطريقة مشابهة يمكن إثبات أن الحقل $Q(\sqrt{3})$ هو تمديد غالوا للحقل Q .

٢ - لما كان كل من $\sqrt{2}, \sqrt{3}$ هي عناصر جبرية فوق Q فإنه حسب المبرهنة (٣-٣-٣)

(٩) يكون الحقل $Q(\sqrt{2}, \sqrt{3})$ تمديداً منتهياً للحقل Q ، فضلاً عن ذلك، لما كان كل

تمديد منته هو تمديد جبري نجد أن الحقل $Q(\sqrt{2}, \sqrt{3})$ هو تمديد جبري للحقل Q .

لما كان أيضاً مميز الحقل Q يساوي الصفر فإنه حسب التمهيدية (٥-٣-١) يكون

الحقل $Q(\sqrt{2}, \sqrt{3})$ تمديداً منفصلاً للحقل Q ، مما سبق نجد أن الحقل $Q(\sqrt{2}, \sqrt{3})$

هو تمديد غالوا للحقل Q .

٣ - وجدنا حسب التمرين المحلول (٧-٤) أن الزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q)$ تتألف من

أربعة عناصر هي:

$$\tau_i : Q(\sqrt{2}, \sqrt{3}) \rightarrow Q(\sqrt{2}, \sqrt{3}) \quad i = 1, 2, 3, 4$$

$$\tau_1 : Q(\sqrt{2}, \sqrt{3}) \rightarrow Q(\sqrt{2}, \sqrt{3}) \quad \tau_1(\sqrt{2}) = \sqrt{2}, \quad \tau_1(\sqrt{3}) = \sqrt{3}$$

$$\begin{aligned}\tau_2 : Q(\sqrt{2}, \sqrt{3}) &\rightarrow Q(\sqrt{2}, \sqrt{3}) & \tau_2(\sqrt{2}) &= -\sqrt{2}, \quad \tau_2(\sqrt{3}) = \sqrt{3} \\ \tau_3 : Q(\sqrt{2}, \sqrt{3}) &\rightarrow Q(\sqrt{2}, \sqrt{3}) & \tau_3(\sqrt{2}) &= \sqrt{2}, \quad \tau_3(\sqrt{3}) = -\sqrt{3} \\ \tau_4 : Q(\sqrt{2}, \sqrt{3}) &\rightarrow Q(\sqrt{2}, \sqrt{3}) & \tau_4(\sqrt{2}) &= -\sqrt{2}, \quad \tau_4(\sqrt{3}) = -\sqrt{3}\end{aligned}$$

٤ - وجدنا حسب (٣) أن مرتبة الزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q)$ تساوي 4 وبالتالي فهي

تبديلية وتتألف من العناصر $\tau_1, \tau_2, \tau_3, \tau_4$ ، حيث $\tau_1 = I_{Q(\sqrt{2}, \sqrt{3})}$.

نلاحظ أن مرتبة العنصر τ_2 تساوي 2 وذلك لأن:

$$\begin{aligned}\tau_2^2(\sqrt{2}) &= \tau_2(\tau_2(\sqrt{2})) = \tau_2(-\sqrt{2}) = \tau_2(-1)\tau_2(\sqrt{2}) = -(-\sqrt{2}) = \sqrt{2} \\ \tau_2^2(\sqrt{3}) &= \tau_2(\tau_2(\sqrt{3})) = \tau_2(\sqrt{3}) = \sqrt{3}\end{aligned}$$

ولما كان τ_2^2 هو Q - تماثلاً ذاتياً للحقل $Q(\sqrt{2}, \sqrt{3})$ نجد أن $\tau_2^2 = I_{Q(\sqrt{2}, \sqrt{3})}$ وهذا يبين

أن العنصر τ_2 يولد زمرة جزئية من الزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q)$ مؤلفة من عنصرين

$$\langle \tau_2 \rangle = \{\tau_1, \tau_2\} \cong Z_2 \cong Z/2Z \quad \text{أما } \tau_1, \tau_2 \text{ أي أن}$$

أيضاً، نلاحظ أن مرتبة العنصر τ_3 تساوي 2 وذلك لأن:

$$\tau_3^2(\sqrt{2}) = \tau_3(\tau_3(\sqrt{2})) = \tau_3(\sqrt{2}) = \sqrt{2}$$

$$\tau_3^2(\sqrt{3}) = \tau_3(\tau_3(\sqrt{3})) = \tau_3(-\sqrt{3}) = \tau_3(-1)\tau_3(\sqrt{3}) = -(-\sqrt{3}) = \sqrt{3}$$

ولما كان τ_3^2 هو Q - تماثلاً ذاتياً للحقل $Q(\sqrt{2}, \sqrt{3})$ نجد أن $\tau_3^2 = I_{Q(\sqrt{2}, \sqrt{3})}$ وهذا يبين

أن العنصر τ_3 يولد زمرة جزئية من الزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q)$ مؤلفة من عنصرين

$$\langle \tau_3 \rangle = \{\tau_1, \tau_3\} \cong Z_2 \cong Z/2Z \quad \text{أما } \tau_1, \tau_3 \text{ أي أن}$$

ولما كانت الزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q)$ تبديلية وأن $\langle \tau_2 \rangle \oplus \langle \tau_3 \rangle \cong Z_2 \oplus Z_2$ نجد أن

$$\langle \tau_2 \rangle \oplus \langle \tau_3 \rangle \text{ زمرة جزئية من الزمرة } G(Q(\sqrt{2}, \sqrt{3})/Q) \text{ مرتبتها 4 ومنه يكون:}$$

$$G(Q(\sqrt{2}, \sqrt{3})/Q) \cong \langle \tau_2 \rangle \oplus \langle \tau_3 \rangle \cong Z_2 \oplus Z_2 \cong Z/2Z \times Z/2Z$$

٥ - أثبت أن العنصر $\sqrt[3]{2} - i$ جبرياً فوق الحقل Q .

الحل.

نفرض أن $a = \sqrt[3]{2} - i$ فنجد أن $a^2 = \sqrt[3]{2} - i$ ومنه فإن $a^2 + i = \sqrt[3]{2}$ وبالتالي يكون

$$(a^2 + i)^3 = 2 \quad \text{وبالتالي نجد أن:}$$

$$a^6 + 3a^4i - 3a^2 - i = 2$$

وهذا يبين لنا أن:

$$(a^6 - 3a^2) + (3a^4 - 1)i = 2$$

أي أن $(3a^4 - 1)i = 2 + (3a^2 - a^6)$ ومنه نجد أن:

$$-(3a^4 - 1)^2 = (2 + (3a^2 - a^6))^2$$

$$-9a^8 + 6a^4 - 1 = 4 + 4(3a^2 - a^6) + (3a^2 - a^6)^2$$

ومنه نجد أن $a^{12} + 3a^8 - 4a^6 + 3a^4 + 12a^2 + 5 = 0$ وهكذا نجد أن:

$$h(x) = x^{12} + 3x^8 - 4x^6 + 3x^4 + 12x^2 + 5 \in Q[x]$$

وأن $h(a) = h(\sqrt[3]{2} - i) = 0$ وهذا يبين أن العنصر a جبرياً فوق Q .

الفصل التاسع

نظرية غالوا الحديثة

في هذا الفصل سوف ندرس مبرهنة غالوا الأساسية عموماً، أي لأجل الحقول غير المنتهية والتي تتطابق في بعض جوانبها مع المبرهنة (٨-٢-٥). ولذلك فإن جميع الحقول المدروسة في هذا الفصل هي حقول غير منتهية، بمعنى آخر، جميع الحقول هنا هي حقول مميزها يساوي الصفر. بسبب الحجم الكبير لهذه المبرهنة سوف نقوم بسردها على عدة خطوات. لابد من الإشارة هنا إلى أننا سوف نعتمد الرموز الآتية: سوف نرمز لمجموعة كل التماثلات الذاتية للحقل K بالشكل $Aut(K)$ التي تشكل زمرة بالنسبة لعملية تركيب التطبيقات. وسوف نرمز بالشكل $G(K/F)$ لمجموعة كل الـ F -تماثلات الذاتية للحقل K وذلك لأجل أي حقل جزئي F من K ، أي التماثلات الذاتية σ للحقل K التي تحقق الشرط $\sigma(a) = a$ أيّاً كان $a \in F$ والتي تشكل زمرة جزئية من الزمرة $Aut(K)$ والتي سندعوها زمرة غالوا للتمديد K فوق F .

٩ - ١. نظرية غالوا والتمديدات المنتهية.

في هذه الفقرة سوف ندرس مبرهنة غالوا الأساسية من خلال الحقول المنتهية فقط.

تمهيدية ٩-١-١.

ليكن الحقل K تمديداً منتهياً للحقل F وأن $G(K/F)$ زمرة غالوا للحقل K فوق F .

عندئذ:

١ - إذا كانت H زمرة جزئية من الزمرة $G(K/F)$ فإن المجموعة:

$$F(H) = \{a : a \in K; \sigma(a) = a \ \forall \sigma \in H\}$$

تشكل حقلاً جزئياً من الحقل K يحوي F .

٢ - بفرض أن $\mathfrak{I}$ هي مجموعة كل الزمر الجزئية من الزمرة $G(K/F)$ وأن $\mathfrak{I}_0$ مجموعة كل الحقول الجزئية من الحقل K التي يحوي كل منها F ، عندئذ يوجد تطبيق

$$\Gamma : \mathfrak{I} \rightarrow \mathfrak{I}_0$$

٣ - إذا كانت H_1, H_2 زميرتين جزئيتين من الزمرة $G(K/F)$ بحيث $H_1 \subseteq H_2$ عندئذ يكون $F(H_2) \subseteq F(H_1)$.
البرهان.

١ - لنفرض أن H زمرة جزئية من الزمرة $G(K/F)$. واضح أن المجموعة $F(H)$ هي مجموعة جزئية في K وليست خالية لأن $0 \in F(H)$.

ليكن $a, b \in F(H)$ ، عندئذ فإن $a, b \in K$ ومنه $a - b \in K$ وأياً كان $\sigma \in H$ فإن $\sigma : K \rightarrow K$ هو F -تماثل ذاتي للحقل K لأجله $\sigma(a) = a, \sigma(b) = b$ ومنه نجد:
$$\sigma(a - b) = \sigma(a) - \sigma(b) = a - b$$
 وإذا كان $b \neq 0$ فإن $ab^{-1} \in K$ وأن:

$$\sigma(ab^{-1}) = \sigma(a)\sigma(b^{-1}) = \sigma(a)(\sigma(b))^{-1} = ab^{-1}$$

وهذا يبين أن $a - b, ab^{-1} \in F(H)$ وبالتالي فإن $F(H)$ هو حقل جزئي من الحقل K وهو أيضاً يحوي F ، لأنه أياً كان $d \in F(H)$ ولما كان كل $\sigma \in H$ هو F -تماثل ذاتي للحقل K فإن $\sigma(d) = d$ ومنه $d \in F(H)$ وبالتالي الحقل $F(H)$ يحوي F .
٢ - لنعرف العلاقة $\Gamma : \mathfrak{S} \rightarrow \mathfrak{S}_0$ بالشكل الآتي: أياً كان $H \in \mathfrak{S}$ لنضع:

$$\Gamma(H) = F(H)$$

ف نجد أن Γ هو تطبيق، لأنه إذا كانت $H_1, H_2 \in \mathfrak{S}$ بحيث $H_1 = H_2$ فإن $F(H_1) = F(H_2)$ لأنه إذا كان $a \in F(H_1)$ فإن $\sigma(a) = a$ وذلك أياً كان $\sigma \in H_1$ ولما كان $H_1 = H_2$ فإنه لأجل كل $\sigma \in H_2$ يكون $\sigma(a) = a$ ومنه فإن $a \in F(H_2)$ وهذا يبين أن $F(H_1) \subseteq F(H_2)$. بطريقة مشابهة يمكن إثبات الاحتواء المعاكس، ومنه نجد أن $F(H_1) = F(H_2)$ أي أن $\Gamma(H_1) = \Gamma(H_2)$ وبالتالي يكون Γ تطبيقاً.

٣ - لنفرض أن H_1, H_2 زميرتان جزئيتان من الزمرة $G(K/F)$ بحيث $H_1 \subseteq H_2$.
ليكن $a \in F(H_2)$ عندئذ أياً كان $\tau \in H_1$ فإن $\tau \in H_2$ ومنه فإن $\tau(a) = a$ وهذا يبين أن $a \in F(H_1)$ ومنه نجد أن $F(H_2) \subseteq F(H_1)$. ◊

ملاحظة.

إن الشرطين (٢) و (٣) من التمهيدية السابقة يمكن التعبير عنهما بالشكل الآتي: إن

التطبيق $\Gamma: \mathfrak{S} \rightarrow \mathfrak{S}_0$ يعكس علاقة الاحتواء المعرفة على المجموعة $\mathfrak{S}$.

تمهيدية ٩-١-٢.

ليكن الحقل K تمديداً منتهياً للحقل F وأن $a \in K$. إذا كانت $f(x) \in F[x]$ وكان $f(a) = 0$ ، عندئذ يكون $f(\sigma(a)) = 0$ وذلك لأجل كل $\sigma \in G(K/F)$.
البرهان.

نفرض أن $a \in K$ وأن $f(x) = \sum_{i=0}^n b_i x^i \in F[x]$ حيث $b_i \in F$ حدودية تحقق $f(a) = 0$ ، عندئذ يكون $f(a) = \sum_{i=0}^n b_i a^i = 0$ وبالتالي يكون:

$$\sigma(\sum_{i=0}^n b_i a^i) = \sigma(0) = 0$$

$$\sum_{i=0}^n \sigma(b_i) \sigma(a^i) = 0$$

وذلك أياً كان $\sigma \in G(K/F)$ ، ولما كان σ هو F -تماثلاً ذاتياً للحقل K نجد أن:

$$\sum_{i=0}^n b_i \sigma(a^i) = 0$$

ومنه يكون $f(\sigma(a)) = 0$ وهذا يبين أن العنصر $\sigma(a) \in K$ هو صفر للحدودية $f(x)$.
♦

قبل المتابعة بدراسة نظرية غالوا للتمديدات المنتهية لحقول غير منتهية (مميزها يساوي الصفر) لا بد لنا من التذكير بالحقائق الآتية: حسب التمهيدية (٥-٣-١) فإن كل تمديد جبري لحقل غير منته (مميزه يساوي الصفر) هو تمديد منفصل ولما كان كل تمديد منته هو تمديد جبري فإن كل تمديد منته لحقل غير منتهي (مميزه يساوي الصفر) هو تمديد منفصل.

أيضاً لدينا المبرهنة (٥-٣-١٤) التي تنص على أن كل تمديد منته لحقل غير منته هو تمديد بسيط.

مبرهنة ٩-١-٣.

ليكن الحقل K تمديداً منتهياً للحقل F . عندئذ فإن $[K:F] \leq (G(K/F):1)$.

البرهان.

نفرض أن الحقل K تمديد منتهي للحقل F . لما كان مميز الحقل F يساوي الصفر فإنه

حسب التمهيدية (١-٣-٥) يكون الحقل K تمديداً منفصلاً للحقل F وحسب المبرهنة (١٤-٣-٥) يوجد $a \in K$ بحيث $K = F(a)$.

نفرض أن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F ، عندئذ حسب التمهيدية (٢-١-٩) فإنه لأجل كل $\sigma \in G(K/F)$ يكون $f(\sigma(a)) = 0$ وهذا يبين أن $f(x)$ هي الحدودية الأصغرية للعنصر $\sigma(a)$ فوق F وحسب المبرهنة (٣-٣-٧) فإن عدد جميع الـ F -تماثلات الذاتية للحقل K أصغر أو يساوي $[K:F]$ ومنه نجد أن $\diamond (G(K/F):1) \leq [K:F]$.

مبرهنة ١-٩-٤.

ليكن الحقل K تمديداً منتهياً للحقل F وأن H زمرة جزئية من الزمرة $G(K/F)$. عندئذ:

$$١ - [K:F(H)] = (H:1) = (G(K/F(H)):1)$$

$$٢ - G(K/F(H)) = H$$

البرهان.

١ - لدينا حسب التمهيدية (١-١-٩) أن $F(H)$ حقل جزئي في K يحوي F ، أي أن $F \subseteq F(H) \subseteq K$. لما كان الحقل K تمديداً منتهياً للحقل F فإن الحقل K هو أيضاً تمديد منته للحقل $F(H)$ وحسب المبرهنة (١٤-٣-٥) يوجد $a \in K$ بحيث $K = F(H)(a)$. نفرض أن $g(x) \in F(H)[x]$ الحدودية الأصغرية للعنصر a فوق الحقل $F(H)$ ، عندئذ يكون:

$$[K:F(H)] = \partial g(x)$$

من جهة أخرى، لما كانت $H \subseteq G(K/F)$ فإنه حسب التمهيدية (٢-١-٩) لأجل كل $\sigma \in H$ فإن $\sigma(a) \in K$ هو صفر للحدودية $g(x)$. لنأخذ الحدودية:

$$f(x) = \prod_{\sigma \in H} (x - \sigma(a))$$

فنجد أن $f(x) \in F(H)[x]$ وأن العنصر a صفر للحدودية $f(x)$ ومنه يكون:

$$\partial g(x) \leq \partial f(x)$$

$$\partial f(x) = (H:1)$$

ومنه نجد أن:

$$[K : F(H)] = \partial g(x) \leq \partial f(x) = (H : 1)$$

أي أن $[K : F(H)] \leq (H : 1)$.

من جهة ثالثة، نلاحظ أن H هي زمرة جزئية من الزمرة $G(K/F(H))$ وذلك لأنه أياً كان $\sigma \in H$ فإن $\sigma : K \rightarrow K$ هو F -تماثل ذاتي للحقل K وأنه أياً كان $b \in F(H)$ فإن $\tau(b) = b$ وذلك لأجل كل $\tau \in H$ وهذا يبين أن σ هو $F(H)$ -تماثل ذاتي للحقل K ، أي أن $\sigma \in G(K/F(H))$ ومنه فإن $H \subseteq G(K/F(H))$ وهكذا نجد أن:

$$(H : 1) \leq (G(K/F(H)) : 1)$$

لما كان الحقل K تمديداً منتهياً للحقل F وأن $F \subseteq F(H) \subseteq K$ فإن الحقل K هو تمديد منته للحقل $F(H)$ وحسب المبرهنة (٩-١-٣) يكون:

$$(G(K/F(H)) : 1) \leq [K : F(H)]$$

وهكذا يكون $[K : F(H)] \leq (H : 1)$ ، مما سبق نجد أن:

$$[K : F(H)] = (H : 1) = (G(K/F(H)) : 1)$$

٢ - وجدنا حسب (١) أن H هي زمرة جزية من الزمرة $G(K/F(H))$ وأن:

$$(H : 1) = (G(K/F(H)) : 1)$$

وهذا يبين أن $G(K/F(H)) = H$.

تمهيدية ٩-١-٥.

ليكن الحقل K تمديداً منتهياً للحقل F وأن $\mathfrak{S}$ هي مجموعة كل الزمر الجزئية من الزمرة $G(K/F)$ وأن $\mathfrak{S}_0$ مجموعة كل الحقول الجزئية من الحقل K التي كل منها يحوي F ، عندئذ:

١ - التطبيق $\Gamma : \mathfrak{S} \rightarrow \mathfrak{S}_0$ المعروف بالشكل: أياً كان $H \in \mathfrak{S}$ فإن $\Gamma(H) = F(H)$ متباين.

٢ - لأجل أي زمرة جزئية H من الزمرة $G(K/F)$ فإن $G(K/\Gamma(H)) = H$.

البرهان.

١ - وجدنا حسب التمهيدية (٩-١-١) أن $\Gamma : \mathfrak{S} \rightarrow \mathfrak{S}_0$ هو تطبيق.

لنبرهن على أنه متباين. ليكن $H_1, H_2 \in \mathfrak{S}$ ، عندئذ كل من H_1, H_2 هي زمرة جزئية من الزمرة $G(K/F)$. لنفرض أن $\Gamma(H_1) = \Gamma(H_2)$ عندئذ يكون $F(H_1) = F(H_2)$ وحسب المبرهنة (٩-١-٤) نجد أن:

$$H_1 = G(K/F(H_1)) = G(K/F(H_2)) = H_2$$

وهذا يبين أن التطبيق Γ متباين.

٢ - واضح. ◊

مبرهنة ٩-١-٦.

ليكن الحقل K تمديداً منتهياً للحقل F . عندئذ يكون الحقل K حقل تفريق حدودية ما فوق الحقل $F(G(K/F))$.

البرهان.

لنفرض أن:

$$E = F(G(K/F)) = \{a : a \in K; \sigma(a) = a \ \forall \sigma \in G(K/F)\}$$

فنجد أن E هو حقل جزئي من الحقل K يحوي F وحسب المبرهنة (٩-١-٤) يكون:

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

ومنه فإن $F(G(K/E)) = E$. لما كان الحقل K تمديداً منتهياً للحقل F فإنه يوجد $a \in K$ بحيث $K = F(a)$. لنأخذ الحدودية:

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

فنجد أن $f(x) \in F(G(K/E))[x] = E[x]$ وتملك a صفراً لها وهذا يبين أن $K = E(a)$ ومنه يكون K حقل تفريق الحدودية $f(x)$ فوق الحقل E . ◊

مبرهنة ٩-١-٧.

ليكن الحقل K تمديداً منتهياً للحقل F . عندئذ:

١ - إذا كان E حقلاً جزئياً من الحقل K يحوي F ، أي أن $F \subseteq E \subseteq K$ ، عندئذ لأجل كل $\sigma \in G(K/F)$ فإن:

$$G(K/\sigma(E)) = \sigma \cdot G(K/E) \cdot \sigma^{-1}$$

٢ - إذا كانت H من الزمرة $G(K/F)$ ، عندئذ لأجل كل $\sigma \in G(K/F)$ فإن:

$$. F(\sigma \cdot H \cdot \sigma^{-1}) = \sigma(F(H))$$

البرهان.

١ - لنفرض أن E حقلاً جزئياً من الحقل K يحوي F ، أي أن $F \subseteq E \subseteq K$. عندئذ
أيضاً كان $\sigma \in G(K/F)$ فإن $\sigma(F) \subseteq \sigma(E) \subseteq \sigma(K)$ ولما كان $\sigma(F) = F$ و
 $\sigma(K) = K$ نجد أن $F \subseteq \sigma(E) \subseteq K$ ، أي أن $\sigma(E)$ هو حقل جزئي من الحقل K
يحوي F .

ليكن $\tau \in G(K/\sigma(E))$ عندئذ $\tau: K \rightarrow K$ هو $\sigma(E)$ -تماثل ذاتي للحقل K ومنه
أيضاً كان $a \in E$ فإن $\tau(\sigma(a)) = \sigma(a)$ ومنه نجد أن $\sigma^{-1} \cdot \tau \cdot \sigma(a) = a$ وهذا يبين
أن $\sigma^{-1} \cdot \tau \cdot \sigma \in G(K/E)$ وبالتالي يكون $\tau \in \sigma \cdot G(K/E) \cdot \sigma^{-1}$ ومنه نجد أن:
 $G(K/\sigma(E)) \subseteq \sigma \cdot G(K/E) \cdot \sigma^{-1}$

الاحتواء المعاكس. ليكن $\sigma \in G(K/F)$ ولنفرض أن $\tau \in \sigma \cdot G(K/E) \cdot \sigma^{-1}$ عندئذ
يوجد $\lambda \in G(K/E)$ بحيث يكون $\tau = \sigma \cdot \lambda \cdot \sigma^{-1}$. إن λ من σ هو تماثل ذاتي
للحقل K وبالتالي فإن τ هو تماثل ذاتي للحقل K ، فضلاً عن ذلك أيضاً كان $a \in E$ فإن

$$\tau(\sigma(a)) = \sigma \cdot \lambda \cdot \sigma^{-1}(\sigma(a)) = \sigma \cdot \lambda(a)$$

ولما كان λ هو E -تماثلاً ذاتياً للحقل K نجد أن $\tau(\sigma(a)) = \sigma \cdot \lambda(a) = \sigma(a)$
وهذا يبين لنا أن τ هو $\sigma(E)$ -تماثل ذاتي للحقل K وبالتالي $\tau \in G(K/\sigma(E))$ ومنه
فإن $G(K/\sigma(E)) \subseteq \sigma \cdot G(K/E) \cdot \sigma^{-1}$ ، مما سبق نجد أن:

$$G(K/\sigma(E)) = \sigma \cdot G(K/E) \cdot \sigma^{-1}$$

٢ - لنفرض أن H هي زمرة جزئية من الزمرة $G(K/F)$ وليكن $\sigma \in G(K/F)$ عندئذ
لأجل كل $a \in F(\sigma \cdot H \cdot \sigma^{-1})$ فإن $a \in K$ ، فضلاً عن ذلك فإنه لأجل كل $\tau \in H$
يكون $\sigma \cdot \tau \cdot \sigma^{-1}(a) = a$ ومنه يكون $\tau(\sigma^{-1}(a)) = \sigma^{-1}(a)$ وهذا يبين أن
 $\sigma^{-1}(a) \in F(H)$ ومنه نجد أن $a \in \sigma(F(H))$ وهكذا يكون:

$$F(\sigma \cdot H \cdot \sigma^{-1}) \subseteq \sigma(F(H))$$

الاحتواء المعاكس. ليكن $b \in \sigma(F(H))$ عندئذ يكون $b = \sigma(a)$ حيث $a \in F(H)$
ولما كان لأجل كل $\tau \in H$ فإن $\tau(a) = a$ نجد أن:

$b = \sigma(a) = \sigma \cdot \tau(a) = \sigma \cdot \tau \cdot \sigma^{-1}(\sigma(a)) = \sigma \cdot \tau \cdot \sigma^{-1}(b)$
وهذا يبين أن $b \in F(\sigma \cdot H \cdot \sigma^{-1})$ وبالتالي يكون $\sigma(F(H)) \subseteq F(\sigma \cdot H \cdot \sigma^{-1})$
وهكذا نجد أن $F(\sigma \cdot H \cdot \sigma^{-1}) = \sigma(F(H))$ ♦

مبرهنة ٩-١-٨.

ليكن الحقل K تمديداً منتهياً للحقل F . إذا كان E_1, E_2 حقلين جزئيين من الحقل K
كل منهما يحوي F ، عندئذ يكون:

$$G(K/E_1 \cdot E_2) = G(K/E_1) \cap G(K/E_2)$$

البرهان.

لنفرض أن E_1, E_2 حقلان جزئيان من الحقل K كل منهما يحوي F ، أي أن:

$$F \subseteq E_1, E_2 \subseteq K$$

ليكن $\sigma \in G(K/E_1 \cdot E_2)$ عندئذ فإن $\sigma : K \rightarrow K$ هو تماثل ذاتي للحقل K
ولما كان $E_1 \subseteq E_1 \cdot E_2$ نجد أن σ هو تماثل ذاتي للحقل K وبالتالي يكون
 $\sigma \in G(K/E_1)$

أيضاً لما كان $E_2 \subseteq E_1 \cdot E_2$ نجد أن σ هو تماثل ذاتي للحقل K وبالتالي يكون
 $\sigma \in G(K/E_2)$ ، ومنه نجد أن $\sigma \in G(K/E_1) \cap G(K/E_2)$ وبالتالي يكون:

$$G(K/E_1 \cdot E_2) \subseteq G(K/E_1) \cap G(K/E_2)$$

الاحتواء المعاكس. ليكن $\tau \in G(K/E_1) \cap G(K/E_2)$ عندئذ إن $\tau : K \rightarrow K$ هو
تماثل ذاتي للحقل K وأيضاً E_2 تماثل ذاتي للحقل K ومنه أياً كان $a \in E_1$
وأياً كان $b \in E_2$ فإن $ab \in E_1 \cdot E_2 \subseteq K$ وأن $\tau(ab) = \tau(a) \cdot \tau(b) = ab$ وهذا
يبين لنا أن τ هو تماثل ذاتي للحقل K وبالتالي فإن $\tau \in G(K/E_1 \cdot E_2)$
ومنه نجد أن $G(K/E_1) \cap G(K/E_2) \subseteq G(K/E_1 \cdot E_2)$ ، مما سبق نجد أن:

$$G(K/E_1 \cdot E_2) = G(K/E_1) \cap G(K/E_2)$$

وهو المطلوب إثباته. ♦

مبرهنة ٩-١-٩.

ليكن الحقل K تمديداً منتهياً للحقل F وأن H_1, H_2 زمرتان جزئيتان من الزمرة $G(K/F)$. إذا كانت $H_1 \subseteq H_2$ عندئذ يكون:

$$[F(H_1) : F(H_2)] = (H_2 : H_1)$$

البرهان.

لنفرض أن H_1, H_2 زمرتان جزئيتان من الزمرة $G(K/F)$ وأن $H_1 \subseteq H_2$ عندئذ يكون $F(H_2) \subseteq F(H_1)$ وذلك لأنه إذا كان $a \in F(H_2)$ فإنه لأجل كل $\tau \in H_1$ فإن $\tau(a) = a$ وبالتالي $\tau \in H_2$ ومنه يكون $a \in F(H_1)$. لما كان $F(H_2)$ حقلاً جزئياً من الحقل K يحوي F نجد أن $F \subseteq F(H_2) \subseteq F(H_1) \subseteq K$ أيضاً لما كان الحقل K تمديداً منتهياً للحقل F فإن الحقل K يكون تمديداً منتهياً للحقل $F(H_2)$ ويحقق:

$$[K : F(H_2)] = [K : F(H_1)] \cdot [F(H_1) : F(H_2)]$$

وبحسب المبرهنة (٩-١-٤) يكون:

$$[K : F(H_2)] = (H_2 : 1), \quad [K : F(H_1)] = (H_1 : 1)$$

ومنه نجد أن:

$$\begin{aligned} [F(H_1) : F(H_2)] &= [K : F(H_2)] / [K : F(H_1)] = \\ &= (H_2 : 1) / (H_1 : 1) = (H_2 : H_1) \end{aligned}$$

وذلك لأن $(H_2 : 1) = (H_2 : H_1)(H_1 : 1)$ ♦

٩ - ٢. نظرية غالوا وحقول التفريق.

في هذه الفقرة سوف ندرس مبرهنة غالوا الأساسية من خلال حقول التفريق.

مبرهنة ٩-٢-١.

ليكن الحقل K تمديداً منتهياً للحقل F . الشروط الآتية متكافئة:

١ - K هو حقل تفريق حدودية ما فوق الحقل F .

٢ - $(G(K/F):1) = [K:F]$.

٣ - $F(G(K/F)) = F$.

٤ - كل حدودية أولية في $F[x]$ تملك صفراً في K تتفرق في $K[x]$ إلى مضارب خطية.

البرهان.

١ - لنفرض أن الحقل K هو حقل تفريق حدودية ما $f(x) \in F[x]$ ولنفرض أيضاً أن

$a_1, a_2, \dots, a_n$ هي جميع أصفار الحدودية $f(x)$ في K ، عندئذ يكون:

$$K = F(a_1, a_2, \dots, a_n)$$

من جهة أخرى، لما كان الحقل K تمديداً منتهياً للحقل F فإنه يوجد $b \in K$ بحيث

يكون $K = F(b)$. لنفرض أن $g(x) \in F[x]$ الحدودية الأصغرية للعنصر b فوق F

وأن L حقل تفريق الحدودية $g(x)$ فوق F . لما كانت $\partial g(x) > 0$ وأن مميز الحقل F

يساوي الصفر فإنه حسب التمهيدية (٥-٢-٢) تكون الحدودية $g(x)$ منفصلة فوق F .

لنفرض أن $b = b_1, b_2, \dots, b_m$ هي جميع أصفار الحدودية $g(x)$ عندئذ حسب المبرهنة

(٥-٢-٦) تكون هذه الأصفار بسيطة وبالتالي فهي مختلفة مثنى مثنى ومنه يكون:

$$L = F(b_1, b_2, \dots, b_m)$$

وهذا يبين أن $K \subseteq L$ ، لأن:

$$K = F(b) \subseteq F(b_1, b_2, \dots, b_m) = L$$

ولما كانت الحدودية $g(x)$ هي الحدودية الأصغرية للعنصر b فوق F وأن العناصر

$b_1, b_2, \dots, b_m$ هي أصفار للحدودية $g(x)$ فإن العناصر $b_1, b_2, \dots, b_m$ هي عناصر

مترافقة مع b فوق F وحسب المبرهنة (٧-١-٢) توجد تماثلات:

$$\sigma_j : F(b) \rightarrow F(b_j)$$

تحقق أن $\sigma_j(b) = b_j$ وأن $\sigma_j(\alpha) = \alpha$ وذلك لأجل كل $\alpha \in F$ ، أي أن σ_j هي F -تماثلات للحقل $F(b)$ في الحقل $F(b_j)$ وذلك لأجل كل $1 \leq j \leq m$.
لنأخذ في الحلقة $F[x]$ الحدوديات $p_j(x) \in F[x]$ التي تحقق أن:

$$b = p_1(a_1) \cdot p_2(a_2) \cdots p_n(a_n)$$

ف نجد أن:

$$b_j = \sigma_j(b) = p_1(\sigma_j(a_1)) \cdot p_2(\sigma_j(a_2)) \cdots p_n(\sigma_j(a_n))$$

وذلك لأجل كل $1 \leq j \leq m$.

ولما كانت الحدودية $g(x)$ هي الحدودية الأصغرية للعناصر b_j فوق F نجد أن:

$$[F(b) : F] = \partial g(x) = [F(b_j) : F]$$

ومنه نجد أن $K = F(b_j)$ وذلك لأجل كل $1 \leq j \leq m$ وهذا يبين لنا أن التماثلات

$$\sigma_j \in G(K/F) \text{ وذلك لأجل كل } 1 \leq j \leq m, \text{ ومنه نجد أن:}$$

$$(G(K/F) : 1) \geq \partial g(x) = [K : F]$$

من جهة أخرى، لدينا حسب المبرهنة (٩-١-٣) أن:

$$(G(K/F) : 1) \leq [K : F]$$

مما سبق نجد أن $(G(K/F) : 1) = [K : F]$.

(٢) $\Leftarrow$ (٣). لما كان الحقل $F(G(K/F))$ حقلاً جزئياً من الحقل K يحوي F وذلك

لأن كل عنصر من الزمرة $G(K/F)$ هو F -تماثل ذاتي للحقل K فإن:

$$F \subseteq F(G(K/F)) \subseteq K$$

وأن الحقل K هو تمديد منته للحقل F ، نجد أن:

$$[K : F] = [K : F(G(K/F))] \cdot [F(G(K/F)) : F]$$

من جهة أخرى، لدينا حسب المبرهنة (٩-١-٤) أن:

$$[K : F(G(K/F))] = (G(K/F) : 1)$$

ولدينا أيضاً حسب الفرض أن $(G(K/F) : 1) = [K : F]$ ، ومنه نجد أن:

$$[K : F(G(K/F))] = [K : F]$$

وهذا يبين لنا أن:

$$[F(G(K/F)) : F] = \frac{[K : F]}{[K : F(G(K/F))]} = \frac{[K : F]}{[K : F]} = 1$$

ومنه نجد أن $F(G(K/F)) = F$.

(٣) $\Leftarrow$ (٤). ليكن $a \in K$ وأن $f(x) \in F[x]$ حدودية أولية فوق F تملك a صفراً لها.

لنفرض أن $g(x) = \prod_{\sigma \in G(K/F)} (x - \sigma(a))$ فنجد أن $g(x) \in F(G(K/F))[x]$

وحسب الفرض، لما كان $F(G(K/F)) = F$ نجد أن $g(x) \in F[x]$.

من جهة أخرى، لما كان a صفراً للحدودية $f(x)$ ، لأن $I_K \in G(K/F)$ فإن

$g(a) = 0$ ولما كانت الحدودية $f(x)$ هي الحدودية الأصغرية للعنصر a فوق F

نجد أن $f(x)$ تقسم $g(x)$ في $F[x]$. ولما كانت $g(x)$ تتفرق في $K[x]$ إلى مضاريب

خطية نجد أن $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية.

(٤) $\Leftarrow$ (١). لما كان الحقل K تمديداً منتهياً للحقل F فإنه يوجد $a \in K$ بحيث يكون

$K = F(a)$. لنفرض أن $h(x) \in F[x]$ هي الحدودية الأصغرية للعنصر a فوق F

ف نجد أن $h(x)$ هي الحدودية أولية في $F[x]$ تملك a صفراً لها وحسب الفرض $h(x)$

تتفرق في $K[x]$ إلى مضاريب خطية ولما كان $K = F(a)$ نجد أن K هو حقل تفريق

الحدودية $f(x)$ فوق F .

مبرهنة ٩-٢-٢.

ليكن K حقل تفرق حدودية ما فوق الحقل F ولنفرض أن $\mathfrak{I}$ هي مجموعة كل الزمر

الجزئية من الزمرة $G(K/F)$ وأن $\mathfrak{I}_0$ هي مجموعة كل الحقول الجزئية من الحقل K

التي كل منها يحوي F . عندئذ:

١ - التطبيق $\mathfrak{I}_0 \rightarrow \mathfrak{I} : \Gamma$ المعروف بالشكل الآتي: لأجل أي زمرة جزئية H من الزمرة

$G(K/F)$ ، أي لأجل أي $H \in \mathfrak{I}$ فإن $\Gamma(H) = F(H)$ هو تقابل يعكس علاقة

الترتيب المعرفة على المجموعة $\mathfrak{I}$ (الاحتواء).

٢ - لأجل أي حقل جزئي E من الحقل K يحوي F ، أي لأجل أي $E \in \mathfrak{I}_0$ فإن:

$$\Gamma^{-1}(E) = G(K/E)$$

البرهان.

١ - لما كان الحقل K هو حقل تفرق حدودية ما $f(x) \in F[x]$ فإن K هو تمديد منته للحقل F .

وجدنا حسب التمهيدية (٩-١-١) أن Γ هو تطبيق يعكس علاقة الترتيب المعرفة على المجموعة $\mathfrak{S}$ (الاحتواء). أيضاً وجدنا حسب التمهيدية (٩-١-٥) أن التطبيق Γ متباين. لنبرهن على أن التطبيق Γ غامر.

ليكن $E \in \mathfrak{S}_0$ عندئذ فإن E هو حقل جزئي من الحقل K يحوي F ، أي أن:

$$F \subseteq E \subseteq K$$

ولما كان الحقل K تمديداً منتهياً للحقل F فإن الحقل K هو تمديد منته للحقل E . من جهة أخرى، لما كان K هو حقل تفرق الحدودية $f(x) \in F[x]$ فوق F فإن $K = F(a_1, a_2, \dots, a_n)$ حيث $a_1, a_2, \dots, a_n \in K$ هي جميع أصفار الحدودية $f(x)$ في K ، ومنه نجد أن $f(x) \in E[x]$ وأن:

$$K = F(a_1, a_2, \dots, a_n) \subseteq E(a_1, a_2, \dots, a_n) \subseteq K$$

وبالتالي يكون $K = E(a_1, a_2, \dots, a_n)$ وهذا يبين أن K هو حقل تفرق الحدودية $f(x) \in E[x]$ فوق الحقل E . وحسب المبرهنة (٩-٢-١) نجد أن:

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

ولما كانت الزمرة $G(K/E)$ هي زمرة جزئية من الزمرة $G(K/F)$ وذلك لأن كل $E -$ تماثل ذاتي للحقل K هو $F -$ تماثل ذاتي للحقل K ، لأن $F \subseteq E$ ومنه فإن $G(K/E) \in \mathfrak{S}$ وأن:

$$\Gamma(G(K/E)) = F(G(K/E)) = E$$

وهذا يبين أن التطبيق Γ غامر.

٢ - ليكن $E \in \mathfrak{S}_0$ وجدنا حسب (١) أن $G(K/E) \in \mathfrak{S}$ وأن $\Gamma(G(K/E)) = E$ ومنه نجد أن $\Gamma^{-1}(E) = G(K/E)$ وذلك لأن Γ تقابل. ◊

مبرهنة ٩-٢-٣.

ليكن الحقل K تمديداً منتهياً للحقل F ليس بالضرورة حقل تفريق فوق F .

لنفرض أن $\mathfrak{S}$ هي مجموعة كل الزمر الجزئية من الزمرة $G(K/F)$ وأن $\mathfrak{S}_0$ هي مجموعة كل الحقول الجزئية من الحقل K التي كل منها يحوي F .

لنفرض أيضاً أن $\mathfrak{S}_1$ هي مجموعة كل الحقول الجزئية E من الحقل K التي كل منها يحوي F وتحقق الشرط: أن الحقل K هو حقل تفريق فوق E . عندئذ فإن:

$$١ - \text{المجموعة } \mathfrak{S}_1 \text{ ليست خالية وأن } \mathfrak{S}_1 \subseteq \mathfrak{S}_0.$$

$$٢ - \text{إذا كان الحقل } K \text{ حقل تفريق فوق } F \text{ فإن } \mathfrak{S}_1 = \mathfrak{S}_0.$$

$$٣ - \text{الحقل } F(G(K/F)) \text{ هو عنصر أصغر في المجموعة } \mathfrak{S}_1.$$

$$٤ - \text{العلاقة } \Gamma_1: \mathfrak{S} \rightarrow \mathfrak{S}_1 \text{ المعرفة بالشكل الآتي: أيًا كانت } H \in \mathfrak{S} \text{ فإن:}$$

$$\Gamma_1(H) = F(H)$$

هي تطبيق متباين وغامر.

البرهان.

١ - لما كان الحقل K تمديدًا منتهيًا للحقل F فإنه حسب المبرهنة (٩-١-٦) يكون الحقل K حقل تفريق فوق الحقل $F(G(K/F))$ وأن الحقل $F(G(K/F))$ هو حقل جزئي من الحقل K يحوي F ، وذلك لأن كل عنصر من الزمرة $G(K/F)$ هو F -تماثل ذاتي للحقل K ، أي أنه أيًا كان $a \in F$ فإن $\tau(a) = a$ وذلك لأجل كل $\tau \in G(K/F)$ ، مما سبق نجد أن $F(G(K/F)) \in \mathfrak{S}_1$ وبالتالي المجموعة $\mathfrak{S}_1$ ليست خالية. واضح حسب التعريف أن $\mathfrak{S}_1 \subseteq \mathfrak{S}_0$.

٢ - لنفرض أن الحقل K هو حقل تفريق حدودية ما $f(x) \in F[x]$ فوق F ، عندئذ حسب المبرهنة (٩-٢-١) يكون $F(G(K/F)) = F$ ومنه نجد أن:

$$F(G(K/F)) \in \mathfrak{S}_0$$

ليكن $E \in \mathfrak{S}_0$ ، عندئذ E هو حقل جزئي من الحقل K يحوي F ، أي أن $F \subseteq E \subseteq K$ ولما كان K حقل تفريق الحدودية $f(x) \in F[x]$ فوق F فإن $K = F(a_1, a_2, \dots, a_n)$ حيث $a_1, a_2, \dots, a_n \in K$ هي جميع أصفار الحدودية $f(x)$ في K ، ومنه نجد أن $f(x) \in E[x]$ وأن:

$$K = F(a_1, a_2, \dots, a_n) \subseteq E(a_1, a_2, \dots, a_n) \subseteq K$$

ومنه فإن $K = E(a_1, a_2, \dots, a_n)$ وهذا يبين أن K هو حقل تفريق الحدودية $f(x)$ فوق E ومنه نجد أن $E \in \mathfrak{S}_1$ وبالتالي يكون $\mathfrak{S}_0 \subseteq \mathfrak{S}_1$ وحسب (١) لدينا $\mathfrak{S}_1 \subseteq \mathfrak{S}_0$ ، مما سبق نجد أن $\mathfrak{S}_1 = \mathfrak{S}_0$.

٣ - ليكن $E \in \mathfrak{S}_1$ ، عندئذ E هو حقل جزئي من الحقل K يحوي F ، أي أن $F \subseteq E \subseteq K$ وأن K هو حقل تفريق فوق E وحسب المبرهنة (٩-٢-١) يكون $F(G(K/E)) = E$.

من جهة أخرى، لما كانت الزمرة $G(K/E)$ زمرة جزئية من الزمرة $G(K/F)$ وذلك لأن كل E - تماثل ذاتي للحقل K هو F - تماثل ذاتي للحقل K لأن $F \subseteq E$ ، أي لما كانت $G(K/E) \subseteq G(K/F)$ نجد أن:

$$F(G(K/F)) \subseteq F(G(K/E)) = E$$

وهذا يبين أن الحقل $F(G(K/F))$ هو عنصر أصغر في المجموعة $\mathfrak{S}_1$.

٤ - إن العلاقة $\Gamma_1: \mathfrak{S} \rightarrow \mathfrak{S}_1$ المعرفة بالشكل الآتي: أيأ كانت $H \in \mathfrak{S}$ فإن:

$$\Gamma_1(H) = F(H)$$

هي تطبيق. لنبرهن أولاً أن $F(H) \in \mathfrak{S}_1$. حسب التعريف فإن $F(H)$ هو حقل جزئي من الحقل K يحوي F . لنبرهن على أن K هو حقل تفريق فوق $F(H)$. لدينا حسب المبرهنة (٩-١-٦) أن K هو حقل تفريق فوق الحقل $F(G(K/F))$ ولما كانت H زمرة جزئية من الزمرة $G(K/F)$ ، أي أن $H \subseteq G(K/F)$ نجد أن:

$$F(G(K/F)) \subseteq F(H)$$

ولما كان K هو حقل تفريق فوق الحقل $F(G(K/F))$ نجد أن K هو حقل تفريق فوق الحقل $F(H)$ ومنه فإن $F(H) \in \mathfrak{S}_1$.

ليكن $H_1, H_2 \in \mathfrak{S}$ بحيث $H_1 = H_2$ عندئذ يكون $F(H_1) = F(H_2)$ ومنه فإن Γ_1 تطبيق وهو أيضاً متباين، لأنه إذا كانت $F(H_1) = F(H_2)$ ومنه يكون:

$$G(K/F(H_1)) = G(K/F(H_2))$$

وحسب المبرهنة (٩-١-٤) نجد أن:

$$H_1 = G(K/F(H_1)) = G(K/F(H_2)) = H_2$$

أي أن التطبيق Γ_1 متباين. لنبرهن على أن التطبيق Γ_1 غامر.
ليكن $E \in \mathfrak{S}_1$ ، عندئذ فإن E هو حقل جزئي من الحقل K يحوي F ، أي أن $F \subseteq E \subseteq K$ وأن K حقل تفريق فوق E ومنه تكون الزمرة $G(K/E)$ زمرة جزئية من الزمرة $G(K/F)$ ، أي أن $G(K/E) \in \mathfrak{S}$ وأن:

$$\Gamma_1(G(K/E)) = F(G(K/E)) = E$$

وذلك حسب المبرهنة (٩-٢-١) وذلك لأن K حقل تفريق فوق E وهكذا نجد أن التطبيق Γ_1 غامر. ♦

مبرهنة ٩-٢-٤.

ليكن الحقل K تمديداً منتهياً للحقل F وأن H_1, H_2 زمرتان جزئيتان من الزمرة $G(K/F)$. عندئذ يكون:

$$F(H_1 \cap H_2) = F(H_1) \cdot F(H_2)$$

البرهان.

لنفرض أن H_1, H_2 زمرتان جزئيتان من الزمرة $G(K/F)$ ، عندئذ فإن $F(H_1)$ و $F(H_2)$ حقلا جزئيان من الحقل K كل منهما يحوي الحقل F وحسب المبرهنة (٩-١-٨) يكون لدينا:

$$G(K/F(H_1) \cdot F(H_2)) = G(K/F(H_1)) \cap G(K/F(H_2))$$

من جهة أخرى، لدينا حسب المبرهنة (٩-١-٤) أن:

$$G(K/F(H_1)) = F(H_1), \quad G(K/F(H_2)) = F(H_2)$$

ومنه نجد أن:

$$G(K/F(H_1) \cdot F(H_2)) = H_1 \cap H_2 \quad (*)$$

لنبرهن على أن كلا من $F(H_1), F(H_2)$ هو حقل جزئي من الحقل K يحوي F وأن K هو حقل تفريق فوق كل من $F(H_1), F(H_2)$.

حسب التعريف فإن كلا من $F(H_1), F(H_2)$ هو حقل جزئي من الحقل K يحوي F .
لما كانت H_1 زمرة جزئية من الزمرة $G(K/F)$ ، أي أن $H_1 \subseteq G(K/F)$ فإن:

$$F(G(K/F)) \subseteq F(H_1)$$

ولما كان K هو حقل تفريق فوق الحقل $F(G(K/F))$ وذلك حسب المبرهنة (٩-١-٦) نجد أن K هو حقل تفريق فوق الحقل $F(H_1)$.

بطريقة مشابهة نجد أن K هو حقل تفريق فوق الحقل $F(H_2)$. حسب المبرهنة (٩-٢-٤) نجد أن $F(H_1), F(H_2) \in \mathfrak{S}_1$ ، حيث $\mathfrak{S}_1$ هي مجموعة كل الحقول الجزئية E من الحقل K التي كل منها يحوي F وتحقق أن K هو حقل تفريق فوق E . لنبرهن على أن $F(H_1) \cdot F(H_2) \in \mathfrak{S}_1$.

لما كان كل من $F(H_1), F(H_2)$ حقلاً جزئياً من الحقل K يحوي F فإن $F(H_1) \cdot F(H_2)$ هو أيضاً حقل جزئي من الحقل K يحوي F . أيضاً لما كان:

$$F(H_1) \subseteq F(H_1) \cdot F(H_2) \subseteq K$$

وأن K هو حقل تفريق فوق $F(H_1)$ نجد أن K هو حقل تفريق فوق $F(H_1) \cdot F(H_2)$ مما سبق نجد أن $F(H_1) \cdot F(H_2) \in \mathfrak{S}_1$.

ولما كان التطبيق $\Gamma_1: \mathfrak{S} \rightarrow \mathfrak{S}_1$ تقابلاً (متبايناً وغامراً) وأن $F(H_1) \cdot F(H_2) \in \mathfrak{S}_1$ ولما كانت H_1, H_2 زميرتين جزئيتين من الزمرة $G(K/F)$ فإن $H_1 \cap H_2$ زمرة جزئية من الزمرة $G(K/F)$ وبالتالي فإن $H_1 \cap H_2 \in \mathfrak{S}$ ومنه يكون:

$$\Gamma_1(H_1 \cap H_2) = F(H_1 \cap H_2)$$

وحسب العلاقة (*) نجد أن:

$$\Gamma_1(H_1 \cap H_2) = F(H_1 \cap H_2) = F(G(K/F(H_1) \cdot F(H_2)))$$

ولما كان K هو حقل تفريق فوق $F(H_1) \cdot F(H_2)$ فإنه حسب المبرهنة (٩-٢-١) نجد أن:

$$F(G(K/F(H_1) \cdot F(H_2))) = F(H_1) \cdot F(H_2)$$

وهكذا يكون لدينا $F(H_1 \cap H_2) = F(H_1) \cdot F(H_2)$.

مبرهنة ٩-٢-٥.

ليكن K حقل تفريق حدودية ما فوق الحقل F وأن E_1, E_2 حقلاً جزئيان من الحقل K كل منهما يحوي F . إذا كان $E_1 \subseteq E_2$ عندئذ يكون:

$$(G(K/E_1):G(K/E_2)) = [E_2:E_1]$$

البرهان.

لنفرض أن E_1, E_2 حقلان جزئيان من الحقل K كل منهما يحوي F وأن $E_1 \subseteq E_2$. لنفرض أن $H_1 = G(K/E_1)$, $H_2 = G(K/E_2)$ ، فنجد أن H_1 هي زمرة جزئية من الزمرة $G(K/F)$ وذلك لأن كل E_1 - تماثل ذاتي للحقل K هو F - تماثل ذاتي للحقل K وذلك لأن $F \subseteq E_1$.

كذلك الأمر، إن H_2 هي زمرة جزئية من الزمرة $G(K/F)$ وذلك لأن كل E_2 - تماثل ذاتي للحقل K هو F - تماثل ذاتي للحقل K وذلك لأن $F \subseteq E_2$. لما كان $E_1 \subseteq E_2$ فإن هذا يبين أن كل E_2 - تماثل ذاتي للحقل K هو E_1 - تماثل ذاتي للحقل K ومنه نجد أن:

$$H_2 = G(K/E_2) \subseteq G(K/E_1) = H_1$$

ولما كان الحقل K تمديداً منتهياً للحقل F فإنه حسب المبرهنة (٩-١-٩) يكون لدينا:

$$[F(H_2) : F(H_1)] = (H_1 : H_2)$$

وذلك لأن $H_2 \subseteq H_1$.

من جهة أخرى، لما كان الحقل K حقل تفريق فوق الحقل F فإنه حسب المبرهنة (٩-٢-٢) نجد أن:

$$E_1 = F(G(K/E_1)) = F(H_1)$$

$$E_2 = F(G(K/E_2)) = F(H_2)$$

وبالتالي يكون:

$$(H_1 : H_2) = [F(H_2) : F(H_1)] = [E_2 : E_1]$$

وهكذا نجد أن:

$$\diamond \cdot (G(K/E_1) : G(K/E_2)) = (H_1 : H_2) = [E_2 : E_1]$$

مبرهنة ٦-٢-٩.

ليكن F حقلاً مميزه يساوي الصفر وليكن K حقل تفريق فوق F . لنفرض أن E حقلاً جزئياً في K يحوي F . عندئذ الشروط الآتية متكافئة:

١ - الحقل E هو حقل تفريق فوق F .

٢ - أياً كان $\sigma \in G(K/F)$ فإن $\sigma(E) = E$.

٣ - زمرة جزئية ناظرية في الزمرة $G(K/F)$.

البرهان.

لما كان K حقل تفريق فوق F فإن K تمديد منته للحقل F ولما كان $F \subseteq E \subseteq K$ نجد أن E تمديد منته للحقل F وبالتالي فهو تمديد جبري للحقل F ، لما كان مميز الحقل F يساوي الصفر نجد أن E هو تمديد منفصل للحقل F وذلك حسب التمهيدية (١-٣-٥) وحسب المبرهنة (١٤-٣-٥) فإنه يوجد $a \in E$ بحيث $E = F(a)$.

(١) $\Leftarrow$ (٢). لنفرض أن E حقل تفريق فوق F وأن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F . حسب التمهيدية (٢-١-٩) فإن $\sigma(a)$ هو صفر للحدودية $f(x)$ وذلك أياً كان $\sigma \in G(K/F)$ وحسب المبرهنة (١-٢-٩) يكون $\sigma(a) \in E$ ومنه نجد:

$$\sigma(E) = \sigma(F)(\sigma(a)) = F(\sigma(a)) \subseteq E$$

أي أن $\sigma(E) \subseteq E$ وذلك أياً كان $\sigma \in G(K/F)$ ولما كان $\sigma^{-1} \in G(K/F)$ نجد أن $\sigma^{-1}(E) \subseteq E$ ومنه يكون $\sigma(\sigma^{-1}(E)) \subseteq \sigma(E)$ وهذا يبين أن $E \subseteq \sigma(E)$ وهكذا فإن $\sigma(E) = E$.

(٢) $\Leftarrow$ (٣). لنفرض أن $\sigma(E) = E$ وذلك أياً كان $\sigma \in G(K/F)$. لما كان $F \subseteq E \subseteq K$ نجد أن كل E -تماثل ذاتي للحقل K هو F -تماثل ذاتي للحقل K ومنه فإن $G(K/E)$ زمرة جزئية في الزمرة $G(K/F)$. ليكن $\sigma \in G(K/F)$ عندئذ حسب المبرهنة (٧-١-٩) فإن:

$$G(K/\sigma(E)) = \sigma \cdot G(K/E) \cdot \sigma^{-1}$$

ولما كان $\sigma(E) = E$ نجد أن:

$$G(K/E) = \sigma \cdot G(K/E) \cdot \sigma^{-1}$$

وذلك أياً كان $\sigma \in G(K/F)$ وهذا يبين أن الزمرة الجزئية $G(K/E)$ ناظرية في الزمرة $G(K/F)$.

(٣) $\Leftarrow$ (١). لنفرض أن الزمرة الجزئية $G(K/E)$ ناظرية في $G(K/F)$. لما كان K

حقل تفريق فوق F فإنه حسب المبرهنة (١-٢-٩) يكون $F(G(K/F)) = F$.

لما كان لأجل كل $\sigma \in G(K/F)$:

$$G(K/E) = \sigma \cdot G(K/E) \cdot \sigma^{-1}$$

وأن الحقل K هو تمديد منته للحقل F فإنه حسب المبرهنة (٩-١-٧) يكون:

$$G(K/\sigma(E)) = \sigma \cdot G(K/E) \cdot \sigma^{-1}$$

ومنه نجد أن $G(K/\sigma(E)) = G(K/E)$ وبالتالي يكون:

$$F(G(K/\sigma(E))) = F(G(K/E))$$

وحسب المبرهنة (٩-٢-٢) نجد أن $\sigma(E) = E$ وذلك أيًا كان $\sigma \in G(K/F)$.

لنأخذ الحدودية $g(x) = \prod_{\sigma \in G(K/F)} (x - \sigma(x))$ فنجد أن:

$$g(x) \in F(G(K/F))[x] = F[x]$$

وأن العنصر a صفر لها ولما كان $\sigma(a) \in E$ نجد أن الحدودية $g(x)$ تتفرق فوق

الحقل E ومنه يكون E هو حقل تفريق $g(x)$ فوق F .

مبرهنة ٩-٢-٧.

ليكن K حقل تفريق فوق F . لنفرض أن E حقلًا جزئيًا في K يحوي F . عندئذ فإن:

$$G(E/F) \cong \frac{G(K/F)}{G(K/E)}$$

البرهان.

لنفرض أن K حقل تفريق فوق F وأن E حقل جزئي في K يحوي F ، عندئذ حسب

المبرهنة (٩-٢-٦) تكون الزمرة $G(K/E)$ ناظرية في الزمرة $G(K/F)$.

لنعرف العلاقة $f: G(K/F) \rightarrow G(E/F)$ بالشكل الآتي: ليكن $\sigma \in G(K/F)$

عندئذ فإن $\sigma: K \rightarrow K$ هو F -تماثل ذاتي للحقل K ومنه فإن $\sigma|_E: E \rightarrow E$ هو

F -تماثل للحقل E في الحقل K وحسب المبرهنة (٩-٢-٦) فإن $\sigma(E) = E$ وهذا

يبين أن $\sigma|_E: E \rightarrow E$ هو F -تماثل ذاتي للحقل E ومنه فإن $\sigma|_E \in G(E/F)$.

لنضع $f(\sigma) = \sigma|_E$ فنجد أن f هو تطبيق، لأنه إذا كان $\sigma', \sigma'' \in G(K/F)$ بحيث

$\sigma' = \sigma''$ نجد أن:

$$f(\sigma') = \sigma'|_E = \sigma''|_E = f(\sigma'')$$

وهو أيضاً تشاكل لأن $f(\sigma' \cdot \sigma'') = \sigma' \cdot \sigma''|_E$ ومنه أياً كان $b \in E$ فإن:

$$\sigma' \cdot \sigma''|_E(b) = \sigma' \cdot \sigma''(b) = \sigma'(\sigma''(b)) = \sigma'(\sigma''|_E(b))$$

ولما كان $\sigma''(E) = E$ نجد أن:

$$\sigma' \cdot \sigma''|_E(b) = \sigma'(\sigma''|_E(b)) = \sigma'|_E(\sigma''|_E(b)) = \sigma'|_E \cdot \sigma''|_E(b)$$

ومنه نجد أن $\sigma' \cdot \sigma''|_E = \sigma'|_E \cdot \sigma''|_E$ وبالتالي يكون:

$$f(\sigma' \cdot \sigma'') = f(\sigma') \cdot f(\sigma'')$$

لنبرهن على أن $\text{Ker}(f) = G(K/E)$. ليكن $\tau \in \text{Ker}(f)$ عندئذ فإن $f(\tau) = \tau|_E$

وأن $f(\tau) = I_K$ ومنه نجد أن $\tau|_E = I_K$ ومنه أياً كان $b \in E$ فإن:

$$\tau(b) = \tau|_E(b) = I_K(b) = b$$

وهذا يبين أن τ هو E -تماثل ذاتي للحقل K ، أي أن $\tau \in G(K/E)$ ومنه فإن:

$$\text{Ker}(f) \subseteq G(K/E)$$

ليكن $\mu \in G(K/E)$ عندئذ فإن $\mu: K \rightarrow K$ هو F -تماثل ذاتي للحقل K وبالتالي

فإن $\mu \in G(K/F)$ وأن $\mu|_E = I_E$ ، لأن μ هو E -تماثل.

لما كانت $G(K/E)$ زمرة جزئية من الزمرة $G(K/F)$ فإن $I_E = I_K$ وبالتالي يكون

$f(\mu) = I_K$ أي أن $\mu \in \text{Ker}(f)$ ، وهكذا نجد أن $G(K/E) \subseteq \text{Ker}(f)$ ، مما

سبق نجد أن $\text{Ker}(f) = G(K/E)$. وحسب مبرهنة التماثل الزمري الأولى نجد أن:

$$\frac{G(K/F)}{G(K/E)} = \frac{G(K/F)}{\text{Ker}(f)} \cong \text{Im}(f)$$

لنبرهن على أن f غامر. لما كان K حقل تفريق فوق F فإن K هو تمديد منته

للحقل F وحسب المبرهنة (٩-٢-١) فإن:

$$(G(K/F):1) = [K:F]$$

وهذا يبين أن الزمرة $G(K/F)$ منتهية.

من جهة أخرى، لما كان K حقل تفريق فوق F وأن $F \subseteq E \subseteq K$ فإنه حسب

التمهيدية (٩-٢-٤) يكون K حقل تفريق فوق E ، لأن مميز الحقل F يساوي الصفر

ومنه فإن K تمديد منتهي للحقل E وحسب المبرهنة (٩-٢-١) يكون:

$$(G(K/E):1)=[K:E]$$

وهذا يبين أن الزمرة $G(K/E)$ منتهية وبالتالي الزمرة الجزئية $Im(f)$ تكون منتهية، ولما كانت $Im(f) \cong \frac{G(K/F)}{G(K/E)}$ نجد أن:

$$(Im(f):1) = \left(\frac{G(K/F)}{G(K/E)}:1\right) = (G(K/F):G(K/E))$$

ولما كان $F \subseteq E$ فإنه حسب المبرهنة (٩-٢-٥) يكون:

$$(G(K/F):G(K/E))=[E:F]=(G(E/F))$$

ومنه نجد أن $Im(f)$ زمرة جزئية في $G(K/F)$ ولهما المرتبة نفسها ومنه فإن:

$$Im(f) = G(K/F)$$

وهذا يبين أن التطبيق f غامر وبالتالي فإن $G(E/F) \cong \frac{G(K/F)}{G(K/E)}$.

مبرهنة ٩-٢-٨.

ليكن F حقلاً مميزه يساوي الصفر وليكن K حقل تفريق فوق F . لنفرض أن الحقل

L تمديد منته للحقل F . عندئذ فإن:

١ - الحقل $K \cdot L$ هو حقل تفريق فوق L .

٢ - $G(K \cdot L/L) \cong G(K/K \cap L)$.

٣ - $[K \cdot L:L]=[K:K \cap L]$.

٤ - $[K \cdot L:F] = \frac{[K:F] \cdot [L:F]}{[K \cap L:F]}$.

البرهان.

(١) و (٣) و (٤) حسب المبرهنة (٨-١-٤).

٢ - لما كان K حقل تفريق فوق F فإن K هو تمديد منته للحقل F وبالتالي فهو تمديد

جبري للحقل F ولما كان مميز الحقل F يساوي الصفر فإنه حسب التمهيدية (٥-٣-١)

فإن K هو تمديد منفصل للحقل F وحسب المبرهنة (٥-٣-٤) فإنه يوجد $\theta \in K$

بحيث $K = F(\theta)$. لنفرض أن الحدودية $f(x) \in F[x]$ هي الحدودية الأصغرية

للعنصر θ فوق F ، حسب المبرهنة (٩-٢-١) فإن K هو حقل تفريق الحدودية $f(x)$ فوق F . لنعرف العلاقة:

$$\varphi: G(K \cdot L/L) \rightarrow G(K/F)$$

بالشكل الآتي: ليكن $\sigma \in G(K \cdot L/L)$ عندئذ حسب التمهيدية (٩-٢-١) فإن $\sigma(\theta)$ هو صفر للحدودية $f(x)$ ولما كان K هو حقل تفريق الحدودية $f(x)$ فوق F نجد أن $\sigma(\theta) \in K$ ومنه فإن $\sigma|_K: K \rightarrow K$ هو تماثل ذاتي للحقل K ، لما كان $F \subseteq L$ نجد أن $\sigma|_K$ هو F -تماثل ذاتي للحقل K وبالتالي فإن $\sigma|_K \in G(K/F)$. لنضع $f(\sigma) = \sigma|_K$ نجد أن f تطبيق، لأنه إذا كان $\sigma', \sigma'' \in G(K \cdot L/L)$ بحيث $\sigma' = \sigma''$ نجد أن كلا منهما $\sigma'|_K, \sigma''|_K: K \rightarrow K$ هو F -تماثل ذاتي للحقل K وأنه أياً كان $b \in K \subseteq K \cdot L$ فإن:

$$\sigma'|_K(b) = \sigma'(b) = \sigma''(b) = \sigma''|_K(b)$$

وبالتالي يكون $\sigma'|_K = \sigma''|_K$ أي أن $f(\sigma') = f(\sigma'')$ كما أن f هو تشاكل لأن:

$$f(\sigma' \cdot \sigma'') = \sigma' \cdot \sigma''|_K = \sigma'|_K \cdot \sigma''|_K = f(\sigma') \cdot f(\sigma'')$$

وذلك لأن $\sigma''|_K(b) \in K$ وذلك أياً كان $b \in K$.

لنبرهن على أن f متباين. ليكن $\tau \in \text{Ker}(f)$ عندئذ فإن $\tau|_K = I_K$ ولما كان $\tau: K \cdot L \rightarrow K \cdot L$ هو L -تماثل ذاتي للحقل $K \cdot L$ نجد أنه أياً كان $b \in K$ و $c \in L$ فإن:

$$\tau(b \cdot c) = \tau(b) \cdot \tau(c) = \tau|_K(b) \cdot \tau(c) = b \cdot c$$

وهذا يبين أن $\tau = I_{K \cdot L}$ ، أي أن $\text{Ker}(\tau) = \{I_{K \cdot L}\}$ ومنه نجد أن f متباين. وحسب مبرهنة التماثل الأولى نجد أن

$$G(K \cdot L/L) = \frac{G(K \cdot L/L)}{\text{Ker}(f)} \cong \text{Im}(f)$$

ولما كان الحقل K هو حقل تفريق فوق F فإن K هو تمديد منته للحقل F وأن $\text{Im}(f)$ زمرة جزئية من الزمرة $G(K/F)$ وحسب المبرهنة (٩-١-٤) يكون:

$$G(K/F(\text{Im}(f))) = \text{Im}(f)$$

أصبح لدينا:

$$G(K \cdot L/L) \cong G(K/F(Im(f))) \quad (*)$$

من جهة أخرى، لدينا حسب (١) أن $K \cdot L$ هو حقل تفريق فوق L وحسب المبرهنة (٩-٩-

$$F(G(K \cdot L/L)) = L \quad (١-٢)$$

لنبرهن على أن $F(Im(f)) = K \cap F(G(K \cdot L/L)) = K \cap L$ لدينا:

$$F(Im(f)) = \{a : a \in K; \tau(a) = a; \forall \tau \in Im(f)\}$$

وذلك لأن $Im(f) \subseteq G(K/F)$ وأن $F(Im(f)) \subseteq K$ ولدينا أيضاً:

$$F(G(K \cdot L/L)) = \{b : b \in K \cdot L; \mu(b) = b; \forall \mu \in G(K \cdot L/L)\}$$

ليكن $a \in F(Im(f))$ عندئذ فإن $a \in K$ وأنه أياً كان $\mu \in G(K \cdot L/L)$ فإن:

$$f(\mu) = \mu|_K \in Im(f)$$

ويحقق $\mu(a) = \mu|_K(a) = a$ وهذا يبين أن $a \in F(G(K \cdot L/L))$ ومنه نجد أن:

$$F(Im(f)) \subseteq K \cap F(G(K \cdot L/L))$$

ليكن $b \in K \cap F(G(K \cdot L/L))$ عندئذ $b \in K$ وأنه أياً كان $\lambda \in Im(f)$ فإن

$$\lambda = f(\theta) \text{ حيث } \theta \in G(K \cdot L/L) \text{ ومنه فإن } \theta(b) = b \text{ ولما كان:}$$

$$\lambda = f(\theta) = \theta|_K$$

نجد أن $\lambda(b) = \theta|_K(b) = \theta(b) = b$ وهذا يبين أن $b \in F(Im(f))$ وهكذا فإن:

$$K \cap F(G(K \cdot L/L)) \subseteq F(Im(f))$$

وبالتالي يكون $F(Im(f)) = K \cap F(G(K \cdot L/L))$ مما سبق نجد أن:

$$F(Im(f)) = K \cap L$$

وحسب العلاقة (*) نجد أن:

$$G(K \cdot L/L) \cong G(K/F(Im(f))) = G(K/K \cap L)$$

مبرهنة ٩-٢-٩.

ليكن K_1, K_2 حقلَي تفريق فوق الحقل F بحيث $K_1 \cap K_2 = F$ عندئذ فإن:

$$G(K_1 \cdot K_2/F) \cong G(K_1/F) \times G(K_2/F)$$

البرهان.

لما كان K_i حيث $i=1,2$ حقل تفريق فوق F فإن K_i هو تمديد منته للحقل F وبالتالي هو تمديد جبري للحقل F ولما كان مميز الحقل F يساوي الصفر فإنه حسب التمهيدية (١-٣-٥) فإن K_i هو تمديد منفصل للحقل F وحسب المبرهنة (١٤-٣-٥) فإنه يوجد $\theta_i \in K_i$ بحيث يكون $K_i = F(\theta_i)$.

لنفرض أن $f_i(x) \in F[x]$ الحدودية الأصغرية للعنصر θ_i فوق F ، لما كان لأجل كل $\sigma \in G(K_i/F)$ فإن $\sigma(\theta_i)$ هو صفر للحدودية $f_i(x)$ وذلك حسب التمهيدية (٩-٢-١) نجد أن K_i هو حقل تفريق الحدودية $f_i(x)$ فوق F ومنه نجد أن:

$$K_1 \cdot K_2 = F(\theta_1) \cdot F(\theta_2) = F(\theta_1, \theta_2)$$

هو حقل تفريق الحدودية $f_1(x) \cdot f_2(x) \in F[x]$ فوق F .

ليكن $\sigma \in G(K_1 \cdot K_2/F)$ عندئذ فإن $\sigma: K_1 \cdot K_2 \rightarrow K_1 \cdot K_2$ هو F -تماثل ذاتي للحقل $K_1 \cdot K_2$ ومنه فإن $\sigma|_{K_i}: K_i \rightarrow K_1 \cdot K_2$ تشاكل للحقل K_i في الحقل $K_1 \cdot K_2$ وحسب المبرهنة (٩-٢-٦) يكون $\sigma|_{K_i}: K_i \rightarrow K_i$ هو F -تماثل ذاتي للحقل K_i وذلك لأن K_i حقل تفريق فوق F ، أي أن:

$$\sigma|_{K_1} \in G(K_1/F), \quad \sigma|_{K_2} \in G(K_2/F)$$

لنعرف العلاقة:

$$f: G(K_1 \cdot K_2/F) \rightarrow G(K_1/F) \times G(K_2/F)$$

بالشكل الآتي: أي أن $\sigma \in G(K_1 \cdot K_2/F)$ فإن:

$$f(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2}) \in G(K_1/F) \times G(K_2/F)$$

ف نجد أن f تطبيق، لأنه إذا كان $\sigma', \sigma'' \in G(K_1 \cdot K_2/F)$ بحيث $\sigma' = \sigma''$ فإنه أيًا كان $a \in K_i \subseteq K_1 \cdot K_2$ فإن:

$$\sigma'|_{K_i}(a) = \sigma'(a) = \sigma''(a) = \sigma''|_{K_i}(a)$$

ومنه نجد أن $\sigma'|_{K_i} = \sigma''|_{K_i}$ ، أي أن:

$$f(\sigma') = (\sigma'|_{K_1}, \sigma'|_{K_2}) = (\sigma''|_{K_1}, \sigma''|_{K_2}) = f(\sigma'')$$

وأن f تشاكل، لأن $(\sigma' \cdot \sigma'')|_{K_i} = (\sigma' \cdot \sigma'')|_{K_i}$ وهنا نجد أنه لأجل كل $a \in K_i \subseteq K_1 \cdot K_2$ فإن:

$$\begin{aligned}\sigma' \cdot \sigma''|_{K_i}(a) &= \sigma' \cdot \sigma''(a) = \sigma'(\sigma''(a)) = \sigma'(\sigma''|_{K_i}(a)) = \\ &= \sigma'(\sigma''|_{K_i}(a)) = \sigma'|_{K_i}(\sigma''|_{K_i}(a)) = \sigma'|_{K_i} \cdot \sigma''|_{K_i}(a)\end{aligned}$$

وبالتالي فإن $\sigma' \cdot \sigma''|_{K_i} = \sigma'|_{K_i} \cdot \sigma''|_{K_i}$ وهذا يبين أن:

$$\begin{aligned}f(\sigma' \cdot \sigma'') &= (\sigma' \cdot \sigma''|_{K_1}, \sigma' \cdot \sigma''|_{K_2}) = (\sigma'|_{K_1} \cdot \sigma''|_{K_1}, \sigma'|_{K_2} \cdot \sigma''|_{K_2}) = \\ &= f(\sigma') \cdot f(\sigma'')\end{aligned}$$

لنبرهن على أن f متباين. ليكن $\tau \in \text{Ker}(f)$ عندئذ فإن:

$$f(\tau) = (I_{K_1}, I_{K_2}), \quad f(\tau) = (\tau|_{K_1}, \tau|_{K_2})$$

ومنه نجد أن $(\tau|_{K_1}, \tau|_{K_2}) = (I_{K_1}, I_{K_2})$ أي أن $\tau|_{K_i} = I_{K_i}$ حيث $i=1,2$. ومنه أيضاً كان $b_1 \in K_1, b_2 \in K_2$ فإن:

$$\tau(b_1 \cdot b_2) = \tau(b_1) \cdot \tau(b_2) = \tau|_{K_1}(b_1) \cdot \tau|_{K_2}(b_2) = I_{K_1}(b_1) \cdot I_{K_2}(b_2) = b_1 \cdot b_2$$

وهذا يبين أن $\tau = I_{K_1 \cdot K_2}$ ، أي أن $\text{Ker}(f) = \{I_{K_1 \cdot K_2}\}$ ومنه فإن f متباين. وحسب مبرهنة التماثل الزمري الأولى نجد أن:

$$\begin{aligned}G(K_1 \cdot K_2/F) &= G(K_1 \cdot K_2/F)/\text{Ker}(f) \cong \text{Im}(f) \subseteq \\ &\subseteq G(K_1/F) \times G(K_2/F)\end{aligned}$$

ولما كان كل من K_1, K_2 حقل تفريق فوق F فإنه حسب المبرهنة (٩-٢-١) يكون:

$$(G(K_1/F):1) = [K_1:F], \quad (G(K_2/F):1) = [K_2:F]$$

أيضاً لما كان $K_1 \cdot K_2$ حقل تفريق فوق F فإنه حسب المبرهنة (٩-٢-١) يكون:

$$(G(K_1 \cdot K_2/F):1) = [K_1 \cdot K_2:F]$$

ولما كان حسب الفرض $K_1 \cap K_2 = F$ فإنه حسب المبرهنة (٩-٢-٨) يكون:

$$[K_1 \cdot K_2:F] = [K_1:F] \cdot [K_2:F]$$

ومنه يكون:

$$\begin{aligned}(G(K_1 \cdot K_2/F):1) &= (G(K_1/F):1) \cdot (G(K_2/F):1) = \\ &= G(K_1/F) \times G(K_2/F) \quad (*)\end{aligned}$$

ولما كان

$$G(K_1 \cdot K_2/F) \cong \text{Im}(f) \subseteq G(K_1/F) \times G(K_2/F)$$

فإنه حسب العلاقة (*) نجد أن $G(K_1 \cdot K_2/F) \cong G(K_1/F) \times G(K_2/F)$.

مبرهنة ٩-٢-١٠.

ليكن K حقل تفريق فوق F ولنفرض أن الحقل L تمديد للحقل F وأن M حقل تفريق فوق L . عندئذ فإن:

١ - الحقل $K \cap M$ هو حقل تفريق فوق $K \cap L$.

$$٢ - [K \cap M : K \cap L] = [(K \cap M) \cdot L : L] = \frac{[M : L]}{[K \cdot M : K \cdot M]}$$

$$٣ - G(K \cap M / K \cap L) \cong G((K \cap M) \cdot L / L)$$

البرهان.

١ - لما كان K حقل تفريق فوق F فإن K هو تمديد منته وبالتالي جبري للحقل F ولما كان:

$$F \subseteq K \cap L \subseteq K \cap M \subseteq K$$

نجد أن $K \cap M$ هو تمديد منته وبالتالي جبري للحقل $K \cap L$ ولما كان مميز الحقل F يساوي الصفر نجد أن الحقل $K \cap M$ هو أيضاً تمديد منفصل للحقل $K \cap L$ وحسب المبرهنة (٥-٣-١٤) يوجد $\theta \in K \cap M$ بحيث يكون:

$$K \cap M = (K \cap L)(\theta)$$

لنفرض أن $f(x) \in (K \cap L)[x]$ الحدودية الأصغرية للعنصر θ فوق $K \cap L$. من جهة أخرى، لما كان K حقل تفريق فوق F وأن $F \subseteq K \cap L \subseteq K$ فإنه حسب التمهيدية (٤-٢-٩) يكون K حقل تفريق فوق $K \cap L$ ولما كانت $f(x)$ الحدودية الأصغرية للعنصر θ فوق $K \cap L$ فإنه حسب المبرهنة (٩-٢-٩) الحدودية $f(x)$ تتفرق في $K[x]$ إلى مضاريب خطية وحسب المبرهنة (٨-١-١٤) فإن $f(x) \in L[x]$ هي ذاتها الحدودية الأصغرية للعنصر θ فوق L .

لما كان M حقل تفريق فوق L فإن $f(x)$ تتفرق في $M[x]$ إلى مضاريب خطية ومنه فإن $f(x)$ تتفرق في $(K \cap M)[x]$ إلى مضاريب خطية وهذا يبين أن $K \cap M$ هو حقل تفريق فوق $K \cap L$.

٢ - وجدنا حسب (١) أن $K \cap M$ هو حقل تفريق فوق $K \cap L$.
 من جهة أخرى، لما كان $F \subseteq K \cap L \subseteq L \subseteq M$ حقل تفريق فوق L فإن
 M تمديد منته للحقل L وبالتالي يكون L تمديداً منتهياً للحقل $K \cap L$ وحسب المبرهنة
 (٨-٢-٩) يكون الحقل $(K \cap M) \cdot L$ حقل تفريق فوق L .
 أيضاً حسب المبرهنة (٨-٢-٩) نجد أن:

$$[(K \cap M) \cdot L : L] = [K \cap M : K \cap L]$$

من جهة ثالثة، لما كان K حقل تفريق فوق F وأن L تمديد للحقل F فإنه حسب
 المبرهنة (٨-٢-٩) يكون:

$$[K \cdot L : L] = [K : K \cap L]$$

أيضاً لما كان K حقل تفريق فوق F وأن M تمديد منته للحقل F فإنه حسب المبرهنة
 (٨-٢-٩) يكون:

$$[K \cdot M : M] = [K : K \cap M]$$

ولما كان $K \cap L \subseteq K \cap M \subseteq K$ نجد أن:

$$[K : K \cap L] = [K : K \cap M] \cdot [K \cap M : K \cap L]$$

ومنه يكون:

$$[K \cap M : K \cap L] = \frac{[K : K \cap L]}{[K : K \cap M]} = \frac{[K \cdot L : L]}{[K \cdot M : M]}$$

أيضاً لما كان $L \subseteq K \cdot L \subseteq K \cdot M$ نجد أن:

$$[K \cdot M : L] = [K \cdot M : K \cdot L] \cdot [K \cdot L : L]$$

ومنه يكون:

$$\begin{aligned} [K \cap M : K \cap L] &= \frac{[K \cdot L : L]}{[K \cdot M : M]} = \frac{[K \cdot M : L] / [K \cdot M : K \cdot L]}{[K \cdot M : M]} = \\ &= \frac{[K \cdot M : L]}{[K \cdot M : K \cdot L] \cdot [K \cdot M : M]} \end{aligned}$$

ولما كان $L \subseteq M \subseteq K \cdot M$ نجد أن:

$$[K \cap M : K \cap L] = \frac{[K \cdot M : L]}{[K \cdot M : K \cdot L] \cdot [K \cdot M : M]} =$$

$$= \frac{[K \cdot M : M] \cdot [M : L]}{[K \cdot M : K \cdot L] \cdot [K \cdot M : M]} = \frac{[M : L]}{[K \cdot M : K \cdot L]}$$

٣ - وجدنا حسب (١) أن $K \cap M$ حقل تفريق فوق $K \cap L$ ومنه حسب المبرهنة (٨-٢-٩) فإن:

$$G(K \cap M / K \cap L) \cong G((K \cap M) \cdot L / L)$$

وهو المطلوب إثباته. ◊

٩ - ٣. تطبيقات على نظرية غالوا.

في هذه الفقرة سوف نورد عدداً من التطبيقات على نظرية غالوا.

تطبيق ٩-٣-١.

لتكن $p(x) = x^4 - 2x^2 - 4 \in Q[x]$. لنفرض أن:

$$\alpha = \sqrt{1 + \sqrt{5}}, \quad \beta = i\sqrt{\sqrt{5} - 1}$$

والمطلوب:

١ - أثبت أن كلاً من α, β هي أصفار للحدودية $p(x)$ ، ثم أوجد جميع الأصفار الأخرى للحدودية $p(x)$.

٢ - أثبت أن الحدودية $p(x)$ أولية فوق Q .

٣ - أوجد درجة تمديد الحقل $K = Q(\alpha)$ فوق Q ثم أثبت أن الحقل $K_0 = Q(\alpha, i)$ هو حقل تفريق الحدودية $p(x)$ فوق Q .

٤ - أثبت أن الحقل K_0 هو تمديد غالوا للحقل Q .

الحل.

١ - لما كان $\alpha = \sqrt{1 + \sqrt{5}}$ نجد أن $\alpha^2 = 1 + \sqrt{5}$ ومنه يكون:

$$\alpha^4 = 6 + 2\sqrt{5} = 4 + 2(1 + \sqrt{5}) = 4 + 2\alpha^2$$

ومنه يكون $\alpha^4 - 2\alpha^2 - 4 = 0$ وهذا يبين أن α هو صفر للحدودية $p(x)$.

أيضاً لدينا $\beta = i\sqrt{\sqrt{5} - 1}$ ومنه فإن $\beta^2 = 1 - \sqrt{5}$ ومنه يكون:

$$\beta^4 = 6 - 2\sqrt{5} = 4 + 2(1 - \sqrt{5}) = 4 + 2\beta^2$$

ومنه يكون $\beta^4 - 2\beta^2 - 4 = 0$ وهذا يبين أن β هو صفر للحدودية $p(x)$.

بطريقة مشابهة يمكن التأكد أن أصفار الحدودية $p(x)$ هي:

$$\pm \alpha = \pm \sqrt{1 + \sqrt{5}}, \quad \pm \beta = \pm i\sqrt{\sqrt{5} - 1}$$

٢ - من الواضح أن $\pm \beta = \pm i\sqrt{\sqrt{5} - 1} \notin Q$.

أيضاً إن $\pm \alpha = \pm \sqrt{1 + \sqrt{5}} \notin Q$ ، لأنه إذا كان $\alpha = \sqrt{1 + \sqrt{5}} \in Q$ عندئذ يكون

$1 + \sqrt{5} \in Q$ وبالتالي يكون $\sqrt{5} \in Q$ وهذا غير ممكن. ومنه نجد أن جميع أصفار

الحدودية $p(x)$ لا تنتمي للحقل Q . وهنا سوف نناقش الحالات الآتية:

- لما كانت الأصفار الأربعة السابقة لا تنتمي للحقل Q فإن الحدودية $p(x)$ لا يمكن كتابتها على شكل جداء لحدوديات من الحلقة $Q[x]$ درجة كل منها يساوي الواحد.

- لنفرض جديلاً أن $p(x) = f(x) \cdot g(x)$ حيث $f(x), g(x) \in Q[x]$ وأنه إما:

$$\partial f(x) = 1 \text{ أو } \partial g(x) = 1$$

إذا كان $\partial f(x) = 1$ عندئذ فإن $f(x) = x - a$ حيث $a \in Q$ وأن:

$$a \in \{\pm\alpha = \pm\sqrt{1+\sqrt{5}}, \pm\beta = \pm i\sqrt{\sqrt{5}-1}\}$$

وهذا غير ممكن.

بالطريقة نفسها نجد أنه من غير الممكن أن يكون $\partial g(x) = 1$.

- لنفرض جديلاً أن $p(x) = f(x) \cdot g(x)$ حيث $f(x), g(x) \in Q[x]$ وأن:

$$\partial f(x) = \partial g(x) = 2$$

لما كان $p(\alpha) = 0$ نجد أن $f(\alpha) \cdot g(\alpha) = 0$ ومنه إما $f(\alpha) = 0$ أو $g(\alpha) = 0$. لنفرض أن $f(\alpha) = 0$ ولما كانت $\partial f(x) = 2$ نجد أن $f(x) = x^2 - \alpha \notin Q[x]$. بالطريقة نفسها نجد أنه لا يمكن إيجاد $g(x) \in Q[x]$ بحيث $\partial g(x) = 2$ و $g(\alpha) = 0$. بهذا الشكل نجد أنه لا يمكن كتابة $p(x)$ على شكل جداء لحدوديات من $Q[x]$ درجة كل منها أقل تماماً من 4 وهذا يبين أن الحدودية $p(x)$ أولية فوق Q .

٣ - وجدنا حسب (٢) أن الحدودية $p(x)$ أولية فوق Q وأن α صفر لها ومنه نجد أن $p(x)$ هي الحدودية الأصغرية للعنصر α فوق Q وحسب المبرهنة (٣-٣-٥) نجد أن

$$[K : Q] = [Q(\alpha) : Q] = \partial p(x) = 4$$

لدينا حسب التعريف أن حقل تفريق الحدودية $p(x)$ فوق Q هو الحقل $Q(\alpha, \beta)$ ، لأنه أصغر حقل يحوي كلاً من Q وجميع أصفار الحدودية $p(x)$. لنبرهن على أن $Q(\alpha, \beta) = Q(\alpha, i)$.

لما كان $\alpha, \beta \in Q(\alpha, \beta)$ فإن $\alpha \cdot \beta \in Q(\alpha, \beta)$ وأن:

$$\alpha \cdot \beta = (\sqrt{1+\sqrt{5}}) \cdot (i\sqrt{\sqrt{5}-1}) = i \cdot \sqrt{(1+\sqrt{5}) \cdot (1-\sqrt{5})} = 2i$$

ولما كان $1/2 \in Q(\alpha, \beta)$ نجد أن $i = 1/2 \alpha \cdot \beta \in Q(\alpha, \beta)$ وهذا يبين أن:

$$Q(\alpha, i) \subseteq Q(\alpha, \beta)$$

من جهة أخرى، لما كان $\alpha \in Q(\alpha, \beta)$ فإن $\alpha^{-1} \in Q(\alpha, \beta)$ وأيضاً لدينا $a \cdot \beta = 2i$ ومنه نجد أن $\beta = 2i\alpha^{-1} \in Q(\alpha, i)$ وبالتالي يكون $Q(\alpha, \beta) \subseteq Q(\alpha, i)$ ، مما سبق نجد أن $Q(\alpha, \beta) = Q(\alpha, i)$ ، وهذا يبين أن الحقل $K_0 = Q(\alpha, i)$ هو حقل تفريق الحدودية $p(x)$ فوق Q .

٤ - لما كان مميز الحقل Q يساوي الصفر وأن $p(x) \in Q[x]$ و $\partial p(x) > 0$ فإنه حسب التمهيدية (٥-٢-٢) تكون الحدودية $p(x)$ منفصلة فوق Q ولما كان K_0 حقل تفريق الحدودية المنفصلة $p(x)$ فوق Q فإنه حسب المبرهنة (٩-٣-٦) يكون الحقل K_0 تمديد غالوا للحقل Q .

وجدنا حسب (٣) أن الحقل $K_0 = Q(\alpha, i)$ هو حقل تفريق الحدودية $p(x)$ فوق Q وحسب المبرهنة (٩-٢-١) يكون:

$$(G(K_0/Q):1) = [K_0:Q] = [Q(\alpha, i):Q]$$

ولما كان الحقل $Q(\alpha, i)$ تمديداً منتهياً للحقل Q وأن $Q \subseteq Q(\alpha) \subseteq Q(\alpha, i)$ فإن:

$$[Q(\alpha, i):Q] = [Q(\alpha, i):Q(\alpha)] = [Q(\alpha):Q]$$

وجدنا حسب (٣) أن $[Q(\alpha):Q] = 4$.

لنوجد الآن $[Q(\alpha, i):Q(\alpha)]$.

لما كانت الحدودية $x^2 + 1 \in Q(\alpha)[x]$ هي الحدودية الأصغرية للعنصر $i \in Q(\alpha, i)$ فوق $Q(\alpha)$ وأن $\partial(x^2 + 1) = 2$ نجد أن:

$$[Q(\alpha, i):Q(\alpha)] = \partial(x^2 + 1) = 2$$

مما سبق نجد أن $[Q(\alpha, i):Q] = 4 \cdot 2 = 8$. بهذا الشكل نجد أن الزمرة $G(K_0/Q)$ تتألف من ثمانية عناصر كل منها هو Q -تماثل ذاتي للحقل $K_0 = Q(\alpha, i)$ ، أي أن الزمرة $G(K_0/Q)$ تتألف من العناصر الآتية:

$$\sigma_j : Q(\alpha, i) \rightarrow Q(\alpha, i)$$

حيث $j = 1, 2, \dots, 8$ وأن كلاً من العناصر السابقة هو Q -تماثل ذاتي للحقل $Q(\alpha, i)$. لنفرض أن $\sigma_1 = I_{Q(\alpha, i)}$ ، سوف نورد العناصر السابقة من خلال الجدول الآتي:

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
$\alpha \rightarrow$	α	$-\alpha$	β	$-\beta$	α	$-\alpha$	β	$-\beta$
$i \rightarrow$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

نلاحظ أن جميع عناصر الزمرة $G(K_0/Q)$ المختلفة عن المحايد لها مرتبة تساوي 2. لنوجد على سبيل المثال مرتبة العنصر σ_4 .

$$\sigma_4^2(\alpha) = \sigma_4(\sigma_4(\alpha)) = \sigma_4(-\beta) = -\sigma_4(\beta)$$

ولما كان $\alpha\beta = 2i$ نجد أن:

$$\sigma_4(\alpha\beta) = \sigma_4(2i) = 2\sigma_4(i) = 2i = \alpha\beta$$

ومنه فإن $\sigma_4(\alpha) \cdot \sigma_4(\beta) = \alpha\beta$ وبالتالي يكون $\beta \cdot \sigma_4(\beta) = \alpha\beta$ - ومنه نجد أن $\sigma_4(\beta) = -\alpha$ وهكذا فإن:

$$\sigma_4^2(\alpha) = -\sigma_4(\beta) = -(-\alpha) = \alpha$$

$$\sigma_4^2(i) = \sigma_4(\sigma_4(i)) = \sigma_4(i) = i$$

ولما كان σ_4 هو Q -تماثلاً ذاتياً للحقل K_0 نجد أن $\sigma_4^2 = I_{K_0}$ وهذا يبين أن $o(\sigma_4) = 2$. بالطريقة نفسها نوجد مراتب العناصر الأخرى. ♦

تطبيق ٩-٣-٢.

لنأخذ الحقل $Q(\sqrt{2}, i)$ والمطلوب:

- ١ - أوجد درجة تمديد الحقل $Q(\sqrt{2}, i)$ فوق Q .
- ٢ - أثبت أن الحقل $Q(\sqrt{2}, i)$ هو حقل تفريق فوق Q .
- ٣ - أثبت أن الحقل $Q(\sqrt{2}, i)$ هو تمديد غالوا لكل من $Q(\sqrt{2})$ و Q وأن الحقل $Q(\sqrt{2})$ هو تمديد غالوا للحقل Q .
- ٤ - أوجد الزمرة $G(Q(\sqrt{2}, i)/Q)$.
- ٥ - أثبت أن الزمرة $G(Q(\sqrt{2}, i)/Q)$ ليست دوارة.
- ٦ - أثبت أن $G(Q(\sqrt{2}, i)/Q) \cong Z_2 \oplus Z_2$.
- ٧ - أوجد كل من $G(Q(\sqrt{2}, i)/Q(\sqrt{2}))$, $G(Q(\sqrt{2}, i)/Q(i))$.

الحل.

١ - لما كان الحقل $Q(\sqrt{2}, i)$ تمديداً منتهياً للحقل $Q(\sqrt{2})$ وأن الحقل $Q(\sqrt{2})$ تمديد منته للحقل Q فإن:

$$[Q(\sqrt{2}, i) : Q] = [Q(\sqrt{2}, i) : Q(\sqrt{2})] \cdot [Q(\sqrt{2}) : Q]$$

لما كانت $x^2 - 2 \in Q[x]$ الحدودية الأصغرية للعنصر $\sqrt{2}$ فوق Q فإن:

$$[Q(\sqrt{2}) : Q] = \partial(x^2 - 2) = 2$$

أيضاً لما كانت الحدودية $x^2 + 2 \in Q(\sqrt{2})[x]$ هي الحدودية الأصغرية للعنصر i فوق الحقل $Q(\sqrt{2})$ فإن:

$$[Q(\sqrt{2}, i) : Q(\sqrt{2})] = \partial(x^2 + 1) = 2$$

ومنه نجد أن $[Q(\sqrt{2}, i) : Q] = 2 \cdot 2 = 4$.

٢ - إن الحدودية $p(x) = x^4 - x^2 - 2 \in Q[x]$ وأن أصفارها هي $\{\pm\sqrt{2}, \pm i\}$.
لما كان الحقل $Q(\sqrt{2}, i)$ مولداً فوق الحقل Q بجميع أصفار الحدودية $p(x)$ فإن $Q(\sqrt{2}, i)$ هو حقل تفريق الحدودية $p(x)$ فوق Q .

٣ - لما كان مميز الحقل Q يساوي الصفر وأن $p(x) \in Q[x]$ و $\partial p(x) > 0$ فإنه حسب التمهيدية (٢-٢-٥) تكون الحدودية $p(x)$ منفصلة فوق Q ولما كان الحقل $Q(\sqrt{2}, i)$ هو حقل تفريق الحدودية المنفصلة $p(x)$ فوق Q فإنه حسب المبرهنة (٩-٦-٣) يكون الحقل $Q(\sqrt{2}, i)$ هو تمديد غالوا للحقل Q ولما كان $Q(\sqrt{2})$ هو حقل جزئي من الحقل $Q(\sqrt{2}, i)$ ويحوي Q ، أي $Q \subseteq Q(\sqrt{2}) \subseteq Q(\sqrt{2}, i)$ فإنه حسب التمهيدية (٩-٣-٧) يكون الحقل $Q(\sqrt{2}, i)$ تمديد غالوا للحقل $Q(\sqrt{2})$.

أيضاً إن الحقل $Q(\sqrt{2})$ هو تمديد غالوا للحقل Q لأنه حقل تفرق الحدودية المنفصلة $x^2 - 2 \in Q[x]$ فوق Q .

٤ - لما كان الحقل $Q(\sqrt{2}, i)$ هو حقل تفريق فوق Q فإنه حسب المبرهنة (٩-٢-١) يكون:

$$(G(Q(\sqrt{2}, i)/Q) : 1) = [Q(\sqrt{2}, i) : Q] = 4$$

ومنه فإن الزمرة $G(Q(\sqrt{2}, i)/Q)$ تتألف من أربعة عناصر لنرمز لها:

$$\sigma_j : Q(\sqrt{2}, i) \rightarrow Q(\sqrt{2}, i)$$

حيث $j = 1, 2, 3, 4$ وأن $\sigma_1 = I_{Q(\sqrt{2}, i)}$ وكل من هذه العناصر هو Q - تماثل ذاتي للحقل $Q(\sqrt{2}, i)$. الجدول الآتي يبين لنا هذه العناصر:

	σ_1	σ_2	σ_3	σ_4
$\sqrt{2} \rightarrow$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$i \rightarrow$	i	$-i$	i	$-i$

٥ - لنوجد مرتبة عناصر الزمرة $G(Q(\sqrt{2}, i)/Q)$ ، إن $o(\sigma_2) = o(\sigma_3) = 2$ لأن:

$$\sigma_2^2(\sqrt{2}) = \sigma_2(\sigma_2(\sqrt{2})) = \sigma_2(\sqrt{2}) = \sqrt{2}$$

$$\sigma_2^2(i) = \sigma_2(\sigma_2(i)) = \sigma_2(i) = i$$

ولما كان σ_2 هو Q - تماثلاً ذاتياً للحقل $Q(\sqrt{2}, i)$ فإن σ_2^2 هو أيضاً Q - تماثل ذاتي

للحقل $Q(\sqrt{2}, i)$ ، وهذا يبين أن $\sigma_2^2 = I_{Q(\sqrt{2}, i)}$ ومنه $o(\sigma_2) = 2$.

أيضاً إن $o(\sigma_3) = 2$ ، لأن:

$$\sigma_3^2(\sqrt{2}) = \sigma_3(\sigma_3(\sqrt{2})) = \sigma_3(-\sqrt{2}) = -\sigma_3(\sqrt{2}) = -(-\sqrt{2}) = \sqrt{2}$$

$$\sigma_3^2(i) = \sigma_3(\sigma_3(i)) = \sigma_3(i) = i$$

لما كان σ_3 هو Q - تماثلاً ذاتياً للحقل $Q(\sqrt{2}, i)$ فإن σ_3^2 هو أيضاً Q - تماثل ذاتي

للحقل $Q(\sqrt{2}, i)$ ومنه نجد أن $\sigma_3^2 = I_{Q(\sqrt{2}, i)}$ وبالتالي تكون $o(\sigma_3) = 2$.

بطريقة مشابهة نجد أن $o(\sigma_4) = 2$ ومنه نجد أن الزمرة $G(Q(\sqrt{2}, i)/Q)$ لا تحوي عنصراً مرتبته 4 وبالتالي فهي دوار.

٦ - لما كان $o(\sigma_2) = o(\sigma_3) = 2$ فإن كلا من σ_2, σ_3 يولد زمرة جزئية دوار مرتبتها 2 وهذه الزمر هي:

$$\langle \sigma_2 \rangle = \{\sigma_1, \sigma_2\}, \quad \langle \sigma_3 \rangle = \{\sigma_1, \sigma_3\}$$

ولما كانت الزمرة $G(Q(\sqrt{2}, i)/Q)$ تبديلية فإن الجداء $\langle \sigma_2 \rangle \times \langle \sigma_3 \rangle$ يكون زمرة جزئية

في $G(Q(\sqrt{2}, i)/Q)$. لنبرهن على أن $\langle \sigma_2 \rangle \times \langle \sigma_3 \rangle = G(Q(\sqrt{2}, i)/Q)$.

لنشكل الجدول الآتي:

	σ_1	σ_2
σ_1	σ_1	σ_2
σ_3	σ_3	$\sigma_3 \cdot \sigma_2$

لنبرهن على أن $\sigma_3 \cdot \sigma_2 = \sigma_4$. نلاحظ أن:

$$\sigma_3 \cdot \sigma_2(\sqrt{2}) = \sigma_3(\sigma_2(\sqrt{2})) = \sigma_3(\sqrt{2}) = -\sqrt{2} = \sigma_4(\sqrt{2})$$

$$\sigma_3 \cdot \sigma_2(i) = \sigma_3(\sigma_2(i)) = \sigma_3(-i) = -\sigma_3(i) = -i = \sigma_4(i)$$

ولما كان كل من $\sigma_3, \sigma_2, \sigma_4$ هو Q -تماثلاً ذاتياً للحقل $Q(\sqrt{2}, i)$ نجد أن $\sigma_3 \cdot \sigma_2 = \sigma_4$ وهذا يبين أن:

$$\langle \sigma_2 \rangle \times \langle \sigma_3 \rangle = \{\sigma_1, \sigma_2, \sigma_3, \sigma_3 \cdot \sigma_2 = \sigma_4\}$$

ومنه نجد أن:

$$G(Q(\sqrt{2}, i)/Q) = \langle \sigma_2 \rangle \times \langle \sigma_3 \rangle \cong Z_2 \oplus Z_2 \cong Z/2Z \times Z/2Z$$

٧ - لنوجد أولاً كل من $F(\langle \sigma_2 \rangle), F(\langle \sigma_3 \rangle)$.

لما كان σ_2 هو Q -تماثلاً ذاتياً للحقل $Q(\sqrt{2}, i)$ وأن $\sigma_2(\sqrt{2}) = \sqrt{2}$ نجد أن:

$$F(\langle \sigma_2 \rangle) = Q(\sqrt{2})$$

أيضاً لما كان σ_3 هو Q -تماثلاً ذاتياً للحقل $Q(\sqrt{2}, i)$ وأن $\sigma_3(i) = i$ نجد أن:

$$F(\langle \sigma_3 \rangle) = Q(i)$$

ومنه نجد أن:

$$G(Q(\sqrt{2}, i)/Q(\sqrt{2})) = G(Q(\sqrt{2}, i)/F(\langle \sigma_2 \rangle)) = \langle \sigma_2 \rangle$$

وذلك حسب المبرهنة (٩-١-٤). أيضاً إن:

$$G(Q(\sqrt{2}, i)/Q(i)) = G(Q(\sqrt{2}, i)/F(\langle \sigma_3 \rangle)) = \langle \sigma_3 \rangle$$

وذلك حسب المبرهنة (٩-١-٤). ◊

تطبيق ٩-٣-٣.

لنأخذ التمديد $K = Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$ للحقل Q . والمطلوب:

١ - أثبت أن الحقل K هو تمديد غالوا للحقل Q .

٢ - أثبت أن الحقل K هو تمديد غالوا للحقل لكل من الحقول الآتية $Q(\sqrt{2}, \sqrt{3})$ و $Q(\sqrt{2})$. ثم بين أن الحقل $Q(\sqrt{2}, \sqrt{3})$ هو تمديد غالوا للحقل $Q(\sqrt{2})$.

٣ - أوجد الزمرة $G(K/Q)$.

٤ - أوجد كلاً من الزمر الآتية $G(Q(\sqrt{2})/Q)$ و $G(Q(\sqrt{2}, \sqrt{3})/Q(\sqrt{2}))$ و $G(Q(\sqrt{2}, \sqrt{3})/Q)$.

الحل.

١ - لنأخذ الحدودية $p(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5) \in Q[x]$. إن:

$$p(x) = x^6 - 10x^4 + 31x^2 - 30 \in Q[x]$$

التي مجموعة أصفارها هي $\{\pm\sqrt{2}, \pm\sqrt{3}, \pm\sqrt{5}\}$. نلاحظ أن الحقل K مولد فوق Q بجميع أصفار الحدودية $p(x)$ ، أي أن الحقل K هو حقل تفريق الحدودية $p(x)$ فوق Q ولما كان مميز الحقل Q يساوي الصفر وأن $\partial(p(x)) > 0$ فإنه حسب التمهيدية (٢-٢-٥) تكون الحدودية $p(x)$ منفصلة فوق Q ومنه نجد أن الحقل K هو حقل تفريق حدودية منفصلة فوق Q وبالتالي حسب المبرهنة (٩-٣-٦) يكون الحقل K تمديد غالوا للحقل Q .

٢- وجدنا حسب (١) أن الحقل K هو تمديد غالوا للحقل Q ولما كان كل من $Q(\sqrt{2})$ و $Q(\sqrt{2}, \sqrt{3})$ حقلاً جزئياً في K يحوي Q ، أي:

$$Q \subseteq Q(\sqrt{2}, \sqrt{3}) \subseteq K, \quad Q \subseteq Q(\sqrt{2}) \subseteq K$$

فإنه حسب التمهيدية (٩-٣-٧) يكون الحقل K تمديد غالوا لكل من الحقليين $Q(\sqrt{2})$ و $Q(\sqrt{2}, \sqrt{3})$.

لنأخذ الحدودية $q(x) = (x^2 - 2)(x^2 - 3) = x^4 - 5x^2 + 6 \in Q[x]$ التي مجموعة أصفارها $\{\pm\sqrt{2}, \pm\sqrt{3}\}$ فنجد أن الحقل $Q(\sqrt{2}, \sqrt{3})$ مولد فوق الحقل Q بجميع أصفار الحدودية $q(x)$ ولما كان مميز الحقل Q يساوي الصفر وأن $\partial(q(x)) > 0$ فإنه حسب التمهيدية (٢-٢-٥) تكون الحدودية $q(x)$ منفصلة فوق الحقل Q ومنه نجد أن الحقل $Q(\sqrt{2}, \sqrt{3})$ هو حقل تفريق حدودية منفصلة فوق Q وحسب المبرهنة (٩-٣-٦) يكون الحقل $Q(\sqrt{2}, \sqrt{3})$ هو تمديد غالوا للحقل Q .

لما كان $Q \subseteq Q(\sqrt{2}) \subseteq Q(\sqrt{2}, \sqrt{3})$ فإنه حسب التمهيدية (٩-٣-٧) يكون الحقل $Q(\sqrt{2}, \sqrt{3})$ هو تمديد غالوا للحقل $Q(\sqrt{2})$.

٣ - وجدنا حسب (١) أن الحقل K هو حقل تفريق الحدودية $p(x)$ فوق Q وحسب المبرهنة (٩-٢-١) يكون:

$$(G(K/Q):1) = [K:Q]$$

ولما كان الحقل K تمديداً منتهياً للحقل Q وأن $Q \subseteq Q(\sqrt{2}) \subseteq K$ يكون:

$$[K:Q] = [K:Q(\sqrt{2})] \cdot [Q(\sqrt{2}):Q]$$

ولما كانت الحدودية $x^2 - 2 \in Q[x]$ هي الحدودية الأصغرية للعنصر $\sqrt{2}$ فوق Q نجد أن $2 = \partial(x^2 - 2) = [Q(\sqrt{2}):Q]$. وأن:

$$[Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2})] = \partial(x^2 - 3) = 2$$

فإنه يكون:

$$[K:Q(\sqrt{2})] = [K:Q(\sqrt{2})(\sqrt{3})] \cdot [Q(\sqrt{2})(\sqrt{3}):Q(\sqrt{2})] = 2 \cdot 2 = 4$$

مما سبق نجد أن $(G(K/Q):1) = 8$. أي أن الزمرة (K/Q) مؤلفة من ثمانية عناصر سوف نرمز لها $K \rightarrow \sigma_j$ حيث $j = 1, 2, \dots, 8$ وأن $\sigma_1 = I_K$. لنورد عناصر الزمرة (K/Q) من خلال الجدول الآتي:

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
$\sqrt{2} \rightarrow$	$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3} \rightarrow$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$
$\sqrt{5} \rightarrow$	$\sqrt{5}$	$-\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$	$\sqrt{5}$	$-\sqrt{5}$

إن كلاً من العناصر السابقة هو Q تماثل ذاتي للحقل K .

٤ - إن الحقل $Q(\sqrt{2})$ هو تمديد غالوا للحقل Q لأنه حقل تفريق الحدودية المنفصلة $x^2 - 2 \in Q[x]$ فوق Q وحسب المبرهنة (٩-١-٢) فإن:

$$(G(Q(\sqrt{2})/Q):1)=[Q(\sqrt{2}):Q]=2$$

وبالتالي فإن الزمرة $G(Q(\sqrt{2})/Q)$ تتألف من عنصرين هما σ_1, σ_2 وكل منهما هو Q -تماثل ذاتي للحقل $Q(\sqrt{2})$.

بفرض أن $\sigma_1 = I_{Q(\sqrt{2})}$ فيكون $\sigma_2: Q(\sqrt{2}) \rightarrow Q(\sqrt{2})$ يحقق $\sigma_2(\sqrt{2}) = -\sqrt{2}$. إن مرتبة العنصر σ_2 تساوي 2، لأن:

$$\sigma_2^2(\sqrt{2}) = \sigma_2(\sigma_2(\sqrt{2})) = \sigma_2(-\sqrt{2}) = -\sigma_2(\sqrt{2}) = -(-\sqrt{2}) = \sqrt{2}$$

ومنه فإن $G(Q(\sqrt{2})/Q) \cong Z_2 \cong Z/2Z$. كما أن $F(G(Q(\sqrt{2})/Q)) = Q$. لنوجد الزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q(\sqrt{2}))$.

لما كان الحقل $(Q(\sqrt{2}, \sqrt{3}))$ تمديداً منتهياً للحقل $Q(\sqrt{2})$ وحسب (٣) لدينا:

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

نجد أن:

$$(G(Q(\sqrt{2}, \sqrt{3})/Q(\sqrt{2})):1)=[Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2})]=2$$

ومنه فإن الزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q(\sqrt{2}))$ تتألف من عنصرين هما τ_1, τ_2 كل منهما هو $Q(\sqrt{2})$ -تماثل ذاتي للحقل $(Q(\sqrt{2}, \sqrt{3}))$. إذا كان $\tau_1 = I_{Q(\sqrt{2}, \sqrt{3})}$ عندئذ يكون:

$$\tau_2: Q(\sqrt{2}, \sqrt{3}) \rightarrow Q(\sqrt{2}, \sqrt{3})$$

ويحقق $\tau_2(\sqrt{3}) = -\sqrt{3}$ ، كما أن مرتبة العنصر τ_2 تساوي 2، لأن:

$$\tau_2^2(\sqrt{3}) = \tau_2(\tau_2(\sqrt{3})) = \tau_2(-\sqrt{3}) = -\tau_2(\sqrt{3}) = -(-\sqrt{3}) = \sqrt{3}$$

ومنه فإن الزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q(\sqrt{2}))$ دارة مولدة بالعنصر τ_2 ومنه يكون:

$$G(Q(\sqrt{2}, \sqrt{3})/Q(\sqrt{2})) \cong Z_2 \cong Z/2Z$$

كما أن $F(G(Q(\sqrt{2}, \sqrt{3})/Q(\sqrt{2}))) = Q(\sqrt{2})$.

أما بالنسبة للزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q)$ فإن مرتبتها تساوي 4، لأن:

لنفرض أن $G(Q(\sqrt{2}, \sqrt{3})/Q)$ تتألف من العناصر $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ وكل منها هو Q -تماثل ذاتي للحقل $Q(\sqrt{2}, \sqrt{3})$. هذه العناصر سنوردها من خلال الجدول الآتي:

	φ_1	φ_2	φ_3	φ_4
$\sqrt{2} \rightarrow$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3} \rightarrow$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$

نلاحظ أن كلا من φ_2, φ_3 مرتبته تساوي 2 ، لأن:

$$\varphi_2^2(\sqrt{2}) = \varphi_2(\varphi_2(\sqrt{2})) = \varphi_2(\sqrt{2}) = \sqrt{2}$$

$$\varphi_2^2(\sqrt{3}) = \varphi_2(\varphi_2(\sqrt{3})) = \varphi_2(-\sqrt{3}) = -\varphi_2(\sqrt{3}) = -(-\sqrt{3}) = \sqrt{3}$$

ومنه فإن $o(\varphi_2) = 2$. بالمثل نشبت أن $o(\varphi_3) = 2$ وبالتالي فإن كلا منهما يولد زمرة جزئية دوارة مرتبتها 2 . بفرض أن:

$$H_1 = \langle \varphi_2 \rangle \cong Z_2 \cong Z/2Z$$

$$H_3 = \langle \varphi_3 \rangle \cong Z_2 \cong Z/2Z$$

لما كانت مرتبة الزمرة $G(Q(\sqrt{2}, \sqrt{3})/Q)$ تساوي 4 فإنها تكون تبديلية ومنه فإن $H_1 \cdot H_2$ زمرة جزئية في $G(Q(\sqrt{2}, \sqrt{3})/Q)$. لنوجد عناصر الزمرة $H_1 \cdot H_2$ وذلك من خلال الجدول الآتي:

	φ_1	φ_2
φ_1	φ_1	φ_2
φ_3	φ_3	$\varphi_3\varphi_2$

ومنه فإن $H_1 \cdot H_2 = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$ وهكذا نجد أن:

$$G(Q(\sqrt{2}, \sqrt{3})/Q) = H_1 \cdot H_2 \cong Z_2 \oplus Z_2 \cong Z/2Z \times Z/2Z$$

تطبيق ٩-٣-٤.

لتكن $x^3 - 2 \in Q[x]$ حدودية فوق الحقل Q . والمطلوب:

١ - أوجد حقل التفريق K للحدودية $x^3 - 2$ فوق الحقل Q .

٢ - أثبت أن الحقل K هو تمديد غالوا للحقل Q .

٣ - أوجد درجة تمديد K فوق Q .

- ٤ - أوجد كلاً من الزمرة $G(K/Q)$.
- ٥ - هل الحقل $Q(\sqrt[3]{2})$ هو تمديد غالوا للحقل Q .
- ٦ - هل الحقل $Q(j)$ هو تمديد غالوا للحقل Q .
- ٧ - أثبت أن الحقل K هو تمديد غالوا لكل من الحقليين $Q(j)$ و $Q(\sqrt[3]{2})$ ، ثم أوجد الزمرتين $G(K/Q(j))$ و $G(K/Q(\sqrt[3]{2}))$ ثم بين أن $Q(j) \cap Q(\sqrt[3]{2}) = Q$.
- الحل.**

١ - نلاحظ أن الحدودية $x^3 - 2 \in Q[x]$ أولية فوق Q وأن أصفار هذه الحدودية هي:

$$\sqrt[3]{2}, \sqrt[3]{2}j, \sqrt[3]{2}j^2$$

حيث $j = \frac{-1+i\sqrt{3}}{2}$. ومنه فإن الحقل $K = Q(\sqrt[3]{2}, j)$ هو حقل تفريق الحدودية $x^3 - 2$ فوق Q .

٢ - انفصالية الحقل K . لما كان مميز الحقل Q يساوي الصفر وأن $\partial(x^3 - 2) > 0$ فإنه حسب التمهيدية (٥-٢-٢) تكون الحدودية $x^3 - 2$ منفصلة فوق Q ولما كانت الحدودية $x^3 - 2$ أولية فوق Q فإن $x^3 - 2$ هي الحدودية الأصغرية للعناصر $j, \sqrt[3]{2}$ وحسب التعريف تكون العناصر $j, \sqrt[3]{2}$ منفصلة فوق الحقل Q وحسب المبرهنة (٥-٣-٩) يكون الحقل K تمديداً جبرياً منفصلاً للحقل Q .

من جهة أخرى، إن الحقل $K = Q(\sqrt[3]{2}, j)$ هو تمديد ناظمي للحقل Q وذلك لأنه حقل تفريق حدودية أولية فوق Q وذلك بحسب المبرهنة (٨-١-١). مما سبق نجد أن الحقل K هو تمديد غالوا للحقل Q وذلك لأنه تمديد ناظمي ومنفصل للحقل Q .

٣ - واضح أن $K = Q(\sqrt[3]{2}, j) = Q(\sqrt[3]{2})(j) \subseteq Q(\sqrt[3]{2}) \subseteq Q$ ولما كان الحقل K تمديداً منتهياً للحقل Q نجد أن:

$$[K : Q] = [K : Q(\sqrt[3]{2})] \cdot [Q(\sqrt[3]{2}) : Q]$$

لما كانت الحدودية $x^3 - 2 \in Q[x]$ هي الحدودية الأصغرية للعنصر $\sqrt[3]{2}$ فوق Q فإن $[Q(\sqrt[3]{2}) : Q] = \partial(x^3 - 2) = 3$.

أيضاً لما كانت الحدودية $x^2 + x + 1 \in Q(\sqrt[3]{2})[x]$ هي الحدودية الأصغرية للعنصر j

فوق الحقل $Q(\sqrt[3]{2})$ نجد أن:

$$[Q(\sqrt[3]{2}, j) : Q(\sqrt[3]{2})] = \partial(x^2 + x + 1) = 2$$

مما سبق نجد أن $[K : Q] = 2 \cdot 3 = 6$.

٤ - لما كان الحقل K هو حقل تفريق فوق Q فإنه حسب المبرهنة (٩-٢-١) فإن:

$$(G(K/Q) : 1) = [K : Q]$$

وحسب (٣) يكون $(G(K/Q) : 1) = 6$ ومنه نجد أن الزمرة $G(K/Q)$ تتألف من 6 عناصر وكل من هذه العناصر هو Q -تماثل ذاتي للحقل K . لنرمز لهذه العناصر بالشكل $\sigma_j : K \rightarrow K$ حيث $j = 1, 2, 3, 4, 5, 6$ هذه العناصر سنوردها من خلال الجدول الآتي:

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
$j \rightarrow$	j	j	j	j^2	j^2	j^2
$\sqrt[3]{2} \rightarrow$	$\sqrt[3]{2}$	$\sqrt[3]{2} j$	$\sqrt[3]{2} j^2$	$\sqrt[3]{2}$	$\sqrt[3]{2} j$	$\sqrt[3]{2} j^2$

ومنه فإن $G(K/Q) = \{\sigma_1 = I_K, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$.

٥ - نلاحظ أن الحقل $Q(\sqrt[3]{2})$ ليس تمديداً ناظمياً للحقل Q ، لأنه توجد حدودية أولية $x^3 - 2 \in Q[x]$ تملك صفراً $\sqrt[3]{2} \in Q(\sqrt[3]{2})$ وأن هذا الحقل لا يحوي العناصر المترافقة مع العنصر $\sqrt[3]{2}$ فوق Q والتي هي $\{j\}$. بمعنى آخر، إن الحقل $Q(\sqrt[3]{2})$ لا يحوي جميع أصفار الحدودية $x^3 - 2$ ومنه فإن الحقل $Q(\sqrt[3]{2})$ ليس تمديد غالوا للحقل Q .

٦ - لما كانت الحدودية $x^2 + x + 1$ هي الحدودية الأصغرية للعنصر j فوق Q وأن أصفارها هي $j, j^2 \in Q(j)$ نجد أن الحقل $Q(j)$ هو حقل تفريق حدودية أولية فوق Q وحسب المبرهنة (٨-١-١) نجد أن الحقل $Q(j)$ هو تمديد ناظمي للحقل Q .

من جهة أخرى، لما كانت الحدودية $x^2 + x + 1 \in Q[x]$ أولية فوق Q وأن j صفر لها فإن الحدودية $x^2 + x + 1$ هي الحدودية الأصغرية للعنصر j فوق Q ، ولما كان مميز الحقل Q يساوي الصفر وأن $\partial(x^2 + x + 1) > 0$ فإنه حسب التمهيدية (٥-٢-٢) تكون الحدودية $x^2 + x + 1$ منفصلة فوق Q وبالتالي يكون العنصر j منفصلاً فوق Q .

وحسب المبرهنة (٥-٣-٩) يكون الحقل $Q(j)$ تمديداً منفصلاً للحقل Q ، مما سبق نجد أن الحقل $Q(j)$ هو تمديد غالوا للحقل Q .

٧ - وجدنا حسب (٢) أن الحقل K هو تمديد غالوا للحقل Q ، لما كان:

$$Q \subseteq Q(\sqrt[3]{2}) \subseteq K, \quad Q \subseteq Q(j) \subseteq K$$

وحسب التمهيدية (٩-٣-٧) نجد أن الحقل K هو تمديد غالوا للحقل $Q(\sqrt[3]{2})$ وأن K أيضاً هو تمديد غالوا للحقل $Q(j)$.

لنبرهن على أن $Q(\sqrt[3]{2}) \cap Q(j) = Q$.

نلاحظ أن $Q(\sqrt[3]{2}) \cap Q(j)$ هو حقل جزئي في كل من الحقول $Q(\sqrt[3]{2})$ ، $Q(j)$ ويحوي Q ، أي أن:

$$Q \subseteq Q(\sqrt[3]{2}) \cap Q(j) \subseteq Q(\sqrt[3]{2})$$

$$Q \subseteq Q(\sqrt[3]{2}) \cap Q(j) \subseteq Q(j)$$

ومنه نجد أن $[Q(\sqrt[3]{2}) \cap Q(j) : Q]$ تقسم كلاً من $[Q(\sqrt[3]{2}) : Q]$ و $[Q(j) : Q]$ وذلك لأن كلاً من $Q(\sqrt[3]{2})$ ، $Q(j)$ هو تمديد منته للحقل Q .

لما كان $[Q(\sqrt[3]{2}) : Q] = 3$ و $[Q(j) : Q] = 2$ وأن العددين 2,3 أوليان فيما بينهما نجد أن $[Q(\sqrt[3]{2}) \cap Q(j) : Q] = 1$ وهذا يبين أن $Q(\sqrt[3]{2}) \cap Q(j) = Q$.

لنوجد الزمرة $G(K/Q(j))$.

وجدنا أن $[K : Q] = 6$ وأن $[Q(j) : Q] = 2$ ولما كان $Q \subseteq Q(j) \subseteq K$ وأن K تمديد منته للحقل Q فإن:

$$[K : Q] = [K : Q(j)] \cdot [Q(j) : Q]$$

ومنه نجد أن $[K : Q(j)] = 6/2 = 3$ ومنه فإن الزمرة $G(K/Q(j))$ تتألف من ثلاثة

عناصر هي $\{\sigma_1, \sigma_2, \sigma_3\}$ $G(K/Q(j)) =$ ولما كانت مرتبة الزمرة $G(K/Q(j))$ تساوي 3 فإنها تكون دوائر وتمائل Z_3 ، أي أن $Z_3 \cong Z/3Z \cong G(K/Q(j))$.

لنوجد مولد هذه الزمرة.

نلاحظ أن العنصر $\sigma_2 \in G(K/Q(j))$ ومرتبته تساوي 3، لأن:

$$\sigma_2(j) = j, \quad \sigma_2^2(j) = \sigma_2(\sigma_2(j)) = \sigma_2(j) = j$$

$$\sigma_2^3(j) = \sigma_2(\sigma_2^2(j)) = \sigma_2(j) = j$$

كما أن:

$$\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2} \cdot j$$

$$\sigma_2^2(\sqrt[3]{2}) = \sigma_2(\sigma_2(\sqrt[3]{2})) = \sigma_2(\sqrt[3]{2} \cdot j) = \sigma_2(\sqrt[3]{2}) \cdot \sigma_2(j) = \sqrt[3]{2} \cdot j^2$$

$$\sigma_2^3(\sqrt[3]{2}) = \sigma_2(\sigma_2^2(\sqrt[3]{2})) = \sigma_2(\sqrt[3]{2} \cdot j^2) =$$

$$= \sigma_2(\sqrt[3]{2}) \cdot \sigma_2(j^2) = \sqrt[3]{2} \cdot j^3 = j$$

ولما كان σ_2 هو Q -تماثل ذاتي للحقل K نجد أن $\sigma_2^3 = I_K$ ومنه نجد أن مرتبة العنصر σ_2 تساوي 3 وبالتالي يكون $\langle \sigma_2 \rangle = G(K/Q(j))$.

لنوجد الزمرة $G(K/Q(\sqrt[3]{2}))$.

لما كان $Q \subseteq Q(\sqrt[3]{2}) \subseteq K$ نجد أن:

$$[K : Q] = [K : Q(\sqrt[3]{2})] \cdot [Q(\sqrt[3]{2}) : Q]$$

ولما كان $[Q(\sqrt[3]{2}) : Q] = 3$, $[K : Q] = 6$, نجد أن $[K : Q(\sqrt[3]{2})] = 2$ ومنه نجد

أن الزمرة $G(K/Q(\sqrt[3]{2}))$ تتألف من عنصرين هما σ_1, σ_4 ولما كان $\sigma_1 = I_K$ نجد أن

$$G(K/Q(\sqrt[3]{2})) = \langle \sigma_4 \rangle \cong Z_2 \cong Z/2Z$$

لنفرض أن:

$$G = G(K/Q), \quad H_1 = G(K/Q(j)), \quad H_2 = G(K/Q(\sqrt[3]{2}))$$

واضح أن $H_1 \cap H_2 = \langle e \rangle$ لأن مرتبة كل من H_1, H_2 أعداد أولية فيما بينها. لما

كانت $(H_1 : 1) = 3$ وأن $(G : 1) = 6$ نجد أن $(G : H_1) = \frac{(G : 1)}{(H_1 : 1)} = 2$ وبالتالي

تكون الزمرة الجزئية H_1 ناظمية في G ومنه فإن $H_1 \cdot H_2$ زمرة جزئية في G مؤلفة من

6 عناصر ومنه تكون:

$$_\diamond G = H_1 \cdot H_2 \cong Z/2Z \times Z/2Z$$

تطبيق ٩-٣-٥.

لنفرض أن $p(x) = x^4 - 2 \in Q[x]$. المطلوب:

١ - أوجد حقل التفرق K للحدودية $p(x)$ فوق Q ثم أوجد درجة تمديد K فوق Q

وقاعدته.

٢ - أوجد الزمرة $G(K/Q)$ ثم أثبت أنها ليست تبديلية.

٣ - أثبت أن $G(K/Q) \cong Z/2Z \times Z/2Z \times Z/2Z$.

الحل.

١ - إن الحدودية $p(x)$ أولية فوق Q وذلك حسب معيار إيزنشتاين لأجل العدد الأولي $p=2$. نلاحظ أن العدد الحقيقي $\sqrt[4]{2}$ هو صفر للحدودية $p(x)$ ، لنفرض أن $\alpha = \sqrt[4]{2}$ فنجد أن مجموعة أصفار الحدودية $p(x)$ هي $\{\pm\alpha, \pm i\alpha\}$ ومنه نجد أن الحقل $K = Q(\alpha, i)$ هو حقل تفريق الحدودية $p(x)$ فوق Q وذلك لأنه أصغر حقل يحوي كلاً من Q ومجموعة أصفار الحدودية $p(x)$.

لنفرض أن $E = Q(\alpha)$ ، لما كانت الحدودية $p(x)$ أولية فوق Q وأن $p(\alpha) = 0$ نجد أن $p(x)$ هي الحدودية الأصغرية للعنصر $\alpha = \sqrt[4]{2}$ فوق Q ومنه يكون:

$$[E : Q] = [Q(\alpha) : Q] = \partial p(x) = 4$$

وأن المجموعة $\{1, \alpha, \alpha^2, \alpha^3\}$ تشكل قاعدة للتمديد E فوق Q .

أيضاً لما كانت الحدودية $[x] \in Q(\alpha)[x]$ هي الحدودية الأصغرية للعنصر i فوق $Q(\alpha)$ نجد أن:

$$[Q(\alpha)(i) : Q(\alpha)] = \partial(x^2 + 1) = 2$$

لما كان الحقل K تمديداً منتهياً للحقل Q وأن:

$$Q \subseteq Q(\alpha) \subseteq Q(\alpha)(i) = K$$

نجد أن:

$$\begin{aligned} [K : Q] &= [K : Q(\alpha)] \cdot [Q(\alpha) : Q] = \\ &= [Q(\alpha)(i) : Q(\alpha)] \cdot [Q(\alpha) : Q] = 2 \cdot 4 = 8 \end{aligned}$$

وأن المجموعة $\{1, i\}$ هي قاعدة للتمديد $Q(\alpha)(i)$ فوق $Q(\alpha)$ ومنه نجد أن المجموعة:

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

هي قاعدة التمديد K للحقل Q .

٢ - لما كان الحقل K هو حقل تفرق فوق Q فإنه حسب المبرهنة (٩-٢-١) يكون:

$$(G(K/Q):1)=[K:Q]=8$$

أي أن الزمرة $G(K/Q)$ تتألف من ثمانية عناصر، لنفرض أن هذه العناصر هي:

$$\sigma_1, \sigma_2, \dots, \sigma_8$$

وأن $\sigma_1 = I_K$. إن كلاً من العناصر السابقة هو σ_1 تماثل ذاتي للحقل K هذه العناصر سنوردها من خلال الجدول الآتي:

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
$\alpha \rightarrow$	α	$i\alpha$	$-\alpha$	$-i\alpha$	α	$i\alpha$	$-\alpha$	$-i\alpha$
$i \rightarrow$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

لنبرهن على أن الزمرة $G(K/Q)$ ليست تبديلية. نلاحظ أن:

$$\sigma_5 \cdot \sigma_2(\alpha) = \sigma_5(\sigma_2(\alpha)) = \sigma_5(i\alpha) = \sigma_5(i) \cdot \sigma_5(\alpha) = -i\alpha$$

$$\sigma_5 \cdot \sigma_2(i) = \sigma_5(\sigma_2(i)) = \sigma_5(i) = -i$$

وهذا يبين أن $\sigma_5 \cdot \sigma_2 = \sigma_8$. كما أن:

$$\sigma_2 \cdot \sigma_5(\alpha) = \sigma_2(\sigma_5(\alpha)) = \sigma_2(\alpha) = i\alpha$$

$$\sigma_2 \cdot \sigma_5(i) = \sigma_2(\sigma_5(i)) = \sigma_2(-i) = -\sigma_2(i) = -i$$

وهذا يبين أن $\sigma_2 \cdot \sigma_5 = \sigma_6$. مما سبق نجد أن $\sigma_5 \cdot \sigma_2 \neq \sigma_2 \cdot \sigma_5$ وبالتالي الزمرة $G(K/Q)$ ليست تبديلية.

٣ - نلاحظ أن $o(\sigma_5) = 2$ وذلك لأن:

$$\sigma_5^2(\alpha) = \sigma_5(\sigma_5(\alpha)) = \sigma_5(\alpha) = \alpha$$

$$\sigma_5^2(i) = \sigma_5(\sigma_5(i)) = \sigma_5(-i) = -\sigma_5(i) = -(-i) = i$$

ومنه نجد أن $\sigma_5^2 = I_K$ وبالتالي يكون $o(\sigma_5) = 2$.

لنفرض أن $H_1 = \langle \sigma_5 \rangle$ فنجد أن H_1 زمرة جزئية من الزمرة $G(K/Q)$ وأن مرتبتها

تساوي 2 ومنه نجد أن $H_1 \cong Z_2 \cong Z/2Z$.

نلاحظ أيضاً أن $o(\sigma_2) = 4$ وذلك لأن:

$$\sigma_2^2(\alpha) = \sigma_2(\sigma_2(\alpha)) = \sigma_2(i\alpha) = \sigma_2(i) \cdot \sigma_2(\alpha) = i(i\alpha) = -\alpha$$

$$\sigma_2^4(\alpha) = \sigma_2^2(\sigma_2^2(\alpha)) = \sigma_2^2(-\alpha) = -\sigma_2^2(\alpha) = -(-\alpha) = \alpha$$

$$\sigma_2^2(i) = \sigma_2(\sigma_2(i)) = \sigma_2(i) = i$$

$$\sigma_2^4(i) = \sigma_2^2(\sigma_2^2(i)) = \sigma_2^2(i) = i$$

ومنه نجد أن $\sigma_2^4 = I_K$ وبالتالي يكون $o(\sigma_2) = 4$.

لنفرض أن $H_2 = \langle \sigma_2 \rangle$ فنجد أن H_2 زمرة جزئية من الزمرة $G(K/Q)$ وأن مرتبتها تساوي 4. حسب لاغرانج فإن:

$$(G(K/Q) : H_2) = \frac{(G(K/Q) : 1)}{(H_2 : 1)} = \frac{8}{4} = 2$$

وهذا يبين أن الزمرة الجزئية H_2 ناظمية في $G(K/Q)$ وبالتالي يكون $H_1 \cdot H_2$ زمرة جزئية في $G(K/Q)$.

فضلاً عن ذلك إن $H_2 = \langle \sigma_2 \rangle = \{\sigma_1, \sigma_2, \sigma_2^2, \sigma_2^3\}$ وجدنا سابقاً أن:

$$\sigma_2^2(\alpha) = -\alpha, \quad \sigma_2^2(i) = i$$

ومنه نجد أن $\sigma_2^2 = \sigma_3$. لنوجد σ_2^3 . إن:

$$\sigma_2^3(\alpha) = \sigma_2 \cdot \sigma_2^2(\alpha) = \sigma_2(-\alpha) = -\sigma_2(\alpha) = -i\alpha$$

$$\sigma_2^3(i) = \sigma_2 \cdot \sigma_2^2(i) = \sigma_2(i) = i$$

وهذا يبين أن $\sigma_2^3 = \sigma_4$ ومنه نجد أن $H_2 = \langle \sigma_2 \rangle = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$.

واضح أن $H_1 \cap H_2 = \langle 1 \rangle$ ومنه نجد أن الزمرة $H_1 \cdot H_2$ تتألف من ثمانية عناصر وبالتالي فإن:

$$G(K/Q) \cong Z/2Z \times Z/2Z \times Z/2Z$$

تمارين (٩)

١ - بفرض K حقل تفريق الحدودية:

$$p(x) = x^4 - 5x^2 + 6 \in Q[x]$$

أوجد زمرة غالوا $G(K/Q)$.

٢ - بفرض K حقل تفريق الحدودية $p(x) = x^3 - 1 \in Q[x]$. أوجد زمرة غالوا $G(K/Q)$.

٣ - لنفرض أن $K = Q(\sqrt[3]{2}, i\sqrt{3})$. أوجد الحدودية التي يكون K حقل تفريق لها فوق Q . ثم أوجد الزمرة $G(K/Q)$.

٤ - ادرس زمرة التماثلات للحدودية $p(x) = x^4 - 1 \in Q[x]$ فوق الحقل Q .

٥ - بفرض K حقل تفريق الحدودية $p(x) = x^3 - 2 \in Q[x]$. ادرس زمرة غالوا $G(K/Q)$.

٦ - لنفرض أن K حقل تفريق الحدودية:

$$p(x) = x^3 - x + 1 \in Q[x]$$

ادرس زمرة غالوا للحقل K فوق Q .

٧ - لنفرض أن $\alpha_1, \alpha_2, \alpha_3 \in C$ أصفار للحدودية:

$$g(x) = x^3 - 4x^2 + 6x - 2 \in Q[x]$$

أوجد الحدوديات التي تملك:

- $\alpha_1 + \alpha_2 + \alpha_3$ صفراً لها.

- $\alpha_1^2, \alpha_2^2, \alpha_3^2$ أصفاراً لها.

- $(\alpha_1 - \alpha_2)^2, (\alpha_1 - \alpha_3)^2, (\alpha_2 - \alpha_3)^2$ أصفاراً لها.

الفصل العاشر

نظرية غالوا الأساسية

١٠ - ١. نظرية غالوا الأساسية.

في هذه الفقرة سوف ندرس مبرهنة غالوا الأساسية عموماً، أي لأجل الحقول غير المنتهية. لابد من التذكير أن الحقول المدروسة في هذه الفقرة هي حقول غير منتهية، بمعنى آخر جميع الحقول هنا هي حقول مميزها يساوي الصفر. بسبب الحجم الكبير لهذه المبرهنة سوف نقوم بسردها على عدة خطوات.

مبرهنة ١٠-١-١.

ليكن الحقل K تمديداً جبرياً للحقل F وأن $\sigma : K \rightarrow K$ هو F -تشاكل، عندئذ التشاكل σ يكون F -تماثل ذاتي للحقل K .
البرهان.

لما كان σ تشاكلاً فإن σ متباين. لنبرهن على أنه غامر.
ليكن $a \in K$ حسب الفرض فإن a هو عنصر جبري فوق F . لنفرض أن $p(x)$ هي الحدودية الأصغرية للعنصر a في $F[x]$ وأن $p(x) = \sum_{i=0}^n c_i x^i$ حيث $c_i \in F$ وذلك أيأ كان $0 \leq i \leq n$. لنفرض أن $a = a_1, a_2, \dots, a_t \in K$ جميع أصفار الحدودية $p(x)$ في K وأن:

$$E = F(a_1, a_2, \dots, a_t)$$

ف نجد أن E حقل جزئي في K يحوي F .

ليكن $b \in \{a_1, a_2, \dots, a_t\}$ ، لما كان $p(b) = 0$ فإن $\sum_{i=0}^n c_i b^i = 0$ ومنه فإن:

$$\sigma(\sum_{i=0}^n c_i b^i) = \sigma(0) = 0$$

وبالتالي يكون $\sum_{i=0}^n \sigma(c_i) \cdot \sigma(b^i) = 0$ منه فإن $\sum_{i=0}^n c_i \cdot \sigma(b)^i = 0$ وهذا يبين أن

$p(\sigma(b)) = 0$ أي أن $\sigma(b)$ هو صفر للحدودية $p(x)$. وهذا يبين أن العناصر:

$$\sigma(a) = \sigma(a_1), \sigma(a_2), \dots, \sigma(a_t) \in K$$

هي أصفار للحدودية $p(x)$ وبالتالي فإن $\sigma(a_1), \sigma(a_2), \dots, \sigma(a_t) \in E$ وهكذا نجد أن $\sigma(E) \subseteq E$ ولما كان $\sigma(E)$ فضاءً جزئياً في E فوق F وأن:

$$\sigma(E) = F(\sigma(a_1), \sigma(a_2), \dots, \sigma(a_t))$$

نجد أن $[\sigma(E):F] = [E:F]$ ومنه يكون $\sigma(E) = E$ ولما كان $a \in K$ صفراً للحدودية $p(x)$ فإن $a \in E = \sigma(E) \subseteq \sigma(K)$ وهكذا يكون $K \subseteq \sigma(K)$ ومنه نجد أن $\sigma(K) = K$ وبالتالي σ هو F -تماثل ذاتي للحقل K . ◊

مبرهنة ١٠-١-٢.

ليكن F حقلاً $f(x) \in F[x]$ حدودية منفصلة فوق F . إذا كان E هو حقل تفريق الحدودية $f(x)$ فوق F ، عندئذ فإن:

$$(\text{Aut}(E/F):1) = [E:F]$$

البرهان.

لنفرض أن $a_1, a_2, \dots, a_n \in E$ هي جميع أصفار الحدودية $f(x)$ في E . لما كانت الحدودية $f(x)$ منفصلة فوق F وأن E هو حقل تفريق الحدودية $f(x)$ فوق F فإنه حسب المبرهنة (٥-٢-٨) تكون جميع تلك الأصفار بسيطة وهذا يبين أن جميع أصفار الحدودية $f(x)$ مختلفة، كما أن $\partial f(x) = n$ وحسب المبرهنة (٧-٣-٣) ومن أجل $K = E$ نجد أن $[E:F] = n$ وهذا العدد يساوي عدد جميع الـ F -تشاكلات $\varphi: E \rightarrow E$ ولما كان كل F -تشاكل $\varphi: E \rightarrow E$ هو F -تماثل نجد أن:

$$\diamond (\text{Aut}(E/F):1) = n = [E:F]$$

مبرهنة ١٠-١-٣.

ليكن الحقل L تمديداً للحقل F وأن K, E حقلاً جزئياً في L كل منهما يحوي F ، أي أن $F \subseteq K, E \subseteq L$. عندئذ لأجل أي تمديد $L' L$ للحقل L ولأجل أي تشاكل $\sigma: L \rightarrow L'$ فإن $\sigma(E \cdot K) = \sigma(E) \cdot \sigma(K)$.

البرهان.

لما كان كل من K, E حقلين جزئيين من الحقل L وكل منهما يحوي F فإنه حسب التمرين المحلول (٣-١٠) يكون $K \cdot E$ حقلاً جزئياً في L يحوي F .
ليكن $y \in K \cdot E$ عندئذ فإن $y = a_1 b_1 + a_2 b_2 + \dots + a_n b_n$ حيث $a_i \in K, b_i \in E$ وذلك أياً كان $1 \leq i \leq n$ ، ومنه يكون:

$$\begin{aligned}\sigma(y) &= \sigma(a_1 b_1 + a_2 b_2 + \dots + a_n b_n) = \\ &= \sigma(a_1 b_1) + \sigma(a_2 b_2) + \dots + \sigma(a_n b_n) = \\ &= \sigma(a_1)\sigma(b_1) + \sigma(a_2)\sigma(b_2) + \dots + \sigma(a_n)\sigma(b_n) \in \sigma(E) \cdot \sigma(K) \\ &\text{ومنه نجد أن } \sigma(E \cdot K) \subseteq \sigma(E) \cdot \sigma(K)\end{aligned}$$

ليكن $y' \in \sigma(E) \cdot \sigma(K)$ عندئذ فإن $y' = c_1 d_1 + c_2 d_2 + \dots + c_n d_n$ حيث $c_i \in \sigma(E)$ و $d_i \in \sigma(K)$ وذلك أياً كان $1 \leq i \leq n$. ومنه يوجد $d'_i \in K, c'_i \in E$ بحيث يكون $\sigma(d'_i) = d_i, \sigma(c'_i) = c_i$ وذلك أياً كان $1 \leq i \leq n$. ومنه نجد أن:

$$\begin{aligned}y' &= c_1 d_1 + c_2 d_2 + \dots + c_n d_n = \\ y' &= \sigma(c'_1)\sigma(d'_1) + \sigma(c'_2)\sigma(d'_2) + \dots + \sigma(c'_n)\sigma(d'_n) =\end{aligned}$$

$$\begin{aligned}y' &= \sigma(c'_1 d'_1) + \sigma(c'_2 d'_2) + \dots + \sigma(c'_n d'_n) = \\ y' &= \sigma(c'_1 d'_1 + c'_2 d'_2 + \dots + c'_n d'_n) \in \sigma(E \cdot K)\end{aligned}$$

ومنه يكون $\sigma(E) \cdot \sigma(K) \subseteq \sigma(E \cdot K)$ ، مما سبق نجد أن:
 $\diamond \cdot \sigma(E \cdot K) = \sigma(E) \cdot \sigma(K)$

مبرهنة ١٠-١-٤.

ليكن E حقلاً و G زمرة جزئية منتهية من الزمرة $Aut(G)$. بفرض أن $F = F(G)$ عندئذ يكون $[E : F] \leq (G : 1)$.
البرهان.

لنفرض أن $G = \{\sigma_1 = I_E, \sigma_2, \dots, \sigma_n\}$ زمرة جزئية منتهية من الزمرة $Aut(G)$ وأن:
 $F = F(G) = \{a : a \in E; \sigma(a) = a \quad \forall \sigma \in G\}$

ولنأخذ الحقل:

$$E^n = \{(a_1, a_2, \dots, a_n) : a_i \in E, 1 \leq i \leq n\}$$

بالنسبة لعملية جمع وضرب المركبات، فنجد أن E^n فضاء متجهي فوق الحقل E وأن $[E^n : E] = n$ فضلاً عن ذلك فإن المجموعة $S = \{e_1, e_2, \dots, e_n\} \subset E^n$ حيث $e_i = (0, \dots, 0, \underset{i}{1}, 0, \dots, 0)$ كان $1 \leq i \leq n$ فإن:

$$e_i = (0, \dots, 0, \underset{i}{1}, 0, \dots, 0)$$

قاعدة للفضاء E^n فوق E ، ومنه فإن أي مجموعة جزئية من E^n ومؤلفة من m عنصر حيث $m > n$ تكون مرتبطة خطياً فوق E .

لنبرهن على أن أي مجموعة جزئية من E ومؤلفة من m عنصر حيث $m > n$ تكون مرتبطة خطياً فوق E . لتكن $S' = \{y_1, y_2, \dots, y_{n+1}\} \subset E$ مجموعة جزئية من E ومؤلفة من $n+1$ عنصر:

- إذا كان أحد عناصر المجموعة S' يساوي الصفر عندئذ تكون المجموعة S' مرتبطة خطياً فوق E .

- لنفرض أن جميع عناصر المجموعة S' مختلفة عن الصفر. لنضع:

$$v_j = (\sigma_1(y_j), \sigma_2(y_j), \dots, \sigma_n(y_j))$$

لأجل كل $1 \leq j \leq n+1$ ، فنجد أن المجموعة:

$$S'' = \{v_1, v_2, \dots, v_n, v_{n+1}\} \subset E^n$$

مجموعة جزئية من E^n ومؤلفة من $n+1$ وبالتالي فهي مرتبطة خطياً فوق E ومنه توجد عناصر $c_1, c_2, \dots, c_n, c_{n+1} \in E$ ليست جميعها معدومة لأجلها $\sum_{i=1}^{n+1} c_i \cdot v_i = 0$ ومنه فإن:

$$c_1 \cdot v_1 + c_2 \cdot v_2 + \dots + c_n \cdot v_n + c_{n+1} \cdot v_{n+1} = 0$$

$$c_1 \cdot (\sigma_1(y_1), \sigma_2(y_1), \dots, \sigma_n(y_1)) +$$

$$c_2 \cdot (\sigma_1(y_2), \sigma_2(y_2), \dots, \sigma_n(y_2)) +$$

.....

$$c_{n+1} \cdot (\sigma_1(y_{n+1}), \sigma_2(y_{n+1}), \dots, \sigma_n(y_{n+1})) = (0, 0, \dots, 0)$$

وهكذا نجد أن:

$$c_1 \cdot \sigma_1(y_1) + c_2 \cdot \sigma_1(y_2) + \dots + c_{n+1} \cdot \sigma_1(y_{n+1}) = 0$$

$$c_1 \cdot \sigma_2(y_1) + c_2 \cdot \sigma_2(y_2) + \dots + c_{n+1} \cdot \sigma_2(y_{n+1}) = 0$$

.....

$$c_1 \cdot \sigma_n(y_1) + c_2 \cdot \sigma_n(y_2) + \dots + c_{n+1} \cdot \sigma_n(y_{n+1}) = 0$$

وبالتالي يكون $\sum_{j=1}^{n+1} c_j \cdot \sigma_i(y_j) = 0$ وأن $1 \leq i \leq n$

نفرض أن M_0 هي أسرة المجموعات الجزئية $\{a_1, a_2, \dots, a_{n+1}\}$ من عناصر الحقل E

غير المعدومة جميعها والتي لأجلها $\sum_{j=1}^{n+1} a_j \cdot \sigma_i(y_j) = 0$ حيث $1 \leq i \leq n$

واضح أن المجموعة M_0 غير خالية، لأن $\{c_1, c_2, \dots, c_{n+1}\} \in M_0$

لنأخذ أيضاً المجموعة M_1 المؤلفة من الأعداد الطبيعية r حيث $1 \leq r \leq n+1$ والتي

لأجلها توجد مجموعة $\{b_1, b_2, \dots, b_{n+1}\} \in M_0$ بحيث يكون r هو عدد العناصر المختلفة

عن الصفر في المجموعة $\{b_1, b_2, \dots, b_{n+1}\}$. واضح أن المجموعة M_1 ليست خالية لأن

المجموعة M_0 ليست خالية، ولما كانت $\phi \neq M_1 \subset N$ فإن M_1 تحوي عنصراً أصغر

وليكن t . بما أن $t \in M_1$ فإنه توجد مجموعة:

$$\{d_1, d_2, \dots, d_{n+1}\} \in M_0$$

بحيث أن عدد العناصر المغايرة للصفر فيها يساوي t ، نفرض أن هذه العناصر هي

$d_{l_1}, d_{l_2}, \dots, d_{l_t}$ عندئذ يكون $\sum_{j=1}^{n+1} d_j \cdot \sigma_i(y_j) = 0$ حيث $1 \leq i \leq n$ ، أي أن:

$$d_1 \cdot \sigma_i(y_1) + d_2 \cdot \sigma_i(y_2) + \dots + d_{n+1} \cdot \sigma_i(y_{n+1}) = 0 \quad \forall 1 \leq i \leq n$$

ومنه نجد أن:

$$d_{l_1} \cdot \sigma_i(y_{l_1}) + d_{l_2} \cdot \sigma_i(y_{l_2}) + \dots + d_{l_t} \cdot \sigma_i(y_{l_t}) = 0 \quad \forall 1 \leq i \leq n$$

ولما كان $d_{l_1} \in E$ ينتج أن:

$$\begin{aligned} &\sigma_i(y_{l_1}) + (d_{l_1}^{-1} d_{l_2}) \cdot \sigma_i(y_{l_2}) + (d_{l_1}^{-1} d_{l_3}) \cdot \sigma_i(y_{l_3}) + \dots + \\ &+ (d_{l_1}^{-1} d_{l_t}) \cdot \sigma_i(y_{l_t}) = 0 \quad (*) \end{aligned}$$

وذلك أيّاً كان $1 \leq i \leq n$

لنبرهن على أن $\sigma_i(d_{l_1}^{-1} d_{l_s}) = d_{l_1}^{-1} d_{l_s}$ وذلك أيّاً كان $1 \leq i \leq n$, $2 \leq s \leq t$

بالعودة إلى المساواة الأخيرة، وبأخذ الصورة المباشرة لها وفق التماثل σ_1 نجد أن:

$$\sigma_1(\sigma_i(y_{l_1}) + (d_{l_1}^{-1}d_{l_2}) \cdot \sigma_i(y_{l_2}) + (d_{l_1}^{-1}d_{l_3}) \cdot \sigma_i(y_{l_3}) + \dots + (d_{l_1}^{-1}d_{l_t}) \cdot \sigma_i(y_{l_t})) = 0$$

ومنه فإن:

$$(\sigma_1 \cdot \sigma_i)(y_{l_1}) + \sigma_1(d_{l_1}^{-1}d_{l_2}) \cdot (\sigma_1 \cdot \sigma_i)(y_{l_2}) + \sigma_1(d_{l_1}^{-1}d_{l_3}) \cdot (\sigma_1 \cdot \sigma_i)(y_{l_3}) + \dots + \sigma_1(d_{l_1}^{-1}d_{l_t}) \cdot (\sigma_1 \cdot \sigma_i)(y_{l_t}) = 0$$

ولما كان $\sigma_1 \in G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$ نجد أن:

$$\{\sigma_1 \cdot \sigma_1, \sigma_1 \cdot \sigma_2, \dots, \sigma_1 \cdot \sigma_n\} = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$$

لنفرض أن $\sigma_1 \cdot \sigma_i = \sigma_\lambda$ حيث $1 \leq \lambda \leq n$ فنجد أن:

$$\sigma_\lambda(y_{l_1}) + \sigma_1(d_{l_1}^{-1}d_{l_2}) \cdot \sigma_\lambda(y_{l_2}) + \sigma_1(d_{l_1}^{-1}d_{l_3}) \cdot \sigma_\lambda(y_{l_3}) + \dots + \sigma_1(d_{l_1}^{-1}d_{l_t}) \cdot \sigma_\lambda(y_{l_t}) = 0$$

وهكذا نجد أن:

$$\begin{aligned} & \sigma_\lambda(y_{l_1}) + \sigma_1(d_{l_1}^{-1}d_{l_2}) \cdot \sigma_\lambda(y_{l_2}) + \sigma_1(d_{l_1}^{-1}d_{l_3}) \cdot \sigma_\lambda(y_{l_3}) + \\ & + \dots + \sigma_1(d_{l_1}^{-1}d_{l_t}) \cdot \sigma_\lambda(y_{l_t}) = \\ & = \sigma_\lambda(y_{l_1}) + (d_{l_1}^{-1}d_{l_2}) \cdot \sigma_\lambda(y_{l_2}) + (d_{l_1}^{-1}d_{l_3}) \cdot \sigma_\lambda(y_{l_3}) + \dots + \\ & + (d_{l_1}^{-1}d_{l_t}) \cdot \sigma_\lambda(y_{l_t}) \end{aligned}$$

ومنه فإن:

$$(\sigma_1(d_{l_1}^{-1}d_{l_2}) - d_{l_1}^{-1}d_{l_2}) \cdot \sigma_\lambda(y_{l_2}) + (\sigma_1(d_{l_1}^{-1}d_{l_3}) - d_{l_1}^{-1}d_{l_3}) \cdot \sigma_\lambda(y_{l_3}) + \dots + (\sigma_1(d_{l_1}^{-1}d_{l_t}) - d_{l_1}^{-1}d_{l_t}) \cdot \sigma_\lambda(y_{l_t}) = 0$$

ولما كان t أصغر عدد صحيح موجب في M_1 نجد أن:

$$\sigma_1(d_{l_1}^{-1}d_{l_s}) - d_{l_1}^{-1}d_{l_s} = 0 \quad \forall 2 \leq s \leq t$$

$$\sigma_1(d_{l_1}^{-1}d_{l_s}) = d_{l_1}^{-1}d_{l_s} \quad \forall 2 \leq s \leq t$$

بهذا الشكل نكون قد أثبتنا أن كل مجموعة جزئية من E ومؤلفة من $n+1$ عنصر تكون

مرتبطة خطياً فوق F وهذا يبين أن $[E:F] \leq (G:1)$ ♦

مبرهنة ١٠-١-٥.

ليكن E حقلاً و G زمرة جزئية منتهية من الزمرة $Aut(G)$ ، عندئذ فإن:

$$G = \text{Aut}(E/F(G))$$

حيث $F(G) = \{a : a \in E; \sigma(a) = a \quad \forall \sigma \in G\}$ البرهان.

وجدنا سابقاً أن $F(G)$ هو حقل جزئي من الحقل E ، أي أن $F(G) \subseteq E$.
ليكن $\sigma \in G$ عندئذ $\sigma \in \text{Aut}(G)$ وأنه أيضاً كان $a \in F(G)$ فإن $\sigma(a) = a$ ومنه نجد أن σ هو $F(G)$ -تماثل ذاتي للحقل E وبالتالي يكون $G \subseteq \text{Aut}(E/F(G))$ وهذا يبين أن $(G:1) \leq (\text{Aut}(E/F(G)):1)$.
من جهة أخرى، لدينا حسب المبرهنة (١٠-١-٤) أن $[E:F(G)] \leq (G:1)$ وبالتالي يكون:

$$[E:F(G)] \leq (\text{Aut}(E/F(G)):1)$$

وحسب النتيجة (٢) للمبرهنة (٧-٣-٣) فإن $(\text{Aut}(E/F(G)):1) \leq [E:F(G)]$ ، مما سبق نجد أن $(G:1) = [E:F(G)]$ وهذا يبين أن $G = \text{Aut}(E/F(G))$. ◊

مبرهنة ١٠-١-٦.

ليكن الحقل E تمديداً للحقل F . عندئذ الشروط الآتية متكافئة:

- ١ - الحقل E هو تمديد غالوا للحقل F .
- ٢ - الحقل E هو تمديد ناظمي ومنفصل ومنته للحقل F .
- ٣ - الحقل E هو حقل تفريق حدودية منفصلة فوق F .

البرهان.

(١) $\Leftrightarrow$ (٢). لنفرض أن الحقل E هو تمديد غالوا للحقل F . ليكن $a \in E$ عندئذ فإن a هو عنصر جبيري منفصل فوق F . لنفرض أن $p(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F عندئذ فإن $p(x)$ حدودية منفصلة فوق F . لما كان الحقل E تمديداً ناظماً للحقل F فإن الحقل E يحوي جميع العناصر المترافقة مع a فوق F .
لنفرض أن $a = a_1, a_2, \dots, a_n \in E$ هي جميع العناصر المترافقة مع a فوق F ومنه فإن العناصر $a_1, a_2, \dots, a_n$ هي أصفار للحدودية $p(x)$ ولما كانت الحدودية $p(x)$

منفصلة فإن هذه العناصر هي أصفار بسيطة للحدودية $p(x)$.

لنأخذ الحقل $F(a_1, a_2, \dots, a_n)$ فنجد أن $F \subseteq F(a_1, a_2, \dots, a_n) \subseteq E$ ومنه فإن:

$$a \in F(a_1, a_2, \dots, a_n)$$

وبالتالي يكون $E = F(a_1, a_2, \dots, a_n)$ وهذا يبين أن الحقل هو تمديد منته للحقل F .

(٢) $\Leftarrow$ (٣). لنفرض أن الحقل E هو تمديد ناظمي ومنته للحقل F ، عندئذ توجد

عناصر $b_1, b_2, \dots, b_m \in E$ بحيث يكون $E = F(b_1, b_2, \dots, b_m)$ ولما كان الحقل E

تمديداً منفصلاً للحقل F فإن العناصر b_i حيث $1 \leq i \leq m$ هي عناصر منفصلة فوق F .

لنفرض أن $p_i(x) \in F[x]$ هي الحدودية الأصغرية للعنصر b_i وذلك لأجل كل

$1 \leq i \leq m$ ، فنجد أن الحدودية $p_i(x)$ منفصلة فوق F .

لنضع $p(x) = \prod_{i=1}^m p_i(x)$ ، فنجد أن $p(x) \in F[x]$ ، لما كان الحقل E تمديداً ناظماً

للحقل F وأن كلاً من $p_i(x)$ حدودية أولية في $F[x]$ تملك صفراً في E فإن كلاً من

$p_i(x)$ تنفرد في $E[x]$ إلى مضارب خطية وبالتالي فإن الحدودية $p(x)$ تنفرد في

$E[x]$ إلى مضارب خطية. فضلاً عن ذلك فإن الحدودية $p(x)$ هي حدودية منفصلة

فوق F وذلك لأن الحقل E هو تمديد منفصل للحقل F وأن جميع الحدوديات الأولية

التي تقسم $p(x)$ في $F[x]$ هي حدوديات منفصلة في $F[x]$.

(٣) $\Leftarrow$ (١). لنفرض أن الحقل E هو حقل تقرييق حدودية منفصلة $f(x) \in F[x]$ فوق

F ، عندئذ يكون $E = F(a_1, a_2, \dots, a_n)$ حيث أن $a_1, a_2, \dots, a_n \in E$ هي جميع

أصفار الحدودية $f(x)$ في الحقل E وهذا يبين أن لنا أن الحقل E هو تمديد منته

للحقل F . لما كانت الحدودية $f(x)$ منفصلة فوق F سوف نميز حالتين:

- إذا كانت الحدودية $f(x)$ أولية في $F[x]$ عندئذ تكون $f(x)$ هي الحدودية

الأصغرية للعناصر $a_1, a_2, \dots, a_n$ فوق F ، فضلاً عن ذلك لما كانت $f(x)$ منفصلة

فوق F نجد أن $a_1, a_2, \dots, a_n$ هي عناصر منفصلة فوق F وهذا يبين لنا أن الحقل E

هو تمديد منفصل للحقل F .

- لنفرض أن الحدودية $f(x)$ غير أولية في $F[x]$. لما كانت العناصر:

$$a_1, a_2, \dots, a_n \in E$$

هي عناصر جبرية فوق F ، لنفرض أن $p_i(x) \in F[x]$ الحدودية الأصغرية للعنصر a_i فوق F وذلك لأجل كل $1 \leq i \leq n$ ومنه فإن $p_i(x)$ هي حدودية أولية في $F[x]$ وتقسم $f(x)$ في $F[x]$ ولما كانت الحدودية $f(x)$ منفصلة فوق F نجد أن الحدودية $p_i(x)$ منفصلة فوق F وبالتالي يكون العنصر a_i عنصراً منفصلاً فوق F وذلك لأجل كل i وهذا يبين أن الحقل E هو تمديد منفصل للحقل F .
لنبرهن على أن الحقل E هو تمديد ناظمي للحقل F .
لنفرض أن $G = \text{Aut}(E/F)$ وأن:

$$F' = F(G) = \{a : a \in E; \sigma(a) = a \quad \forall \sigma \in G\}$$

عندئذ يكون $F \subseteq F'$ ومنه فإن $f(x) \in F'[x]$ حدودية منفصلة فوق F' وأن E هو حقل تقريب الحدودية $f(x)$ فوق F' وحسب المبرهنة (١٠-١-٢) يكون:

$$[E : F] = (\text{Aut}(E/F) : 1)$$

$$[E : F'] = (\text{Aut}(E/F') : 1)$$

ولما كان الحقل E تمديداً منتهياً للحقل F فإن الزمرة $\text{Aut}(E/F)$ تكون منتهية.
أيضاً لما كان $F \subseteq F' \subseteq E$ فإن الحقل E هو تمديد منته للحقل F' وبالتالي الزمرة $\text{Aut}(E/F')$ تكون منتهية وحسب التمهيدية (١٠-١-٥) يكون:

$$G = \text{Aut}(E/F(G)) = \text{Aut}(E/F')$$

وهذا يبين أن $\text{Aut}(E/F) = \text{Aut}(E/F')$ وهكذا نجد أن $F = F'$ وبالتالي يكون $F = F(G)$. لما كانت الحدودية $f(x)$ منفصلة فإن $\partial f(x) \geq 1$ وحسب المبرهنة (٨-١-٧) يكون الحقل E تمديداً ناظماً ومنتهياً للحقل F ، مما سبق نجد أن E هو تمديد غالوا للحقل F . ◊

تمهيدية ١٠-١-٧.

ليكن الحقل E تمديداً للحقل F و L حقلاً جزئياً في E يحوي F . إذا كان E هو تمديد غالوا للحقل F عندئذ يكون E هو تمديد غالوا للحقل L .
البرهان.

لنفرض أن E هو تمديد غالوا للحقل F عندئذ وحسب المبرهنة (١٠-١-٦) فإن E هو تمديد ناظمي ومنفصل ومنته للحقل F وبالتالي يكون الحقل E تمديداً منتهياً للحقل L وحسب التمهيدية (٥-٣-٥) يكون E تمديداً منفصلاً للحقل L وأيضاً حسب التمهيدية (٨-١-٣) يكون الحقل E تمديداً ناظماً للحقل L ، مما سبق نجد أن الحقل E هو تمديد ناظمي ومنفصل ومنته للحقل L وحسب المبرهنة (١٠-١-٦) يكون الحقل E تمديد غالوا للحقل L . ◊

مبرهنة ٨-١-١٠.

ليكن الحقل E تمديد غالوا للحقل F وأن $G = G(E/F)$. لنفرض أن $\mathfrak{T}$ هي مجموعة الزمر الجزئية من الزمرة G وأن $\mathfrak{T}_0$ هي مجموعة الحقول الجزئية في E التي كل منها يحوي F ، أي أن:

$$\mathfrak{T} = \{H : G \text{ زمرة جزئية في } H\}$$

$$\mathfrak{T}_0 = \{L : F \subseteq L \subseteq E; \text{ } L \text{ حقل جزئي في } E \text{ يحوي } F\}$$

عندئذ:

- ١ - يوجد تطبيق $f : \mathfrak{T} \rightarrow \mathfrak{T}_0$.
- ٢ - يوجد تطبيق $g : \mathfrak{T}_0 \rightarrow \mathfrak{T}$.
- ٣ - كل من f, g يحققان $f \cdot g = I_{\mathfrak{T}_0}$, $g \cdot f = I_{\mathfrak{T}}$.

البرهان.

- ١ - لنعرف العلاقة $f : \mathfrak{T} \rightarrow \mathfrak{T}_0$ بالشكل الآتي: أيّاً كان $H \in \mathfrak{T}$ ، أي لأجل أي زمرة جزئية من الزمرة G ، لنضع $f(H) = F(H)$. لما كان:

$$F(H) = \{a : a \in E; \sigma(a) = a \forall \sigma \in H\}$$

فإنه حسب التمهيدية (٨-٢-٢) يكون $F(H)$ حقلاً جزئياً في E . لنبرهن على أن $F \subseteq F(H)$. ليكن $a \in F$ عندئذ أيّاً كان $\beta \in H$ فإن $\beta(a) = a$ ومنه فإن $a \in F(H)$ وبالتالي فإن $\beta(a) = a$ وهذا يبين أن $a \in F(H)$ ومنه فإن $F(H)$ يحوي F أي أن $F(H) \in \mathfrak{T}_0$ ومنه $F(H) \in \mathfrak{T}_0$ يحوي F هو حقل جزئي في E يحوي F ومنه $F(H) \in \mathfrak{T}_0$ لنبرهن على أن f تطبيق. ليكن $H_1, H_2 \in \mathfrak{T}$ ، أي أن H_1, H_2 زميرتان جزئيتان من

الزمرة $G(E/F)$ ، لنفرض أن $H_1 = H_2$ وليكن $b \in F(H_1)$ عندئذ أيّ كان $\alpha \in H_1$ فإن $\alpha(b) = b$ ولما كان $H_1 = H_2$ نجد أنه أيّ كان $\alpha \in H_2$ يكون $\alpha(b) = b$ ومنه فإن $b \in F(H_2)$ وهكذا نجد أن $F(H_1) \subseteq F(H_2)$. بطريقة مشابهة يمكن إثبات الاحتواء المعاكس، مما سبق نجد أن f هو تطبيق.

٢ - لنعرف العلاقة $\mathfrak{S} \rightarrow \mathfrak{S}_0 : g$ بالشكل الآتي: أيّ كان $L \in \mathfrak{S}_0$ فإن L هو حقل جزئي من الحقل E يحوي F . لنضع $g(L) = G(E/L)$. لما كان $F \subseteq L$ فإن كل L - تماثل ذاتي للحقل E هو F - تماثل ذاتي للحقل E ومنه فإن:

$$G(E/L) \subseteq G(E/F) = G$$

أي أن $G(E/L) \in \mathfrak{S}$ هي زمرة جزئية من الزمرة G وبالتالي فإن $G(E/L) \in \mathfrak{S}$. لنبرهن على أن g هو تطبيق. ليكن $L_1, L_2 \in \mathfrak{S}_0$ ، عندئذ فإن كلا من L_1, L_2 حقلان جزئيان من الحقل E كل منهما يحوي F . إذا كان $L_1 = L_2$ عندئذ يكون:

$$g(L_1) = G(E/L_1) = G(E/L_2) = g(L_2)$$

٣ - لنبرهن أولاً على أن $g \cdot f = I_{\mathfrak{S}}$. لتكن $H \in \mathfrak{S}$ ، عندئذ فإن H هي زمرة جزئية من الزمرة G وأن:

$$g \cdot f(H) = g(F(H)) = G(E/F(H))$$

لنبرهن على أن $G(E/F(H)) = H$. لما كان E هو تمديد غالوا للحقل F وحسب المبرهنة (١٠-١-٦) فإن E هو تمديد منته للحقل F وحسب النتيجة (٢) للمبرهنة (٧-٣-٣) فإن $[E:F] \leq (G(E/F):1)$ وهذا يبين أن الزمرة $G(E/F)$ منتهية، ولما كان $H \subseteq G(E/F) \subseteq \text{Aut}(E)$ فإن الزمرة الجزئية H تكون أيضاً منتهية وحسب التمهيدية (١٠-١-٥) يكون $H = G(E/F(H))$ ، مما سبق نجد أن:

$$g \cdot f(H) = g(F(H)) = G(E/F(H)) = H$$

وبالتالي يكون $g \cdot f = I_{\mathfrak{S}}$.

لنبرهن الآن على أن $f \cdot g = I_{\mathfrak{S}_0}$.

ليكن $L \in \mathfrak{S}_0$ عندئذ فإن L هو حقل جزئي من الحقل E يحوي F أي أن $F \subseteq L \subseteq E$ ومنه فإن:

$$f \cdot g(L) = f(G(E/L)) = F(G(E/L))$$

ولما كان الحقل E تمديد غالوا للحقل F فإنه حسب التمهيدية (١٠-١-٥) يكون E تمديد غالوا للحقل L وهذا يبين أن $F(G(E/L)) = L$ ومنه يكون $f \cdot g(L) = L$ وبالتالي فإن $\diamond \cdot f \cdot g = I_{\mathfrak{A}_0}$

مبرهنة ١٠-١-٩.

ليكن الحقل E تمديد غالوا للحقل F وأن $G = G(E/F)$. لنفرض أن H_1, H_2 زميرتان جزئيتان من الزمرة G . عندئذ:

$$1 - H_1 \subseteq H_2 \text{ عندما وفقط عندما يكون } F(H_2) \subseteq F(H_1).$$

$$2 - \text{إذا كانت } H_1 \subseteq H_2 \text{ عندئذ يكون } (H_2 : H_1) = [F(H_1) : F(H_2)].$$

البرهان.

١ - لزوم الشرط. لنفرض أن $H_1 \subseteq H_2$ وليكن $a \in F(H_2)$ عندئذ أيًا كان $\tau \in H_2$ فإن $\tau(a) = a$ ولما كانت $H_1 \subseteq H_2$ نجد أنه أيًا كان $\tau \in H_1$ فإن $\tau(a) = a$ وهذا يبين أن $a \in F(H_1)$ ومنه نجد أن $F(H_2) \subseteq F(H_1)$.
كفاية الشرط. لنفرض أن $F(H_2) \subseteq F(H_1)$. لما كان الحقل E هو تمديد غالوا للحقل F فإنه حسب المبرهنة (١٠-١-٦) يكون E حقل تفريق حدودية منفصلة فوق F وحسب المبرهنة (١٠-١-٢) يكون:

$$(G(E/F) : 1) = [E : F]$$

لما كان التمديد E للحقل F منتهياً نجد أن الزمرة $G(E/F)$ منتهية وبالتالي تكون كل من الزمرتين الجزئيتين H_1, H_2 منتهية وحسب التمهيدية (١٠-١-٥) يكون:

$$H_1 = G(E/F(H_1)), \quad H_2 = G(E/F(H_2))$$

ولما كان $F(H_2) \subseteq F(H_1)$ فإن كلاً $F(H_1)$ - تماثل ذاتي للحقل E هو $F(H_2)$ - تماثل ذاتي للحقل E وبالتالي يكون:

$$H_1 = G(E/F(H_1)) \subseteq G(E/F(H_2)) = H_2$$

٢ - لنفرض أن $H_1 \subseteq H_2$ ، لما كانت الزمرة الجزئية H_2 منتهية فإنه حسب مبرهنة لاغرانج يكون $(H_2 : 1) = (H_2 : H_1)(H_1 : 1)$.

من جهة أخرى، لدينا حسب (١) أن $F(H_2) \subseteq F(H_1)$ ومنه نجد أن:

$$F \subseteq F(H_2) \subseteq F(H_1) \subseteq E$$

ولما كان الحقل E هو تمديد غالوا للحقل F فإن الحقل E يكون تمديداً منتهياً للحقل F وبالتالي يكون الحقل E تمديداً منتهياً للحقل $F(H_2)$ ومنه نجد أن:

$$[E : F(H_2)] = [E : F(H_1)] \cdot [F(H_1) : F(H_2)]$$

من جهة ثالثة، لما كان E هو تمديد غالوا للحقل F وأن $F \subseteq F(H_1) \subseteq E$ فإنه حسب التمهيدية (١٠-١-٧) يكون الحقل E هو تمديد غالوا للحقل $F(H_1)$ وحسب المبرهنة (١٠-١-٦) فإن E هو حقل تفريق حدودية منفصلة فوق $F(H_1)$ وحسب المبرهنة (١٠-١-٢) نجد أن:

$$(G(E/F(H_1)) : 1) = [E : F(H_1)]$$

أيضاً لما كان $F \subseteq F(H_2) \subseteq E$ وكان E هو تمديد غالوا للحقل F نجد أن E هو تمديد غالوا للحقل $F(H_2)$ وحسب المبرهنة (١٠-١-٦) فإن E هو حقل تفريق حدودية منفصلة فوق $F(H_2)$ وحسب المبرهنة (١٠-١-٢) نجد أن:

$$(G(E/F(H_2)) : 1) = [E : F(H_2)]$$

وهكذا حسب التمهيدية (١٠-١-٥) نجد أن:

$$\begin{aligned} (H_2 : H_1) &= \frac{(H_2 : 1)}{(H_1 : 1)} = \frac{(G(E/F(H_2)) : 1)}{(G(E/F(H_1)) : 1)} \\ &= \frac{[E : F(H_2)]}{[E : F(H_1)]} = [F(H_1) : F(H_2)] \end{aligned}$$

وهو المطلوب إثباته. ◊

مبرهنة ١٠-١-١٠.

ليكن الحقل E تمديد غالوا للحقل F وأن $G = G(E/F)$. لنفرض أن H زمرة جزئية من الزمرة G وأن L حقل جزئي من الحقل E يحوي F ، أي أن $F \subseteq L \subseteq E$. عندئذ:

$$١ - \text{أياً كان } \sigma \in G \text{ فإن } \sigma(F(H)) = F(\sigma H \sigma^{-1}).$$

$$٢ - \text{أياً كان } \sigma \in G \text{ فإن } \sigma G(E/L) \sigma^{-1} = G(E/\sigma(L)).$$

البرهان.

١ - ليكن $\sigma \in G$. لما كانت H زمرة جزئية من الزمرة G فإن المجموعة:

$$\sigma H \sigma^{-1} = \{\sigma \tau \sigma^{-1} : \forall \tau \in H\}$$

هي زمرة جزئية من الزمرة G .

ليكن $a \in F(H)$ عندئذ أياً كان $\tau \in H$ فإن $\tau(a) = a$ ومنه نجد أن:

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

وهذا يبين أن $\sigma(a) \in F(\sigma H \sigma^{-1})$ ومنه يكون $\sigma(F(H)) \subseteq F(\sigma H \sigma^{-1})$.

ليكن $b \in F(\sigma H \sigma^{-1})$ عندئذ أياً كان $\tau \in H$ فإن $\sigma\tau\sigma^{-1}(b) = b$ ومنه يكون:

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

وهذا يبين أن $\sigma^{-1}(b) = \tau\sigma^{-1}(b)$ ومنه نجد أن $\sigma^{-1}(b) \in F(H)$ وبالتالي يكون

$b \in \sigma(F(H))$ وهكذا نجد أن $F(\sigma H \sigma^{-1}) \subseteq \sigma(F(H))$ ، مما سبق نجد أن:

$$\sigma(F(H)) = F(\sigma H \sigma^{-1})$$

٢ - ليكن $\sigma \in G$ ، عندئذ أياً كان $\tau \in G(E/\sigma(L))$ فإن $\tau : E \rightarrow E$ هو $\sigma(L)$ -

تماثل ذاتي للحقل E ومنه نجد أنه أياً كان $a \in L$ فإن $\tau(\sigma(a)) = \sigma(a)$ وبالتالي

$$\text{يكون } \sigma^{-1}(\tau(\sigma(a))) = \sigma^{-1}(\sigma(a)) = a.$$

لنضع $\mu = \sigma^{-1}\tau\sigma : E \rightarrow E$ فنجد أن μ هو تماثل ذاتي للحقل E ، لما كان

$\mu(a) = a$ وذلك أياً كان $a \in L$ نجد أن μ هو L - تماثل ذاتي للحقل E ومنه فإن

$\mu \in G(E/L)$ ، فضلاً عن ذلك فإن:

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

وهذا يبين أن:

$$\tau = \sigma\mu\sigma^{-1} \in \sigma \cdot G(E/L) \cdot \sigma^{-1}$$

ومنه نجد أن:

$$G(E/\sigma(L)) \subseteq \sigma \cdot G(E/L) \cdot \sigma^{-1}$$

ليكن $\varphi \in \sigma \cdot G(E/L) \cdot \sigma^{-1}$ عندئذ يوجد $\tau \in G(E/L)$ بحيث $\varphi = \sigma \cdot \tau \cdot \sigma^{-1}$ ومنه

فإن $\varphi : E \rightarrow E$ هو تماثل ذاتي للحقل E وأنه أياً كان $b \in \sigma(L)$ فإن $b = \sigma(a)$

حيث $a \in L$ وبالتالي فإن:

$$\varphi(b) = \sigma\tau\sigma^{-1}(b) = \sigma\tau\sigma^{-1}(\sigma(a)) = \sigma\tau(a)$$

ولما كان $\tau \in G(E/L)$ فإن τ هو L -تماثل ذاتي للحقل E وبالتالي يكون:

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

وهذا يبين أن φ هو $\sigma(L)$ -تماثل ذاتي للحقل E ، أي أن $\varphi \in G(E/\sigma(L))$ وهكذا

نجد أن $G(E/\sigma(L)) = \sigma \cdot G(E/L) \cdot \sigma^{-1}$ ، مما سبق نجد أن:

$$G(E/\sigma(L)) = \sigma \cdot G(E/L) \cdot \sigma^{-1}$$

وهو المطلوب إثباته. ◊

مبرهنة ١٠-١-١١.

ليكن الحقل E تمديد غالوا للحقل F وأن $G = G(E/F)$. لنفرض أن H زمرة جزئية من الزمرة G . عندئذ:

١ - الشرط اللازم والكافي كي تكون الزمرة الجزئية H ناظمية في G هو أن يكون الحقل $F(H)$ تمديداً ناظمياً للحقل F .

٢ - إذا كانت الزمرة الجزئية H ناظمية في الزمرة G عندئذ يكون:

$$G(F(H)/F) \cong G/H$$

البرهان.

١ - لزوم الشرط. لنفرض أن الزمرة الجزئية H ناظمية في G . لنفرض جـداً أن التمديد $F(H)$ للحقل F ليس ناظمياً عندئذ يوجد F -تشاكل $\tau: F(H) \rightarrow E$ لأجله:

$$\tau(F(H)) \neq F(H)$$

لنقم بتمديد التشاكل τ إلى E بالشكل الآتي: لنعرف $\tau': E \rightarrow E$ بالشكل الآتي: أياً كان $a \in E$ ، لنضع:

$$\tau'(a) = \begin{cases} a & a \notin F(H) \\ \tau(a) & a \in F(H) \end{cases}$$

ف نجد أن τ' هو F -تماثل ذاتي للحقل E وبالتالي $\tau' \in G$ وهو تمديد للتشاكل τ . لما كانت الزمرة الجزئية H ناظمية في G ، نجد أن $H = \tau'H\tau'^{-1}$ وحسب المبرهنة (١٠-١-١٠) نجد أن:

$$F(H) = F(\tau'H\tau'^{-1}) = \tau'(F(H)) = \tau(F(H))$$

وهذا تناقض، مما سبق نجد أن التمديد $F(H)$ للحقل F هو تمديد ناظمي.

كفاية الشرط. لنفرض أن التمديد $F(H)$ للحقل F هو تمديد ناظمي ولنفرض أيضاً أن $G' = G(F(H)/F)$. لنعرف العلاقة $\varphi: G \rightarrow G'$ بالشكل الآتي: أيّاً كان $\sigma \in G$ لنضع $\varphi(\sigma) = \sigma|_{F(H)}$ ، فنجد أن $\sigma|_{F(H)}: F(H) \rightarrow E$ هو F -تشاكل للحقل $F(H)$ في الحقل E ولما كان الحقل E هو تمديد غالوا للحقل F فإن E هو تمديد منته للحقل F وأن $F \subseteq F(H) \subseteq E$ ومنه نجد أن:

$$[E : F] = [E : F(H)] \cdot [F(H) : F]$$

وهذا يبين أن الحقل $F(H)$ هو تمديد منته للحقل F .

من جهة أخرى، لما كان الحقل $F(H)$ تمديداً ناظماً للحقل F فإنه حسب المبرهنة (٨-١-٩) يكون $\sigma|_{F(H)}$ هو F -تماثل ذاتي للحقل $F(H)$ ، أي أن:

$$\sigma|_{F(H)}: F(H) \rightarrow F(H)$$

وأن $\sigma(F(H)) = F(H)$ ومنه نجد أن:

$$\varphi(\sigma) = \sigma|_{F(H)} \in G' = G(F(H)/F)$$

واضح أن φ هو تطبيق وأنه أيضاً تشاكل، لأنه إذا كان $\sigma, \sigma' \in G$ فإن $\sigma \cdot \sigma' \in G$ وأن $\varphi(\sigma \cdot \sigma') = \sigma \cdot \sigma'|_{F(H)}$ ومنه أيّاً كان $a \in F(H)$ فإن $\sigma(a) = a \in F(H)$ وهذا يبين أن:

$$\begin{aligned} \sigma \cdot \sigma'|_{F(H)}(a) &= \sigma \cdot \sigma'(a) = \sigma(\sigma'(a)) = \sigma|_{F(H)}(\sigma'|_{F(H)}(a)) = \\ &= \sigma|_{F(H)} \cdot \sigma'|_{F(H)}(a) \end{aligned}$$

ومنه نجد أن $\sigma \cdot \sigma'|_{F(H)} = \sigma|_{F(H)} \cdot \sigma'|_{F(H)}$ وبالتالي يكون:

$$\varphi(\sigma \cdot \sigma') = \varphi(\sigma) \cdot \varphi(\sigma')$$

ومنه نجد أن φ تشاكل زمري. لنبرهن الآن على أن $\text{Ker}(\varphi) = H$.

ليكن $\tau \in H$ ، إن $\tau: E \rightarrow E$ هو F -تماثل ذاتي للحقل E وأنه أيّاً كان $a \in F(H)$ فإن $\tau(a) = a$ وهذا يبين أن $\tau|_{F(H)} = I_{F(H)}$ ولما كان $\tau \in G$ نجد أن:

$$\varphi(\tau) = \tau|_{F(H)} = I_{F(H)}$$

وهذا يبين أن $\tau \in \text{Ker}(\varphi)$ وبالتالي يكون $H \subseteq \text{Ker}(\varphi)$.

ليكن $\sigma \in \text{Ker}(\varphi)$ عندئذ يكون $\sigma : E \rightarrow E$ هو F - تماثل ذاتي للحقل E وأن:

$$\varphi(\sigma) = \sigma|_{F(H)} = I_{F(H)}$$

وهذا يبين أن $\sigma(F(H)) = F(H)$ وبالتالي أيّاً كان $a \in F(H)$ فإن:

$$\sigma(a) = I_{F(H)}(a) = a$$

ومنه يكون $\sigma \in H$ وبالتالي نجد أن $\text{Ker}(\varphi) \subseteq H$ ، مما سبق نجد أن $\text{Ker}(\varphi) = H$

وبالتالي الزمرة الجزئية H ناظمية في G .

٢ - لنفرض أن الزمرة الجزئية H ناظمية في G . وجدنا حسب (١) أن التطبيق:

$$\varphi : G \rightarrow G' = G(F(H)/F)$$

هو تشاكل زمري، لما كانت الزمرة الجزئية H ناظمية في G فإن التمديد $F(H)$ للحقل

F هو تمديد ناظمي وبالتالي فإن $\text{Ker}(\varphi) = H$. لنبرهن على أن التشاكل φ غامر.

ليكن $\sigma' \in G'$ عندئذ فإن $\sigma' : F(H) \rightarrow F(H)$ هو F - تماثل ذاتي للحقل $F(H)$.

لنمدد التشاكل σ' إلى التشاكل $\sigma : E \rightarrow F(H)$ بحيث يكون $\sigma|_{F(H)} = \sigma'$. لما كان

التمديد E للحقل F ناظمياً وأن $F \subseteq F(H) \subseteq E$ نجد أن E هو تمديد ناظمي للحقل

$F(H)$ ومنه يكون $\sigma(E) = E$ أي أن σ هو F - تماثل ذاتي للحقل E وبالتالي يكون

$\sigma \in G$ وأن $\varphi(\sigma) = \sigma|_{F(H)} = \sigma'$ وهذا يبين أن التشاكل φ غامر، وحسب مبرهنة

التماثل الأولى يكون:

$$G/H = G/\text{Ker}(\varphi) \cong G(F(H)/F) = G'$$

وهو المطلوب إثباته. ♦

مبرهنة ١٠-١-١٢.

ليكن الحقل E, L تمديدين للحقل F وأن K حقل يحوي كلا من E, L . إذا كان الحقل

E هو تمديد غالوا للحقل F ، عندئذ يكون:

١ - الحقل $E \cdot L$ هو تمديد غالوا للحقل L .

٢ - الحقل E هو تمديد غالوا للحقل $E \cap L$.

٣ - $G(E \cdot L/L) \cong G(E/E \cap L)$.

البرهان.

١ - لما كان E, L حقلين جزئيين من الحقل K فإن $E \cdot L$ هو حقل جزئي من الحقل K ولما كان كل من E, L يحوي F نجد أن $F \subseteq E \cdot L \subseteq K$.
من جهة أخرى، لما كان E هو تمديد غالوا للحقل F فإنه حسب المبرهنة (١٠-١-٦) يكون الحقل E حقل تفريق حدودية منفصلة $f(x) \in F[x]$ فوق F ومنه فإن:

$$E = F(a_1, a_2, \dots, a_n)$$

حيث $a_1, a_2, \dots, a_n \in E$ هي جميع أصفار الحدودية $f(x)$ في E وهي أصفار بسيطة. لما كان $F \subseteq L$ نجد أن $f(x) \in L[x]$ هي حدودية منفصلة فوق L ، كما أن:

$$E = F(a_1, a_2, \dots, a_n) \subseteq L(a_1, a_2, \dots, a_n) \subseteq E$$

وهذا يبين أن $E = L(a_1, a_2, \dots, a_n)$ وبالتالي يكون:

$$E \cdot L = L(a_1, a_2, \dots, a_n) \cdot L = L(a_1, a_2, \dots, a_n)$$

ومنه نجد أن $E \cdot L$ هو حقل تفريق حدودية منفصلة $f(x) \in L[x]$ فوق L وحسب المبرهنة (١٠-١-٦) يكون الحقل $E \cdot L$ تمديد غالوا للحقل L .

٢ - لما كان $F \subseteq E \cap L \subseteq E$ وأن الحقل E هو تمديد غالوا للحقل F فإنه حسب التمهيدية (١٠-١-٧) يكون الحقل E هو تمديد غالوا للحقل $E \cap L$.

٣ - لنعرف العلاقة:

$$\varphi: G(E \cdot L/L) \rightarrow G(E/E \cap L)$$

بالشكل الآتي: أي أن $\sigma \in G(E \cdot L/L)$ ، لنضع:

$$\varphi(\sigma) = \sigma|_E: E \rightarrow E \cdot L$$

ف نجد أن $\sigma|_E$ هو L -تشاكل متباين للحقل E في الحقل $E \cdot L$ وبالتالي يكون $\sigma|_E$ هو $(E \cap L)$ -تشاكل متباين للحقل E في الحقل $E \cdot L$. كي يكون:

$$\varphi(\sigma) = \sigma|_E \in G(E/E \cap L)$$

يكفي إثبات أن $\sigma(E) = E$.

وجدنا حسب (١) أن E هو حقل تفريق حدودية منفصلة $f(x) \in L[x]$ فوق L ، أي أن

$E = L(a_1, a_2, \dots, a_n)$ حيث $a_1, a_2, \dots, a_n \in E$ هي جميع أصفار الحدودية $f(x)$

في E . لنفرض أن $f(x) = \sum_{i=0}^m b_i x^i$ حيث $b_i \in F$ لأجل كل $0 \leq i \leq m$.

لما كانت العناصر a_j أصفاراً للحدودية $f(x)$ نجد أن:

$$f(a_j) = \sum_{i=0}^m b_i (a_j)^i = 0$$

ومنه يكون $\sigma(\sum_{i=0}^m b_i (a_j)^i) = \sigma(0) = 0$ وبالتالي فإن $\sum_{i=0}^m \sigma(b_i) \sigma((a_j)^i) = 0$

ولما كان σ هو L -تماثل ذاتي للحقل $E \cdot L$ نجد أن:

$$\sum_{i=0}^m b_i \cdot \sigma((a_j)^i) = 0 = f(\sigma(a_j))$$

وهذا يبين أن:

$$\sigma(a_1), \sigma(a_2), \dots, \sigma(a_n) \in \{a_1, a_2, \dots, a_n\}$$

ولما كان σ تشاكلاً متبايناً نجد أن:

$$\{\sigma(a_1), \sigma(a_2), \dots, \sigma(a_n)\} = \{a_1, a_2, \dots, a_n\}$$

فضلاً عن ذلك لما كان σ هو L -تماثل نجد أن $\sigma(L) = L$ ومنه نجد أن:

$$\sigma(L)(\sigma(a_1), \sigma(a_2), \dots, \sigma(a_n)) = L(a_1, a_2, \dots, a_n)$$

وهكذا نجد أن $\sigma(E) = E$ ، مما سبق نجد أن $\varphi(\sigma) = \sigma|_E \in G(E/E \cap L)$.

واضح أن φ هو تطبيق وأنه أيضاً تشاكل زمري، لأنه إذا كان $\sigma_1, \sigma_2 \in G(E \cdot L/L)$

فإن $\sigma_1 \cdot \sigma_2 \in G(E \cdot L/L)$ وأن:

$$\varphi(\sigma_1 \cdot \sigma_2) = \sigma_1 \cdot \sigma_2|_E$$

ولما كان لأجل كل $a \in E$ فإن $\sigma_2(a) \in E$ نجد أن:

$$\begin{aligned} \sigma_1 \cdot \sigma_2|_E(a) &= \sigma_1 \cdot \sigma_2(a) = \sigma_1(\sigma_2(a)) = \sigma_1|_E(\sigma_2(a)) = \\ &= \sigma_1|_E(\sigma_2|_E(a)) = \sigma_1|_E \cdot \sigma_2|_E(a) \end{aligned}$$

ومنه نجد أن:

$$\varphi(\sigma_1 \cdot \sigma_2) = \sigma_1 \cdot \sigma_2|_E = \sigma_1|_E \cdot \sigma_2|_E = \varphi(\sigma_1) \cdot \varphi(\sigma_2)$$

لنبرهن الآن على أن التشاكل φ متباين.

ليكن $\sigma \in \text{Ker}(\varphi)$ عندئذ فإن $\sigma : E \cdot L \rightarrow E \cdot L$ هو L -تماثل ذاتي للحقل $E \cdot L$ وأن $\varphi(\sigma) = \sigma|_E = I_E$ ومنه نجد أنه أياً كان $a \in E$ فإن:

$$\sigma(a) = \sigma|_E(a) = I_E(a) = a$$

أيضاً لما كان σ هو L -تماثل ذاتي للحقل $E \cdot L$ فإنه أياً كان $b \in L$ فإن $\sigma(b) = b$ ومنه نجد أنه لأجل كل $a \in E$ و $b \in L$ فإن

$$\sigma(ab) = \sigma(a) \cdot \sigma(b) = \sigma|_E(a) \cdot \sigma(b) = ab = I_E(ab)$$

وهذا يبين أن $\sigma = I_E$ ومنه فإن $\text{Ker}(\varphi) = I_E$ وبالتالي يكون التشاكل φ متبايناً. لنبرهن على أن التشاكل φ غامر. ليكن $\tau \in G(E/E \cap L)$ فنجد أن $\tau : E \rightarrow E$ هو $(E \cap L)$ -تماثل ذاتي للحقل E . لنمدد τ إلى التشاكل $\sigma : E \cdot L \rightarrow E \cdot L$ بالشكل الآتي:

$$\sigma(a) = \begin{cases} a & a \in L \\ \tau(a) & a \notin L \end{cases}$$

ف نجد أن σ هو L -تماثل ذاتي للحقل $E \cdot L$ وأنه أياً كان $a \in E$ فإن $\sigma(a) = \tau(a)$ ومنه نجد أن $\sigma \in G(E \cdot L/L)$ وأن $\sigma|_E = \tau$ وهذا يبين أن التشاكل φ غامر، مما سبق نجد أن φ تماثل وبالتالي يكون $G(E \cdot L/L) \cong G(E/E \cap L)$. ♦

مبرهنة ١٠-١-١٣.

ليكن الحقل E تمديداً للحقل F وأن E_1, E_2 حقلان جزئيان من الحقل E كل منهما يحوي F ، أي أن $E_1, E_2 \subseteq E$ و $F \subseteq E_1, E_2$. إذا كان كل من E_1, E_2 هو تمديد غالوا للحقل F ، عندئذ يكون:

١ - الحقل $E_1 \cdot E_2$ هو تمديد غالوا للحقل F .

٢ - الحقل $E_1 \cap E_2$ هو تمديد غالوا للحقل F .

٣ - الزمرة $G(E_1 \cdot E_2/F)$ تماثل زمرة جزئية من الزمرة $G(E_1/F) \times G(E_2/F)$. البرهان.

١ - لما كان E_1 هو تمديد غالوا للحقل F فإن E_1 هو حقل تفريق حدودية منفصلة

$f_1(x) \in F[x]$ فوق F ومنه فإن $E_1 = F(a_1, a_2, \dots, a_n)$ ، حيث العناصر $a_i \in E_1$ لأجل كل $1 \leq i \leq n$ هي جميع أصفار الحدودية $f_1(x)$ في E .

أيضاً لما كان E_2 هو تمديد غالوا للحقل F فإن E_2 هو حقل تفريق حدودية منفصلة $f_2(x) \in F[x]$ فوق F ومنه فإن $E_2 = F(b_1, b_2, \dots, b_m)$ ، حيث العناصر $b_i \in E_2$ لأجل كل $1 \leq i \leq m$ هي جميع أصفار الحدودية $f_2(x)$ في E .

وهكذا نجد أن $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m \in E$ هي جمع أصفار الحدودية:

$$f_1(x) \cdot f_2(x) \in F[x]$$

وأن

$$E_1 \cdot E_2 = F(a_1, a_2, \dots, a_n) \cdot F(b_1, b_2, \dots, b_m) =$$

$$= F(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_m) = F(a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m)$$

ولما كان مميز الحقل F يساوي الصفر وأن كلاً من $f_1(x), f_2(x) \in F[x]$ حدودية منفصلة فوق F فإن $f_1(x) \cdot f_2(x) \in F[x]$ وأن $\partial(f_1(x) \cdot f_2(x)) \geq 1$ وحسب التمهيدية (٥-٢-٢) نجد أن $f_1(x) \cdot f_2(x)$ هي حدودية منفصلة فوق F وأن $E_1 \cdot E_2$ هو حقل تفريق الحدودية $f_1(x) \cdot f_2(x)$ فوق F وحسب المبرهنة (١٠-١-٦) نجد أن الحقل $E_1 \cdot E_2$ هو تمديد غالوا للحقل F .

٢ - لما كان E_1 هو تمديد غالوا للحقل F فإن E_1 هو تمديد ناظمي ومنفصل ومنته للحقل F ولما كان $F \subseteq E_1 \cap E_2 \subseteq E$ وكان E_1 تمديداً منتهياً للحقل F نجد أن $E_1 \cap E_2$ هو تمديد منته للحقل F .

من جهة أخرى، لما كان E_1 تمديداً منفصلاً للحقل F نجد أن $E_1 \cap E_2$ هو تمديد منفصل للحقل F . لنبرهن على أن $E_1 \cap E_2$ هو تمديد ناظمي للحقل F .

ليكن $a \in E_1 \cap E_2$ وأن $f(x) \in F[x]$ الحدودية الأصغرية للعنصر a فوق F وأن $\partial f(x) = n$. لما كان E_1 هو تمديد ناظمي ومنفصل للحقل F نجد أن العنصر a منفصل فوق F وبالتالي تكون الحدودية $f(x)$ منفصلة فوق F ومنه فإن جميع أصفار الحدودية $f(x)$ هي أصفار بسيطة ومنه فإن $f(x)$ تملك n صفراً مختلفاً في الحقل E_1 . كذلك الأمر، إن الحدودية $f(x)$ تملك n صفراً مختلفاً في الحقل E_2 . ولما كانت

الحدودية $f(x)$ منفصلة فوق F وأن $\partial f(x) = n$ نجد أن $f(x)$ تملك على الأكثر n صفراً مختلفاً في الحقل $E_1 \cdot E_2$. بهذا الشكل نجد أن $f(x)$ تملك n صفراً مختلفاً في الحقل $E_1 \cap E_2$ وحسب التعريف يكون الحقل $E_1 \cap E_2$ تمديداً ناظمياً للحقل F . مما سبق نجد أن الحقل $E_1 \cap E_2$ هو تمديد غالوا للحقل F .

٣ - لنعرف العلاقة:

$$\varphi : G(E_1 \cdot E_2 / F) \rightarrow G(E_1 / F) \times G(E_2 / F)$$

بالشكل الآتي: ليكن $\sigma \in G(E_1 \cdot E_2 / F)$ فنجد أن $\sigma : E_1 \cdot E_2 \rightarrow E_1 \cdot E_2$ هو $-F$ تماثل ذاتي للحقل $E_1 \cdot E_2$ ومنه فإن $\sigma|_{E_1} : E_1 \rightarrow E_1 \cdot E_2$ هو $-F$ تماثل للحقل E_1 في الحقل $E_1 \cdot E_2$. لما كان E_1 هو تمديد غالوا للحقل F فإن E_1 هو تمديد ناظمي ومنته للحقل F وحسب المبرهنة (٨-١-٩) يكون $\sigma|_{E_1} : E_1 \rightarrow E_1$ هو $-F$ تماثل ذاتي للحقل E_1 وبالتالي فإن $\sigma|_{E_1} \in G(E_1 / F)$.

أيضاً لما كان E_2 هو تمديد غالوا للحقل F فإن E_2 هو تمديد ناظمي ومنته للحقل F وحسب المبرهنة (٨-١-٩) يكون $\sigma|_{E_2} : E_2 \rightarrow E_2$ هو $-F$ تماثل ذاتي للحقل E_2 وبالتالي فإن $\sigma|_{E_2} \in G(E_2 / F)$. لنضع:

$$\varphi(\sigma) = (\sigma|_{E_1}, \sigma|_{E_2}) \in G(E_1 / F) \times G(E_2 / F)$$

فنجد أن φ هو تطبيق وهو أيضاً تماثل، لأنه إذا كان $\sigma_1, \sigma_2 \in G(E_1 \cdot E_2 / F)$ فإن $\sigma_1 \cdot \sigma_2 \in G(E_1 \cdot E_2 / F)$

وأن $\sigma_1 \cdot \sigma_2 : E_1 \cdot E_2 \rightarrow E_1 \cdot E_2$ هو $-F$ تماثل ذاتي للحقل $E_1 \cdot E_2$ ، كما أن:

$$\sigma_1 \cdot \sigma_2|_{E_1} : E_1 \rightarrow E_1$$

هو $-F$ تماثل ذاتي للحقل E_1 كما هو موضح سابقاً ويحقق:

$$\sigma_1 \cdot \sigma_2|_{E_1} = \sigma_1|_{E_1} \cdot \sigma_2|_{E_1}$$

أيضاً إن $\sigma_1 \cdot \sigma_2|_{E_2} : E_2 \rightarrow E_2$ هو $-F$ تماثل ذاتي للحقل E_2 كما هو موضح سابقاً ويحقق

$$\sigma_1 \cdot \sigma_2|_{E_2} = \sigma_1|_{E_2} \cdot \sigma_2|_{E_2}$$

$$\varphi(\sigma_1 \cdot \sigma_2) = (\sigma_1 \cdot \sigma_2|_{E_1}, \sigma_1 \cdot \sigma_2|_{E_2}) =$$

$$\begin{aligned}
&= (\sigma_1|_{E_1} \cdot \sigma_2|_{E_1}, \sigma_1|_{E_2} \cdot \sigma_2|_{E_2}) = \\
&= (\sigma_1|_{E_1}, \sigma_1|_{E_2}) \cdot (\sigma_2|_{E_1}, \sigma_2|_{E_2}) = \varphi(\sigma_1) \cdot \varphi(\sigma_2)
\end{aligned}$$

ومنه نجد أن φ هو تشاكل. لنبرهن على أن التشاكل φ متباين.
ليكن $\sigma \in \text{Ker}(\varphi)$ عندئذ فإن $\sigma \in G(E_1 \cdot E_2/F)$ أي أن σ هو F - تماثل ذاتي للحقل $E_1 \cdot E_2$ وأن:

$$\varphi(\sigma) = (\sigma|_{E_1}, \sigma|_{E_2}) = (I_{E_1}, I_{E_2})$$

ومنه نجد أن $\sigma|_{E_1} = I_{E_1}$ ، $\sigma|_{E_2} = I_{E_2}$ وبالتالي أيًا كان $a \in E_1$ ، $b \in E_2$ فإن:

$$\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b) = \sigma|_{E_1} \cdot \sigma|_{E_2} = a \cdot b$$

وهذا يبين أن $\sigma = I_{E_1 \cdot E_2}$. مما سبق نجد أن $\text{Ker}(\varphi) = I_{E_1 \cdot E_2}$ وبالتالي التشاكل φ متباين. لנأخذ المجموعة:

$$H = \{(\sigma|_{E_1}, \sigma|_{E_2}) \mid \forall \sigma \in G(E_1 \cdot E_2/F)\}$$

لما كان لأجل كل $\sigma \in G(E_1 \cdot E_2/F)$ فإن $\sigma|_{E_1} \in G(E_1/F)$ وأن:

$$\sigma|_{E_2} \in G(E_2/F)$$

نجد أن H هي مجموعة جزئية من الزمرة:

$$G(E_1/F) \times G(E_2/F)$$

وهي ليست خالية طالما أن $G(E_1 \cdot E_2/F)$ زمرة. لنبرهن على أن H هي زمرة جزئية من الزمرة:

$$G(E_1/F) \times G(E_2/F)$$

ليكن $(\sigma|_{E_1}, \sigma|_{E_2}), (\sigma'|_{E_1}, \sigma'|_{E_2}) \in H$ حيث $\sigma, \sigma' \in G(E_1 \cdot E_2/F)$ عندئذ فإن

$\sigma^{-1} \in G(E_1 \cdot E_2/F)$ وبالتالي يكون $\sigma' \cdot \sigma^{-1} \in G(E_1 \cdot E_2/F)$ كما أن:

$$(\sigma'^{-1}|_{E_1}, \sigma'^{-1}|_{E_2}) \in H$$

فضلاً عن ذلك فإن:

$$(\sigma'|_{E_1}, \sigma'|_{E_2}) \cdot (\sigma|_{E_1}, \sigma|_{E_2})^{-1} = (\sigma'|_{E_1}, \sigma'|_{E_2}) \cdot (\sigma^{-1}|_{E_1}, \sigma^{-1}|_{E_2}) =$$

$$(\sigma'|_{E_1} \cdot \sigma^{-1}|_{E_1}, \sigma'|_{E_2} \cdot \sigma^{-1}|_{E_2}) = (\sigma' \cdot \sigma^{-1}|_{E_1}, \sigma' \cdot \sigma^{-1}|_{E_2}) \in H$$

وذلك لأن $\sigma' \cdot \sigma^{-1} \in G(E_1 \cdot E_2/F)$ وهذا يبين أن H هي زمرة جزئية من الزمرة $G(E_1/F) \times G(E_2/F)$. ولما كان لأجل كل $\sigma \in G(E_1 \cdot E_2/F)$ فإن:

$$\varphi(\sigma) = (\sigma|_{E_1}, \sigma|_{E_2}) \in H$$

نجد أن $H \rightarrow G(E_1 \cdot E_2/F)$ هو تشاكل متباين. لنبرهن على أن φ غامر.

ليكن $(\tau|_{E_1}, \tau|_{E_2}) \in H$ حيث $\tau \in G(E_1 \cdot E_2/F)$ فنجد أن $\varphi(\tau) = (\tau|_{E_1}, \tau|_{E_2})$ ،

وهكذا نجد أن φ غامر وبالتالي فهو تماثل ومنه نجد أن:

$$G(E_1 \cdot E_2/F) \cong H \subseteq G(E_1/F) \times G(E_2/F)$$

وهو المطلوب إثباته. ♦

تمارين محلولة (١٠)

١ - لنأخذ الحدودية $p(x) = x^4 - 2 \in Q[x]$. المطلوب:

أ - أوجد حقل التفريق K للحدودية $p(x)$ فوق الحقل Q .

ب - أثبت أن الحقل K هو تمديد غالوا للحقل Q .

ت - أوجد الزمرة $G(K/Q)$.

ث - أوجد الزمر الجزئية في الزمرة $G(K/Q)$.

ج - أوجد الحقول الجزئية في K المثبتة من خلال الزمر الجزئية السابقة.

الحل.

أ - إن $p(x) = x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) \in Q[x]$ ومنه فإن أصفار الحدودية $p(x)$ هي $\pm \sqrt[4]{2}, \pm i \cdot \sqrt[4]{2}$.

لنفرض أن الحقل K هو حقل تفريق الحدودية $p(x)$ فوق فنجد أن $K = Q(\sqrt[4]{2}, i)$.

ب - واضح أن الحدودية $p(x)$ أولية فوق الحقل Q لأنها لا تملك أصفاراً في الحقل Q ، أو حسب معيار إيرنشتاين ولأجل $p = 2$ نجد أن الحدودية $p(x)$ أولية فوق الحقل Q ، ولما كان مميز الحقل Q يساوي الصفر وأن $\partial p(x) > 0$ نجد أن $p(x)$ حدودية منفصلة فوق الحقل Q وبالتالي يكون الحقل K هو تمديد غالوا للحقل Q .

ت - لما كان $Q \subseteq Q(\sqrt[4]{2}) \subseteq K$ وأن K تمديد منته للحقل Q نجد أن:

$$[K : Q] = [K : Q(\sqrt[4]{2})] \cdot [Q(\sqrt[4]{2}) : Q]$$

من جهة أخرى، لما كانت الحدودية $p(x)$ أولية فوق Q وأن $p(\sqrt[4]{2}) = 0$ نجد أن $p(x)$ هي الحدودية الأصغرية للعنصر $\sqrt[4]{2}$ فوق Q ومنه فإن:

$$[Q(\sqrt[4]{2}) : Q] = \partial p(x) = 4$$

أيضاً لما كانت الحدودية $q(x) = (x^2 + \sqrt{2}) \in Q(\sqrt[4]{2})[x]$ أولية فوق الحقل $Q(\sqrt[4]{2})$ لأنها لا تملك أصفاراً في الحقل $Q(\sqrt[4]{2})$ وأن $q(i) = 0$ نجد أن الحدودية $q(x)$ هي الحدودية الأصغرية للعنصر i فوق الحقل $Q(\sqrt[4]{2})$ ، ومنه نجد أن:

$$[K : Q(\sqrt[4]{2})] = [Q(\sqrt[4]{2})(i) : Q(\sqrt[4]{2})] = \partial(q(x)) = 2$$

مما سبق نجد أن $[K : Q] = 8$.

لما كان K هو حقل تفريق الحدودية $p(x)$ فوق Q فإنه حسب المبرهنة (٩-٢-١) يكون:

$$(G(K/Q):1) = [K : Q] = 8$$

ومنه فإن الزمرة $G(K/Q)$ تتألف من ثمانية عناصر، لنفرض أن هذه العناصر هي:

$$\sigma_i : K \rightarrow K \quad i = 1, 2, \dots, 8$$

وكل من هذه العناصر هو Q -تماثل ذاتي للحقل K وذلك لأجل كل $1 \leq i \leq 8$. لنشكل جدولاً لهذه العناصر:

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
$i \rightarrow$	i	i	i	i	$-i$	$-i$	$-i$	$-i$
$\sqrt[4]{2} \rightarrow$	$\sqrt[4]{2}$	$\sqrt[4]{2}$	$i \cdot \sqrt[4]{2}$	$-i \cdot \sqrt[4]{2}$	$i \cdot \sqrt[4]{2}$	$-i \cdot \sqrt[4]{2}$	$i \cdot \sqrt[4]{2}$	$-i \cdot \sqrt[4]{2}$

إن الزمرة $G(K/Q)$ تحوي خمسة عناصر مرتبة كل منها تساوي 2 وهذه العناصر هي:

$$\sigma_2, \sigma_5, \sigma_6, \sigma_7, \sigma_8$$

لنختبر على سبيل المثال العنصر σ_6 ، إن:

$$\begin{aligned} \sigma_6^2(i) &= \sigma_6(\sigma_6(i)) = \sigma_6(-i) = -(-i) = i \\ \sigma_6^2(\sqrt[4]{2}) &= \sigma_6(\sigma_6(\sqrt[4]{2})) = \sigma_6(-i \cdot \sqrt[4]{2}) = -\sigma_6(i) \cdot \sigma_6(\sqrt[4]{2}) = \\ &= -(-i)(-i \cdot \sqrt[4]{2}) = -i^2 \cdot \sqrt[4]{2} = \sqrt[4]{2} \end{aligned}$$

وهذا يبين أن $o(\sigma_2) = 2$. بطريقة مشابهة يمكن اختبار مراتب العناصر الأخرى.

كما أن الزمرة $G(K/Q)$ تحوي عنصر مرتبته 4 هو σ_4 ، لأن:

$$\begin{aligned} \sigma_4^2(i) &= \sigma_4(\sigma_4(i)) = \sigma_4(i) = i \\ \sigma_4^4(i) &= \sigma_4^2(\sigma_4^2(i)) = \sigma_4^2(i) = i \\ \sigma_4^2(\sqrt[4]{2}) &= \sigma_4(\sigma_4(\sqrt[4]{2})) = \sigma_4(-i \cdot \sqrt[4]{2}) = -\sigma_4(i) \cdot \sigma_4(\sqrt[4]{2}) = \end{aligned}$$

$$= -(-i)(-i \cdot \sqrt[4]{2}) = -\sqrt[4]{2}$$

$$\sigma_4^4(\sqrt[4]{2}) = \sigma_4^2(\sigma_4^2(\sqrt[4]{2})) = \sigma_4^2(-\sqrt[4]{2}) = -\sigma_4^2(i) = -(-\sqrt[4]{2}) = \sqrt[4]{2}$$

وهذا يبين أن $o(\sigma_4) = 2$

ث - لنبرهن على أن $Q(i \cdot \sqrt[4]{2}) \cap Q(i) = Q$ لنفرض جـلاً أن:

$$Q(i \cdot \sqrt[4]{2}) \cap Q(i) \neq Q$$

عندئذ يوجد $x \in Q(i \cdot \sqrt[4]{2}) \cap Q(i)$ ، ولما كان $[Q(i) : Q] = 2$ فإن $x = a + i \cdot b$ حيث $a, b \in Q, b \neq 0$. أيضاً لما كان $[Q(i) : Q] = 2$ نجد أن $x = a_1 + i \cdot b_1 \cdot \sqrt[4]{2}$ حيث $a_1, b_1 \in Q, b_1 \neq 0$ ، ومنه نجد أن $a - a_1 = i \cdot (b_1 \cdot \sqrt[4]{2} - b)$ وهذا ممكن فقط عندما $b_1 \cdot \sqrt[4]{2} - b = 0$ ومنه فإن $b = b_1 \cdot \sqrt[4]{2}$ ولما كان $b_1 \neq 0$ نجد أن:

$$\sqrt[4]{2} = b \cdot b_1^{-1} \in Q$$

وهذا غير ممكن، ومنه نجد أن $Q(i \cdot \sqrt[4]{2}) \cap Q(i) = Q$. أصبح لدينا:

$$K = Q(\sqrt[4]{2}, i) = Q(i \cdot \sqrt[4]{2}) \cdot Q(i)$$

وأن كلاً من $Q(i)$, $Q(i \cdot \sqrt[4]{2})$ هو حقل تفريق فوق الحقل Q وبحققان:

$$Q(i \cdot \sqrt[4]{2}) \cap Q(i) = Q$$

وحسب المبرهنة (٩-٢-٩) نجد أن:

$$G(K/Q) \cong G(Q(i \cdot \sqrt[4]{2})/Q) \times G(Q(i)/Q)$$

ج - لنوجد الحقول الجزئية في الحقل $K = Q(\sqrt[4]{2}, i)$.

وجدنا أن العنصر $\sigma_3 \in G(K/Q)$ مرتبته 4 لأن $\sigma_3^4(\sqrt[4]{2}) = \sqrt[4]{2}$ ، $\sigma_3(i) = -i$ وأن:

$$\sigma_3^2(i) = \sigma_3(\sigma_3(i)) = \sigma_3(i) = i$$

$$\sigma_3^4(i) = \sigma_3^2(\sigma_3^2(i)) = \sigma_3^2(i) = i$$

$$\sigma_3^2(\sqrt[4]{2}) = \sigma_3(\sigma_3(\sqrt[4]{2})) = \sigma_3(i \cdot \sqrt[4]{2}) =$$

$$= \sigma_3(i) \cdot \sigma_3(\sqrt[4]{2}) = i \cdot (i \cdot \sqrt[4]{2}) = -\sqrt[4]{2}$$

$$\sigma_3^4(\sqrt[4]{2}) = \sigma_3^2(\sigma_3^2(\sqrt[4]{2})) = \sigma_3^2(-\sqrt[4]{2}) = -(-\sqrt[4]{2}) = \sqrt[4]{2}$$

وهذا يبين أن $o(\sigma_3) = 4$

إن العنصر σ_3 مرتبته تساوي 2 وبالتالي فهو يولد زمرة جزئية دوارة مرتبتها 2. لنفرض

أن $H = \langle \sigma_3^2 \rangle$ ، فنجد أن الحقل المثبت من خلال هذه الزمرة هو الحقل $Q(\sqrt{2}, i)$ ، أي
 أن $F(H) = Q(\sqrt{2}, i)$ ، لأن:

$$\sigma_3^2(i) = i$$

$$\sigma_3^2(\sqrt{2}) = \sigma_3^2(\sqrt[4]{2} \cdot \sqrt[4]{2}) = \sigma_3^2(\sqrt[4]{2}) \cdot \sigma_3^2(\sqrt[4]{2}) = (-\sqrt[4]{2}) \cdot (-\sqrt[4]{2}) = \sqrt{2}$$

وجدنا أيضاً أن العنصر $\sigma_7 \in G(K/Q)$ وأن مرتبته 2 ، فضلاً عن ذلك فإن:

$$\sigma_7^2(\sqrt[4]{2}) = \sqrt[4]{2}$$

لنفرض أن $M = \langle \sigma_7 \rangle$ فنجد أن M زمرة جزئية من الزمرة $G(K/Q)$ وأن:

$$F(M) = Q(\sqrt{2})$$

وذلك لأن $\sigma_3^2(\sqrt{2}) = \sqrt{2}$ وأن:

$$\sigma_7(\sqrt{2}) = \sigma_7(\sqrt[4]{2} \cdot \sqrt[4]{2}) = \sigma_7(\sqrt[4]{2}) \cdot \sigma_7(\sqrt[4]{2}) = \sqrt[4]{2} \cdot \sqrt[4]{2} = \sqrt{2}$$

لنأخذ الزمرة الجزئية $S = \langle \sigma_3^2, \sigma_3, \sigma_7 \rangle$ فنجد أن:

$$\begin{aligned} \sigma_3^2(i \cdot \sqrt{2}) &= \sigma_3^2(i) \cdot \sigma_3^2(\sqrt{2}) = i \cdot \sigma_3^2(\sqrt[4]{2} \cdot \sqrt[4]{2}) = i \cdot \sigma_3^2(\sqrt[4]{2}) \cdot \sigma_3^2(\sqrt[4]{2}) = \\ &= i \cdot (-\sqrt[4]{2}) \cdot (-\sqrt[4]{2}) = i \cdot \sqrt{2} \end{aligned}$$

$$\begin{aligned} \sigma_3 \cdot \sigma_7(i \cdot \sqrt{2}) &= \sigma_3(\sigma_7(i) \cdot \sigma_7(\sqrt{2})) = \sigma_3(-i \cdot \sqrt{2}) = \\ &= -\sigma_3(i) \cdot \sigma_3(\sqrt{2}) = -i \cdot \sigma_3(\sqrt[4]{2} \cdot \sqrt[4]{2}) = -i \cdot \sigma_3(\sqrt[4]{2}) \cdot \sigma_3(\sqrt[4]{2}) = \\ &= -i \cdot (i \cdot \sqrt[4]{2}) \cdot (i \cdot \sqrt[4]{2}) = i \cdot \sqrt{2} \end{aligned}$$

ومنه نجد أن الحقل المثبت من خلال هذه الزمرة هو $F(S) = Q(i \cdot \sqrt{2})$. بطريقة
 مشابهة نوجد بقية الزمر الجزئية والحقول المثبتة المقابلة لها.

٢ - لنأخذ الحدودية $p(x) = x^3 - 2 \in Q[x]$. أثبت أن حقل التفريق للحدودية $p(x)$
 فوق Q هو تمديد غالوا للحقل Q ثم أوجد زمرة غالوا لهذا التمديد وعلاقتها بالزمرة
 التناظرية.

الحل.

نلاحظ أن أصفار الحدودية $p(x)$ هي $\sqrt[3]{2} \cdot j, \sqrt[3]{2} \cdot j^2, \sqrt[3]{2}$ حيث:

$$j = \cos\left(\frac{3\pi}{2}\right) + i \cdot \sin\left(\frac{3\pi}{2}\right) = \frac{-1 + i \cdot \sqrt{3}}{2}$$

لما كانت هذه الأصفار لا تنتمي للحقل Q نجد أن الحدودية $p(x)$ أولية فوق الحقل Q ،
أو حسب معيار أيزنشتاين ولأجل العدد $p = 2$ نجد أن الحدودية $p(x)$ أولية فوق Q .
إن حقل تفريق الحدودية $p(x)$ فوق Q هو الحقل $Q(\sqrt[3]{2}, j)$ ، ولما كان مميز
الحقل Q يساوي الصفر وأن $\partial p(x) > 0$ نجد أن الحدودية $p(x)$ منفصلة فوق Q ومنه
فإن K هو حقل تفريق حدودية منفصلة فوق Q وبالتالي فإن K هو تمديد غالوا
للحقل Q .

لما كان الحقل K تمديداً منتهياً للحقل Q نجد أن:

$$[K : Q] = [Q(\sqrt[3]{2}, j) : Q] = \\ = [Q(\sqrt[3]{2}, j) : Q(\sqrt[3]{2})] \cdot [Q(\sqrt[3]{2}) : Q]$$

ولما كانت الحدودية $p(x) = x^3 - 2 \in Q[x]$ أولية فوق Q وأن $p(\sqrt[3]{2}) = 0$ نجد أن
الحدودية $p(x)$ هي الحدودية الأصغرية للعنصر $\sqrt[3]{2}$ فوق Q ومنه فإن:

$$[Q(\sqrt[3]{2}) : Q] = \partial p(x) = 3$$

من جهة أخرى، إن الحدودية:

$$q(x) = x^2 + x + 1 \in Q(\sqrt[3]{2})[x]$$

أصفارها $\frac{-1 \pm i \cdot \sqrt{3}}{2} \notin Q(\sqrt[3]{2})$ وبالتالي فإن الحدودية $q(x)$ أولية فوق Q وأن
 $q(j) = 0$ وهذا يبين أن الحدودية $q(x)$ هي الحدودية الأصغرية للعنصر j فوق الحقل
 $Q(\sqrt[3]{2})$ ، ومنه نجد أن:

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

مما سبق نجد أن $[K : Q] = 6$.

لما كان الحقل K هو تمديد غالوا للحقل Q فإن:

$$(G(K/Q) : 1) = [K : Q] = 6$$

ومنه نجد أن الزمرة $G(K/Q)$ تتألف من ستة عناصر. لنفرض أن هذه العناصر هي:

$$\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6$$

وكل منها هو Q -تماثل ذاتي للحقل K . لنشكل جدولاً للعناصر السابقة:

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
$\sqrt[3]{2} \rightarrow$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2} \cdot j$	$\sqrt[3]{2} \cdot j$	$\sqrt[3]{2} \cdot j^2$	$\sqrt[3]{2} \cdot j^2$
$j \rightarrow$	j	j^2	j	j^2	j	j^2

يوجد تقابل بين الزمرة $G(K/Q)$ والزمرة التناظرية S_3 التي تتألف من العناصر الآتية:

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad (12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad (13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$(23) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad (123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad (132) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

أي أن $S_3 = \{I, (12), (13), (23), (123), (132)\}$. لنضع:

$$I \leftrightarrow \sigma_1, \quad (23) \leftrightarrow \sigma_2, \quad (123) \leftrightarrow \sigma_3$$

$$(12) \leftrightarrow \sigma_4, \quad (123) \leftrightarrow \sigma_5, \quad (13) \leftrightarrow \sigma_6$$

٣ - لنأخذ الحقل $K = Q(\sqrt{3}, i)$. المطلوب:

أ - أثبت أن الحقل K هو تمديد غالوا للحقل Q .

ب - أوجد الحقول الجزئية في K .

ت - أوجد الزمر الجزئية المقابلة للحقول الجزئية السابقة.

الحل.

أ - إن الحقل K هو حقل تفريق الحدودية $p(x) = x^2 + 3 \in Q[x]$ وأن الحدودية $p(x)$ هي حدودية أولية فوق Q ، لأنها لا تملك أصفاراً في الحقل Q وهي حدودية منفصلة فوق Q ، لأن مميز الحقل Q يساوي الصفر وأن $\partial p(x) > 0$ ومنه فإن K هو حقل تفريق حدودية منفصلة فوق Q وبالتالي فإن K هو تمديد غالوا للحقل Q .

ب - لما كان الحقل K تمديداً منتهياً للحقل Q فإن:

$$[K : Q] = [Q(\sqrt{3}, i) : Q] =$$

$$= [Q(\sqrt{3}, i) : Q(\sqrt{3})] \cdot [Q(\sqrt{3}) : Q]$$

لما كانت الحدودية $q(x) = x^2 - 3 \in Q[x]$ أولية فوق Q وأن $q(\sqrt{3}) = 0$ نجد أن $q(x)$ هي الحدودية الأصغرية للعنصر $\sqrt{3}$ فوق Q ومنه فإن $[Q(\sqrt{3}) : Q] = 2$.
من جهة أخرى، إن الحدودية $x^2 + 1 \in Q(\sqrt{3})[x]$ هي الحدودية الأصغرية للعنصر i فوق الحقل $Q(\sqrt{3})$ ، ومنه فإن:

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

مما سبق نجد أن $[K : Q] = 4$.

لما كان الحقل K هو تمديد غالوا للحقل Q فإن:

$$(G(K/Q) : 1) = [K : Q] = 4$$

ومنه نجد أن الزمرة $G(K/Q)$ تتألف من أربعة عناصر. لنفرض أن هذه العناصر هي:

$$\sigma_1, \sigma_2, \sigma_3, \sigma_4$$

وكل منها هو Q -تماثل ذاتي للحقل K . لنشكل جدولاً للعناصر السابقة:

	σ_1	σ_2	σ_3	σ_4
$i \rightarrow$	i	i	$-i$	$-i$
$\sqrt{3} \rightarrow$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$

إن العنصر σ_3 مرتبته تساوي 2، لأن:

$$\sigma_3^2(i) = \sigma_3(\sigma_3(i)) = \sigma_3(-i) = -\sigma_3(i) = -(-i) = i$$

$$\sigma_3^2(\sqrt{3}) = \sigma_3(\sigma_3(\sqrt{3})) = \sigma_3(\sqrt{3}) = \sqrt{3}$$

ومنه فإن $o(\sigma_3) = 2$. بطريقة مشابهة نجد أن $o(\sigma_2) = 2$. لنفرض أن:

$$H = \langle \sigma_2 \rangle, \quad N = \langle \sigma_3 \rangle$$

فنجد أن كلا من H, N هي زمرة جزئية دوارة مرتبتهما 2، لذلك فإن:

$$H = \langle \sigma_2 \rangle \cong Z/2Z, \quad N = \langle \sigma_3 \rangle \cong Z/2Z$$

إن الحقل المثبت من خلال الزمرة H هو $F(H) = Q(i)$ ، وذلك لأن $\sigma_2(i) = i$.

كما أن الحقل المثبت من خلال الزمرة N هو $F(N) = Q(\sqrt{3})$ ، وذلك

$$\text{لأن } \sigma_3(\sqrt{3}) = \sqrt{3}.$$

نلاحظ أيضاً أن $\sigma_4 = \sigma_2 \cdot \sigma_3$ وذلك لأن:

$$\sigma_2 \cdot \sigma_3(i) = \sigma_2(\sigma_3(i)) = \sigma_2(-i) = -\sigma_3(i) = -i = \sigma_4(i)$$

$$\sigma_2 \cdot \sigma_3(\sqrt{3}) = \sigma_2(\sigma_3(\sqrt{3})) = \sigma_2(\sqrt{3}) = -\sqrt{3} = \sigma_4(\sqrt{3})$$

كما أن $o(\sigma_4) = o(\sigma_2 \cdot \sigma_3) = 2$ لنفرض أن $M = \langle \sigma_2 \cdot \sigma_3 \rangle$ فنجد أن M زمرة جزئية من الزمرة $G(K/Q)$ وأن الحقل المثبت من خلال هذه الزمرة هو $F(M) = Q(i \cdot \sqrt{3})$ وذلك لأن:

$$\begin{aligned} \sigma_2 \cdot \sigma_3(i \cdot \sqrt{3}) &= \sigma_2(\sigma_3(i) \cdot \sigma_3(\sqrt{3})) = \sigma_2(-i \cdot \sqrt{3}) = \\ &= \sigma_2(i) \cdot \sigma_2(\sqrt{3}) = -i \cdot (-\sqrt{3}) = i \cdot \sqrt{3} \end{aligned}$$

وأن الزمرة $M = \langle \sigma_2 \cdot \sigma_3 \rangle \cong Z/2Z$ ، ولما كانت الزمرة $G(K/Q)$ مرتبتها 4 وليست دوارة، لأنها لا تحوي عنصراً مرتبته 4 نجد أن:

$$G(K/Q) \cong Z/2Z \times Z/2Z$$

الفصل الحادي عشر

الحقول الدوارة

١١ - ١. الجذور الأولية للواحد.

إن لجذور الواحد دوراً مميزاً في إيجاد أصفار الحدوديات وجذور المعادلات. في هذه الفقرة سوف نورد عدداً من النتائج المتعلقة بجذور الواحد وذلك لمتابعة دراستنا لنظرية غالوا.

لا بد من التذكير هنا أن جميع الحقول التي سوف تتم دراستها في هذا الفصل هي حقول غير منتهية.

التابع φ .

لنفرض أن $N = \{1, 2, 3, \dots\}$ مجموعة الأعداد الصحيحة الموجبة (الطبيعية). نسمي التابع (التطبيق) $\varphi: N \rightarrow N$ المعروف بالشكل الآتي: أيّاً كان $n \in N$ فإن:

$$\varphi(n) = \text{Card} \{k : k \in N; 1 \leq k \leq n; \gcd(n, k) = 1\}$$

تابع أولر.

على سبيل المثال فإن: $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(10) = 4$.

اعتماداً على التعريف السابق يمكننا صياغة النتيجة الآتية:

نتيجة.

لأجل أي عدد أولي p فإن $\varphi(p) = p - 1$.

إن للتابع φ عدداً من الخواص سوف نذكرها فيما يأتي:

- إذا كان m, n عددين صحيحين موجبين أوليين فيما بينهما فإن:

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

- إذا كان n عدداً صحيحاً موجباً من الشكل:

$$n = p_1^{t_1} \cdot p_2^{t_2} \cdot \dots \cdot p_m^{t_m}$$

حيث $p_1, p_2, \dots, p_m$ أعداد أولية مختلفة مثني مثني، فإن:

$$\varphi(n) = p_1^{t_1-1} \cdot (p_1 - 1) \cdot p_2^{t_2-1} \cdot (p_2 - 1) \cdots p_m^{t_m-1} \cdot (p_m - 1)$$

تعريف.

ليكن F حقلاً مميزه يساوي الصفر و n عدداً صحيحاً موجباً. نسمي كل صفر للحدودية $x^n - 1 \in F[x]$ جذراً نونياً للواحد (جذر للواحد من المرتبة n).
 التعريف السابق يمكننا صياغته بالشكل الآتي:

- ١ - نقول عن العنصر $a \in F$ إنه جذر نوني للواحد إذا كان $a^n = 1$.
- ٢ - نقول عن العنصر $a \in F$ إنه جذر أولي للواحد من المرتبة n إذا كان $a^n = 1$ وأن $a^m \neq 1$ وذلك أيأ كان $1 < m < n$.

سوف نرمز لمجموعة الجذور النونية للواحد بالشكل μ_n ولمجموعة الجذور الأولية للواحد من المرتبة n بالشكل π_n . فنجد أن:

$$\mu_n = \{\xi : \xi \in F; \xi^n = 1\}$$

$$\pi_n = \{\zeta : \zeta \in F; \zeta^n = 1; \zeta^m \neq 1 \forall 1 < m < n\}$$

اعتماداً على التعريف السابق يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن F حقلاً منتهياً مرتبته p^n حيث p عدد أولي، عندئذ فإن كل عنصر $a \in F$ هو جذر للواحد من المرتبة p^{n-1} .

اعتماداً على ما سبق يمكننا صياغة التمهيدية الآتية:

تمهيدية ١-١-١١.

ليكن F حقلاً مميزه يساوي الصفر وأن $x^n - 1 \in F[x]$. عندئذ فإن:

- ١ - $\pi_n \subseteq \mu_n$.
- ٢ - $\text{Card } \mu_n = n$.
- ٣ - المجموعة μ_n تشكل زمرة بالنسبة لعملية الضرب المعرفة على الحقل F .

٤ - المجموعة μ_n زمرة دوارة.

٥ - $Card \pi_n = \varphi(n)$.

البرهان.

١ - واضح من خلال التعريف.

٢ - لما كان مميز الحقل F يساوي الصفر فإن:

$$(x^n - 1)' = nx^{n-1} \neq 0$$

من جهة أخرى، لما كانت $\partial(x^n - 1) > 0$ فإن الحدودية $x^n - 1$ تكون منفصلة فوق الحقل F وبالتالي فإن جميع أصفارها تكون بسيطة، إن هذا يبين أن جميع أصفار الحدودية $x^n - 1$ مختلفة مثلي مثلي.

لما كانت $\partial(x^n - 1) = n$ نجد أن الحدودية $x^n - 1$ تملك بالتحديد n صفراً مختلفاً وبالتالي يكون $Card \mu_n = n$.

٣ - واضح أن μ_n مجموعة جزئية في F وليست خالية، لأن $1 \in \mu_n$.

ليكن $a, b \in \mu_n$ عندئذ يكون $a^n = 1, b^n = 1$ ومنه فإن $a^n b^n = 1$ وبالتالي $(ab)^n = 1$ وبالتالي يكون $a \cdot b \in \mu_n$ ، إن هذا يبين أن المجموعة μ_n مغلقة بالنسبة لعملية الضرب المعرفة على الحقل F ، وهذه العملية تجميعية. إذا كان $a \in \mu_n$ عندئذ فإن $a^{-1} \in F$ وأن $(a^{-1})^n = a^{-n} = 1$ ومنه فإن $a^{-1} \in \mu_n$ ، مما سبق نجد أن المجموعة μ_n تشكل زمرة بالنسبة لعملية الضرب المعرفة على الحقل F .

٤ - وجدنا حسب (٣) أن المجموعة μ_n تشكل زمرة جزئية من الزمرة $(F^*, \cdot)$ ولما كانت μ_n منتهية فإنه حسب المبرهنة (٦-١-٤) تكون الزمرة μ_n دوارة.

٥ - وجدنا حسب (٤) أن الزمرة μ_n دوارة. ليكن $\zeta \in \pi_n$ عندئذ فإن $\zeta \in \mu_n$ وأن $\zeta^m \neq 1$ لأجل كل $1 < m < n$ ومنه نجد أن مرتبة العنصر ζ تساوي n ، أي أن $o(\zeta) = n$ وبالتالي يكون العنصر ζ مولداً للزمرة μ_n .

لما كان العنصر ζ مولداً للزمرة μ_n فإن $\gcd(n, m) = 1$ أي أن العددين n, m أوليان فيما بينهما ولما كان $\varphi(n)$ هو عدد كل الأعداد الأولية مع n نجد أن:

$$\diamond. Card \pi_n = \varphi(n)$$

اعتماداً على التمهيدية الأخيرة يمكننا إعادة صياغة المجموعتين μ_n و π_n وذلك من خلال النتيجة الآتية:

نتيجة.

ليكن n عدداً صحيحاً موجباً، عندئذ فإن:

$$\pi_n = \{\zeta : \zeta \in \mu_n; o(\zeta) = n\}$$

لما كانت الزمرة μ_n دوارة فإنه يوجد $\xi \in \mu_n$ بحيث يكون:

$$\mu_n = \langle \xi \rangle = \{\xi^k : 1 \leq k \leq n\}$$

ولما كانت π_n مجموعة جزئية في μ_n نجد أن:

$$\pi_n = \{\zeta^k : 1 \leq k \leq n; \gcd(k, n) = 1\}$$

اعتماداً على ما سبق يمكننا صياغة التمهيدية الآتية:

تمهيدية ١١-١-٢.

ليكن F حقلاً مميزه يساوي الصفر وأن K حقل تفريق الحدودية $x^n - 1 \in F[x]$ فوق F . عندئذ فإن:

$$١ - \text{إذا كان } \langle \xi \rangle = \mu_n \text{ فإن } F(\xi) = F(\mu_n).$$

$$٢ - \text{ليكن } m \text{ عدداً صحيحاً موجباً و } \zeta \in \pi_m \text{ عندئذ } F(\zeta) = F(\mu_m).$$

$$٣ - F(\xi, \zeta) = F(\mu_n, \mu_m) = F(\mu_m, \zeta).$$

البرهان.

$$١ - \text{لنفرض أن } \langle \xi \rangle = \mu_n. \text{ لما كان } \xi \in \mu_n \text{ فإن } F(\xi) \subseteq F(\mu_n).$$

من جهة أخرى، ليكن $\varepsilon \in \mu_n$ عندئذ فإن $\varepsilon = \xi^k$ حيث $1 \leq k \leq n$ ولما كان $\xi \in F(\xi)$ نجد أن $\varepsilon \in F(\xi)$ ومنه $\mu_n \subseteq F(\xi)$ وبالتالي فإن $F(\mu_n) \subseteq F(\xi)$ ، مما سبق نجد أن $F(\xi) = F(\mu_n)$.

$$٢ - \text{لنفرض أن } \zeta \in \pi_m \text{ عندئذ لما كان } \zeta \in \pi_m \subseteq \mu_m \text{ فإنه حسب (١) ينتج أن:}$$

$$F(\zeta) = F(\mu_m)$$

٣ - لدينا:

$$F(\xi, \zeta) = F(\xi) \cdot F(\zeta) = F(\mu_n) \cdot F(\mu_m) = F(\mu_m, \mu_n)$$

$$F(\xi, \zeta) = F(\xi)(\zeta) = F(\mu_m)(\xi) = F(\mu_m, \xi)$$

وهو المطلوب إثباته. ♦

مثال.

لنأخذ الحقل $(Z_{11}, +, \cdot)$ بالنسبة لعمليتي الجمع والضرب بالمقاس 11. حسب المبرهنة (٦-١-٤) فإن الزمرة الضربية $(Z_{11}^*, \cdot)$ دوارة وذلك لأن الحقل $(Z_{11}, +, \cdot)$ منته.

لما كانت $(Z_{11}^*, \cdot)$ زمرة مرتبتها 10 وأن $2 \in Z_{11}^*$ فإن $o(2)$ تقسم 10. ومنه فإن:

$$o(2) \in \{1, 2, 5, 10\}$$

لما كان $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^5 = 10 \neq 1$ نجد أن $o(2) = 10$.
أيضاً لما كان $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^3 = 8 \neq 1$, $2^4 = 5 \neq 1$, $2^5 = 10 \neq 1$ فإن 2 هو جذر
نجد أنه أياً كان $1 < k < 10$ فإن $2^k \neq 1$ وأن $2^{10} = 1$ وهذا يبين لنا أن 2 هو جذر
أولي للواحد من المرتبة 10 في $(Z_{11}, +, \cdot)$ ، كما أن $\langle 2 \rangle = (Z_{11}^*, \cdot)$. ♦

لنتابع دراسة خواص المجموعات μ_n وذلك من خلال المبرهنة الآتية:

مبرهنة ١١-١-٣.

ليكن n عدداً صحيحاً موجباً، عندئذ:

- ١ - لأجل أي عدد صحيح موجب m ، فإن m يقسم n عندما فقط عندما $\mu_m \subseteq \mu_n$.
- ٢ - لنفرض أن $\mathfrak{I}$ هي مجموعة قواسم العدد n عندئذ المجموعات $\{\mu_m : m \in \mathfrak{I}\}$ تشكل تجزئة للمجموعة μ_n .
- ٣ - إذا كان $\zeta \in \pi_n$ وكان d قاسماً للعدد n فإن $\zeta^{n/d} \in \pi_d$.

البرهان.

- ١ - لزوم الشرط. لنفرض أن العدد m يقسم n عندئذ يوجد عدد صحيح موجب k يحقق $n = mk$. ليكن $\zeta \in \mu_m$ فإن $o(\zeta) = m$ ، أي أن $\zeta^m = 1$ ومنه نجد أن:

$$\xi^n = \xi^{mk} = (\xi^m)^k = 1$$

ومنه نجد أن $\xi \in \mu_n$ وبالتالي يكون $\mu_m \subseteq \mu_n$.

كفاية الشرط. لنفرض أن $\mu_m \subseteq \mu_n$ وليكن $\varepsilon \in \mu_m$ عندئذ فإن $o(\varepsilon) = m$ ، لما كان $\mu_m \subseteq \mu_n$ فإن $\varepsilon \in \mu_n$ ومنه فإن $\varepsilon^n = 1$ وهذا يبين أن العدد m يقسم n .

٢ - واضح أنه لأجل كل $m \in \mathfrak{I}$ فإن المجموعة μ_m ليست خالية. ليكن $m, k \in \mathfrak{I}$ عندئذ كل من m, k قاسم للعدد n . إذا كان $\mu_m \cap \mu_k = \Phi$ يتم المطلوب.

لنفرض أن $\mu_m \cap \mu_k \neq \Phi$ عندئذ يوجد $a \in \mu_m \cap \mu_k$ ومنه فإن $a \in \mu_m$ وبالتالي تكون $o(a) = m$ وأن $a \in \mu_k$ وبالتالي يكون $o(a) = k$ ومنه فإن m يقسم k و k يقسم m ، أي أن $m \leq k, k \leq m$ ومنه $m = k$ وبالتالي يكون $\mu_m = \mu_k$.

واضح أن $\bigcup_{m \in \mathfrak{I}} \mu_m \subseteq \mu_n$ وذلك لأنه إذا كان $m \in \mathfrak{I}$ فإن m يقسم k وحسب (١) يكون $\mu_m \subseteq \mu_n$. لما كان $n \in \mathfrak{I}$ فإن $\mu_n \subseteq \bigcup_{m \in \mathfrak{I}} \mu_m$ ومنه نجد أن $\mu_n = \bigcup_{m \in \mathfrak{I}} \mu_m$ وبالتالي المجموعات السابقة تشكل تجزئة للمجموعة μ_n .

٣ - ليكن $\xi \in \pi_n$ عندئذ فإن ξ هو جذر أولي للواحد من المرتبة n . لنفرض أن d يقسم n عندئذ $n/d \in \mathbb{Z}$ وأن $(\xi^{n/d})^d = 1$ ومنه فإن $\xi^{n/d} \in \mu_d$ ، لما كان لأجل كل $1 < t < n$ فإن $(\xi^{n/d})^t \neq 1$ وذلك لأن $nt/d < n$ نجد أن $\xi^{n/d} \in \pi_d$.

اعتماداً على ضرب المجموعات الجزئية في البنى الجبرية، لنفرض أن m, n عددين صحيحان موجبان، لنفرض أن:

$$\mu_m \cdot \mu_n = \{\xi_1 \cdot \xi_2 : \xi_1 \in \mu_m, \xi_2 \in \mu_n\}$$

$$\pi_m \cdot \pi_n = \{\zeta_1 \cdot \zeta_2 : \zeta_1 \in \pi_m, \zeta_2 \in \pi_n\}$$

اعتماداً على المجموعات السابقة لنورد المبرهنة الآتية:

مبرهنة ١١-١-٤.

ليكن m, n عددين صحيحين موجبيين أوليين فيما بينهما. عندئذ:

$$\mu_{m \cdot n} = \mu_m \cdot \mu_n$$

٢ - كل عنصر $\xi \in \mu_{m \cdot n}$ يكتب بصورة وحيدة على الشكل $\xi = \xi' \cdot \xi''$ حيث $\xi' \in \mu_m$

$$\cdot \mathcal{E} \in \mu_n$$

$$\cdot \pi_{m \cdot n} = \pi_m \cdot \pi_n - 3$$

٤ - كل عنصر $\zeta \in \pi_{m \cdot n}$ يكتب بصورة وحيدة على الشكل $\zeta = \zeta \cdot \mathcal{E}$ حيث $\zeta \in \pi_m$

$$\cdot \mathcal{E} \in \pi_n$$

البرهان.

١ - لما كان العددين m, n أوليين فيما بينهما فإنه يوجد $s, t \in \mathbb{Z}$ بحيث $1 = sm + tn$.

ليكن $\zeta \in \mu_{m \cdot n}$ عندئذ فإن $\zeta^{sm+tn} = \zeta^{sm} \cdot \zeta^{tn}$. لأن:

$$(\zeta^{s \cdot m})^n = (\zeta^{n \cdot m})^s = 1$$

$$(\zeta^{t \cdot n})^m = (\zeta^{m \cdot n})^t = 1$$

ومنه نجد أن $\zeta^{sm+tn} = \zeta^{s \cdot m} \cdot \zeta^{t \cdot n} \in \mu_m \cdot \mu_n$. وهذا يبين لنا أن $\mu_{m \cdot n} \subseteq \mu_m \cdot \mu_n$.

ليكن $\zeta \in \mu_m$, $\mathcal{E} \in \mu_n$ عندئذ فإن:

$$(\zeta \cdot \mathcal{E})^{n \cdot m} = \zeta^{n \cdot m} \cdot \mathcal{E}^{n \cdot m} = (\zeta^m)^n \cdot (\mathcal{E}^n)^m = 1$$

ومنه نجد أن $\zeta \cdot \mathcal{E} \in \mu_{m \cdot n}$ ومنه فإن $\mu_m \cdot \mu_n \subseteq \mu_{m \cdot n}$ ، مما سبق نجد أن

$$\cdot \mu_{m \cdot n} = \mu_m \cdot \mu_n$$

٢ - لدينا حسب التمهيدية (١-١-١) أن $\text{Card } \mu_{m \cdot n} = m \cdot n$ ولما كان:

$$\text{Card } \mu_m \cdot \text{Card } \mu_n \leq m \cdot n$$

نجد أنه لأجل كل $\zeta \in \mu_m$, $\mathcal{E} \in \mu_n$ فإن $\zeta \cdot \mathcal{E}$ هو العنصر الوحيد في $\mu_{m \cdot n}$.

٣ - ليكن $\zeta \in \pi_m$, $\mathcal{E} \in \pi_n$ عندئذ فإن $o(\zeta) = m$, $o(\mathcal{E}) = n$.

لما كان العددين m, n أوليين فيما بينهما نجد أن $o(\zeta \cdot \mathcal{E}) = o(\zeta) \cdot o(\mathcal{E}) = m \cdot n$

ومنه يكون $\zeta \cdot \mathcal{E} \in \pi_{m \cdot n}$ ، وبالتالي يكون $\pi_m \cdot \pi_n \subseteq \pi_{m \cdot n}$.

من جهة أخرى، لما كان العددين m, n أوليين فيما بينهما فإنه يوجد $s, t \in \mathbb{Z}$ بحيث

$$1 = tm + sn \quad \text{وأن} \quad \gcd(t, m) = 1, \quad \gcd(s, n) = 1$$

$$\gcd(t \cdot m, m \cdot m) = m, \quad \gcd(s \cdot n, n \cdot n) = n$$

ليكن $\mathcal{E} \in \pi_{m \cdot n}$ عندئذ فإن $o(\mathcal{E}) = m \cdot n$ وأن:

$$\mathcal{E} = \mathcal{E}^{tm+sn} = \mathcal{E}^{tm} \cdot \mathcal{E}^{sn}$$

وأن نجد أن $\varepsilon^{tm} \in \pi_n$, $\varepsilon^{sn} \in \pi_m$ وذلك لأن:

$$(\varepsilon^{t \cdot m})^n = (\varepsilon^{n \cdot m})^t = 1$$

$$(\varepsilon^{s \cdot n})^m = (\varepsilon^{n \cdot m})^s = 1$$

ومنه نجد أن $\varepsilon = \varepsilon^{tm+sn} = \varepsilon^{tm} \cdot \varepsilon^{sn} \in \pi_m \cdot \pi_n$ وهذا يبين أن $\pi_{m \cdot n} \subseteq \pi_m \cdot \pi_n$ ، مما

سبق نجد أن $\pi_{m \cdot n} = \pi_m \cdot \pi_n$

٤ - حسب (٢). ◊

١١ - ٢. الحدوديات الدوارة.

نعلم أن العدد العقدي $i = \sqrt{-1}$ هو صفر للحدودية $x^2 + 1 \in Q[x]$ ونعلم أيضاً أن:

$$(\cos(\theta_1) + i \sin(\theta_1)) \cdot (\cos(\theta_2) + i \sin(\theta_2)) = \\ = \cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)$$

بالاستقراء لأجل $\theta_1 = \theta_2 = \theta$ نجد أن:

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

ولأجل $\theta = \frac{2\pi}{n}$ نجد أن:

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

ومنه فإن $\cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ هو جذر نوني (من المرتبة n) للواحد سوف نرمز له ξ_n ، أي أن:

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

مثال.

إن الجذر الثامن للواحد هو:

$$\xi_8 = \cos\left(\frac{2\pi}{8}\right) + i \sin\left(\frac{2\pi}{8}\right) = \cos\left(\frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{4}\right) = \\ = \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}} = \frac{1+i}{\sqrt{2}}$$

وأن الجذور الأولية للواحد التي تنتمي للحقل Q هي:

$$\xi_8, \xi_8^3, \xi_8^5, \xi_8^7$$

تعريف.

لنفرض أن $\xi_n = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ جذر أولي للواحد من المرتبة n ، عندئذ فإن

مجموعة الجذور النونية للواحد هي المجموعة:

$$\mu_n = \langle \xi_n \rangle = \{ \xi_n^k : 1 \leq k \leq n \}$$

وأن مجموعة الجذور الأولية للواحد من المرتبة n هي المجموعة:

$$\pi_n = \{ \xi_n^k : 1 \leq k \leq n; \gcd(k, n) = 1 \}$$

نسمي الحدودية:

$$\Phi_n(x) = \prod_{\xi \in \pi_n} (x - \xi)$$

الحدودية الدوارة من المرتبة n .

اعتماداً على التعريف السابق يمكننا صياغة المبرهنة الآتية:

مبرهنة ١١-٢-١.

لأجل أي عدد صحيح موجب n فإن:

١ - الحدودية $\Phi_n(x) = \prod_{\xi \in \pi_n} (x - \xi)$ هي حدودية أولية في $Z[x]$ أمثال أكبر قوة للمتحوّل x فيها يساوي الواحد.

$$٢ - \partial \Phi_n = \varphi(n)$$

٣ - $x^n - 1 = \prod_{d \in \mathfrak{D}} \Phi_d(x)$ حيث $\mathfrak{D}$ هي مجموعة قواسم العدد n .
البرهان.

١ - واضح أن الحدودية $\Phi_n(x)$ أولية في $Z[x]$ أمثال أكبر قوة للمتحوّل x فيها يساوي الواحد. لنبرهن بالاستقراء على أن $\Phi_n(x) \in Z[x]$.

من أجل $n=1$ فإن $\Phi_1(x) = x-1$. من أجل $n=2$ فإن $\Phi_2(x) = x+1$.
لنفرض أنها صحيحة لأجل $n > 1$ ، لدينا:

$$x^n - 1 = \prod_{\xi \in \mu_n} (x - \xi) = \prod_{d \in \mathfrak{D}} \left[\prod_{\xi \in \pi_d} (x - \xi) \right]$$

وذلك لأجل كل $1 \leq d < n$ وحيث $\mathfrak{D}$ هي مجموعة قواسم العدد n .

لنفرض أن $h(x) = \prod_{\substack{\xi \in \pi_d \\ d \neq 1}} (x - \xi)$ ، حسب الفرض الاستقرائي فإن $h(x) \in Z[x]$ وأن:

$$\Phi_n(x) = \frac{x^n - 1}{h(x)}$$

ولما كان $h(x) \in Z[x]$ ، $x^n - 1$ نجد أن $\Phi_n(x) \in Z[x]$.

٢ - لما كان $\Phi_n(x) = \prod_{\xi \in \pi_n} (x - \xi)$ فإنه حسب التمهيدية (١-١-١) فإن:

$$\text{Card } \pi_n(x) = \varphi(n)$$

ومنه يكون $\partial \Phi_n(x) = \text{Card } \pi_n(x) = \varphi(n)$.

٣ - حسب (١).

لنورد من خلال الجدول الآتي الحدوديات $\Phi_n(x)$ من أجل $n = 1, 2, \dots, 10$:

n	$\Phi_n(x)$
1	$x - 1$
2	$x + 1$
3	$x^2 + x + 1$
4	$x^2 + 1$
5	$x^4 + x^3 + x^2 + x + 1$
6	$x^2 - x + 1$
7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
8	$x^4 + 1$
9	$x^6 + x^3 + 1$
10	$x^4 - x^3 + x^2 - x + 1$

مبرهنة ١١-٢-٢.

لتكن $f(x) \in Z[x]$ حدودية ما و p عدداً أولياً. عندئذ:

$$(f(x))^p = f(x^p) + pg(x)$$

حيث $g(x) \in Z[x]$.

البرهان.

لنفرض أن $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ حيث $a_i \in Z$ أيأ كان

$0 \leq i \leq n$. فنجد أن:

$(f(x))^p = a_n^p x^{np} + a_{n-1}^p x^{(n-1)p} + \dots + a_1^p x^p + a_0^p + ph(x)$
 حيث $h(x) \in Z[x]$. لما كان العدد p أولياً فإن $a_i^p = a_i + b_i p$ حيث $b_i \in Z$ أيّاً كان $0 \leq i \leq n$. لنضع:

$$r(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$$

ف نجد أن $r(x) \in Z[x]$ وأن:

$$\begin{aligned} (f(x))^p &= (a_n + b_n p)x^{np} + (a_{n-1} + b_{n-1} p)x^{(n-1)p} + \dots + \\ &+ (a_1 + b_1 p)x^p + (a_0 + b_0 p) + ph(x) = \\ &= (a_n x^{np} + a_{n-1} x^{(n-1)p} + \dots + a_1 x^p + a_0) + \\ &+ p(b_n x^{np} + b_{n-1} x^{(n-1)p} + \dots + b_1 x^p + b_0) + ph(x) \end{aligned}$$

$$(f(x))^p = f(x^p) + pr(x) + ph(x)$$

لنضع $g(x) = r(x) + h(x) \in Z[x]$ نجد أن:

$$(f(x))^p = f(x^p) + pg(x)$$

وهو المطلوب لإثباته. ◊

مبرهنة ١١-٢-٣.

ليكن n عدداً صحيحاً موجباً وأن ξ جذراً أولياً للواحد من المرتبة n . عندئذ:

١ - الحدودية $\Phi_n(x)$ هي الحدودية الأصغرية للعنصر ξ فوق الحقل Q .

٢ - $[Q(\xi) : Q] = \varphi(n)$.

البرهان.

١ - لما كان ξ عنصراً جبرياً فوق Q ، لأنه صفر للحدودية $h(x) = x^n - 1 \in Q[x]$ لنفرض أن $f(x)$ الحدودية الأصغرية للعنصر ξ فوق الحقل Q . لما كانت الحدودية $f(x)$ منفصلة فوق Q فإن جميع أصفارها بسيطة.

من جهة أخرى، لما كانت $h(x) = x^n - 1 \in Z[x]$ وأن $\partial h(x) > 0$ فإنه حسب المبرهنة (٢-١-٩) يمكن كتابة $h(x)$ على الشكل الآتي:

$$h(x) = g_1(x) \cdot g_2(x) \cdots g_m(x)$$

حيث $g_i(x)$ حدوديات في $Z[x]$ درجة كل منها أكبر من الصفر لأجل كل $1 \leq i \leq m$.

لأجل كل عدد صحيح موجب k لنضع $f_k(x) = f(x^k)$ فنجد أن:

$$f_k(x), f(x^k) \in Z[x]$$

ولما كانت $f(x)$ أولية فإنه حسب خوارزمية القسمة لأجل الحدوديتين $f_k(x), f(x)$

يوجد $q_k(x), r_k(x) \in Z[x]$ بحيث:

$$f_k(x) = q_k(x) \cdot f(x) + r_k(x) \quad (*)$$

حيث إما $r_k(x) = 0$ أو $\partial r_k(x) < \partial f(x)$. سوف نجزي البرهان إلى الخطوات الآتية:
الخطوة الأولى. لنبرهن على أن:

$$\{r_k(x) : k = 1, 2, 3, \dots\} = \{r_1(x), r_2(x), \dots, r_n(x)\}$$

نلاحظ أن ξ هو صفر للحدودية $f_k(x) - f_{k+n}(x)$ ، لأن:

$$f_{k+n}(\xi) = f(\xi^{k+n}) = f(\xi^k \cdot \xi^n) = f(\xi^k) = f_k(\xi)$$

ومنه يكون $f_{k+n}(\xi) - f_k(\xi) = f_k(\xi) - f_k(\xi) = 0$

لما كانت $f(x)$ الحدودية الأصغرية للعنصر ξ نجد أن $f(x)$ تقسم $f_{k+n}(x) - f_k(x)$ في $Z[x]$ وبالتالي يوجد $\mu(x) \in Z[x]$ بحيث يكون:

$$f_{k+n}(x) - f_k(x) = f(x) \cdot \mu(x)$$

من جهة أخرى، لدينا:

$$\begin{aligned} f_{k+n}(x) - f_k(x) &= q_{k+n}(x) \cdot f(x) + r_{k+n}(x) - q_k(x) \cdot f(x) - r_k(x) = \\ &= [q_{k+n}(x) - q_k(x)] \cdot f(x) + (r_{k+n}(x) - r_k(x)) \end{aligned}$$

ومنه نجد أن:

$$= [\mu(x) - q_{k+n}(x) + q_k(x)] f(x) = r_{k+n}(x) - r_k(x)$$

وهذا يبين لنا أن $f(x)$ تقسم $r_{k+n}(x) - r_k(x)$ في $Z[x]$.

لنفرض جلاً أن $r_{k+n}(x) - r_k(x) \neq 0$ عندئذ نجد أن:

$$\partial(r_{k+n}(x) - r_k(x)) \geq \partial f(x)$$

من جهة أخرى، لما كان $\partial r_k(x) \leq \partial f(x)$ نجد أن:

$$\partial(r_{k+n}(x) - r_k(x)) < \partial f(x)$$

وهذا تناقض، ومنه يكون $r_{k+n}(x) - r_k(x) = 0$ وهذا يبين أن $r_{k+n}(x) = r_k(x)$

وبالتالي يكون $\{r_k(x) : k = 1, 2, 3, \dots\} = \{r_1(x), r_2(x), \dots, r_n(x)\}$
الخطوة الثانية. لنفرض أن $c(r_i(x))$ هو رئيس الحدودية $r_i(x)$ لأجل كل $i = 1, 2, \dots, n$
ولنضع:

$$C = \max \{c(r_1(x)), c(r_2(x)), \dots, c(r_n(x))\}$$

لنبرهن على أنه لأجل أي عدد أولي p يحقق $p > C$ فإن الحدودية $f(x)$ تقسم $f_p(x)$ في $Z[x]$.

ليكن p عدداً أولياً ولنفرض أن $p > C$. لدينا حسب المبرهنة (١١-٢-٢) أن:

$$(f(x))^p = f_p(x) - pg_p(x)$$

حيث $g_p(x) \in Z[x]$ ولما كانت الحدودية $f(x)$ أولية في $Z[x]$ فإنه حسب خوارزمية القسمة لأجل $f(x)$ و $g_p(x)$ يوجد $q_p^*(x), r_p^*(x) \in Z[x]$ بحيث يكون:

$$g_p(x) = q_p^*(x) \cdot f(x) + r_p^*(x)$$

حيث إما $r_p^*(x) = 0$ أو $\partial r_p^*(x) < \partial f(x)$ ومنه نجد أن:

$$\begin{aligned} f_p(x) &= (f(x))^p + pg_p(x) = \\ &= (f(x))^p + p \cdot q_p^*(x) \cdot f(x) + p \cdot r_p^*(x) = \\ &= [(f(x))^{p-1} + p \cdot q_p^*(x)] \cdot f(x) + p \cdot r_p^*(x) \end{aligned}$$

وأنه إما $p \cdot r_p^*(x) = 0$ أو $\partial p \cdot r_p^*(x) = \partial r_p^*(x) < \partial f(x)$

أصبح لدينا:

$$f_p(x) = [(f(x))^{p-1} + p \cdot q_p^*(x)] \cdot f(x) + p \cdot r_p^*(x)$$

وأنه إما $p \cdot r_p^*(x) = 0$ أو $\partial p \cdot r_p^*(x) < \partial f(x)$ وأيضاً حسب العلاقة (*) إن:

$$f_p(x) = q_p(x) \cdot f(x) + r_p(x)$$

وأنه إما $r_p(x) = 0$ أو $\partial r_p(x) < \partial f(x)$. ولما كان كل من ناتج وباقي القسمة في

خوارزمية القسمة يتعين بشكل وحيد نجد أن $r_p(x) = p \cdot r_p^*(x)$ ومنه يكون:

$$c(r_p(x)) = p \cdot c(r_p^*(x))$$

لنفرض أن $r_p(x) \neq 0$ عندئذ يكون $c(r_p(x)) \geq p > C$. من جهة أخرى، لدينا حسب

الخطوة الأولى أن $c(r_p(x)) < C$ وهذا غير ممكن، ومنه نجد أن $r_p(x) = 0$ وبالتالي فإن $f(x)$ تقسم $f_p(x)$.

الخطوة الثالثة. ليكن k عدداً صحيحاً موجباً أصغر من n وأولياً مع n ، أي أن $1 \leq k < n$ وأن $\gcd(k, n) = 1$ ولنبرهن على أن ξ^k هو صفر للحدودية $f(x)$. لنفرض كما في الخطوة (٢) أن:

$$C = \max \{c(r_1(x)), c(r_2(x)), \dots, c(r_n(x))\}$$

ولنفرض أيضاً أن P هو جداء كل الأعداد الأولية التي هي أصغر أو تساوي C ولا تقسم k ، لنضع $N = k + nP$ فنجد أن:

$$\xi^N = \xi^{k+np} = \xi^k \cdot \xi^{np} = \xi^k$$

لذلك لأجل إثبات أن ξ^k هو صفر للحدودية $f(x)$ يكفي إثبات أن ξ^N هو صفر للحدودية $f(x)$. لما كان $1 \leq k < n$ وأن $\gcd(k, n) = 1$ نجد أن $\gcd(k, np) = 1$ وذلك لأن $k < n < np$ وأن P هو جداء كل الأعداد الأولية التي هي أصغر أو تساوي C ولا تقسم k ، وهذا يبين أن أي عدد أولي يقسم N هو أكبر من C ولما كان N عدداً صحيحاً موجباً، لنفرض أن $N = p_1 \cdot p_2 \cdots p_t$ حيث p_i أعداد أولية ليس بالضرورة مختلفة أكبر من C أيأ كان $1 \leq k \leq t$.

حسب الخطوة (٢) فإن $f(x)$ يقسم $f_{p_1}(x)$ وبالتالي يوجد $\lambda_1(x) \in Z[x]$ بحيث:

$$f_{p_1}(x) = \lambda_1(x) \cdot f(x)$$

لما كان ξ صفراً للحدودية $f(x)$ نجد أن ξ صفر للحدودية $f_{p_1}(x)$ أي أن $f_{p_1}(\xi) = 0$ ومنه نجد أن $f(\xi^{p_1}) = f_{p_1}(\xi) = 0$ وهذا يبين أن ξ^{p_1} صفر للحدودية $f(x)$.

أيضاً إن $f(x)$ يقسم $f_{p_2}(x)$ وبالتالي يوجد $\lambda_2(x) \in Z[x]$ بحيث:

$$f_{p_2}(x) = \lambda_2(x) \cdot f(x)$$

لما كان ξ^{p_1} صفراً للحدودية $f(x)$ نجد أن ξ^{p_1} صفر للحدودية $f_{p_2}(x)$ أي أن:

$$f_{p_2}(\xi^{p_1}) = 0$$

وهذا يبين لنا أن $\xi^{p_1 p_2}$ صفر للحدودية $f(x)$ ، لأن:

$$f(\xi^{p_1 p_2}) = f((\xi^{p_1})^{p_2}) = f_{p_2}(\xi^{p_1}) = 0$$

نتابع بهذا الشكل نجد أن $\xi^N = \xi^{p_1 p_2 \dots p_t}$ صفر للحدودية $f(x)$ وبالتالي يكون ξ^k صفرًا للحدودية $f(x)$.

الخلاصة. لما كان ξ صفرًا للحدوديتين $f(x)$ و $\Phi_n(x)$ وأن $f(x)$ هي الحدودية الأصغرية للعنصر ξ فوق Q نجد أن $f(x)$ تقسم $\Phi_n(x)$ في $Q[x]$ ومنه يكون:

$$\partial f(x) \leq \partial \Phi_n(x) = \varphi(n)$$

وذلك حسب المبرهنة (١١-٢-١).

من جهة أخرى، وحسب الخطوة (٣) وجدنا أن $\partial f(x) \geq \varphi(n)$ ومنه نجد أن:

$$\partial f(x) = \varphi(n) = \partial \Phi_n(x)$$

ولما كان المعامل الأكبر لكل من $f(x)$ و $\Phi_n(x)$ يساوي الواحد نجد أن $\Phi_n(x) = f(x)$ وهكذا نجد أن $\Phi_n(x)$ هي الحدودية الأصغرية للعنصر ξ فوق Q .

٢ - لدينا:

$$[Q(\xi) : Q] = \partial \Phi_n(x) = \varphi(n)$$

وذلك حسب (١) والمبرهنة (١١-٢-١). ◊

مبرهنة ١١-٢-٤.

ليكن m, n عددين صحيحين موجبين أوليين فيما بينهما وليكن ξ جذراً أولياً للواحد من المرتبة n . عندئذ:

$$1 - Q(\mu_m, \mu_n) = Q(\mu_{m \cdot n})$$

$$2 - [Q(\mu_n) : Q] = \varphi(n)$$

$$3 - Q(\mu_m) \cap Q(\mu_n) = Q$$

$$4 - Q(\mu_n) \text{ حقل تفريق فوق } Q.$$

البرهان.

١ - لدينا حسب المبرهنة (١١-١-٤) أن $\mu_m \cdot \mu_n = \mu_{m \cdot n}$ ولما كان:

$$\mu_m, \mu_n \subseteq \mu_m \cdot \mu_n = \mu_{m \cdot n}$$

$$\text{نجد أن } Q(\mu_m, \mu_n) \subseteq Q(\mu_{m \cdot n})$$

من جهة أخرى، لدينا $\mu_m, \mu_n \subseteq Q(\mu_m, \mu_n)$ ومنه نجد أن $\mu_m \cdot \mu_n \subseteq Q(\mu_m, \mu_n)$

وبالتالي يكون $Q(\mu_m \cdot \mu_n) \subseteq Q(\mu_m, \mu_n)$ وهكذا فإن $Q(\mu_m, \mu_n) = Q(\mu_{m \cdot n})$.

٢ - لما كان ξ جذراً أولياً للواحد من المرتبة n فإن $\xi \in \pi_n$ وحسب التمهيدية (١١-١-١) (٢)(٢) فإن $Q(\xi) = Q(\mu_n)$ وحسب المبرهنة (١١-٢-٣) نجد أن:

$$[Q(\mu_n) : Q] = [Q(\xi), Q] = \varphi(n)$$

٣ - لدينا حسب (١) أن $Q(\mu_m, \mu_n) = Q(\mu_{m \cdot n})$ وحسب (٢) نجد أن:

$$[Q(\mu_m, \mu_n) : Q] = [Q(\mu_{m \cdot n}) : Q] = \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

من جهة أخرى، لما كان الحقل $Q(\mu_m)$ هو حقل تفريق الحدودية $\Phi_m(x)$ فإنه حسب المبرهنة (١٤-١-٨) نجد أن:

$$\begin{aligned} [Q(\mu_m, \mu_n) : Q] &= [Q(\mu_m) \cdot Q(\mu_n) : Q] = \\ &= \frac{[Q(\mu_m) : Q] \cdot [Q(\mu_n) : Q]}{[Q(\mu_m) \cap Q(\mu_n) : Q]} = \frac{\varphi(m) \cdot \varphi(n)}{[Q(\mu_m) \cap Q(\mu_n) : Q]} = \\ &= \frac{[Q(\mu_m, \mu_n) : Q]}{[Q(\mu_m) \cap Q(\mu_n) : Q]} \end{aligned}$$

وهذا يبين أن $[Q(\mu_m) \cap Q(\mu_n) : Q] = 1$ وبالتالي يكون:

$$Q(\mu_m) \cap Q(\mu_n) = Q$$

وهو المطلوب إثباته.

٤ - ينتج من التمهيدية (١١-٢-١) لأن $Q(\xi) = Q(\mu_n)$.

مبرهنة ١١-٢-٥.

ليكن m, n عددين صحيحين موجبيين أوليين فيما بينهما وليكن ξ جذراً أولياً للواحد من المرتبة n . عندئذ:

$$1 - [Q(\mu_m, \mu_n) : Q(\mu_m)] = [Q(\mu_n) : Q]$$

٢ - الحدودية $\Phi_n(x)$ هي الحدودية الأصغرية للعنصر ξ فوق $Q(\mu_m)$.

البرهان.

١ - لدينا حسب المبرهنة (١١-١-٤) أن $Q(\mu_m, \mu_n) = Q(\mu_{m \cdot n})$ ومنه نجد أن:

$$[Q(\mu_m, \mu_n) : Q(\mu_m)] = [Q(\mu_{m \cdot n}) : Q]$$

ولما كان $Q \subseteq Q(\mu_m) \subseteq Q(\mu_m, \mu_n)$ نجد أن:

$$[Q(\mu_m, \mu_n) : Q] = [Q(\mu_{m \cdot n}) : Q(\mu_m)] \cdot [Q(\mu_m) : Q]$$

ومنه يكون:

$$[Q(\mu_{m \cdot n}) : Q(\mu_m)] = \frac{[Q(\mu_{m \cdot n}) : Q]}{[Q(\mu_m) : Q]} = \frac{\varphi(m \cdot n)}{\varphi(m)} = \frac{\varphi(m) \cdot \varphi(n)}{\varphi(m)} = \varphi(n)$$

من جهة أخرى، لدينا حسب المبرهنة (١١-٢-٤) أن $[Q(\mu_n) : Q] = \varphi(n)$ ومنه نجد أن:

$$[Q(\mu_m, \mu_n) : Q(\mu_m)] = [Q(\mu_n) : Q]$$

٢ - لنفرض أن $h(x) \in Q(\mu_m)[x]$ الحدودية الأصغرية للعنصر ξ فوق $Q(\mu_m)$ عندئذ يكون:

$$\partial h(x) = [Q(\mu_m)(\xi) : Q(\mu_m)]$$

من جهة أخرى، لما كان ξ جذراً أولياً للواحد من المرتبة n فإن $\xi \in \pi_n$ وحسب التمهيدية (١١-٢-١) فإن $Q(\mu_n) = Q(\xi)$ ومنه نجد أن:

$$\partial h(x) = [Q(\mu_m)(\xi) : Q(\mu_m)] = [Q(\mu_m, \mu_n) : Q(\mu_m)]$$

وحسب (١) يكون:

$$\partial h(x) = [Q(\mu_n) : Q] = [Q(\xi) : Q]$$

وحسب المبرهنة (١١-٢-٣) نجد أن $\partial h(x) = \varphi(n)$ وحسب المبرهنة (١١-٢-١) يكون $\partial h(x) = \varphi(n) = \partial \Phi_n(x)$ ولما كان ξ صفراً للحدودية $\Phi_n(x)$ نجد أن $h(x)$ تقسم $\Phi_n(x)$ وأيضاً لما كانت كل منهما أولية وأكبر معاملات $\Phi_n(x)$ تساوي الواحد نجد أن $\Phi_n(x) = h(x)$ أي أن $\Phi_n(x)$ هي الحدودية الأصغرية للعنصر ξ فوق الحقل $Q(\mu_m)$.

مبرهنة ١١-٢-٦.

ليكن p عدداً أولياً وليكن ξ جذراً أولياً للواحد من المرتبة p . عندئذ فإن:

$$١ - \Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$$

$$٢ - \text{لأجل أي عدد صحيح موجب } k \text{ فإن } \Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$$

$$٣ - \text{لأجل أي عدد صحيح موجب } k \text{ فإن } \xi - x^{p^{k-1}} \text{ حدودية أولية فوق الحقل}$$

$$Q(\mu_{p-1}, \xi)$$

البرهان.

١ - لنفرض أن p عدداً أولياً وليكن ξ جذراً أولياً للواحد من المرتبة p . عندئذ حسب المبرهنة (١-٢-١١) فإن $x^p - 1 = \prod_{d \in \mathfrak{D}} \Phi_d(x)$ حيث $\mathfrak{D}$ هي مجموعة قواسم العدد p ، لما كانت $\mathfrak{D} = \{1, p\}$ نجد أن:

$$x^p - 1 = \Phi_1(x) \cdot \Phi_p(x) = (x - 1) \cdot \Phi_p(x)$$

ومنه نجد أن

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

٢ - ليكن k عدداً صحيحاً موجباً، عندئذ حسب المبرهنة (١-٢-١١) فإن:

$$x^{p^k} - 1 = \prod_{d \in \mathfrak{D}} \Phi_d(x)$$

حيث $\mathfrak{D}$ هي مجموعة قواسم العدد p^k ، لما كانت $\mathfrak{D} = \{1, p, p^2, \dots, p^{k-1}, p^k\}$ نجد أن:

$$x^{p^k} - 1 = [\prod_{j=0}^{k-1} \Phi_{p^j}(x)] \cdot \Phi_{p^k}(x)$$

ولما كان $x^{p^{k-1}} - 1 = \prod_{j=0}^{k-1} \Phi_{p^j}(x)$ نجد أن:

$$x^{p^k} - 1 = (x^{p^{k-1}} - 1) \cdot \Phi_{p^k}(x)$$

ومنه يكون $\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1}$. لنفرض أن $y = x^{p^{k-1}}$ نجد حسب (١) أن:

$$\frac{y^p - 1}{y - 1} = \Phi_p(y)$$

ومنه نجد أن:

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = \Phi_p(x^{p^{k-1}})$$

٣ - ليكن k عدداً صحيحاً موجباً ولنفرض أن η صفر للحدودية $\xi - x^{p^{k-1}}$ عندئذ يكون $\eta^{p^{k-1}} = \xi$ ولما كان ξ جذراً أولياً للواحد من المرتبة p ، أي أن $o(\xi) = p$ نجد أن:

$$1 = \xi^p = (\eta^{p^{k-1}})^p = \eta^{p^k}$$

ومنه نجد أن $o(\eta) = p^k$ وهذا يبين أن η هو جذر أولي للواحد من المرتبة p^k .
لما كان العدان $p, (p-1)$ أوليين فيما بينهما فإنه حسب المبرهنة (١١-٢-٥) نجد أن:

$$[Q(\mu_{p-1}, \mu_p) : Q(\mu_{p-1})] = [Q(\mu_p) : Q]$$

ولما كان ξ جذراً أولياً للواحد من المرتبة p فإنه حسب التمهيدية (١١-٢-٢) يكون:

$$Q(\xi) = Q(\mu_p)$$

ومنه نجد أن:

$$[Q(\mu_{p-1}, \mu_p) : Q(\mu_{p-1})] = [Q(\mu_p) : Q] = [Q(\xi) : Q] = \varphi(p) = p-1$$

وذلك حسب المبرهنة (١١-٢-٣)، ومنه نجد أن:

$$[Q(\mu_{p-1}, \xi) : Q(\mu_{p-1})] = p-1$$

أيضاً لما كان η هو جذراً أولياً للواحد من المرتبة p^k فإنه حسب التمهيدية (١١-٢-١)

(٢)(٢) فإن $Q(\eta) = Q(\mu_{p^k})$ ، ومنه نجد أن:

$$[Q(\mu_{p-1}, \eta) : Q(\mu_{p-1})] = [Q(\mu_{p-1}, \mu_{p^k}) : Q(\mu_{p-1})]$$

وحسب المبرهنة (١١-٢-٥) نجد أن:

$$[Q(\mu_{p-1}, \eta) : Q(\mu_{p-1})] = [Q(\mu_{p-1}, \mu_{p^k}) : Q(\mu_{p-1})] =$$

$$[Q(\mu_{p^k}, \eta) : Q] = [Q(\eta) : Q] = \varphi(p^k) = p^{k-1}(p-1)$$

ولما كان:

$$Q(\mu_{p-1}) \subseteq Q(\mu_{p-1}, \xi) = Q(\mu_{p-1}, \eta)$$

نجد أن:

$$[Q(\mu_{p-1}, \eta) : Q(\mu_{p-1})] = [Q(\mu_{p-1}, \eta) : Q(\mu_{p-1}, \xi)] \cdot$$

$$[Q(\mu_{p-1}, \xi) : Q(\mu_{p-1})]$$

ومنه نجد أن:

$$[Q(\mu_{p-1}, \eta) : Q(\mu_{p-1}, \xi)] = \frac{[Q(\mu_{p-1}, \eta) : Q(\mu_{p-1})]}{[Q(\mu_{p-1}, \xi) : Q(\mu_{p-1})]} =$$

$$= \frac{p^{k-1}(p-1)}{p-1} = p^{k-1}$$

ولما كانت $\xi \in Q(\mu_{p-1}, \xi) - \xi = x^{p^{k-1}} = h(x)$ وأن $\partial h(x) = p-1$ و η صفر لها فإنه حسب المبرهنة (٣-٣-١٠) تكون $h(x)$ أولية فوق $Q(\mu_{p-1}, \xi)$. ◊

مبرهنة ١١-٢-٧.

ليكن n عدداً صحيحاً موجباً وأن ξ جذر أولي للواحد من المرتبة n . عندئذ الحقل $Q(\mu_n)$ هو تمديد غالوا للحقل Q .

البرهان.

لنفرض أن ξ جذراً أولياً للواحد من المرتبة n . لدينا حسب المبرهنة (١١-٢-٣) أن $\Phi_n(x)$ هي الحدودية الأصغرية للعنصر ξ فوق Q وأن $[Q(\xi):Q] = \varphi(n)$ وهذا يبين أن الحقل $Q(\xi)$ هو حقل تفريق الحدودية $\Phi_n(x)$ فوق Q . لما كان مميز الحقل Q يساوي الصفر وأن $\partial \Phi_n(x) > 0$ نجد أن الحدودية $\Phi_n(x)$ منفصلة فوق Q . أصبح لدينا $Q(\xi)$ هو حقل تفريق حدودية منفصلة فوق Q وحسب المبرهنة (١٠-٣-٣) فإن $Q(\xi)$ هو تمديد غالوا للحقل Q ولما كان $Q(\mu_n) = Q(\xi)$ نجد أن $Q(\mu_n)$ هو تمديد غالوا للحقل Q . ◊

١١ - ٣. الحقول الدوارة.

سوف نناقش في هذه الفقرة نوعاً خاصاً من التمديدات المنتهية لحقول غير منتهية، لنبدأ بالتعريف الآتي:

تعريف.

ليكن F حقلاً مميزه يساوي الصفر (حقل غير منته). نسمي حقلاً تفريق الحدودية $x^n - 1 \in F[x]$ فوق F بالحقل الدوار النوني.

المبرهنة الآتية تبين لنا طبيعة التمديد الدوار النوني لحقل غير منته.

مبرهنة ١١-٣-١.

ليكن F حقلاً مميزه يساوي الصفر التمديد الدوار النوني للحقل F هو تمديد منفصل وناظمي للحقل F .

البرهان.

لنفرض أن الحقل E هو التمديد الدوار النوني للحقل F ، عندئذ E هو حقلاً تفريق الحدودية $x^n - 1 \in F[x]$ فوق F . لما كان مميز الحقل F يساوي الصفر وأن E تمديد منته للحقل F فإن E هو تمديد جبري للحقل F وحسب التمهيدية (٥-٣-١) يكون الحقل E تمديداً منفصلاً للحقل F .

من جهة أخرى، لما كان الحقل E مولداً فوق الحقل F بجميع أصفار الحدودية $x^n - 1$ وأن $\partial(x^n - 1) > 0$ فإنه حسب التمهيدية (٨-١-٧) يكون الحقل E تمديداً ناظماً للحقل F .

لتكن R حلقة تبديلية واحدة. سوف نرمز لمجموعة العناصر القابلة للقلب في R بالشكل $R^\times$ التي تشكل زمرة بالنسبة لعملية الضرب المعرفة على الحلقة R . أيضاً سوف نرمز للزمرة الضربية لأي حقل F بالشكل $F^\times = F \setminus \{0\}$.

تمهيدية ١١-٣-٢.

ليكن n عدداً صحيحاً موجباً، عندئذ:

١ - إذا كان $k \in Z$ فإن $k + nZ \in (Z/nZ)^\times$ عندما فقط عندما $\gcd(k, n) = 1$.

٢ - $(Z/nZ)^\times = \{k + nZ : k \in Z; \gcd(k, n) = 1\}$.

٣ - $(Z/nZ)^\times = \{k + nZ : 1 \leq k \leq n; \gcd(k, n) = 1\}$.

البرهان.

لنفرض أن n عدد صحيح موجب، عندئذ فإن nZ مثالي رئيسي في حلقة الأعداد الصحيحة Z وأن حلقة الخارج Z/nZ تتألف من:

$$Z/nZ = \{0 + nZ, 1 + nZ, 2 + nZ, \dots, (n-1) + nZ\}$$

١ - لزوم الشرط. ليكن $k \in Z$ ولنفرض أن $k + nZ \in (Z/nZ)^\times$ عندئذ يوجد $a \in Z$ بحيث $(a + nZ) \cdot (k + nZ) = 1 + nZ$ ومنه يكون $ak + nZ = 1 + nZ$ وبالتالي $ak - 1 \in nZ$ ومنه يوجد $b_0 \in Z$ بحيث $ak - 1 = nb_0$ ومنه يكون $ak + n(-b_0) = 1$ لنفرض أن $b = -b_0$ نجد أن $ak + nb = 1$ وهذا يبين أن العددين k, n أوليان فيما بينهما، أي أن $\gcd(k, n) = 1$.

كفاية الشرط. لنفرض أن k عدد صحيح وأن $\gcd(k, n) = 1$ عندئذ يوجد $t, s \in Z$ بحيث يكون $kt + ns = 1$ ومنه نجد أن:

$$(kt + ns) + nZ = 1 + nZ$$

$$(kt + nZ) + (ns + nZ) = 1 + nZ$$

$$(k + nZ) \cdot (t + nZ) + nZ = 1 + nZ$$

$$(k + nZ) \cdot (t + nZ) = 1 + nZ$$

وهذا يبين لنا أن $k + nZ \in (Z/nZ)^\times$.

٢ - حسب (١) ينتج أن:

$$(Z/nZ)^\times = \{k + nZ : k \in Z; \gcd(k, n) = 1\}$$

٣ - لما كانت $Z/nZ = \{0 + nZ, 1 + nZ, 2 + nZ, \dots, (n-1) + nZ\}$ نجد أن:

$$\diamond (Z/nZ)^\times = \{k + nZ : 1 \leq k \leq n; \gcd(k, n) = 1\}$$

تمهيدية ٣-٣-١١.

ليكن n عدداً صحيحاً موجباً، عندئذ:

$$١ - (Z/nZ)^\times = \{k : 1 \leq k \leq n; \gcd(k, n) = 1\}$$

$$٢ - \text{مرتبة الزمرة } (Z/nZ)^\times \text{ تساوي } \varphi(n).$$

البرهان.

١ - لما كانت $Z/nZ \cong Z_n$ فإنه يمكن المطابقة بين الحلقتين Z/nZ و Z_n وبالتالي يمكن اعتبار أن $Z/nZ = Z_n = \{k : 1 \leq k \leq n; \gcd(k, n) = 1\}$ ومنه نجد أن:

$$(Z/nZ)^\times = \{k : 1 \leq k \leq n; \gcd(k, n) = 1\}$$

٢ - واضح. ◊

اعتماداً على التمهيدية الأخيرة فإنه لأجل أي عدد أولي p فإن الحقل المنتهي الذي مرتبته p هو:

$$F_p = \{0, 1, 2, \dots, p-1\} = Z_p \cong Z/pZ$$

وأن زممرته الضربية هي:

$$F_p^\times = \{1, 2, \dots, p-1\} = Z_p^\times \cong (Z/pZ)^\times$$

$$\text{Card } F_p^\times = \varphi(p) = p-1 = \text{Card } (Z/pZ)^\times$$

لما كان الحقل F_p منتهياً فإنه حسب المبرهنة (٦-١-٤) تكون الزمرة الضربية $F_p^\times$ دوارة وأن مولداتها هي الأعداد التي تنتمي إلى $F_p^\times$ والأولية مع $(p-1)$ وعددها $\varphi(p-1)$.

لنفرض أن $g \in F_p^\times$ هو أحد المولدات للزمرة $F_p^\times$ عندئذ $1 < g < p-1$ ، كما أن:

$$F_p^\times = \langle g \rangle = \{g^k \bmod p; k = 0, 1, \dots, p-2\}$$

اعتماداً على ما سبق يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن ξ جذراً أولياً للواحد من المرتبة p ، عندئذ فإن:

$$\mu_p = \{1, \xi, \xi^2, \xi^3, \dots, \xi^{p-1}\}$$

$$\pi_p = \{1, \xi, \xi^2, \xi^3, \dots, \xi^{p-1}\}$$

تمهيدية ١١-٣-٤.

ليكن ξ جذراً أولياً للواحد من المرتبة n . عندئذ لأجل كل $a \in (Z/nZ)^\times$ يوجد $Q -$ تماثل ذاتي $\sigma_a : Q(\mu_n) \rightarrow Q(\mu_n)$ لأجله $\sigma_a(\xi) = \xi^a$.
البرهان.

لنفرض أن ξ جذر أولي للواحد من المرتبة n . ليكن $a \in (Z/nZ)^\times$ ، لما كان:

$$(Z/nZ)^\times = \{k : 1 \leq k \leq n; \gcd(k, n) = 1\}$$

$$\pi_n = \{\xi^k : 1 \leq k \leq n; \gcd(k, n) = 1\}$$

نجد أن $\pi_n = \{\xi^k : k \in (Z/nZ)^\times\}$ وهذا يبين أن ξ^k هو جذر أولي للواحد من المرتبة n وحسب المبرهنة (١١-٢-٥) نجد أن $\Phi_n(x)$ هي الحدودية الأصغرية لكل من ξ و ξ^k فوق الحقل Q ولما كانت الحدودية $\Phi_n(x)$ أولية فوق Q نجد أن العنصرين ξ و ξ^k مترافقان فوق Q وبالتالي حسب المبرهنة (٧-١-٢) يوجد $Q -$ تماثل ذاتي للحقل $Q(\mu_n) = Q(\xi)$ على الشكل $\sigma_a : Q(\mu_n) \rightarrow Q(\mu_n)$ لأجله $\sigma_a(\xi) = \xi^a$.

اعتماداً على التمهيدية السابقة يمكننا صياغة المبرهنة المهمة الآتية:

مبرهنة ١١-٣-٥.

ليكن n عدداً صحيحاً موجباً وأن ξ جذر أولي للواحد من المرتبة n . عندئذ:

١ - يوجد تماثل $\tau : (Z/nZ)^\times \rightarrow G(Q(\mu_n)/Q)$ معرف بالشكل الآتي: أيّاً كان $a \in (Z/nZ)^\times$ فإن $\tau(a) = \sigma_a$.

٢ - الزمرة $G(Q(\mu_n)/Q)$ تبديلية مرتبتها $\varphi(n)$.

البرهان.

١ - لنفرض أن ξ جذر أولي للواحد من المرتبة n . لنعرف العلاقة:

$$\tau : (Z/nZ)^\times \rightarrow G(Q(\mu_n)/Q)$$

بالشكل الآتي: ليكن $a \in (Z/nZ)^\times$ عندئذ حسب التمهيدية (١١-٣-٤) يوجد $Q -$ تماثل ذاتي σ_a للحقل $Q(\mu_n)$ لأجله $\sigma_a(\xi) = \xi^a$ ومنه فإن $\sigma_a \in G(Q(\mu_n)/Q)$. لنضع $\tau(a) = \sigma_a$. إن τ هو تطبيق، لأنه إذا كان $a, b \in (Z/nZ)^\times$ بحيث $a = b$

نجد أن $\sigma_a(\xi) = \xi^a = \xi^b = \sigma_b(\xi)$ ولما كان كل من σ_a, σ_b هو Q - تماثل ذاتي للحقل $Q(\mu_n)$ نجد أن $\sigma_a = \sigma_b$ ومنه فإن $\tau(a) = \tau(b)$.

كما أن τ هو تشاكل زمري، لأنه إذا كان $a, b \in (Z/nZ)^\times$ فإن $a \cdot b \in (Z/nZ)^\times$ وأن

$$\tau(a \cdot b) = \sigma_{a \cdot b}$$

فضلاً عن ذلك فإن $\sigma_{a \cdot b}(\xi) = \xi^{a \cdot b}$ وأن:

$$\sigma_a \cdot \sigma_b(\xi) = \sigma_a(\sigma_b(\xi)) = \sigma_a(\xi^b) = (\xi^b)^a = \xi^{a \cdot b}$$

ومنه نجد أن $\sigma_{a \cdot b}(\xi) = \sigma_a \cdot \sigma_b(\xi)$. لما كان $a, b, a \cdot b \in (Z/nZ)^\times$ فإن كلاً من $\sigma_a, \sigma_b, \sigma_{a \cdot b}$ هو Q - تماثل ذاتي للحقل $Q(\mu_n) = Q(\xi)$ ومنه أيّاً كان $c \in Q$ فإن:

$$\sigma_{a \cdot b}(c) = c = \sigma_a(c) = \sigma_a(\sigma_b(c)) = \sigma_a \cdot \sigma_b(c)$$

وهكذا نجد أن $\sigma_{a \cdot b} = \sigma_a \cdot \sigma_b$ وبالتالي يكون $\tau(a \cdot b) = \tau(a) \cdot \tau(b)$ ، مما سبق نجد أن τ هو تشاكل زمري.

لنبرهن على أن τ متباين. ليكن $a \in \text{Ker}(\tau)$ عندئذ فإن $\tau(a) = I_{Q(\mu_n)}$ وبالتالي فإن $\sigma_a = I_{Q(\mu_n)}$ ومنه نجد أن $\sigma_a(\xi) = \xi$ أي أن $\xi^a = \xi$ ومنه فإن $\xi^{a-1} = 1$ ولما كان ξ جذراً أولياً للواحد من المرتبة n نجد أن $a-1=0$ وبالتالي يكون $a=1$ ومنه نجد أن $\text{Ker}(\tau) = \{1\}$ ، أي أن τ متباين وهذا يبين أن الزمرة $(Z/nZ)^\times$ تماثل زمرة جزئية من الزمرة $G(Q(\mu_n)/Q)$.

من جهة أخرى، لدينا حسب المبرهنة (١١-٢-٣) أن $[Q(\xi):Q] = \varphi(n)$ ولما كان $Q(\xi)$ حقل تفريق فوق Q فإنه حسب المبرهنة (٩-٢-١) يكون:

$$(G(Q(\mu_n)/Q):1) = [Q(\mu_n):Q] = \varphi(n)$$

ولدينا أيضاً حسب التمهيدية (١١-٣-٣) أن $((Z/nZ)^\times:1) = \varphi(n)$ وهذا يبين أن مرتبة كل من الزمرتين $G(Q(\mu_n)/Q)$ و $(Z/nZ)^\times$ تساوي $\varphi(n)$ ومنه نجد أن τ غامر وبالتالي يكون τ تماثلاً.

٢ - وجدنا حسب (١) أن τ تماثل، ولما كانت الزمرة $(Z/nZ)^\times$ تبديلية نجد أن الزمرة $G(Q(\mu_n)/Q)$ أيضاً تبديلية وأن مرتبتها تساوي $\varphi(n)$.

مبرهنة ١١-٣-٦.

ليكن n, m عددين صحيحين موجبيين أوليين فيما بينهما. عندئذ:

$$\begin{aligned} G(Q(\mu_{m \cdot n})/Q) &\cong G(Q(\mu_m)/Q) \times G(Q(\mu_n)/Q) \cong \\ &\cong (Z/mZ)^\times \times (Z/nZ)^\times \end{aligned}$$

البرهان.

لدينا حسب المبرهنة (١١-٢-٤) أن:

$$\begin{aligned} Q(\mu_{m \cdot n}) &= Q(\mu_m, \mu_n) = Q(\mu_m) \cdot Q(\mu_n) \\ Q(\mu_m) \cap Q(\mu_n) &= Q \end{aligned}$$

وحسب المبرهنة (٩-٢-٩) نجد أن:

$$\begin{aligned} G(Q(\mu_{m \cdot n})/Q) &\cong G(Q(\mu_m)/Q) \times G(Q(\mu_n)/Q) \cong \\ &\cong (Z/mZ)^\times \times (Z/nZ)^\times \end{aligned}$$

وذلك حسب المبرهنة (١١-٣-٥). ◊

مبرهنة ١١-٣-٧.

ليكن p عدداً أولياً. عندئذ الزمرة $G(Q(\mu_p)/Q)$ دوارة مرتبتها $p-1$ وعدد مولداتها $\phi(p-1)$. فضلاً عن ذلك يوجد تقابل بين مولدات الزمرة $(Z/pZ)^\times$ ومولدات الزمرة $G(Q(\mu_p)/Q)$ ، حيث أنه إذا كان g مولداً للزمرة $(Z/pZ)^\times$ فإنه حسب المبرهنة (١١-٣-٥) يكون σ_g مولداً للزمرة $G(Q(\mu_p)/Q)$.

البرهان.

حسب المبرهنة (١١-٣-٥) نجد أن $G(Q(\mu_p)/Q) \cong (Z/pZ)^\times \cong F_p^\times$ ومنه فإن مرتبة الزمرة $G(Q(\mu_p)/Q)$ تساوي $p-1$ أي $\phi(p)$.

لما كان F_p حقلاً منتهياً فإنه حسب المبرهنة (٦-١-٤) تكون الزمرة $F_p^\times$ دوارة وبالتالي تكون الزمرة $G(Q(\mu_p)/Q)$ دوارة وأن عدد مولداتها يساوي $\phi(p-1)$. ◊

ملاحظة.

ليكن p عدداً أولياً و ξ جذراً أولياً للواحد من المرتبة p وليكن g مولداً للزمرة $(Z/pZ)^\times$. بحسب المبرهنة (١١-٣-٧) فإن σ_g مولد للزمرة $G(Q(\mu_p)/Q)$. لما كان $\sigma_g(\xi) = \xi^g$ نجد أن:

$$\sigma_g^2(\xi) = \sigma_g(\sigma_g(\xi)) = \sigma_g(\xi^g) = (\xi^g)^g = \xi^{g^2}$$

ومنه فإن $\sigma_g^j(\xi) = \xi^{g^j}$ حيث $0 \leq j \leq (p-2)$.

لنوضح آلية التعامل مع الجذور الأولية للواحد من المرتبة 11 وذلك من خلال المثال

الآتي:

مثال.

الجذور الأولية للواحد من المرتبة 11.

لدينا حسب المبرهنة (١١-٣-٧) أن الزمرة $G(Q(\mu_{11})/Q)$ دوارة مرتبتها 10 وعدد مولداتها يساوي $\varphi(10) = 4$ ، أي أن الزمرة $G(Q(\mu_{11})/Q)$ لها أربعة مولدات.

لإيجاد هذه المولدات حسب الملاحظة المذكورة سابقاً نوجد أولاً المولدات للزمرة $(Z/11Z)^\times$. إن مولدات الزمرة $(Z/11Z)^\times$ هي $\{2, 6, 7, 8\}$ ومنه فإن مولدات الزمرة $G(Q(\mu_{11})/Q)$ هي $\xi_{11}^{g^i}$ حيث ξ_{11} جذر أولي للواحد من المرتبة 11 وأن $g \in \{2, 6, 7, 8\}$ و $0 \leq i \leq 9$.

لنوجد القيم g^i من أجل $g = 2$ فنجد أن:

i	0	1	2	3	4	5	6	7	8	9
2^i	1	2	4	8	5	10	9	7	3	6

لنفرض أن $\langle \sigma \rangle = G(Q(\mu_{11})/Q)$ فنجد أنه لأجل $g = 2$ و $i = 1$ فإن:

$$\sigma(\xi_{11}) = \xi_{11}^2$$

ولما كانت الزمرة $G(Q(\mu_{11})/Q)$ دوارة مرتبتها 10 فإنها تحوي زمرة جزئية واحدة فقط مرتبتها 5 وهي $\langle \sigma^2 \rangle$ زمرة جزئية أخرى واحدة فقط مرتبتها 2 وهي $\langle \sigma^5 \rangle$ ومنه فإن

الحقل $Q(\mu_{11})$ يحوي تمديداً للحقل Q درجته تساوي 5 وتمديداً آخر للحقل Q درجته تساوي 2 مقابلين للزمريتين الجزئيتين $\langle \sigma^2 \rangle$ و $\langle \sigma^5 \rangle$ على الترتيب.

مبرهنة ١١-٣-٨.

ليكن F حقلاً مميزه يساوي الصفر و n عدداً صحيحاً موجباً. عندئذ:

- ١ - الحقل $F(\mu_n)$ هو حقل تفريق الحدودية $\Phi_n(x)$ فوق F .
- ٢ - الزمرة $G(F(\mu_n)/F)$ تماثل زمرة جزئية من الزمرة $G(Q(\mu_n)/Q)$.
- ٣ - العدد $[F(\mu_n) : F]$ يقسم $\varphi(n)$.
- ٤ - إذا كان p عدداً أولياً فإن الزمرة $G(F(\mu_p)/F)$ دوارة.
- ٥ - إذا كانت الحدودية $\Phi_n(x)$ أولية فوق F ، عندئذ فإن:

$$G(F(\mu_n)/F) \cong G(Q(\mu_n)/Q)$$

وأن $[F(\mu_n) : F] = \varphi(n)$.

البرهان.

- ١ - إن $F(\mu_n)$ هو حقل تفريق الحدودية $\Phi_n(x)$ فوق F ، لأنه مولد فوق F بجميع أصفار الحدودية $\Phi_n(x)$.

- ٢ - لدينا حسب المبرهنة (١١-٢-٤) أن $Q(\mu_n)$ هو حقل تفريق فوق Q ، ولما كان:

$$F(\mu_n) = F(Q(\mu_n))$$

فإنه حسب المبرهنة (٨-٢-٩) يكون:

$$\begin{aligned} G(F(\mu_n)/F) &= G(F(Q(\mu_n))/F) \cong G(Q(\mu_n)/Q(\mu_n) \cap F) \subseteq \\ &\subseteq G(Q(\mu_n)/Q) \end{aligned}$$

وذلك لأن كل $(Q(\mu_n) \cap F)$ - تماثل ذاتي للحقل $Q(\mu_n)$ هو Q - تماثل ذاتي للحقل $Q(\mu_n)$.

- ٣ - لدينا حسب (١) أن الحقل $F(\mu_n)$ هو حقل تفريق الحدودية $\Phi_n(x)$ فوق F وحسب المبرهنة (١١-٢-٩) يكون:

$$(G(F(\mu_n)/F) : 1) = [F(\mu_n) : F]$$

من جهة أخرى، لدينا حسب المبرهنة (١١-٣-٥) أن $(G(Q(\mu_n)/Q) : 1) = \varphi(n)$

وحسب (٢) أن الزمرة $G(F(\mu_n)/F)$ تماثل زمرة جزئية من الزمرة $G(Q(\mu_n)/Q)$ فإن مرتبة الزمرة $G(F(\mu_n)/F)$ تقسم مرتبة الزمرة $G(Q(\mu_n)/Q)$ وبالتالي فهي تقسم العدد $\varphi(n)$ ، أي أن $[F(\mu_n):F]$ يقسم $\varphi(n)$.

٤ - لنفرض أن p عدد أولي، عندئذ حسب المبرهنة (١١-٣-٧) فإن الزمرة $G(Q(\mu_p)/Q)$ تكون دوارة، ولما كان حسب (٢) أن الزمرة $G(F(\mu_p)/F)$ تماثل زمرة جزئية من الزمرة $G(Q(\mu_p)/Q)$ نجد أن الزمرة $G(F(\mu_p)/F)$ أيضاً دوارة.

٥ - لنفرض أن ξ جذر أولي للواحد من المرتبة n ، عندئذ حسب التمهيدية (١١-١-٢) فإن $Q(\mu_n) = Q(\xi)$ ومنه يكون $Q(\mu_n) = F \cdot Q(\xi)$ وهذا يبين أن:

$$F(\mu_n) = F(\xi)$$

من جهة أخرى، لنفرض أن الحدودية $\Phi_n(x)$ أولية فوق F ، عندئذ يكون:

$$[F(\mu_n):F] = [F(\xi):F] = \partial \Phi_n(x) = \varphi(n)$$

ولما كان $F(\mu_n)$ هو حقل تفريق فوق F فإنه حسب المبرهنة (٩-٢-١) نجد أن:

$$\begin{aligned} (G(F(\mu_n)/F):1) &= [F(\mu_n):F] = \varphi(n) = \\ &= [Q(\xi):Q] = [Q(\mu_n):Q] = (G(Q(\mu_n)/Q):1) \end{aligned}$$

وحسب (٢) لدينا أن الزمرة $G(F(\mu_n)/F)$ تماثل زمرة جزئية من الزمرة $G(Q(\mu_n)/Q)$ وهذا يبين أن $G(Q(\mu_n)/Q) \cong G(F(\mu_n)/F)$.

مبرهنة ١١-٣-٩.

ليكن F حقلاً و p عدداً أولياً. لنفرض أن $h(x) = x^p - a \in F[x]$ وأن $a \neq 0$. الشروط الآتية متكافئة:

١ - الحدودية $h(x)$ ليست أولية في $F[x]$.

٢ - يوجد $b \in F$ بحيث $a = b^p$.

٣ - الحدودية $h(x)$ تملك صفراً في F .

البرهان.

(١) $\Leftrightarrow$ (٢). لنفرض أن الحدودية $h(x)$ ليست أولية في $F[x]$ ، عندئذ توجد حدوديتان

$$f(x), g(x) \in F[x] \text{ بحيث } h(x) = f(x) \cdot g(x) \text{ وأن:}$$

$$\partial f(x) = m > 0, \quad \partial g(x) = n > 0$$

كما أن $n, m < p$ وأن $n + m = p$. لنفرض أن:

$$f(x) = \sum_{i=0}^m a_i x^i, \quad \partial g(x) = \sum_{i=0}^n b_i x^i$$

حيث $a_i, b_i \in F$ فنجد أن $a = a_0 \cdot b_0$. لنفرض أن β صفر للحدودية $h(x)$ وأن ξ جذر أولي للواحد من المرتبة p ، عندئذ يكون $a = \beta^p$ كما أنه أيضاً كان $i = 0, 1, 2, \dots, (p-1)$ فإن $\xi^i \cdot \beta$ هي جميع أصفار الحدودية $h(x)$ ، لأن:

$$h(\xi^i \cdot \beta) = (\xi^i \cdot \beta)^p - a = \xi^{i \cdot p} \cdot \beta^p - a = \beta^p - a = 0$$

وهذا يبين أن $a = (\xi^i \cdot \beta)^p$ ولما كان $a = a_0 \cdot b_0$ نجد أن:

$$a_0 = \xi^{i \cdot m} \cdot \beta^m, \quad b_0 = \xi^{i \cdot n} \cdot \beta^n$$

لنفرض أن $m_0 = im, \quad n_0 = in$ فنجد أن $a_0 = \xi^{m_0} \cdot \beta^m, \quad b_0 = \xi^{n_0} \cdot \beta^n$ من جهة أخرى، لما كان $n + m = p$ فإن العددين n, m أوليان فيما بينهما، ومنه يوجد $t, s \in \mathbb{Z}$ بحيث $mt + ns = 1$. لنفرض أن:

$$\gamma = (\xi^{m_0} \cdot \beta^m)^t \cdot (\xi^{n_0} \cdot \beta^n)^s$$

ف نجد أن $\gamma \in F$ وأن:

$$\gamma = (\xi^{m_0 t} \cdot \beta^{m t}) \cdot (\xi^{n_0 s} \cdot \beta^{n s}) = \xi^{m_0 t + n_0 s} \cdot \beta^{m t + n_0 s} = \xi^{m_0 t + n_0 s} \cdot \beta$$

وهذا يبين أن $\gamma = (\xi^p)^{m_0 t + n_0 s} \cdot \beta^p = \beta^p = 0$

(٢) $\Leftarrow$ (٣). لنفرض أنه يوجد $b \in F$ بحيث $a = b^p$ عندئذ يكون:

$$h(b) = b^p - a = a - a = 0$$

ومنه يكون $b \in F$ صفراً للحدودية $h(x)$.

(٣) $\Leftarrow$ (١). لنفرض أن الحدودية $h(x)$ تملك صفراً في F ، $\beta \in F$ ، عندئذ فإن

$x - \beta \in F[x]$ تقسم $h(x)$ في $F[x]$ ، ومنه توجد $\lambda(x) \in F[x]$ بحيث:

$$h(x) = (x - a) \cdot \lambda(x)$$

ولما كانت $\partial h(x) = p$ نجد أن $\partial \lambda(x) = p - 1 > 0$ وهذا يبين أن الحدودية $h(x)$

ليست أولية في $F[x]$. ◊

اعتماداً على المبرهنة الأخيرة، يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن F حقلاً و p عدداً أولياً وأن $h(x) = x^p - a \in F[x]$ وأن $a \neq 0$. لنفرض أن الحقل F يحوي جذراً أولياً للواحد من المرتبة p . إذا كانت الحدودية $h(x)$ ليست أولية في $F[x]$ ، عندئذ فإن $h(x)$ تتفرق في $F[x]$ إلى مضارب خطية.

البرهان.

ينتج مباشرة من المبرهنة السابقة وذلك لأنه ضمن الفرضيات الواردة في النص فإن الحقل F يحوي جميع أصفار الحدودية $h(x)$ ، كما هو وارد في البرهان السابق. ◊

مبرهنة ١١-٣-١٠.

ليكن R حقل الأعداد الحقيقية و F حقلاً جزئياً في R . لنفرض أن $\beta \in R$ وأن $\beta \notin F$. إذا وجد عدد أولي p يحقق $\beta^p \in F$ عندئذ تكون الحدودية $x^p - \beta^p \in F[x]$ أولية فوق F .

البرهان.

لنبرهن على أن الحدودية $h(x) = x^p - \beta^p \in F[x]$ لا تملك أصفاراً في F . لنفرض جداً أنه يوجد $\gamma \in F$ بحيث يكون صفراً للحدودية $h(x)$ ، عندئذ يكون $\gamma^p = \beta^p$ ، ومنه نجد أن $\beta = \zeta \cdot \gamma$ حيث ζ جذر للواحد من المرتبة p . لما كانت العناصر β, γ أعداداً حقيقية نجد أن $\zeta = \beta/\gamma$ ومنه إذا كان $p = 2$ نجد أنه إما $\zeta = 1$ أو $\zeta = -1$. إذا كان $p > 2$ نجد أن $\zeta = 1$ وذلك لأن $\beta \in R$ عدد حقيقي وهذا يبين أن $\beta = \pm \gamma \in F$ ، وهذا غير ممكن فرضاً. مما سبق نجد أن الحدودية $h(x)$ لا تملك أصفاراً في F وحسب المبرهنة (١١-٣-٩) تكون الحدودية $h(x)$ أولية فوق F . ◊

مبرهنة ١١-٣-١١.

ليكن F حقلاً و p عدداً أولياً. لنفرض أن $h(x) = x^p - a \in F[x]$ وأن $a \neq 0$. إذا كان الحقل F يحوي جذراً أولياً للواحد من المرتبة p وإذا كانت الحدودية $h(x)$ ليست أولية فوق F ، عندئذ فإن الحدودية $h(x)$ تتفرق فوق F ، (تتفرق في $F[x]$ إلى مضارب خطية).

البرهان.

لنفرض أن ξ جذر أولي للواحد من المرتبة p وأن $\xi \in F$. لنفرض أيضاً أن الحدودية $h(x)$ ليست أولية فوق F وليكن β صفراً للحدودية في تمديد ما للحقل F . لنفرض أن $[F(\beta):F] = m$ ، عندئذ فإن m يقسم p ، لأن m هي درجة الحدودية الأصغرية للعنصر β فوق F ، ومنه إما $m = p$ أو $m = 1$. لما كانت الحدودية $h(x)$ ليست أولية فوق F فإنه حسب المبرهنة (٣-٣-١٥) يكون $m \neq p$ ، ومنه نجد أن $m = 1$ وبالتالي يكون $F(\beta) = F$ وهذا يبين أن $\beta \in F$. لما كان β صفراً اختيارياً للحدودية $h(x)$ نجد أن الحقل F يحوي جميع أصفار الحدودية $h(x)$ وبالتالي فإن الحدودية $h(x)$ تتفرق فوق F . ◊

١١ - ٤. التمديدات الدائرية.

تعريف.

ليكن الحقل K تمديداً للحقل F . نقول إن K هو تمديد دائري للحقل F إذا كان K حقل تفريق فوق F وكانت الزمرة $G(K/F)$ دائرية (دوارة).

لنفرض أن الحقل K تمديد دائري للحقل F . لما كان K حقل تفريق فوق F فإن K هو تمديد منته للحقل F . لنفرض أن $[K:F] = n$. حسب المبرهنة (٩-٢-١) يكون:

$$(G(K/F):1) = [K:F] = n$$

ولما كانت الزمرة $G(K/F)$ دائرية فإنه يوجد $\sigma \in G(K/F)$ بحيث يكون:

$$G(K/F) = \langle \sigma \rangle = \{\sigma^i : i = 0, 1, 2, \dots, (n-1)\}$$

تعريف.

ليكن الحقل K تمديداً دائرياً للحقل F . لنفرض أن F يحوي جذراً أولياً للواحد من المرتبة n وليكن ξ . عندئذ أياً كان $\alpha \in K$ ، نسمي العنصر:

$$(\xi, \alpha) = \sum_{i=0}^{n-1} \xi^i \cdot \sigma^i(\alpha) = \alpha + \xi \cdot \sigma(\alpha) + \xi^2 \cdot \sigma^2(\alpha) + \dots + \xi^{n-1} \cdot \sigma^{n-1}(\alpha)$$

عنصر لاغرانج، حيث $\sigma \in G(K/F)$ هو مولد الزمرة $G(K/F)$.

مبرهنة ١١-٤-١.

ليكن الحقل K تمديداً دائرياً للحقل F درجته n وأن $G(K/F) = \langle \sigma \rangle$. لنفرض أن F يحوي جذراً أولياً للواحد من المرتبة n وليكن ξ . عندئذ:

١ - أياً كان $\alpha \in K$ فإن:

$$\sigma^i((\xi, \alpha)) = \xi^{-1} \cdot (\xi, \alpha)$$

وذلك لأجل كل $i = 0, 1, 2, \dots, (n-1)$.

٢ - $(\xi, \alpha) \in F$

٣ - $(1, \alpha) \in F$

البرهان.

لما كان $\sigma^n = I_K$ وأن $\sigma(\xi) = \xi$ و $\sigma(\xi^{-1}) = \xi^{-1}$ وذلك لأن $\xi \in F$ وأن σ هو F -تماثل ذاتي للحقل K نجد أن:

$$\begin{aligned}\sigma((\xi, \alpha)) &= \sigma\left(\sum_{i=0}^{n-1} \xi^i \cdot \sigma^i(\alpha)\right) = \sigma(\alpha) + \xi \cdot \sigma^2(\alpha) + \xi^2 \cdot \sigma^3(\alpha) + \cdots + \\ &\quad + \xi^{n-1} \cdot \sigma^n(\alpha) = \\ &= \xi^{-1}(\xi \cdot \sigma(\alpha) + \xi^2 \cdot \sigma^2(\alpha) + \xi^3 \cdot \sigma^3(\alpha) + \cdots + \xi^n \cdot \alpha) = \\ &= \xi^{-1}(\xi \cdot \sigma(\alpha) + \xi^2 \cdot \sigma^2(\alpha) + \xi^3 \cdot \sigma^3(\alpha) + \cdots + \xi^{n-1} \cdot \sigma^{n-1}(\alpha) + \alpha) = \\ &= \xi^{-1} \cdot (\xi, \alpha)\end{aligned}$$

$$\begin{aligned}\sigma^2((\xi, \alpha)) &= \sigma(\sigma((\xi, \alpha))) = \sigma(\xi^{-1} \cdot (\xi, \alpha)) = \\ &= \xi^{-1} \cdot \sigma((\xi, \alpha)) = \xi^{-1} \cdot \xi^{n-1} \cdot (\xi, \alpha) = \xi^{-2} \cdot (\xi, \alpha)\end{aligned}$$

$$\begin{aligned}\sigma^3((\xi, \alpha)) &= \sigma(\sigma^2((\xi, \alpha))) = \sigma(\xi^{-2} \cdot (\xi, \alpha)) = \\ &= \xi^{-2} \cdot \xi^{-1} \cdot (\xi, \alpha) = \xi^{-3} \cdot (\xi, \alpha)\end{aligned}$$

وهكذا لأجل كل $i = 0, 1, 2, \dots, (n-1)$.

٢ - ليكن $\tau \in G(K/F)$ عندئذ فإن $\tau = \sigma^i$ حيث $0 \leq i \leq (n-1)$ ، لأن σ هو مولد الزمرة $G(K/F)$ وحسب (١) نجد أن:

$$\begin{aligned}\tau((\xi, \alpha)^n) &= \sigma^i((\xi, \alpha)^n) = (\sigma^i(\xi, \alpha))^n = \\ &= (\xi^{-i} \cdot (\xi, \alpha))^n = \xi^{-in} \cdot (\xi, \alpha)^n = (\xi, \alpha)^n\end{aligned}$$

وذلك لأن $\xi^n = 1$ ، وهذا يبين أن:

$$(\xi, \alpha)^n \in F(G(K/F)) = F$$

وذلك حسب المبرهنة (٩-٢-١)، لأن الحقل K حقل تفريق فوق F .

٣ - لما كان 1 جذراً للواحد من المرتبة n ، عندئذ حسب (١) نجد أن:

$$\sigma^i((1, \alpha)) = 1^{-i} \cdot (1, \alpha) = (1, \alpha)$$

وذلك أيّاً كان $i = 0, 1, 2, \dots, (n-1)$ ، أي أن العنصر $(1, \alpha)$ مثبت بالنسبة لجميع عناصر الزمرة $G(K/F)$ ، ومنه فإن:

$$(1, \alpha) \in F(G(K/F)) = F$$

وهو المطلوب إثباته. ◊

مبرهنة ١١-٤-٢.

ليكن الحقل K تمديداً دائرياً للحقل F درجته n وأن $\langle \sigma \rangle = G(K/F)$. لنفرض أن الحقل F يحوي جذراً أولياً للواحد من المرتبة n وليكن ξ . عندئذ:

$$١ - \text{أيّاً كان } \alpha \in K \text{ فإن } \alpha = \frac{1}{n} \sum_{i=0}^{n-1} (\xi^i, \alpha)$$

$$٢ - \text{ليكن } \alpha \in K. \text{ إذا كان } (\xi, \alpha) \neq 0 \text{ عندئذ يكون } K = F((\xi, \alpha)).$$

البرهان.

١- ليكن $\alpha \in K$ ، عندئذ لدينا:

$$(\xi, \alpha) = \sum_{j=0}^{n-1} \xi^j \cdot \sigma^j(\alpha) = \alpha + \xi \cdot \sigma(\alpha) + \xi^2 \cdot \sigma^2(\alpha) + \dots + \xi^{n-1} \cdot \sigma^{n-1}(\alpha)$$

ومنه فإن:

$$(\xi^i, \alpha) = \sum_{j=0}^{n-1} (\xi^i)^j \cdot \sigma^j(\alpha) = \alpha + \xi^i \cdot \sigma(\alpha) + (\xi^i)^2 \cdot \sigma^2(\alpha) + \dots + (\xi^i)^{n-1} \cdot \sigma^{n-1}(\alpha)$$

ومنه نجد إن:

$$\begin{aligned} \sum_{i=0}^{n-1} (\xi^i, \alpha) &= \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} (\xi^i)^j \cdot \sigma^j(\alpha) \right) = \\ &= \sum_{j=0}^{n-1} \sigma^j(\alpha) \cdot \left(\sum_{i=0}^{n-1} (\xi^i)^j \right) \end{aligned}$$

لما كان ξ جذراً أولياً للواحد من المرتبة n فإن ξ^j هو صفر للحدودية:

$$x^n - 1 = (x-1) \cdot (x^{n-1} + x^{n-2} + \dots + x + 1)$$

وذلك لأجل كل $j = 0, 1, 2, \dots, (n-1)$ ، لأن:

$$(\xi^j)^n - 1 = (\xi^n)^j - 1 = 1 - 1 = 0$$

ولما كان الجذر ξ أولياً من المرتبة n للواحد نجد أن:

$$\xi^j = 1 \Leftrightarrow j = 0; \quad j = 0, 1, 2, \dots, (n-1)$$

وهذا يبين لنا أن:

$$\sum_{i=0}^{n-1} (\xi^j)^i = \begin{cases} n & j = 0 \\ 0 & 1 \leq j \leq (n-1) \end{cases}$$

وهكذا نجد أن:

$$\sum_{i=0}^{n-1} (\xi^i, \alpha) = n \cdot \sigma^0(\alpha) = n \cdot \alpha$$

$$\alpha = \frac{1}{n} \sum_{i=0}^{n-1} (\xi^i, \alpha)$$

٢ - ليكن $\alpha \in K$. لنفرض أن $\lambda = (\xi, \alpha) \neq 0$ ، لما كان $\lambda \in K$ فإن:

$$F \subseteq F(\lambda) \subseteq K$$

ومنه فإن $G(K/F(\lambda))$ زمرة جزئية من الزمرة $G(K/F)$ ، وذلك لأن كل $F(\lambda) -$

تماثل ذاتي للحقل K هو $F -$ تماثل ذاتي للحقل K .

ليكن $(\tau \in G(K/F(\lambda)))$ عندئذ فإن:

$$\tau \in G(K/F) = \langle \sigma \rangle$$

ومنه يوجد دليل $0 \leq i \leq n-1$ بحيث $\tau = \sigma^i$ ، ولما كان τ هو $F(\lambda) -$ تماثل ذاتي

للحقل K نجد أن $\tau(\lambda) = \sigma^i(\lambda) = \lambda$ وحسب المبرهنة (١١-٤-١) فإن:

$$\sigma^i(\lambda) = \sigma^i((\xi, \alpha)) = \xi^{-i} \cdot (\xi, \alpha) = \xi^{-i} \cdot \lambda$$

ومنه نجد أن $\lambda = \xi^{-i} \cdot \lambda$ وبالتالي يكون $\lambda \cdot (\xi^{-i} - 1) = 0$ ولما كان $\lambda \neq 0$ نجد أن

$\lambda = \xi^{-i} \cdot \lambda$ ولما كان $0 \leq i \leq n-1$ وأن ξ جذر أولي للواحد من المرتبة n نجد أن

$i = 0$ ومنه يكون لدينا:

$$\tau(\lambda) = \sigma^i(\lambda) = \sigma^0(\lambda) = I_G(\lambda) = \lambda$$

وهذا يبين أن كل $F(\lambda) -$ تماثل ذاتي للحقل K هو المطابق على K ومنه يكون:

$$G(K/F(\lambda)) = \langle I_G \rangle$$

وبالتالي فإن $F(G(K/F(\lambda))) = F(\langle I_G \rangle)$.

ولما كان الحقل K تمديداً دائرياً للحقل F فإن K هو حقل تفريق فوق F ، ولما كان

$F \subseteq F(\lambda) \subseteq K$ نجد أن الحقل K هو حقل تفريق فوق $F(\lambda)$ وحسب المبرهنة

(٩-٢-١) نجد أن:

$$F(\lambda) = F(G(K/F(\lambda))) = F(\langle I_G \rangle) = K$$

أي أن $K = F(\lambda)$.

مبرهنة ١١-٤-٣.

ليكن الحقل K تمديداً للحقل F وليكن $\beta \in K$ حيث $0 \neq \beta$ حيث $\beta^n \in K$ حيث $n > 0$ عدد صحيح. إذا كان $F(\beta)$ تمديداً للحقل F درجته m وكان ξ جذراً أولياً للواحد من المرتبة n وإذا كان $\xi \in F$ ، عندئذ فإن:

١ - الحقل $F(\beta)$ هو تمديد دائري للحقل F .

٢ - العدد m يقسم n .

٣ - $\beta^m \in F$ وأن m أصغر عدد صحيح موجب لأجله $\beta^m \in F$.

٤ - الحدودية $x^n - \beta^n \in F[x]$ أولية فوق F عندما وفقط عندما $n = m$.

البرهان.

١ - لنفرض أن $h(x) = x^n - \beta^n \in F[x]$ وأن ξ جذر أولي للواحد من المرتبة n . عندئذ فإن أصفار الحدودية $h(x)$ هي $\xi^i \cdot \beta$ حيث $i = 0, 1, 2, \dots, (n-1)$ ولما كان $\xi \in F$ نجد أن $\xi^i \cdot \beta \in F(\beta)$ لأجل كل $0 \leq i \leq (n-1)$ ومنه يكون:

$$F(\beta, \xi \cdot \beta, \xi^2 \cdot \beta, \dots, \xi^{n-1} \cdot \beta) \subseteq F(\beta)$$

ولما كان $\beta \in F(\beta, \xi \cdot \beta, \xi^2 \cdot \beta, \dots, \xi^{n-1} \cdot \beta)$ نجد أن:

$$F(\beta) = F(\beta, \xi \cdot \beta, \xi^2 \cdot \beta, \dots, \xi^{n-1} \cdot \beta)$$

وهذا يبين أن $F(\beta)$ هو حقل تفرق الحدودية $h(x) = x^n - \beta^n$ فوق F .

لنبرهن الآن على أن الزمرة $G(F(\beta)/F)$ دوارة.

لما كان $F(\beta)$ تمديداً منتهياً للحقل F وأن β صفر للحدودية $h(x)$ فإنه حسب التمهيدية (٩-١-٢) يكون $\sigma(\beta)$ صفراً للحدودية $h(x)$ وهذا يبين أن $(\sigma(\beta))^n = \beta^n$ وبالتالي يكون $\sigma(\beta) = \xi^{\varepsilon(\sigma)} \cdot \beta$ حيث $0 \leq \varepsilon(\sigma) \leq n-1$. لنعرف التطبيق:

$$f : G(F(\beta)/F) \rightarrow (Z/nZ)^+$$

بالشكل الآتي: أيأ كان $\sigma \in G(F(\beta)/F)$ فإن $f(\sigma) = \varepsilon(\sigma)$ وحيث $(Z/nZ)^+$

الزمرة الجمعية في الحلقة Z/nZ . إن f تشاكل زمري، لأنه إذا كان:

$$\sigma, \tau \in G(F(\beta)/F)$$

فإن:

$$\sigma \cdot \tau(\beta) = \sigma(\tau(\beta)) = \sigma(\xi^{\varepsilon(\tau)} \cdot \beta)$$

ولما كان $\xi \in F$ وأن σ هو F -تماثل ذاتي للحقل $F(\beta)$ نجد أن:

$$\begin{aligned} \sigma \cdot \tau(\beta) &= \sigma(\xi^{\varepsilon(\tau)} \cdot \beta) = \xi^{\varepsilon(\tau)} \cdot \sigma(\beta) = \xi^{\varepsilon(\tau)} \cdot \xi^{\varepsilon(\sigma)} \cdot \beta = \\ &= \xi^{\varepsilon(\tau) + \varepsilon(\sigma)} \cdot \beta \end{aligned}$$

ومنه نجد أن:

$$f(\sigma \cdot \tau) = \varepsilon(\tau) + \varepsilon(\sigma) = f(\sigma) + f(\tau)$$

وهذا يبين أن f تشاكل زمري، وهو أيضاً متباين، لأنه إذا كان $\sigma \in \text{Ker}(f)$ فإن:

$$f(\sigma) = nZ, \quad f(\sigma) = \varepsilon(\sigma)$$

ومنه نجد أن $\varepsilon(\sigma) \in nZ$ وبالتالي يوجد $t \in Z$ بحيث $\varepsilon(\sigma) = t \cdot n$ ومنه نجد أن:

$$\sigma(\beta) = \xi^{\varepsilon(\sigma)} \cdot \beta = \xi^{nt} \cdot \beta = \beta$$

ولما كان σ هو F -تماثل ذاتي للحقل $F(\beta)$ وأن $\sigma(\beta) = \beta$ نجد أن $\sigma = I_{F(\beta)}$

وهذا يبين أن $\text{Ker}(f) = \{I_{F(\beta)}\}$ أي أن التشاكل f متباين. مما سبق نجد أن الزمرة

$G(F(\beta)/F)$ تماثل زمرة جزئية من الزمرة $(Z/nZ)^+$ ، ولما كانت الزمرة $(Z/nZ)^+$

دوارة نجد أن الزمرة $G(F(\beta)/F)$. مما سبق نجد أن الحقل $F(\beta)$ هو تمديد دائري للحقل F .

٢ - وجدنا حسب (١) أن الحقل $F(\beta)$ هو حقل تفريق فوق F وحسب المبرهنة (٩) - (١-٢) نجد أن:

$$[G(F(\beta)/F):1] = [F(\beta):F] = m$$

ولما كانت الزمرة $G(F(\beta)/F)$ تماثل زمرة جزئية من الزمرة $(Z/nZ)^+$ التي مرتبتها n

نجد حسب مبرهنة لاگرانج أن m يقسم n .

٣ - وجدنا حسب (١) أن الزمرة $G(F(\beta)/F)$ دوارة. لنفرض أن:

$$G(F(\beta)/F) = \langle \sigma \rangle$$

حيث $\sigma \in G(F(\beta)/F)$ ، عندئذ يكون $o(\sigma) = m$ ، ومنه فإن $\sigma^m = I_{F(\beta)}$.

لنأخذ التشاكل:

$$f : G(F(\beta)/F) \rightarrow (Z/nZ)^+$$

المعرف في (١)، لما كان $f(\sigma) = \varepsilon(\sigma)$ ، لنفرض أن $\eta = \xi^{\varepsilon(\sigma)}$ فنجد أن:

$$\sigma(\beta) = \xi^{\varepsilon(\sigma)} \cdot \beta = \eta \cdot \beta$$

$$\sigma^2(\beta) = \sigma(\eta \cdot \beta)$$

ولما كان σ هو F -تماثل ذاتي للحقل $F(\beta)$ نجد أن:

$$\sigma^2(\beta) = \sigma(\eta \cdot \beta) = \eta \cdot \sigma(\beta) = \eta \cdot \eta \cdot \beta = \eta^2 \cdot \beta$$

ولما كان $o(\sigma) \in (G(F(\beta)/F) : 1) = m$ نجد أن:

$$\beta = \sigma^m(\beta) = \eta^m \cdot \beta$$

ومنه نجد أن $\beta(\eta^m - 1) = 0$ ولما كان $\beta \in K$ نجد أن $\eta^m = 1$ وهذا يبين أن η

جذر للواحد من المرتبة m . لنبرهن على أن η جذر أولي للواحد من المرتبة m .

لنفرض جـدلاً أن η ليس جذراً أولياً للواحد من المرتبة m ، عندئذ يوجد $1 < m_0 < m$ بحيث $\eta^{m_0} = 1$ ومنه نجد أن:

$$\sigma^{m_0}(\beta) = \eta^{m_0} \cdot \beta = \beta$$

وهذا يبين أن $o(\sigma) = m_0 < m$ وهذا غير ممكن. وهكذا فإن η جذر أولي للواحد من المرتبة m وأن:

$$\sigma(\beta^m) = (\sigma(\beta))^m = (\eta \cdot \beta)^m = \eta^m \cdot \beta^m = \beta^m$$

ومنه نجد أن:

$$\beta^m \in F(G(F(\beta)/F)) = F$$

وذلك حسب المبرهنة (٩-٢-١). كما أن m هو أصغر عدد صحيح موجب لأجله

$\beta^m \in F$ ، لأنه إذا كان $k < m$ عدداً صحيحاً موجباً لأجله $\beta^k \in F$ ولما كان σ هو

F -تماثل ذاتي للحقل $F(\beta)$ نجد أن:

$$\beta^k = \sigma(\beta^k) = (\sigma(\beta))^k = \eta^k \cdot \beta^k$$

ومنه يكون $\beta^k(\eta^k - 1) = 0$ ولما كان $\beta^k \in K$ نجد أن $\eta^k = 1$ وهذا يبين أن

$o(\eta) = m$ تقسم k وهذا غير ممكن، لأن η جذر أولي للواحد من المرتبة m .

٤ - وجدنا حسب (٢) أن m يقسم n ومنه يوجد $n_0 \in \mathbb{Z}$ بحيث $n = n_0 m$ وبالتالي فإن

$$\beta^n = \beta^{n_0 m} = (\beta^m)^{n_0}$$

ولما كان حسب (٣) أن $\beta^m \in F$ نجد أن $\beta^n \in F$ وهذا يبين أن:

$$h(x) = x^n - \beta^n \in F[x]$$

- لنفرض أن الحدودية $h(x)$ أولية فوق F ، عندئذ لما كان β صفراً للحدودية $h(x)$ نجد أن $h(x)$ هي الحدودية الأصغرية للعنصر β فوق F ومنه نجد أن:

$$[F(\beta) : F] = \partial h(x) = n$$

ولما كان $[F(\beta) : F] = m$ فرضاً نجد أن $m = n$.

- لنفرض أن $m = n$ ، عندئذ يكون:

$$[F(\beta) : F] = n = \partial h(x)$$

ولما كان β صفراً للحدودية $h(x)$ فإنه حسب المبرهنة (٣-٣-١٥) تكون الحدودية $h(x)$ أولية فوق F .

مبرهنة ١١-٤-٤.

ليكن الحقل K تمديداً دائرياً للحقل F درجته p حيث p عدد أولي. وليكن $0 \neq \theta \in K$ بحيث $\theta \notin F$. لنفرض أن ξ جذر أولي للواحد من المرتبة p وإذا كان $\xi \in F$ ، عندئذ يوجد $1 \leq t \leq p-1$ بحيث يكون:

$$١ - \text{الحقل } K = F(\gamma) \text{ حيث } \gamma = (\xi^t, \theta)$$

$$٢ - \gamma^p \in F$$

$$٣ - \text{الحدودية } h(x) = x^p - \gamma^p \in F[x] \text{ أولية فوق } F.$$

البرهان.

لما كان $[K : F] = p$ وأن $\theta \in K$ نجد أن $F \subseteq F(\theta) \subseteq K$ وهذا يبين أن:

$$[K : F] = [K : F(\theta)] \cdot [F(\theta) : F]$$

ولما كان $\theta \notin F$ نجد أن $[F(\theta) : F] \neq 1$ ومنه فإن $[F(\theta) : F] = p$ وهذا يبين أن

$$[K : F(\theta)] = 1 \text{ وبالتالي يكون } K = F(\theta).$$

١ - لنضع:

$$E = F((1, \theta), (\xi, \theta), (\xi^2, \theta), \dots, (\xi^{p-1}, \theta))$$

لما كان E حقلاً جزئياً في K نجد أن $E \subseteq K = F(\theta)$ من جهة أخرى، لدينا حسب المبرهنة (١١-٤-٢) أنه أياً كان $\alpha \in K$ فإن:

$$\alpha = \frac{1}{n} \sum_{i=0}^{n-1} (\xi^i, \theta)$$

ومنه يكون $E = K = F(\theta)$ وهكذا نجد أن $K = E$ وحسب المبرهنة (١١-٤-١) يكون $(1, \theta) \in F$ وذلك لأن $\theta \in K$. ومنه يوجد $1 \leq t \leq p-1$ بحيث:

$$(\xi^t, \theta) \notin F$$

لأنه إذا كان لأجل كل $1 \leq t \leq p-1$ فإن $(\xi^t, \theta) \in F$ نجد أن $F = E = K$ ولما كان $\theta \in K$ نجد أن $\theta \in F$ وهذا غير ممكن حسب الفرض.

مما سبق نجد أن ξ^t جذر أولي للواحد من المرتبة p .

لنفرض أن $\gamma = (\xi^t, \theta)$ فنجد حسب المبرهنة (١١-٤-١) أن $K = F(\gamma)$.

٢ - حسب المبرهنة (١١-٤-٢) نجد أن $\gamma^p \in F$.

٣ - حسب المبرهنة (١١-٤-٣) نجد أن الحدودية $h(x) = x^p - \gamma^p \in F[x]$ أولية فوق F . ◊

الفصل الثاني عشر

التمديدات الجذرية

١٢ - ١. التمديدات الجذرية.

تعريف.

ليكن F حقلاً. نسمي كل حدودية من الشكل $x^m - a \in F[x]$ حيث m عدد صحيح موجب حدودية ثنائية فوق F .

تعريف.

ليكن الحقل K تمديداً للحقل F . نقول عن التمديد K للحقل F إنه تمديد ثنائي إذا كان $K = F(\beta)$ ، حيث $\beta \in K$ هو صفر لحدودية من الشكل $x^m - a \in F[x]$ وأن m عدد صحيح موجب.

ينتج من التعريف مباشرة أن كل حقل F هو تمديد ثنائي لنفسه، وذلك لأن $1 \in F$ هو صفر للحدودية $x - 1 \in F[x]$.

اعتماداً على التعريف السابق يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن F حقلاً و $m > 1$ عدداً صحيحاً. إذا كانت الحدودية $x^m - a \in F[x]$ عندئذ فإن الحقل $F(\sqrt[m]{a})$ هو تمديد ثنائي للحقل F وذلك لأن $\sqrt[m]{a}$ هو صفر للحدودية $x^m - a$.

نتيجة.

إذا كان الحقل K تمديداً ثنائياً للحقل F وأن $K = F(\beta)$ حيث $\beta \in K$ هو صفر للحدودية $x^m - a \in F[x]$ عندئذ فإن $\beta^m \in F$.

تعريف.

ليكن الحقل R تمديداً للحقل F . نقول عن التمديد R إنه تمديد جذري للحقل F إذا

وجدت متتالية منتهية من الحقول الجزئية في R التي يحوي كل منها F على الشكل:

$$F = R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_i \subset \cdots \subset R_n = R$$

والتي تحقق الشرط الآتي: لأجل كل $i = 1, 2, \dots, n$ فإن R_i هو تمديد ثنائي للحقل R_{i-1} ، أي أنه لأجل كل $i = 1, 2, \dots, n$ يوجد $\beta_i \in R_i$ يحقق $R_i = R_{i-1}(\beta_i)$ وأن β_i هو صفر لحدودية ثنائية فوق R_{i-1} .

تمهيدية ١٢-١-١.

ليكن الحقل R تمديداً جذرياً للحقل F . عندئذ فإن:

١ - الحقل R هو تمديد منته للحقل F .

٢ - الحقل R هو تمديد جبري للحقل F .

البرهان.

لنفرض أن الحقل R هو تمديد جذري للحقل F ، عندئذ توجد متتالية من الحقول الجزئية R_i من الحقل R على الشكل:

$$F = R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_i \subset \cdots \subset R_n = R$$

وحيث أن $R_i = R_{i-1}(\beta_i)$ وأن $\beta_i \in R_i$ هو صفر لحدودية من الشكل:

$$x^{m_i} - a \in R_{i-1}[x]$$

وذلك لأجل كل $i = 1, 2, \dots, n$.

١ - لما كان $x^{m_i} - \beta_i^{m_i} \in R_{i-1}[x]$ فإنه حسب المبرهنة (٧-٣-١٥) يكون

$[R_i : R_{i-1}] \leq m_i$ وهذا يبين أنه لأجل كل $i = 1, 2, \dots, n$ فإن R_i هو تمديد منته للحقل

R_{i-1} ومنه نجد أن:

$$\begin{aligned} [R : F] &= [R_n : R_{n-1}] \cdot [R_{n-1} : R_{n-2}] \cdots [R_2 : R_1] \cdot [R_1 : R_0] \leq \\ &\leq m_n \cdot m_{n-1} \cdots m_2 \cdot m_1 \end{aligned}$$

وهذا يبين أن الحقل R هو تمديد منته للحقل F .

٢ - ينتج من كون كل تمديد منته هو تمديد جبري. ◊

اعتماداً على ما سبق يمكننا صياغة النتيجة الآتية:

نتيجة.

- ١ - كل حقل هو تمديد جذري لنفسه.
- ٢ - كل تمديد ثنائي لحقل ما F هو تمديد جذري للحقل F .

تمهيدية ١٢-١-٢.

إذا كان الحقل M_1 تمديداً جذرياً للحقل F وكان الحقل M_2 تمديداً جذرياً للحقل M_1 ، عندئذ يكون الحقل M_2 تمديداً جذرياً للحقل F .

البرهان.

لدينا $F \subseteq M_1 \subseteq M_2$ وأن M_2 تمديد جذري للحقل M_1 و M_1 تمديد جذري للحقل F . لما كان M_1 تمديداً جذرياً للحقل F فإنه توجد متتالية منتهية من الحقول الجزئية في M_1 على الشكل:

$$F = D_0 \subset D_1 \subset D_2 \subset \dots \subset D_i \subset \dots \subset D_n = M_1$$

وأنه لأجل كل $i = 1, 2, \dots, n$ فإن D_i هو تمديد ثنائي للحقل D_{i-1} . أيضاً لما كان M_2 تمديداً جذرياً للحقل M_1 فإنه توجد متتالية منتهية من الحقول الجزئية في M_2 على الشكل:

$$M_1 = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_i \subset \dots \subset K_m = M_2$$

وأنه لأجل كل $i = 1, 2, \dots, m$ فإن K_i هو تمديد ثنائي للحقل K_{i-1} . بهذا الشكل نحصل على المتتالية المنتهية من الحقول الجزئية في M_2 الآتية:

$$F = D_0 \subset D_1 \subset \dots \subset D_n = M_1 = K_0 \subset K_1 \subset \dots \subset K_m = M_2$$

والتي تحقق الآتي: لأجل كل $i = 1, 2, \dots, n$ فإن D_i هو تمديد ثنائي للحقل D_{i-1} ولأجل كل $j = 1, 2, \dots, m$ فإن الحقل K_j هو تمديد ثنائي للحقل K_{j-1} . وهذا يبين أن الحقل M_2 هو تمديد جذري للحقل F .

مبرهنة ١٢-١-٣.

ليكن الحقل K تمديداً للحقل F و E حقلاً جزئياً في K يحوي F . إذا كان R حقلاً جزئياً في K وكان R تمديداً جذرياً للحقل F ، عندئذ يكون الحقل $E \cdot R$ تمديداً جذرياً للحقل E .

البرهان.

لدينا $F \subseteq E \subseteq K$ و $F \subseteq R \subseteq K$. لنفرض أن الحقل R تمديد جذري للحقل F ، عندئذ توجد متتالية منتهية من الحقول الجزئية في R التي كل منها يحوي F من الشكل:

$$F = R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_i \subset \cdots \subset R_n = R$$

التي تحقق الشرط الآتي: لأجل كل $i = 1, 2, \dots, n$ فإن R_i هو تمديد ثنائي للحقل R_{i-1} ، أي أنه لأجل كل $i = 1, 2, \dots, n$ يوجد $\beta_i \in R_i$ يحقق $R_i = R_{i-1}(\beta_i)$ وأن β_i هو صفر للحدودية الثنائية $x^{m_i} - a \in R_{i-1}[x]$. ومنه يكون $E \cdot R_i$ حقلاً جزئياً في K يحوي E وذلك أياً كان $i = 1, 2, \dots, n$ ، لما كان $R_{i-1} \subset R_i$ فإن $E \cdot R_{i-1} \subset E \cdot R_i$ وبالتالي نحصل على المتتالية من الحقول الجزئية من الشكل:

$$E = E \cdot F = E \cdot R_0 \subset E \cdot R_1 \subset E \cdot R_2 \subset \cdots \subset E \cdot R_n = E \cdot R$$

وأن $E \cdot R_i = E \cdot R_{i-1}(\beta_i)$ حيث $\beta_i \in R_i \subseteq E \cdot R_i$ وهذا يبين لنا أن الحقل $E \cdot R$ تمديد جذري للحقل E . ◊

تعريف.

ليكن F حقلاً $f(x) \in F[x]$. لنفرض أن K هو حقل تفريق الحدودية $f(x)$ فوق F . إذا كان K محتوياً في تمديد جذري للحقل F ، عندئذ نقول إن الحدودية $f(x)$ قابلة للحل جذرياً فوق الحقل F .

مبرهنة ١٢-١-٤.

ليكن F حقلاً $f(x) \in F[x]$. إذا كانت الحدودية $f(x)$ قابلة للحل جذرياً فوق الحقل F ، عندئذ تكون الحدودية $f(x)$ قابلة للحل جذرياً فوق أي تمديد للحقل F .

البرهان.

لنفرض أن الحدودية $f(x)$ قابلة للحل جذرياً فوق الحقل F وليكن K حقل تفريق الحدودية $f(x)$ فوق F ، عندئذ يوجد تمديد جذري R للحقل F يحوي الحقل K . لنفرض أن E تمديد ما للحقل F ، عندئذ حسب المبرهنة (٨-١-١٤) فإن $E \cdot K$ هو حقل تفريق الحدودية $f(x)$ فوق E وحسب المبرهنة (١٢-١-٣) يكون $E \cdot R$ تمديداً جذرياً للحقل E وأن $E \cdot K \subseteq E \cdot R$. ◊

تعريف.

ليكن الحقل E تمديداً للحقل F . نقول عن الحقل E إنه تمديد ثنائي للحقل F إذا كان $E = F(\beta)$ حيث β هو صفر لحدودية ثنائية درجتها عدد أولي.

تعريف.

ليكن F حقلاً. نقول عن الحقل R إنه تمديد جذري أولي للحقل F إذا وجدت متتالية منتهية من الحقول الجزئية في R التي كل منها يحوي F على الشكل:

$$F = R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_i \subset \cdots \subset R_n = R$$

والتي تحقق الشرط الآتي: لأجل كل $i = 1, 2, \dots, n$ فإن R_i هو تمديد ثنائي أولي للحقل R_{i-1} .

مبرهنة ١٢-١-٥.

ليكن F حقلاً و R تمديداً ثنائياً للحقل F . إذا كان $[R:F] > 1$ عندئذ يكون الحقل R تمديد جذري أولي للحقل F .

البرهان.

لنفرض أن R تمديد ثنائي للحقل F وأن $[R:F] > 1$ عندئذ يوجد $\beta \in R$ بحيث $R = F(\beta)$ وأن β هو صفر لحدودية ثنائية من الشكل $x^m - a \in F[x]$ حيث m عدد صحيح موجب. ومنه نجد أن $a = \beta^m \in F$. لما كان $[R:F] > 1$ فإن $m > 1$ ، لأنه إذا كان $m = 1$ نجد أن الحدودية $x - a \in F[x]$ أولية فوق F وأن β صفر لها ومنه فإن الحدودية $x - a$ هي الحدودية الأصغرية للعنصر β فوق F ومنه يكون:

$$[R:F] = [F(\beta):F] = \partial(x-a) = 1$$

وهذا غير ممكن، أي أن $m > 1$.

لنفرض أن $m = p_1 \cdot p_2 \cdots p_n$ حيث p_i أعداد أولية ليست بالضرورة مختلفة ولنفرض أن $m_i = p_1 \cdot p_2 \cdots p_i$ وذلك لأجل كل $i = 1, 2, \dots, n$. لنفرض أن $\gamma_0 = \beta^m$ ولأجل كل $i = 1, 2, \dots, n$ لنفرض أن $\gamma_i = \beta^{\frac{m}{m_i}}$ فنجد أنه لأجل كل $i = 1, 2, \dots, n$ يكون:

$$\gamma_i = \beta^{\frac{m}{m_i}} = \sqrt[m_i]{\beta^m}$$

$$\gamma_i^{p_i} = (\beta^{\frac{m}{m_i}})^{p_i} = \beta^{\frac{m \cdot p_i}{m_i}} = \beta^{\frac{m}{m_{i-1}}} = \gamma_{i-1}$$

وأنه أيضاً لأجل كل $i = 1, 2, \dots, n$ يكون:

$$x^{p_i} - a \in F[x], \quad \partial(x^{p_i} - a) = p_i$$

لنضع:

$$R_0 = F, \quad R_1 = R_0(\gamma_1) = F(\gamma_1)$$

$$R_2 = R_1(\gamma_2) = F(\gamma_1)(\gamma_2) = F(\gamma_1, \gamma_2) = F(\gamma_2)$$

وذلك لأن $\gamma_2^{p_2} = \gamma_1$ ومنه يكون $\gamma_1 = \gamma_2^{p_2} \in F(\gamma_2)$.

وهكذا لأجل كل $i = 1, 2, \dots, n$ لنضع:

$$R_i = R_{i-1}(\gamma_i) = F(\gamma_i)$$

ف نحصل على متتالية منتهية من الحقول الجزئية في R والتي كل منها يحوي F على الشكل الآتي:

$$F = R_0 \subset R_1 \subset R_2 \subset \dots \subset R_i \subset \dots \subset R_n = R$$

لنبرهن الآن على أنه لأجل كل $i = 1, 2, \dots, n$ فإن الحقل R_i هو تمديد ثنائي للحقل R_{i-1} .

لدينا R هو تمديد ثنائي للحقل F وأن $R = F(\beta)$ حيث β هو صفر للحدودية الثنائية $x^m - a \in F[x]$ حيث m عدد صحيح موجب. ومنه فإن $a = \beta^m \in F$. لما كان $R_1 = R_0(\gamma_1)$ فإنه لأجل الحدودية $x^{p_1} - a \in F[x]$ يكون:

$$p_1^{p_1} - a = (\beta^{\frac{m}{p_1}})^{p_1} - a = \beta^m - \beta^m = 0$$

أي أن $\gamma_1 \in R_1$ هو صفر للحدودية الثنائية $x^{p_1} - a \in F[x]$ التي درجتها عدد أولي، وهذا يبين أن الحقل R_1 هو تمديد ثنائي أولي للحقل $R_0 = F$.

أيضاً لما كان الحقل $R_2 = R_1(\gamma_2)$ وأن $\gamma_1 \in R_1$ نجد أن الحدودية $x^{p_2} - \gamma_1 \in R_1[x]$ وأن $\gamma_2^{p_2} - \gamma_1 = \gamma_1 - \gamma_1 = 0$ أي أن $\gamma_2 \in R_2$ هو صفر للحدودية الثنائية $x^{p_2} - \gamma_1 \in R_1[x]$ التي درجتها عدد أولي فوق R_1 وهذا يبين أن الحقل R_2 هو تمديد ثنائي أولي للحقل R_1 .

وهكذا نجد أنه لأجل كل $i = 1, 2, \dots, n$ فإن $\gamma_{i-1} \in R_{i-1}[x]$ وأن $x^{p_i} - \gamma_{i-1} \in R_{i-1}[x]$ وتحقق:

$$\gamma_i^{p_i} - \gamma_{i-1} = \gamma_{i-1} - \gamma_{i-1} = 0$$

أي أن الحقل R_i هو تمديد ثنائي أولي للحقل R_{i-1} . مما سبق نجد أن الحقل R هو تمديد جذري أولي للحقل F .

إن المبرهنة الأخيرة صحيحة لأجل التمديدات الجذرية وهذا ما تبينه لنا المبرهنة الآتية:

مبرهنة ١٢-١-٦.

ليكن F حقلاً. إذا كان الحقل R تمديداً جذرياً للحقل F وإذا كان $[R:F] > 1$ عندئذ يكون الحقل R تمديداً جذرياً أولاً للحقل F .

البرهان.

نفرض أن الحقل R تمديد جذري للحقل F ، عندئذ توجد متتالية منتهية من الحقول الجزئية في R والتي كل منها يحوي F على الشكل الآتي:

$$F = R_0 \subset R_1 \subset R_2 \subset \dots \subset R_i \subset \dots \subset R_n = R$$

التي تحقق الشرط: لأجل كل $i = 1, 2, \dots, n$ فإن الحقل R_i هو تمديد ثنائي للحقل R_{i-1} . لنفرض أن $[R:F] > 1$ ، عندئذ لأجل كل $i = 1, 2, \dots, n$ فإن الحقل R_i هو تمديد ثنائي للحقل R_{i-1} وأن $[R_i : R_{i-1}] > 1$ وحسب المبرهنة (١٢-١-٥) يكون الحقل R_i تمديداً ثنائياً أولاً للحقل R_{i-1} ، ومنه نجد أن الحقل R هو تمديد جذري أولي للحقل F .

تعريف.

ليكن الحقل E تمديداً للحقل F .

- نقول عن الحقل E إنه تمديد ثنائي غير قابل للتفريق للحقل F إذا كان $E = F(\beta)$ حيث $\beta \in E$ هو صفر لحدودية ثنائية وأولية فوق F .

- نقول عن الحقل R إنه تمديد جذري غير قابل للتفريق للحقل F إذا وجدت متتالية منتهية من الحقول الجزئية في R التي كل منها يحوي F على الشكل:

$$F = R_0 \subset R_1 \subset R_2 \subset \dots \subset R_i \subset \dots \subset R_n = R$$

والتي تحقق الشرط الآتي: لأجل كل $i = 1, 2, \dots, n$ فإن R_i هو تمديد ثنائي غير قابل للتفريق للحقل R_{i-1} .

تعريف.

ليكن الحقل E تمديداً للحقل F .

- نقول عن الحقل E إنه تمديد ثنائي أولي وغير قابل للتفريق للحقل F إذا كان $E = F(\beta)$ حيث $\beta \in E$ هو صفر لحدودية ثنائية وأولية فوق F ودرجتها عدد أولي.
- نقول عن الحقل R إنه تمديد جذري أولي غير قابل للتفريق للحقل F إذا وجدت متتالية منتهية من الحقول الجزئية في R التي كل منها يحوي F على الشكل:

$$F = R_0 \subset R_1 \subset R_2 \subset \dots \subset R_i \subset \dots \subset R_n = R$$

والتي تحقق الشرط الآتي: لأجل كل $i = 1, 2, \dots, n$ فإن R_i هو تمديد ثنائي أولي غير قابل للتفريق للحقل R_{i-1} .

مبرهنة ١٢-١-٧.

ليكن F حقلاً و R تمديداً ثنائياً غير قابل للتفريق للحقل F . إذا كان $[R:F] > 1$ عندئذ يكون الحقل R تمديداً جذرياً أولياً غير قابل للتفريق للحقل F . البرهان.

لنفرض أن R تمديد ثنائي غير قابل للتفريق للحقل F وأن $[R:F] > 1$ عندئذ يوجد $\beta \in R$ بحيث $R = F(\beta)$ وأن β هو صفر لحدودية ثنائية وأولية من الشكل $x^m - a \in F[x]$ حيث m عدد صحيح موجب. ومنه نجد أن $a = \beta^m \in F$. لما كان $[R:F] > 1$ فإن $m > 1$ ، لأنه إذا كان $m = 1$ نجد أن الحدودية $x - a \in F[x]$ أولية فوق F وأن β صفراً لها ومنه فإن الحدودية $x - a$ هي الحدودية الأصغرية للعنصر β فوق F ومنه يكون:

$$[R:F] = [F(\beta):F] = \partial(x-a) = 1$$

وهذا غير ممكن، أي أن $m > 1$.

لنفرض أن $m = p_1 \cdot p_2 \cdot \dots \cdot p_n$ حيث p_i أعداد أولية ليست بالضرورة مختلفة ولنفرض أن $m_i = p_1 \cdot p_2 \cdot \dots \cdot p_i$ وذلك لأجل كل $i = 1, 2, \dots, n$. لنفرض أن $\gamma_0 = \beta^m$ ولأجل

كل $i = 1, 2, \dots, n$ لنفرض أن $\gamma_i = \beta^{\frac{m}{m_i}}$ فنجد أنه لأجل كل $i = 1, 2, \dots, n$ يكون:

$$\gamma_i = \beta^{\frac{m}{m_i}} = \sqrt[m_i]{\beta^m}$$

$$\gamma_i^{p_i} = (\beta^{\frac{m}{m_i}})^{p_i} = \beta^{\frac{m \cdot p_i}{m_i}} = \beta^{\frac{m}{m_{i-1}}} = \gamma_{i-1}$$

وأنه أيضاً لأجل كل $i = 1, 2, \dots, n$ يكون:

$$x^{p_i} - a \in F[x], \quad \partial(x^{p_i} - a) = p_i$$

لنضع:

$$R_0 = F, \quad R_1 = R_0(\gamma_1) = F(\gamma_1)$$

$$R_2 = R_1(\gamma_2) = F(\gamma_1)(\gamma_2) = F(\gamma_1, \gamma_2) = F(\gamma_2)$$

وذلك لأن $\gamma_2^{p_2} = \gamma_1$ ومنه يكون $\gamma_1 = \gamma_2^{p_2} \in F(\gamma_2)$.

وهكذا لأجل كل $i = 1, 2, \dots, n$ لنضع:

$$R_i = R_{i-1}(\gamma_i) = F(\gamma_i)$$

فحصل على متتالية منتهية من الحقول الجزئية في R والتي كل منها يحوي F على الشكل الآتي:

$$F = R_0 \subset R_1 \subset R_2 \subset \dots \subset R_i \subset \dots \subset R_n = R$$

لنبرهن الآن على أنه لأجل كل $i = 1, 2, \dots, n$ فإن الحقل R_i هو تمديد ثنائي أولي للحقل R_{i-1} .

لدينا R هو تمديد ثنائي للحقل F وأن $R = F(\beta)$ حيث β هو صفر للحدودية الثنائية

$x^m - a \in F[x]$ حيث m عدد صحيح موجب. ومنه فإن $a = \beta^m \in F$. لما كان

$R_1 = R_0(\gamma_1)$ فإنه لأجل الحدودية $x^{p_1} - a \in F[x]$ يكون:

$$p_1^{p_1} - a = (\beta^{\frac{m}{m_1}})^{p_1} - a = \beta^m - \beta^m = 0$$

أي أن $\gamma_1 \in R_1$ هو صفر لحدودية ثنائية درجتها عدد أولي $x^{p_1} - a \in F[x]$ وهذا يبين

أن الحقل R_1 هو تمديد ثنائي أولي للحقل $R_0 = F$.

أيضاً لما كان الحقل $R_2 = R_1(\gamma_2)$ وأن $\gamma_1 \in R_1$ نجد أن الحدودية $x^{p_2} - \gamma_1 \in R_1[x]$

وأن $0 = \gamma_1 - \gamma_1 = \gamma_2^{p_2} - \gamma_1$ ، أي أن $\gamma_2 \in R_2$ هو صفر لحدودية ثنائية درجتها عدد أولي $\gamma_1 - \gamma_1 \in R_1[x]$ فوق R_1 وهذا يبين أن الحقل R_2 هو تمديد ثنائي أولي للحقل R_1 . وهكذا نجد أنه لأجل كل $i = 1, 2, \dots, n$ فإن $\gamma_{i-1} \in R_{i-1}$ وأن:

$$x^{p_i} - \gamma_{i-1} \in R_{i-1}[x]$$

وتحقق:

$$\gamma_i^{p_i} - \gamma_{i-1} = \gamma_{i-1} - \gamma_{i-1} = 0$$

أي أن الحقل R_i هو تمديد ثنائي أولي للحقل R_{i-1} .

من جهة أخرى، لما كانت الحدودية $x^m - \beta^m \in F[x]$ أولية فوق الحقل F وأن β صفر لها نجد أن $x^m - \beta^m$ هي الحدودية الأصغرية للعنصر β فوق F وهذا يبين أن:

$$[R:F] = [F(\beta):F] = \partial(x^m - \beta^m) = m$$

لأجل كل $i = 1, 2, \dots, n$ ، لنفرض أن $g_i(x) = x^{p_i} - \gamma_i^{p_i}$ ، لما كان $\gamma_i^{p_i} = \gamma_{i-1} \in R_{i-1}$ نجد أن $g_i(x) \in R_{i-1}[x]$ وأن γ_i صفر للحدودية $g_i(x)$ وحسب المبرهنة (٣-٣-١٥) نجد أن:

$$[R_{i-1}(\gamma_i):R_{i-1}] \leq \partial g_i(x) = p_i$$

وهذا يبين أنه لأجل كل $i = 1, 2, \dots, n$ فإن $[R_{i-1}(\gamma_i):R_{i-1}] \leq p_i$ وهكذا نجد أن:

$$m = [R:F] = [R_n:R_{n-1}] \cdot [R_{n-1}:R_{n-2}] \cdots [R_2:R_1] \cdot [R_1:R_0] \leq$$

$$\leq p_n \cdot p_{n-1} \cdots p_2 \cdot p_1 = m$$

ومنه نجد أن $[R_i:R_{i-1}] = p_i$ وذلك لأجل كل $i = 1, 2, \dots, n$ ، وحسب المبرهنة (٣-٣-١٥)

نجد أن الحدودية $g_i(x)$ أولية فوق الحقل R_{i-1} وذلك لأجل كل i . وحسب

التعريف نجد أن الحقل R_i هو تمديد ثنائي أولي غير قابل للتفريق للحقل R_{i-1} . وهكذا

نجد أن الحقل R تمديد جذري أولي غير قابل للتفريق للحقل F . ◊

مبرهنة ١٢-١-٨.

ليكن F حقلاً. إذا كان الحقل R تمديداً جذرياً غير قابل للتفريق للحقل F وإذا كان

$[R:F] > 1$ عندئذ يكون الحقل R تمديداً جذرياً أولاً غير قابل للتفريق للحقل F .

البرهان.

لنفرض أن الحقل R تمديد جذري غير قابل للتفريق للحقل F ، عندئذ توجد متتالية منتهية من الحقول الجزئية في R والتي كل منها يحوي F على الشكل الآتي:

$$F = R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_i \subset \cdots \subset R_n = R$$

التي تحقق الشرط: لأجل كل $i = 1, 2, \dots, n$ فإن الحقل R_i هو تمديد ثنائي غير قابل للتفريق للحقل R_{i-1} . لنفرض أن $[R:F] > 1$ عندئذ لأجل كل $i = 1, 2, \dots, n$ فإن الحقل R_i هو تمديد ثنائي غير قابل للتفريق للحقل R_{i-1} وأن $[R_i : R_{i-1}] > 1$ وحسب المبرهنة (١٢-١-٧) يكون الحقل R_i تمديداً ثنائياً أولاً غير قابل للتفريق للحقل R_{i-1} ، ومنه نجد أن الحقل R هو تمديد جذري أولي غير قابل للتفريق للحقل F .

مبرهنة ١٢-١-٩.

ليكن F عدداً صحيحاً موجباً و ξ جذراً أولياً للواحد من المرتبة n . إذا كان الحقل $Q(\mu_n)$ تمديداً جذرياً غير قابل للتفريق للحقل Q ، عندئذ أي عدد أولي $q > 2$ يقسم $\varphi(n)$ فإنه يقسم n .

البرهان.

لنفرض أن الحقل $Q(\mu_n)$ تمديد جذري غير قابل للتفريق للحقل Q . لدينا حسب المبرهنة (١١-٢-٤) أن $Q(\mu_n, \xi) = Q(\xi)$ حقل تفريق فوق Q وأن:

$$[Q(\mu_n, \xi) : Q] = \varphi(n) > 1$$

وحسب المبرهنة (١٢-١-٦) يكون الحقل $Q(\mu_n)$ تمديداً جذرياً أولاً للحقل Q . ومنه توجد متتالية منتهية من الحقول الجزئية في $Q(\mu_n)$ التي كل منها يحوي Q على الشكل

$$Q = R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_j \subset \cdots \subset R_m = Q(\mu_n)$$

حيث أنه لأجل كل $j = 1, 2, \dots, m$ فإن R_j هو تمديد ثنائي غير قابل للتفريق للحقل R_{j-1} درجته عدد أولي وليكن p_j . عندئذ يكون $R_j = R_{j-1}(\beta_j)$ حيث $\beta_j \in R_j$ وأن $\beta_j^{p_j} \in R_{j-1}$ ، كما أن الحدودية $h_j(x) = x^{p_j} - \beta_j$ هي حدودية أولية فوق الحقل R_{j-1} وذلك لأجل كل $j = 1, 2, \dots, m$ ، ومنه يكون:

$$\varphi(n) = [Q(\mu_n) : Q] = p_1 \cdot p_2 \cdots p_m$$

ليكن $q > 2$ عدداً أولياً يقسم $\varphi(n)$ ، عندئذ يكون $q = p_k$ حيث $1 \leq k \leq m$ ، ولما كان

$Q(\mu_n)$ حقل تفريق فوق Q وأن $Q \subset R_{k-1} \subset Q(\mu_n)$ فإنه حسب التمهيدية (٤-٢-٢-٩) يكون $Q(\mu_n)$ حقل تفريق فوق R_{k-1} وحسب المبرهنة (٩-٢-١) فإن الحدودية $h_k(x)$ تتفرق فوق الحقل $Q(\mu_n)$ ، ومنه فإن الحقل $Q(\mu_n)$ يحوي جذراً أولياً للواحد من المرتبة q وليكن ε وذلك لأن الحدودية $\Phi_q(x)$ تتفرق فوق الحقل $Q(\mu_n)$. لنفرض جدلاً أن العدد q لا يقسم n ، عندئذ لما كانت الحدودية $\Phi_q(x)$ هي الحدودية الأصغرية للعنصر ε فوق الحقل $Q(\mu_n)$ وذلك حسب المبرهنة (١١-٢-٣)، نجد أن الحدودية $\Phi_q(x)$ أولية فوق الحقل $Q(\mu_n)$. أصبح لدينا الحدودية $\Phi_q(x)$ أولية فوق الحقل $Q(\mu_n)$ وتتفرق فوق الحقل $Q(\mu_n)$ وهذا يبين أن $\partial\Phi_q(x) = 1$ ، وحسب المبرهنة (١١-٢-٦) نجد أن $q = 2$ وهذا غير ممكن فرضاً، ومنه فإن q يقسم العدد n .

مبرهنة ١٠-١-١٢.

ليكن الحقل K تمديداً دائرياً للحقل F درجته p حيث p عدد أولي. وليكن $\theta \in K$ $\theta \neq 0$ بحيث $\theta \notin F$. لنفرض أن ξ جذر أولي للواحد من المرتبة p وإذا كان $\xi \in F$ ، عندئذ يوجد $1 \leq t \leq p-1$ بحيث يكون:

$$١ - \text{الحقل } K = F(\gamma) \text{ حيث } (\xi^t, \theta) \gamma = \gamma.$$

$$٢ - \gamma^p \in F.$$

$$٣ - \text{الحدودية } h(x) = x^p - \gamma^p \in F[x] \text{ أولية فوق } F.$$

$$٤ - \text{الحقل } K \text{ تمديد ثنائي غير قابل للتفريق للحقل } F.$$

البرهان.

$$(١) \text{ و } (٢) \text{ و } (٣) \text{ حسب المبرهنة (١١-٤-٤).}$$

٤ - وجدنا حسب (٣) أن الحدودية $h(x) = x^p - \gamma^p \in F[x]$ هي حدودية ثنائية وأولية فوق F وأن γ صفر لها، وحسب (١) لدينا $K = F(\gamma)$ ومنه نجد أن K هو تمديد ثنائي غير قابل للتفريق للحقل F . ◊

مبرهنة ١٢-١-١١.

ليكن الحقل K تمديداً دائرياً للحقل F درجته n . وليكن $\theta \in K$ و $\theta \neq 0$. لنفرض أن ξ جذر أولي للواحد من المرتبة n وأن $\xi \in F$ ، عندئذ يوجد $1 \leq k \leq n-1$ بحيث يكون:

$$١ - \text{الحقل } K = F(\beta) \text{ حيث } \beta = (\xi, \theta^k).$$

$$٢ - \beta^n \in F.$$

$$٣ - \text{الحدودية } h(x) = x^n - \beta^n \in F[x] \text{ أولية فوق } F.$$

$$٤ - \text{الحقل } K \text{ تمديد ثنائي غير قابل للتفريق للحقل } F.$$

البرهان.

نلاحظ أنه إذا كان $n=1$ فإن $K=F$ وأن $\theta \in F$ ومنه $\beta = (\xi, \theta) \in F$ وبالتالي الحدودية $h(x) = x - \beta \in F[x]$ أولية فوق F ومنه فإن الحقل K تمديد ثنائي غير قابل للتفريق للحقل F .

١ - من أجل $n > 1$. لما كان التمديد K للحقل F دائرياً فإن K هو حقل تفريق فوق F وحسب المبرهنة (٩-٢-١) يكون:

$$(G(K/F):1) = [K:F] = n$$

أيضاً لما كان التمديد K للحقل F دائرياً فإن الزمرة $G(K/F)$ تكون دوارة. لنفرض أن:

$$G(K/F) = \langle \sigma \rangle$$

حيث $\sigma \in G(K/F)$ وأن $o(\sigma) = n$. لنبرهن على أن $\beta = (\xi, \theta^k) \neq 0$ لأجل عدد ما $1 \leq k \leq n-1$. لنفرض جـداً أن $(\xi, \theta^i) = 0$ وذلك أيأ كان $1 \leq i \leq n-1$ ، فنجد:

$$(\xi, \theta^i) = \theta^i + \xi \cdot \sigma(\theta^i) + \xi^2 \cdot \sigma^2(\theta^i) + \dots + \xi^{n-1} \cdot \sigma^{n-1}(\theta^i) =$$

$$= \theta^i + \xi \cdot [\sigma(\theta)]^i + \xi^2 \cdot [\sigma^2(\theta)]^i + \dots + \xi^{n-1} \cdot [\sigma^{n-1}(\theta)]^i = 0$$

ولما كان:

$$(\xi, 1) = 1 + \xi + \xi^2 + \dots + \xi^{n-1} = \frac{\xi^n - 1}{\xi - 1}$$

نحصل على جملة المعادلات الآتية:

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \theta & \sigma(\theta) & \sigma^2(\theta) & \cdots & \sigma^{n-1}(\theta) \\ \theta^2 & [\sigma(\theta)]^2 & [\sigma^2(\theta)]^2 & \cdots & [\sigma^{n-1}(\theta)]^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \theta^{n-1} & [\sigma(\theta)]^{n-1} & [\sigma^2(\theta)]^{n-1} & \cdots & [\sigma^{n-1}(\theta)]^{n-1} \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

والتي تملك حلاً غير صفري هو $(1, \xi, \xi^2, \dots, \xi^{n-1})$ ولذلك فإن محدد المصفوفة المربعة $A = [\sigma^i(\theta)]_{nn}^j$ من المرتبة $n \times n$ ، حيث $i, j = 0, 1, 2, \dots, n-1$ يساوي الصفر وهذا يتحقق فقط عندما يوجد i, j بحيث يكون $\sigma^i(\theta) = \sigma^j(\theta)$. ولما كانت عناصر الزمرة $G(K/F)$ تتعين بمعرفة القيمة $\sigma(\theta)$ نحصل على تناقض. وهذا يبين أنه يوجد $1 \leq k \leq n-1$ بحيث يكون $(\xi, \theta^k) \neq 0$. لنضع $\beta = (\xi, \theta^k)$ فنجد حسب المبرهنة (١١-٤-٢) أن $K = F(\beta)$.

٢ - حسب المبرهنة (١١-٤-٤) نجد أن $\beta^n \in F$.

٣ - أيضاً حسب المبرهنة (١١-٤-٤) تكون الحدودية:

$$h(x) = x^n - \beta^n \in F[x]$$

أولية فوق F .

٤ - حسب (٣) نجد أن الحقل K تمديد ثنائي غير قابل للتفريق للحقل F .

مبرهنة ١٢-١-١٢.

ليكن الحقل K تمديداً للحقل F درجته n . لنفرض أن ξ جذر أولي للواحد من المرتبة n ، عندئذ الشروط الآتية متكافئة:

١ - الحقل K هو تمديد دائري للحقل F .

٢ - الحقل K تمديد ثنائي غير قابل للتفريق للحقل F .

البرهان.

(1) $\Leftrightarrow$ (2). ينتج مباشرة من المبرهنة (١٢-٢-١١).

(1) $\Leftrightarrow$ (2). لنفرض أن $\gamma \in K$ بحيث $K = F(\gamma)$ وأن $\gamma^m \in F$ عندئذ تكون الحدودية $g(x) = x^m - \gamma^m \in F[x]$ أولية فوق F وذلك لأن الحقل K تمديد ثنائي

غير قابل للتفريق للحقل F . أصبح لدينا $g(x)$ هي الحدودية الأصغرية للعنصر γ ومنه يكون:

$$m = \partial g(x) = [F(\gamma) : F] = [K : F] = n$$

وحسب المبرهنة (١١-٤-٣) نجد أن الحقل K هو تمديد دائري للحقل F . ◊

مبرهنة ١٢-١-١٣.

ليكن p عدداً أولياً و ξ جذراً أولياً للواحد من المرتبة p ، عندئذ فإن الحقل $Q(\mu_{p-1}, \xi)$ هو تمديد ثنائي غير قابل للتفريق للحقل $Q(\mu_{p-1})$ وأن:

$$[Q(\mu_{p-1}, \xi) : Q(\mu_{p-1})] = p - 1$$

البرهان.

لما كان العددين $p, p-1$ أوليين فيما بينهما فإنه حسب المبرهنة (١١-٢-٥) فإن $\Phi_p(x)$ هي حدودية أولية فوق الحقل $Q(\mu_{p-1})$. من جهة أخرى، لدينا حسب المبرهنة (١١-٣-٨) أن:

$$G(Q(\mu_{p-1}, \xi)/Q(\mu_{p-1})) \cong G(Q(\xi)/Q)$$

وذلك لأن $Q(\mu_p) = Q(\xi)$ حسب التمهيدية (١١-١-٢). كما أن:

$$[Q(\mu_{p-1}, \xi) : Q(\mu_{p-1})] = \varphi(p) = p - 1$$

وحسب المبرهنة (١١-٣-٧) فإن الزمرة $G(K/F)$ دوارة ومنه نجد أن $Q(\mu_{p-1}, \xi)$ هو تمديد دائري للحقل $Q(\mu_{p-1})$ وحسب المبرهنة (١١-٤-٦) نجد أن الحقل $Q(\mu_{p-1}, \xi)$ هو تمديد ثنائي غير قابل للتفريق للحقل $Q(\mu_{p-1})$. ◊

مثال.

ليكن ξ جذراً أولياً للواحد من المرتبة 7. أثبت أن الحقل $Q(\xi)$ هو تمديد غالوا للحقل Q . ثم أوجد الحقول الجزئية في $Q(\xi)$ التي تحوي Q .

الحل.

لما كان العدد 7 أولياً، عندئذ حسب المبرهنة (١١-٢-٦) فإن:

$$\Phi_7(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

وحسب المبرهنة (١١-٢-٣) فإن $\Phi_7(x)$ هي الحدودية الأصغرية للعنصر ξ فوق Q وأن $6 = \varphi(7) = [Q(\xi):Q]$ وحسب المبرهنة (١١-٢-٧) فإن الحقل $Q(\mu_7)$ هو تمديد غالوا للحقل Q وذلك لأن $Q(\mu_7) = Q(\xi)$ اعتماداً على التمهيدية (١١-١-٢). من جهة أخرى، لدينا حسب المبرهنة (١١-٣-٨) أن الزمرة $G(Q(\xi)/Q)$ دوارة وأن مرتبتها تساوي 6. لنفرض أن $\langle \sigma \rangle = G(Q(\xi)/Q)$. لما كانت الزمرة $G(Q(\xi)/Q)$ مرتبتها 6 فإنها تحوي:

- زمرة جزئية واحدة فقط مرتبتها 2 هي $H_1 = \langle \sigma^3 \rangle$.

- زمرة جزئية واحدة فقط مرتبتها 3 هي $H_2 = \langle \sigma^2 \rangle$.

ولما كان الحقل $Q(\xi)$ تمديد غالوا للحقل Q فإنه حسب المبرهنة (٩-١-١) نجد أن كلاً من $F(H_1)$, $F(H_2)$ هو حقل جزئي من الحقل $Q(\xi)$ يحوي Q وحسب المبرهنة (٩-١-٤) نجد أن:

$$[Q(\xi):F(H_1)] = (H_1:1) = 2$$

ولما كان $Q \subseteq F(H_1) \subseteq Q(\xi)$ نجد أن:

$$[F(H_1):Q] = \frac{[Q(\xi):Q]}{[Q(\xi):F(H_1)]} = \frac{6}{2} = 3$$

أيضاً حسب المبرهنة (٩-١-٤) نجد أن:

$$[Q(\xi):F(H_2)] = (H_2:1) = 3$$

ولما كان $Q \subseteq F(H_2) \subseteq Q(\xi)$ نجد أن:

$$[F(H_2):Q] = \frac{[Q(\xi):Q]}{[Q(\xi):F(H_2)]} = \frac{6}{3} = 2$$

تطبيق.

لنفرض أن $p(x) = x^5 - 2 \in Q[x]$. المطلوب:

١ - أوجد حقل تفريق الحدودية $p(x)$ فوق Q ، ثم أوجد درجته.

أثبت أن هذا الحقل هو تمديد غالوا للحقل Q .

الحل.

واضح أن الحدودية $p(x) = x^5 - 2 \in Q[x]$ أولية فوق Q وذلك حسب معيار إيزنشتاين لأجل العدد الأولي $p = 2$.

نلاحظ أن العدد الحقيقي $\sqrt[5]{2}$ هو صفر للحدودية $p(x)$. لنفرض أن ξ جذر أولي للواحد من المرتبة 5، فنجد أن مجموعة أصفار الحدودية $p(x)$ هي:

$$\sqrt[5]{2} \cdot \xi^i, \quad i = 0, 1, 2, 3$$

لنفرض أن $K = Q(\sqrt[5]{2}, \xi)$ فنجد أن K هو حقل تفريق الحدودية $p(x)$ فوق Q وذلك لأنه أصغر حقل يحوي كل من Q وجميع أصفار الحدودية $p(x)$. لنضع:

$$E_1 = Q(\sqrt[5]{2}), \quad E_2 = Q(\xi)$$

لما كانت الحدودية $p(x) \in Q[x]$ أولية فوق Q وأن $\sqrt[5]{2}$ صفر لها، نجد أن $p(x)$ هي الحدودية الأصغرية للعنصر $\sqrt[5]{2}$ فوق Q ومنه فإن:

$$[Q(\sqrt[5]{2}) : Q] = \partial p(x) = 5$$

من جهة أخرى، لما كان ξ جذراً أولياً للواحد من المرتبة 5 فإنه حسب المبرهنة (١١-٢-٣) يكون:

$$[Q(\xi) : Q] = \varphi(5) = 4$$

ولما كان العددا 4,5 أوليين فيما بينهما فإنه حسب المبرهنة (١١-٢-٤) يكون $E_1 \cap E_2 = Q$ وحسب المبرهنة (٩-٢-٨) نجد أن:

$$[K : F] = [Q(\sqrt[5]{2}) : Q] \cdot [Q(\xi) : Q] = 20$$

من جهة أخرى، لدينا حسب المبرهنة (١١-٣-٨) أن $E_2 = Q(\xi) = Q(\mu_5)$ هو حقل تفريق الحدودية $\Phi_5(x)$ فوق Q وحسب المبرهنة (٩-٢-١) فإن $E_2 = Q(\xi)$ هو تمديد غالوا للحقل Q وأن:

$$G(Q(\xi)/Q) \cong (Z/5Z)^\times$$

هي زمرة دوارة مرتبتها 4.

٢ - لما كان الحقل $K = Q(\sqrt[5]{2}, \xi)$ هو حقل تفريق الحدودية الأولية $p(x)$ فوق Q فإنه حسب المبرهنة (٩-٢-١) يكون الحقل K تمديد غالوا للحقل Q . من جهة أخرى، لدينا:

$$E_1 = Q(\sqrt[5]{2}) \subseteq Q(\sqrt[5]{2}, \xi) = K$$

أي أن K هو تمديد للحقل E_1 ، فضلاً عن ذلك فإن K هو حقل تفريق الحدودية:

$$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$$

فوق الحقل E_1 وذلك حسب المبرهنة (١١-٣-٨) وأن:

$$G(K/E_1) \cong G(Q(\xi)/Q)$$

كما أن $[K : E_1] = \varphi(5) = 4$ ، ولما كانت الزمرة $G(Q(\xi)/Q)$ دوارة نجد أن الزمرة $G(K/E_1)$ دوارة.

١٢ - ٢. طرق حل بعض المعادلات.

الحدودية التربيعية.

الحدودية التربيعية هي من الشكل $f(x) = x^2 - ax + b$ حيث $a, b \in Q$ ، أي أن $f(x) \in Q[x]$. إن أصفار الحدودية $f(x)$ هي العناصر α التي تنتمي إلى حقل ما وتحقق الشرط $f(\alpha) = 0$.

لما كانت الحدودية $f(x)$ من الدرجة الثانية فإنها تملك صفرين، لنفرض أنهما α_1, α_2 ومنه فإن $f(x) = (x - \alpha_1) \cdot (x - \alpha_2)$ ، حيث $\alpha_1 + \alpha_2 = a$ ، $\alpha_1 \cdot \alpha_2 = b$. إن الصفرين α_1, α_2 يحققان العلاقة:

$$\alpha_1, \alpha_2 = \frac{a \pm \sqrt{a^2 - 4b}}{2}$$

لنفرض أن:

$$\alpha_1 = \frac{a + \sqrt{a^2 - 4b}}{2}, \quad \alpha_2 = \frac{a - \sqrt{a^2 - 4b}}{2}$$

سوف نجري تغييراً للمتحول x . لنفرض أن $x = y + \frac{a}{2}$ ، بالتعويض في الحدودية $f(x)$ نحصل على الحدودية الآتية $g(y) = y^2 + p$ بالمتحول y ، حيث $p = -\frac{a^2}{4} + b$ ، إن أصفار الحدودية $g(y)$ هي:

$$\beta_1, \beta_2 = \pm \sqrt{-p} = \pm \frac{\sqrt{a^2 - 4b}}{2}$$

ف نجد أن:

$$\alpha_i = \frac{a}{2} \pm \frac{\sqrt{a^2 - 4b}}{2} = \frac{a}{2} + \beta_i$$

ومنه فإن $\beta_i = \alpha_i - \frac{a}{2}$ ، $i = 1, 2$. إن الحدودية $f(x)$ في هذه الحالة تحقق:

$$f(x) = \left(x - \frac{a + \sqrt{a^2 - 4b}}{2}\right) \cdot \left(x - \frac{a - \sqrt{a^2 - 4b}}{2}\right)$$

سوف نرمز للمقدار $a^2 - 4b$ بالشكل $disc(f) = a^2 - 4b = (\alpha_1 - \alpha_2)^2$ ومنه في

حال كون $\alpha_1 = \alpha_2 = \frac{a}{2}$ يكون $disc(f) = 0$ وأن $\alpha_1 = \alpha_2 = \frac{a}{2}$ وللحدودية في هذه الحالة

صفر مضاعف هو $\alpha_1 = \alpha_2 = \frac{a}{2}$ وبالتالي يكون $f(x) = (x - \frac{a}{2})^2$.

الحدودية التكعيبة.

الحدودية التكعيبة هي من الشكل $f(x) = x^3 - ax^2 + bx - c$ حيث $a, b, c \in Q$ ،

أي أن $f(x) \in Q[x]$. إن الحدودية $f(x)$ تملك ثلاثة أصفار لنرمز لها $\alpha_1, \alpha_2, \alpha_3$.

لإيجاد العلاقات التي تعطي الأصفار $\alpha_i : i = 1, 2, 3$ سوف نتبع الخطوات الآتية:

نجري تغييراً للمتحول على الشكل الآتي: لنفرض أن $y = x - \frac{a}{3}$ فنحصل على حدودية

بالمتحول y هي:

$$g(y) = y^3 + py + q \in Q[y]$$

حيث:

$$p = -\frac{a^2}{3} + b, \quad q = -\frac{2a^3}{27} + \frac{ab}{3} - c$$

لما كانت الحدودية $g(y)$ تملك ثلاثة أصفار لنرمز لها $\beta_1, \beta_2, \beta_3$ فنجد أن:

$$\beta_i = \alpha_i - \frac{a}{3} \quad : i = 1, 2, 3$$

لنفرض أن $y = \frac{1}{3}(z - \frac{3p}{z})$ حيث $z \neq 0$. بالتعويض في الحدودية $g(y)$ نجد أن:

$$\frac{z^6 + 27qz^3 - 27p^3}{z^6}$$

لإيجاد أصفار الحدودية $g(y)$ لنوجد أولاً أصفار الحدودية:

$$r(z) = z^6 + 27qz^3 - 27p^3$$

إن $r(z)$ هي حدودية تربيعية بالمتحول z^3 وبالتالي فإن أصفار الحدودية $r(z)$ هي ذاتها

أصفار الحدودية:

$$z^3 - 27\left(-\frac{q}{2} \pm \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}\right)$$

والتي هي:

$$\lambda_1, \lambda_2 = 3 \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

ومنه نجد أن $\lambda_1 \cdot \lambda_2 = -3p$ وبحسب التعريف فإن الجذور التكعيبية للواحد هي أصفار الحدودية $x^3 - 1 = (x-1)(x^2 + x + 1)$. ولما كانت أصفار الحدودية $x^2 + x + 1$ هي $w, w^2 = \frac{-1 \pm i\sqrt{3}}{2}$ حيث $w = \frac{-1 + i\sqrt{3}}{2}$ نجد أن أصفار الحدودية $r(z)$ هي:

$$\lambda_1, w \cdot \lambda_1, w^2 \cdot \lambda_1, \lambda_2, w \cdot \lambda_2, w^2 \cdot \lambda_2$$

ومنه نجد أن للحدودية $g(y)$ ستة أصفار وهذا غير ممكن. لما كان $\lambda_1 \cdot \lambda_2 = -3p$ نجد أن:

$$\frac{1}{3}(\lambda_1 - \frac{3p}{\lambda_1}) = \frac{\lambda_1 + \lambda_2}{3} = \frac{1}{3}(\lambda_2 - \frac{3p}{\lambda_2})$$

$$\frac{1}{3}(w^2 \cdot \lambda_1 - \frac{3p}{w^2 \cdot \lambda_1}) = \frac{w^2 \cdot \lambda_1 + w \cdot \lambda_2}{3} = \frac{1}{3}(w \cdot \lambda_2 - \frac{3p}{w \cdot \lambda_2})$$

$$\frac{1}{3}(w \cdot \lambda_1 - \frac{3p}{w \cdot \lambda_1}) = \frac{w \cdot \lambda_1 + w^2 \cdot \lambda_2}{3} = \frac{1}{3}(w^2 \cdot \lambda_2 - \frac{3p}{w^2 \cdot \lambda_2})$$

ومنه نجد أن الأصفار الثلاثة للحدودية $g(y)$ هي:

$$\beta_1 = \frac{\lambda_1 + \lambda_2}{3}$$

$$\beta_2 = \frac{w^2 \cdot \lambda_1 + w \cdot \lambda_2}{3}$$

$$\beta_3 = \frac{w \cdot \lambda_1 + w^2 \cdot \lambda_2}{3}$$

بتعويض قيم λ_1, λ_2 نجد أن أصفار الحدودية $f(x)$ هي:

$$\beta_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

$$\beta_2 = w^2 \cdot \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + w \cdot \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

$$\beta_3 = w \cdot \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + w^2 \cdot \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

مثال.

لنوجد أصفار الحدودية $g(y) = y^3 + py + q \in Q[y]$ وذلك من أجل $p = 3$ و $q = 4$. تصبح الحدودية $g(y)$ على الشكل $g(y) = y^3 + 3y + 4$. إن أصفار الحدودية $g(y)$ هي:

$$\beta_1 = \sqrt[3]{-2 + \sqrt{5}} + \sqrt[3]{-2 - \sqrt{5}}$$

$$\beta_2 = w^2 \cdot \sqrt[3]{-2 + \sqrt{5}} + w \cdot \sqrt[3]{-2 - \sqrt{5}}$$

$$\beta_3 = w \cdot \sqrt[3]{-2 + \sqrt{5}} + w^2 \cdot \sqrt[3]{-2 - \sqrt{5}}$$

لما كانت أصفار الحدودية $x^2 - 5$ هي $\sqrt{5}, -\sqrt{5}$ وأن أصفار الحدودية $x^3 + 2 - \sqrt{5}$ هي $\sqrt[3]{-2 + \sqrt{5}}, \sqrt[3]{-2 - \sqrt{5}}, \sqrt[3]{-2 - \sqrt{5}}$ نأخذ $\sqrt[3]{-2 + \sqrt{5}}, \sqrt[3]{-2 - \sqrt{5}}$ بحيث يكونان عددين حقيقيين موجبين، لأجل ذلك نفرض أن:

$$\sqrt[3]{-2 - \sqrt{5}} = -\sqrt[3]{-2 + \sqrt{5}}$$

ف نجد أن:

$$\sqrt[3]{-2 + \sqrt{5}} = \frac{-1 + \sqrt{5}}{2}, \quad \sqrt[3]{-2 - \sqrt{5}} = \frac{1 + \sqrt{5}}{2}$$

ومنه يكون $\beta_1 = -1, \beta_2, \beta_3 = \frac{1 \pm i \cdot \sqrt{15}}{2}$. لما كان -1 صفراً للحدودية $g(y)$

نجد أن $g(y) = (y + 1)(y^2 - y + 4)$.

مثال.

أوجد أصفار الحدودية $g(y) = y^3 - 6y - 4$.

نلاحظ مباشرة أن الحدودية $g(y)$ تملك صفراً حقيقياً هو -2 .

إن الحدودية $g(y)$ تملك ثلاثة أصفار هي $\beta_1, \beta_2, \beta_3$ وهذه الأصفار تعطى من

خلال العلاقات الآتية:

$$\beta_1 = \sqrt[3]{2+2i} + \sqrt[3]{2-2i}$$

$$\beta_2 = w^2 \cdot \sqrt[3]{2+2i} + w \cdot \sqrt[3]{2-2i}$$

$$\beta_3 = w \cdot \sqrt[3]{2+2i} + w^2 \cdot \sqrt[3]{2-2i}$$

نلاحظ هنا أن الأصفار الثلاثة السابقة هي أصفار حقيقية وذلك لأن:

$$\sqrt[3]{2+2i} = -1+i, \quad \sqrt[3]{2-2i} = -1-i$$

ومنه يكون $\beta_1 = -2, \beta_2 = 1+\sqrt{3}, \beta_3 = 1-\sqrt{3}$

ومنه فإن الحدودية $g(y)$ تملك تفريقاً على الشكل الآتي:

$$g(y) = (y+2)(y^2-2y-2)$$

الحدودية من الدرجة الرابعة.

إن الحدودية من الدرجة الرابعة هي من الشكل:

$$f(x) = x^4 - ax^3 + bx^3 - cx + d$$

حيث $a, b, c, d \in Q$ ، أي أن $f(x) \in Q[x]$. إن الحدودية $f(x)$ تملك أربعة أصفار،

لنرمز لها $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. نجري تغييراً على المتحول بالشكل الآتي: لنفرض أن:

$$x = y + \frac{a}{4}$$

فنحصل على الحدودية الآتية:

$$g(y) = y^4 + py^2 + qy + r$$

حيث:

$$p = \frac{-3a^2}{8} + b, \quad q = \frac{-a^3}{8} + \frac{ab}{2} - c$$

$$r = \frac{-3a^4}{256} + \frac{a^2b}{16} - \frac{ac}{4} + d$$

لنرمز لأصفار الحدودية $g(y)$ بالشكل $\beta_1, \beta_2, \beta_3, \beta_4$ حيث:

$$\beta_i = \alpha_i - \frac{a}{4}$$

لإيجاد أصفار الحدودية $g(y)$ سوف نقوم بالخطوات الآتية:
 لنفرض أن $g(y) = 0$ فيكون $y^4 = -py^2 - qy - r$ ليكن $\mathcal{G}_1$ عدداً ما بحيث
 $\mathcal{G}_1 \neq p$. نضيف إلى طرفي المعادلة السابقة المقدار $\mathcal{G}_1 \cdot y^2 + \frac{\mathcal{G}_1}{4}$ فنحصل على
 المعادلة الآتية:

$$y^4 = +\mathcal{G}_1 \cdot y^2 + \frac{\mathcal{G}_1}{4} = -py^2 - qy - r + \mathcal{G}_1 \cdot y^2 + \frac{\mathcal{G}_1^2}{4}$$

ونجد أن:

$$(y^2 + \frac{\mathcal{G}_1}{2})^2 = (\mathcal{G}_1 - p)y^2 - qy + \frac{\mathcal{G}_1^2 - 4r}{4}$$

$$(y^2 + \frac{\mathcal{G}_1}{2})^2 = (\mathcal{G}_1 - p)(y^2 - \frac{q}{\mathcal{G}_1 - p}y + \frac{\mathcal{G}_1^2 - 4r}{4(\mathcal{G}_1 - p)})$$

وعلى اعتبار أن:

$$y^2 - \frac{q}{\mathcal{G}_1 - p}y + \frac{\mathcal{G}_1^2 - 4r}{4(\mathcal{G}_1 - p)}$$

حدودية بالمتحول y فإن المعادلة السابقة تكون مربعة إذا كان:

$$\text{disc}(y^2 - \frac{q}{\mathcal{G}_1 - p}y + \frac{\mathcal{G}_1^2 - 4r}{4(\mathcal{G}_1 - p)}) = 0$$

أي إذا كان:

$$(\frac{q}{\mathcal{G}_1 - p})^2 - 4(\frac{\mathcal{G}_1^2 - 4r}{4(\mathcal{G}_1 - p)}) = -\frac{\mathcal{G}_1^3 - p\mathcal{G}_1^2 - 4r\mathcal{G}_1 + 4pr - q^2}{(\mathcal{G}_1 - p)^2}$$

لنفرض أن $\mathcal{G}_1$ هو صفر للحدودية:

$$S(z) = z^3 - pz^2 - 4rz + 4pr - q^2$$

نجد أن:

$$(y^2 + \frac{\mathcal{G}_1}{2})^2 = (\mathcal{G}_1 - p)(y - \frac{q}{\mathcal{G}_1 - p})^2$$

لنضع $\varphi_1 = 4(\mathcal{G}_1 - p)$ بالتعويض في المعادلة الأخيرة نجد أن:

$$\left[y^2 + \left(\frac{\varphi_1^2}{8} + \frac{p}{2} \right) \right]^2 = \left[\left(\frac{\varphi_1}{2} \right) y - \frac{q}{\varphi_1} \right]^2$$

وهذا يكافئ أن:

$$y^2 + \left(\frac{\varphi_1^2}{8} + \frac{p}{2} \right) = \left(\frac{\varphi_1}{2} \right) y - \frac{q}{\varphi_1}$$

$$y^2 + \left(\frac{\varphi_1^2}{8} + \frac{p}{2} \right) = - \left(\frac{\varphi_1}{2} \right) y + \frac{q}{\varphi_1}$$

بإعادة صياغة المعادلتين الأخيرتين نجد أن:

$$y^2 - \frac{\varphi_1}{2} y + \left(\frac{\varphi_1^2}{8} + \frac{p}{2} + \frac{q}{\varphi_1} \right) = 0$$

$$y^2 + \frac{\varphi_1}{2} y + \left(\frac{\varphi_1^2}{8} + \frac{p}{2} - \frac{q}{\varphi_1} \right) = 0$$

لنفرض أن β_1, β_2 جذرا المعادلة الأولى و β_3, β_4 جذرا المعادلة الثانية، نجد أن:

$$\beta_1, \beta_2 = \frac{\varphi_1}{4} \pm \frac{1}{2} \cdot \sqrt{-\frac{\varphi_1^2}{2} - 2p - \frac{4q}{\varphi_1}}$$

$$\beta_3, \beta_4 = -\frac{\varphi_1}{4} \pm \frac{1}{2} \cdot \sqrt{-\frac{\varphi_1^2}{2} - 2p + \frac{4q}{\varphi_1}}$$

نلاحظ هنا أنه في حال استبدال φ_1 بـ $-\varphi_1$ في الجذور السابقة فإننا نحصل على
أصفار الحدودية $g(y)$.

باعتبار $\vartheta_1 = p$ في الحدودية $S(z) = z^3 - pz^2 - 4rz + 4pr - q^2$ نحصل على
الحدودية:

$$S(z) = z^3 - \vartheta_1 z^2 - 4rz + 4\vartheta_1 r - q^2$$

ولما كان ϑ_1 صفراً للحدودية $S(z)$ نجد أن $S(\vartheta_1) = 0$ ومنه يكون $q = 0$ وبالتالي نجد
أن الحدودية:

$$g(y) = y^4 + py^2 + r$$

هي حدودية تربيعية بالمتحول y^2 وأصفارها يمكن إيجادها من خلال الحدوديات التربيعية.

مثال.

أوجد جذور الواحد من المرتبة 5.

لإيجاد جذور الواحد من المرتبة الخامسة سوف نستخدم الطريق الآتية:

لنأخذ الحدودية:

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$

ف نجد أن: $(x^5 - 1) = (x - 1) \cdot \Phi_5(x)$.

لنرمز لأصفار الواحد من المرتبة الخامسة بالشكل $\xi_5, \xi_5^2, \xi_5^3, \xi_5^4$ ، حيث:

$$\xi_5 = \cos\left(\frac{2\pi}{5}\right) + i \cdot \sin\left(\frac{2\pi}{5}\right)$$

لنأخذ الحدودية الموافقة للحدودية $\Phi_5(x)$ التي هي:

$$g(y) = y^4 + \left(\frac{5}{8}\right)y^2 + \left(\frac{5}{8}\right)y + \frac{205}{256}$$

لنشكل الحدودية $S(z)$ التي هي:

$$S(z) = z^3 - \left(\frac{5}{8}\right)z^2 - \left(\frac{205}{64}\right)z + \frac{825}{512}$$

لنأخذ الحدودية الموافقة للحدودية $S(z)$ التي هي:

$$h(y) = y^3 - \left(\frac{10}{3}\right)y + \frac{25}{27}$$

ف نجد أن أصفار الحدودية $h(y)$ هي:

$$\frac{5}{3}, \quad -\frac{5}{8} \pm \frac{\sqrt{5}}{2}$$

لنوجد قيم ρ_1 التي هي $\sqrt{-5 \pm 2\sqrt{5}}$. نختار $\rho_1 = \sqrt{5}$ نجد أن الجذور هي:

$$\xi_5, \xi_5^4 = \frac{-1 + \sqrt{5}}{4} \pm i \cdot \frac{\sqrt{10 + 2\sqrt{5}}}{4}$$

$$\xi_5^2, \xi_5^3 = \frac{-1 - \sqrt{5}}{4} \pm i \cdot \frac{\sqrt{10 - 2\sqrt{5}}}{4}$$

الفصل الثالث عشر

الحقول الحقيقية

إن مصطلح الحقل الحقيقي لا يعني بالضرورة حقل الأعداد الحقيقية. عندما يدور الحديث عن حقل الأعداد الحقيقية سوف نذكر ذلك صراحة.

١٣ - ١. الحقول المرتبة.

تعريف.

ليكن K حقلاً و P مجموعة جزئية وغير خالية في K . نقول عن الحقل K إنه مرتباً بالنسبة للمجموعة P إذا تحققت الشروط الآتية:

١ - أيّاً كان $a \in K$ فإنه إما $a \in P$ أو $a = 0$ أو $-a \in P$.

٢ - أيّاً كان $a, b \in P$ فإن $a + b \in P$.

٣ - أيّاً كان $a, b \in P$ فإن $a \cdot b \in P$.

تعريف.

إذا كان K حقلاً مرتباً بالنسبة للمجموعة P . فإننا نسمي المجموعة P مجموعة العناصر الموجبة في K .

اعتماداً على التعريف السابق يمكننا صياغة النتيجة الآتية:

نتيجة.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P . لنفرض أن:

$$-P = \{a : a \in K; a \neq 0, a \notin P\}$$

نلاحظ أن المجموعات الثلاث الآتية $P, \{0\}, -P$ تشكل تجزئة للحقل K وبالتالي فهي تعرف علاقة تكافؤ على الحقل K .

نسمي المجموعة $-P$ مجموعة العناصر السالبة في الحقل K .

اعتماداً على ما سبق يمكننا صياغة التمهيدية الآتية:

تمهيدية ١٣-١-١.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P . عندئذ:

$$1 \in P - ١.$$

٢ - مميز الحقل K يساوي الصفر.

٣ - أيّاً كان $a \in P$ فإن $a^{-1} \in P$.

البرهان.

١ - لما كان $1 \in K$ وأن $1 \neq 0$ نجد أنه إما $1 \in P$ أو $-1 \in P$.

- إذا كان $1 \in P$ يتم المطلوب.

- إذا كان $-1 \in P$ ، عندئذ حسب الخاصة (٣) من التعريف نجد أن

$$1 = (-1) \cdot (-1) \in P$$

٢ - لما كان K حقلاً فإن $0 \cdot 1 = 0$. من جهة أخرى، لما كان $1 \in P$ وحسب الخاصة

(٢) من التعريف فإنه لأجل أي عدد صحيح موجب m يكون:

$$m \cdot 1 = \underbrace{1+1+\dots+1}_{m \text{ once}} \in P$$

وهذا يبين أن $m \cdot 1 \neq 0$ ، مما سبق نجد أن مميز الحقل K يساوي الصفر.

٣ - ليكن $a \in P$ عندئذ $a \neq 0$ ومنه فإن $a^{-1} \in K$ وبالتالي إما $a^{-1} \in P$ أو

$$-a^{-1} \in P$$

- إذا كان $a^{-1} \in P$ تم المطلوب.

- لنفرض أن $-a^{-1} \in P$ ، لما كان $a \in P$ ، فإنه حسب الخاصة (٣) من التعريف نجد

$$-1 = (a) \cdot (-a^{-1}) \in P \quad \text{أن } a^{-1} \in P \text{ مما سبق نجد أن } a^{-1} \in P.$$

وجدنا سابقاً أنه من خلال المجموعة P في الحقل K يمكن تعريف علاقة تكافؤ على

الحقل K . سنرى الآن أنه من خلال المجموعة P يمكن تعريف علاقة ترتيب على الحقل

K وهذا ما تبينه لنا التمهيدية الآتية:

تمهيدية ١٣-١-٢.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P . عندئذ:

١ - العلاقة ($<$) المعرفة على الحقل K بالشكل الآتي: أياً كان $a, b \in K$ فإن:

$$a < b \Leftrightarrow b - a \in P$$

هي علاقة تخالفية ومتعدية على K .

٢ - العلاقة ($\leq$) المعرفة على الحقل K بالشكل الآتي: أياً كان $a, b \in K$ فإن:

$$a \leq b \Leftrightarrow a = b \text{ or } a < b$$

هي علاقة ترتيب جزئية على الحقل K .

البرهان.

١ - ليكن $a, b \in K$ ولنفرض أن $a < b$ و $b < a$ ، عندئذ حسب التعريف يكون:

$$b - a \in P, a - b \in P$$

لنفرض جلاً أن $a \neq b$ عندئذ يوجد $c, c' \in P$ بحيث $a - b = c$, $b - a = c'$. ومنه نجد أن $c = -c'$ ولما كان $c \in P$ نجد أن $-c' \in P$. أصبح لدينا $c', -c' \in P$ وهذا غير ممكن، مما سبق نجد أن $a = b$ وبالتالي العلاقة ($<$) تخالفية.

لنبرهن على أن العلاقة ($<$) متعدية. ليكن $a, b, c \in K$ بحيث $a < b$, $b < c$ عندئذ يكون $b - a \in P$, $c - b \in P$ وحسب الخاصة (٢) من التعريف نجد أن:

$$c - a = (b - a) + (c - b) \in P$$

وبالتالي يكون $a < c$ ، وهذا يبين أن العلاقة ($<$) متعدية.

٢ - واضح أن العلاقة ($\leq$) انعكاسية. كون العلاقة ($\leq$) تخالفية ومتعدية ينتج مباشرة من (١) وبالتالي العلاقة ($\leq$) هي علاقة ترتيب جزئية على الحقل K .

اعتماداً على التمهيدية السابقة يمكننا صياغة التمهيدية الآتية:

تمهيدية ٣-١-١٣.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P وليكن $a \in K$. عندئذ:

١ - إذا كان $a \in P$ عندما وفقط عندما $a > 0$.

٢ - إذا كان $a \notin P$ عندما وفقط عندما $a < 0$.

٣ - إذا كان $a \in P$ ، عندئذ لأجل أي عنصر $b \in K$ بحيث $b \notin P$ فإن $a > b$.

البرهان.

- ١ - ($\Leftarrow$). لنفرض أن $a \in P$ عندئذ يكون $a = a - 0 \in P$ ومنه يكون $a > 0$.
- ($\Rightarrow$). لنفرض أن $a > 0$ عندئذ يكون $a = a - 0 \in P$ ومنه يكون $a \in P$.
- ٢ - ($\Leftarrow$). لنفرض أن $a \notin P$ عندئذ يكون $-a \in P$ ومنه فإن $0 - a = -a \in P$ وبالتالي $a < 0$.
- ($\Rightarrow$). لنفرض أن $a < 0$ عندئذ يكون $-a = 0 - a \in P$ ومنه يكون $-a \in P$ وبالتالي $a \notin P$.
- ٣ - لنفرض أن $a \in P$ ، وليكن $b \in K$ بحيث $b \notin P$ عندئذ يكون $-a \in P$ ومنه فإن:
- $$a - b = a + (-b) \in P$$
- وبالتالي يكون $a > b$.

نأتي الآن إلى دراسة التمهيدية الآتية:

تمهيدية ١٣-١-٤.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P . عندئذ:

- ١ - إذا كان $a \in K$ وكان $a \neq 0$ فإن $a^2 \in P$ ، أي أن العنصر $a^2 \in P$ موجب.
- ٢ - إذا كان $a, b \in K$ عندئذ إما $a^2 + b^2 = 0$ أو أن $a^2 + b^2 \in P$.
- ٣ - إذا كان $a_1, a_2, \dots, a_n \in K$ ، عندئذ إما $\sum_{i=1}^n a_i^2 = 0$ أو أن $\sum_{i=1}^n a_i^2 \in P$.
- البرهان.**
- ١ - لنفرض أن $a \in K$ وأن $a \neq 0$ عندئذ حسب التعريف إما $a \in P$ أو $-a \in P$.
- إذا كان $a \in P$ عندئذ حسب الخاصة (٣) يكون $a^2 = a \cdot a \in P$.
- إذا كان $-a \in P$ عندئذ حسب الخاصة (٣) يكون $a^2 = (-a) \cdot (-a) \in P$.
- ٢ - ليكن $a, b \in K$. سوف نميز الحالات الآتية:
- إذا كان $a = b = 0$ عندئذ فإن $a^2 + b^2 = 0$.
- إذا كان $a = 0, b \neq 0$ عندئذ حسب (١) يكون $a^2 + b^2 = b^2 \in P$.
- إذا كان $a \neq 0, b \neq 0$ عندئذ حسب (١) يكون $a^2, b^2 \in P$ وحسب الخاصة (٢) من التعريف نجد أن $a^2 + b^2 \in P$.
- مما سبق نجد أنه إما $a^2 + b^2 = 0$ أو أن $a^2 + b^2 \in P$.

٣ - ليكن $a_1, a_2, \dots, a_n \in K$. سوف نورد البرهان بالاستقراء حسب n .

- من أجل $n=1$ ، نجد أنه إما $a_1 = 0$ أو $a_1 \neq 0$.

- إذا كان $a_1 = 0$ ، عندئذ يكون $a_1^2 = 0$.

- إذا كان $a_1 \neq 0$ ، عندئذ حسب (١) يكون $a_1^2 \in P$.

ومنه نجد أنه إما $a_1^2 = 0$ أو $a_1^2 \in P$.

- من أجل $n=2$ حسب (٢).

- لنفرض أن القضية صحيحة لأجل $n-1$ ، عندئذ نجد أنه إما $\sum_{i=1}^{n-1} a_i^2 = 0$ أو أن

$$\sum_{i=1}^{n-1} a_i^2 \in P$$

- إذا كان $\sum_{i=1}^{n-1} a_i^2 = 0$ ، نميز حالتين:

- إذا كان $a_n = 0$ عندئذ يكون $a_n^2 = 0$ ومنه فإن $\sum_{i=1}^n a_i^2 = \sum_{i=1}^{n-1} a_i^2 = 0$.

- إذا كان $a_n \neq 0$ عندئذ حسب (١) يكون $a_n^2 \in P$ ومنه يكون:

$$\sum_{i=1}^n a_i^2 = a_n^2 \in P$$

- إذا كان $\sum_{i=1}^{n-1} a_i^2 \in P$ ، نميز حالتين:

- إذا كان $a_n = 0$ عندئذ يكون $a_n^2 = 0$ ومنه فإن:

$$\sum_{i=1}^n a_i^2 = \sum_{i=1}^{n-1} a_i^2 + a_n^2 = \sum_{i=1}^{n-1} a_i^2 \in P$$

- إذا كان $a_n \neq 0$ عندئذ حسب (١) يكون $a_n^2 \in P$ وحسب الخاصة (٢) من

التعريف نجد أن:

$$\sum_{i=1}^n a_i^2 = \sum_{i=1}^{n-1} a_i^2 + a_n^2 \in P$$

وهو المطلوب. ♦

تمهيدية ١٣-١-٥.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P . وليكن $a, b \in K$ ولنفرض أن:

$$a = \sum_{i=1}^n a_i^2, \quad b = \sum_{i=1}^m b_i^2$$

حيث $a_i, b_j \in K$ لأجل كل $1 \leq j \leq m, 1 \leq i \leq n$. عندئذ:

$$1 - a \cdot b = \sum_{i=1}^{n \cdot m} c_i^2 \quad \text{حيث } c_i \in K$$

$$2 - \text{إذا كان } b \neq 0 \text{ عندئذ } \frac{a}{b} = a \cdot b^{-1} = \sum_{i=1}^{n \cdot m} d_i^2$$

البرهان.

١ - سوف نورد البرهان بالاستقراء حسب n .

من أجل $n=1$ نجد أن:

$$a \cdot b = a_1^2 \cdot (\sum_{i=1}^m b_i^2) = \sum_{i=1}^m (a_1^2 \cdot b_i^2) = \sum_{i=1}^m (a_1 \cdot b_i)^2$$

من أجل $n=2$ نجد أن:

$$\begin{aligned} a \cdot b &= (a_1^2 + a_2^2) \cdot (\sum_{i=1}^m b_i^2) = a_1^2 \cdot (\sum_{i=1}^m b_i^2) + a_2^2 \cdot (\sum_{i=1}^m b_i^2) = \\ &= \sum_{i=1}^m (a_1^2 \cdot b_i^2) + \sum_{i=1}^m (a_2^2 \cdot b_i^2) = \sum_{i=1}^m (a_1 \cdot b_i)^2 + \sum_{i=1}^m (a_2 \cdot b_i)^2 \end{aligned}$$

لنفرض أن القضية صحيحة لأجل $n-1$ ، عندئذ يكون:

$$\begin{aligned} a \cdot b &= (\sum_{i=1}^n a_i^2) \cdot (\sum_{i=1}^m b_i^2) = (\sum_{i=1}^{n-1} a_i^2 + a_n^2) \cdot (\sum_{i=1}^m b_i^2) = \\ &= (\sum_{i=1}^{n-1} a_i^2) \cdot (\sum_{i=1}^m b_i^2) + a_n^2 \cdot (\sum_{i=1}^m b_i^2) \end{aligned}$$

وحسب الفرض الاستقرائي نجد أن:

$$(\sum_{i=1}^{n-1} a_i^2) \cdot (\sum_{i=1}^m b_i^2) = \sum_{i=1}^{(n-1)m} \lambda_i^2$$

$$a \cdot b = \sum_{i=1}^{(n-1)m} \lambda_i^2 + \sum_{i=1}^m (a_n \cdot b_i)^2$$

٢ - لنفرض أن $b \neq 0$ ، حسب (١) لدينا:

$$a \cdot b = (\sum_{i=1}^n a_i^2) \cdot (\sum_{i=1}^m b_i^2) = \sum_{i=1}^{nm} c_i^2 \quad : c_i \in K$$

ولما كان $\frac{a}{b} = (a \cdot b) \cdot (b^{-1})^2$ نجد أن:

$$\frac{a}{b} = a \cdot b^{-1} = (\sum_{i=1}^{nm} c_i^2) \cdot (b^{-1})^2 = (\sum_{i=1}^{nm} c_i \cdot b^{-1})^2$$

وهو المطلوب. ♦

لنتعرف على القيمة المطلقة في الحقول المرتبة.

تعريف.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P . نعرف القيمة المطلقة على K بالشكل

الآتي: أيأ كان $a \in K$ فإن:

$$|a| = \begin{cases} a & a \in P \\ 0 & a = 0 \\ -a & a \notin P \end{cases}$$

اعتماداً على التعريف السابق يمكننا صياغة التمهيدية الآتية:

تمهيدية ١٣-١-٦.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P وليكن $a \in K$ وأن $a \neq 0$. عندئذ:

$$1 - |a| = a \text{ عندما فقط عندما } a > 0.$$

$$2 - |a| = -a \text{ عندما فقط عندما } a < 0.$$

البرهان.

١ - ($\Leftarrow$). لنفرض أن $|a| = a$ عندئذ يكون $a \in P$ ومنه فإن $a - 0 = a \in P$ وبالتالي يكون $a > 0$.

($\Rightarrow$). لنفرض أن $a > 0$ عندئذ يكون $a = a - 0 \in P$.

٢ - ($\Leftarrow$). لنفرض أن $|a| = -a$ عندئذ يكون $a \notin P$ ولما كان $a \neq 0$ نجد أن $a \in P$ ومنه فإن $0 - a = -a \in P$ وبالتالي يكون $a < 0$.

($\Rightarrow$). لنفرض أن $a < 0$ عندئذ يكون $-a = 0 - a \in P$ ومنه نجد أن $a \notin P$ وبالتالي نجد أن $|a| = -a$. ◊

نتابع دراستنا لخواص القيمة المطلقة وذلك من خلال التمهيدية الآتية:

تمهيدية ١٣-١-٧.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P . عندئذ:

$$1 - \text{أياً كان } a \in K \text{ فإن } 0 \neq a \text{ فإن } |a^{-1}| = |a|^{-1}.$$

$$2 - \text{أياً كان } a, b \in K \text{ فإن } |a \cdot b| = |a| \cdot |b|.$$

$$3 - \text{أياً كان } a, b \in K \text{ وكان } b \neq 0 \text{ فإن } \left| \frac{a}{b} \right| = \frac{|a|}{|b|}.$$

البرهان.

١ - ليكن $a \in K, a \neq 0$. نميز حالتين:

- $a \in P$ عندئذ $a^{-1} \in P$. لما كان $a \cdot a^{-1} = 1 \in P$ نجد أن:

$$|a| \cdot |a^{-1}| = a \cdot a^{-1} = 1$$

ومنه يكون $|a^{-1}| = |a|^{-1}$.

- $a \notin P$ عندئذ $a^{-1} \notin P$ ومنه فإن:

$$|a| \cdot |a^{-1}| = (-a) \cdot (-a^{-1}) = 1$$

وبالتالي يكون $|a^{-1}| = |a|^{-1}$.

٢ - إذا كان أحد العنصرين a, b مساوياً للصفر تكون المساواة محققة.

لنفرض أن $a \neq 0, b \neq 0$. سوف نميز الحالات الآتية:

- $a, b \in P$ عندئذ يكون $a \cdot b \in P$ ومنه فإن:

$$|a \cdot b| = a \cdot b = |a| \cdot |b|$$

- $a, b \notin P$ عندئذ يكون $-a, -b \in P$ ومنه فإن $a \cdot b = (-a) \cdot (-b) \in P$ وبالتالي نجد أن:

$$|a \cdot b| = a \cdot b = (-a) \cdot (-b) = |a| \cdot |b|$$

- $a \in P, b \notin P$ عندئذ يكون $a, -b \in P$ ومنه فإن $-(a \cdot b) = a \cdot (-b) \in P$ وبالتالي $a \cdot b \notin P$ ومنه نجد أن:

$$|a \cdot b| = -(a \cdot b) = a \cdot (-b) = |a| \cdot |b|$$

٣ - ليكن $a, b \in K$ و $b \neq 0$ عندئذ فإن:

$$\left| \frac{a}{b} \right| = |a \cdot b^{-1}| = |a| \cdot |b^{-1}| = |a| \cdot |b|^{-1} = \frac{|a|}{|b|}$$

وذلك حسب (١) و (٢).

تمهيدية ١٣-١-٨.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P . عندئذ أيّاً كان $a, b \in K$ فإن:

$$|a + b| \leq |a| + |b| \quad ١$$

$$٢ - |a - b| \geq |a| - |b|.$$

٣ - إذا كان $a < b$ و $z > 0$ عندئذ يكون $a \cdot z < b \cdot z$.

٤ - إذا كان $a > b$ و $a, b > 0$ عندئذ يكون $a^{-1} < b^{-1}$.

البرهان.

١ - سوف نميز الحالات الآتية:

- إذا كان $a, b \in P$ عندئذ يكون $a + b \in P$ ومنه فإن:

$$|a + b| = a + b = |a| + |b|$$

- إذا كان $a, b \notin P$ عندئذ يكون $-a, -b \in P$ ومنه فإن:

$$-(a + b) = (-a) + (-b) \in P$$

وهذا يبين أن $a + b \notin P$ وبالتالي يكون:

$$|a + b| = -(a + b) = (-a) + (-b) = |a| + |b|$$

- إذا كان $a \in P, b \notin P$ عندئذ سوف نميز الحالات الآتية:

- إذا كان $a + b \in P$.

لما كان $b \notin P$ فإن $-b \in P$ ومنه $-b - b \in P$ وأن:

$$(a - b) - (a + b) = -b - b \in P$$

وهذا يبين أن $(a - b) > (a + b)$ ومنه نجد أن:

$$|a + b| = a + b < a - b = |a| + |b|$$

- إذا كان $a + b \notin P$.

لما كان $a \in P$ فإن $a + a \in P$ ومنه فإن:

$$(a - b) - (-a - b) = a + a \in P$$

ومنه يكون $(a - b) > -a - b$ وهكذا فإن:

$$|a + b| = -(a + b) < a - b = |a| + |b|$$

٢ - لدينا $a = (a - b) + b$ ومنه نجد أن:

$$|a| = |(a - b) + b| \leq |a - b| + |b|$$

وهكذا نجد أن $|a - b| \geq |a| - |b|$.

٣ - لنفرض أن $a < b$ و $z > 0$ عندئذ يكون $b - a \in P$ ولما كان $z > 0$ نجد أن $z \in P$ ومنه يكون $(b - a) \cdot z \in P$ أي أن $b \cdot z - a \cdot z \in P$ وهذا يبين أن:

$$a \cdot z < b \cdot z$$

٤ - لنفرض أن $a > b$ وأن $a, b > 0$ ، عندئذ حسب (٣) نجد أن:

$$1 = a \cdot a^{-1} > b \cdot a^{-1}$$

مرة أخرى حسب (٣) نجد أن $a^{-1} > b^{-1}$.

تمهيدية ١٣-١-٩.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P . إذا كان F حقلاً جزئياً في K ، عندئذ

$$P_0 = P \cap F$$

البرهان.

لنفرض أن F حقل جزئي في K ، ولنفرض أن $P_0 = P \cap F$. فنجد أن مجموعة جزئية في F وليست خالية لأن $1 \in P_0$.

ليكن $a \in F$ عندئذ $a \in K$ ومنه إما $a \in P$ أو $a = 0$ أو $-a \in P$ وهذا يبين أنه إما $a \in P_0$ أو $a = 0$ أو $-a \in P_0$.

ليكن $a, b \in P_0$ عندئذ $a, b \in P$ ومنه يكون $a + b \in P$ ، كما أن $a, b \in F$ وأن $a + b \in F$ ومنه نجد أن $a + b \in P \cap F = P_0$.

ليكن $a, b \in P_0$ عندئذ $a, b \in P$ ومنه يكون $a \cdot b \in P$ ، كما أن $a, b \in F$ وأن $a \cdot b \in F$ ومنه نجد أن $a \cdot b \in P \cap F = P_0$.

مما سبق نجد أن الحقل الجزئي F مرتب بالنسبة للمجموعة P_0 .

تعريف.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P وليكن F حقلاً جزئياً في K مرتباً بالنسبة للمجموعة $P_0 = P \cap F$.

- نقول عن العنصر $a \in K$ إنه غير متناه في الكبر فوق F إذا كان $|a| > x$ وذلك أيّاً كان $x \in F$.

- نقول عن العنصر $a \in K$ إنه غير متناه في الصغر فوق F إذا كان $0 \leq |a| < |x|$ وذلك أيأ كان $0 \neq x \in F$.

ينتج مباشرة من التعريف واعتماداً على التمهيدية (١٣-١-٨) أن الشرط اللازم والكافي كي يكون العنصر $a \in K$ غير متناه في الكبر فوق F هو أن يكون العنصر a^{-1} غير متناه في الصغر فوق F .

تعريف.

ليكن K حقلاً مرتباً بالنسبة للمجموعة P وليكن F حقلاً جزئياً في K مرتباً بالنسبة للمجموعة $P_0 = P \cap F$. نقول عن الحقل K إنه حقل أرخميدس فوق F إذا كان K لا يحوي عناصر غير متناهية في الكبر فوق F .

تمهيدية ١٣-١-١٠.

ليكن K حقلاً و F حقلاً جزئياً في K ، وليكن E حقلاً جزئياً في K يحوي F . إذا كان K حقل أرخميدس فوق F عندئذ:

١ - K هو حقل أرخميدس فوق E .

٢ - E حقل أرخميدس فوق F .

البرهان.

لنفرض أن الحقل K مرتب بالنسبة للمجموعة P وأن الحقل F مرتب بالنسبة للمجموعة $P_0 = P \cap F$. لنفرض أن K حقل أرخميدس فوق F .

١ - لنفرض جدياً أن K ليس حقل أرخميدس فوق E ، عندئذ يوجد في K عنصر a غير متناه في الكبر فوق E ، ومنه فإن $|a| > x$ أيأ كان $x \in E$. لما كان $F \subseteq E$ نجد أن $|a| > y$ وذلك أيأ كان $y \in F$ وهذا يبين أن الحقل K يحوي عنصراً غير متناه في الكبر فوق F ، وهذا غير ممكن فرضاً ومنه نجد أن K حقل أرخميدس فوق E .

٢ - لنفرض جدياً أن E ليس حقل أرخميدس فوق F ، عندئذ يوجد في E عنصر b غير متناه في الكبر فوق F ، ومنه فإن $|b| > x$ أيأ كان $x \in F$. لما كان $E \subseteq K$ نجد

أن $b \in K$ وهذا يبين أن الحقل K يحوي عنصراً غير متناه في الكبر فوق F ، وهذا غير ممكن فرضاً ومنه نجد أن E حقل أرخميدس فوق F . ٥

مبرهنة ١٣-١-١١.

ليكن الحقل K تمديداً للحقل F . إذا كان E حقلاً جزئياً في K يحوي F وكان E حقل أرخميدس فوق F ، عندئذ يوجد حقل أرخميدس أعظمي فوق F يحوي E ومحتوى في K .

البرهان.

لنفرض أن الحقل K مرتب بالنسبة للمجموعة P وأن الحقل F مرتب بالنسبة للمجموعة $P_0 = P \cap F$. لنفرض أن $F \subseteq E \subseteq K$ حقل أرخميدس فوق F . لنأخذ المجموعة $\mathfrak{T}$ المؤلفة من الحقول الجزئية L في K التي كل منها يحوي F وتشكل حقل أرخميدس فوق F . فنجد أن المجموعة $\mathfrak{T}$ ليست خالية، لأن $E \in \mathfrak{T}$ وأن المجموعة $\mathfrak{T}$ مرتبة جزئياً بالنسبة لعلاقة الاحتواء. لنكن $\mathfrak{T}_0$ مجموعة جزئية في $\mathfrak{T}$ غير خالية ومرتبة كلياً. لنفرض أن $M = \bigcup_{L \in \mathfrak{T}_0} L$ فنجد أن M حقل جزئي في K وأن $F \subseteq E \subseteq M$. لنبرهن على أن M حقل أرخميدس فوق F .

لنفرض جداً أن M ليس حقل أرخميدس فوق F ، عندئذ يوجد $a \in M$ بحيث $|a| > x$ وذلك أيّاً كان $x \in F$ ، ولما كان $M = \bigcup_{L \in \mathfrak{T}_0} L$ فإنه يوجد $L_0 \in \mathfrak{T}_0$ بحيث $a \in L_0$ وأن $|a| > x$ أيّاً كان $x \in F$ وهذا يناقض كون L_0 حقل أرخميدس فوق F وبالتالي فإن $M \in \mathfrak{T}$. كما أن M هو حد أعلى للمجموعة $\mathfrak{T}_0$ في $\mathfrak{T}$ وذلك لأنه أيّاً كان $L_i \in \mathfrak{T}_0$ فإن $L_i \subseteq \bigcup_{L \in \mathfrak{T}_0} L = M$ وحسب تمهيدية زورن يوجد في $\mathfrak{T}$ عنصر أعظمي وليكن K' . إن K' حقل جزئي في K يحوي F وأن K' أكبر حقل أرخميدس فوق F . ٥

١٣ - ٢. الحقول الحقيقية.

تعريف.

نقول عن الحقل K إنه حقل حقيقي إذا كان $\sum a_i^2 \neq -1$ وذلك لأجل أي مجموعة $\{a_i\}$ من عناصر الحقل K . بمعنى آخر، نقول عن الحقل K إنه حقيقي إذا كان العنصر -1 ليس مجموع مربعات لعناصر من الحقل K .

تعريف.

نقول عن الحقل K إنه حقل حقيقي مغلق إذا حقق الشرطين الآتيين:

- ١ - الحقل K حقيقياً.
- ٢ - إذا كان $\bar{K}$ تمديداً جبرياً للحقل K وكان الحقل $\bar{K}$ حقيقياً إن $K = \bar{K}$.

تعريف.

ليكن K حقلاً و $a \in K$. إن $\sqrt{a}$ هو صفر الحدودية $x^2 - a \in K[x]$. أو بمعنى آخر، نقول عن العنصر $b \in K$ إنه $\sqrt{a}$ إذا كان $b^2 = a$.

تمهيدية ١٣-٢-١.

ليكن K حقلاً حقيقياً. عندئذ أياً كان $a \in K$ إما أن الحقل $K(\sqrt{a})$ حقيقي أو أن الحقل $K(\sqrt{-a})$.

البرهان.

لنفرض أن الحقل K حقيقي وأن $a \in K$. نميز حالتين:

- يوجد $b \in K$ بحيث $b^2 = a$ ، عندئذ يكون $K(\sqrt{a}) = K(b) = K$ وهذا يبين أن الحقل $K(\sqrt{a})$ حقيقي.

- أياً كان $b \in K$ فإن $b^2 \neq a$. إذا كان الحقل $K(\sqrt{a})$ حقيقياً تم المطلوب. لنفرض أن الحقل $K(\sqrt{a})$ ليس حقيقياً، ولما كان الحقل K حقيقياً نجد أن $K(\sqrt{a}) \neq K$ ، أي أن $\sqrt{a} \notin K$. وهذا يبين أن الحدودية $x^2 - a \in K[x]$ أولية فوق K وأن $\sqrt{a}$ صفر لها ومنه فإن الحدودية $x^2 - a$ هي الحدودية الأصغرية للعنصر $\sqrt{a}$ فوق K وبالتالي يكون:

$$[K(\sqrt{a}):K] = \partial(x^2 - a) = 2$$

ومنه فإن المجموعة $\{1, \sqrt{a}\}$ قاعدة للحقل $K(\sqrt{a})$ فوق K .

من جهة أخرى، لما كان الحقل $K(\sqrt{a})$ ليس حقيقياً فإنه يوجد $c_i, b_i \in K$ بحيث:

$$-1 \neq \sum (c_i + b_i \sqrt{a})^2$$

ومنه فإن $-1 \neq \sum (c_i^2 + 2c_i b_i \sqrt{a} + a b_i^2)$ وبالتالي يكون:

$$-1 \neq \sum c_i^2 + 2\sqrt{a} \sum c_i b_i + a \sum b_i^2$$

ولما كانت المجموعة $\{1, \sqrt{a}\}$ مستقلة خطياً نجد أن:

$$-1 \neq \sum c_i^2 + a \sum b_i^2$$

وبالتالي يكون $-a = \frac{1 + \sum b_i^2}{\sum c_i^2}$. ولما كان $a \neq b^2$ أيّاً كان $b \in K$ نجد أن

الحقل $K(\sqrt{-a})$ حقيقياً. ◊

تمهيدية ١٣-٢-٢.

ليكن K حقلاً حقيقياً و $a \in K$. عندئذ:

١ - إذا كان $a = \sum a_i^2$ حيث $a_i \in K$ عندئذ يكون الحقل $K(\sqrt{a})$ حقيقياً.

٢ - إذا كان الحقل $K(\sqrt{a})$ ليس حقيقياً، عندئذ $-a = \sum a_i^2$ حيث $a_i \in K$.

البرهان.

١ - لنفرض أن $a = \sum a_i^2$ حيث $a_i \in K$. لنفرض جـداً أن الحقل $K(\sqrt{a})$ ليس

حقيقياً عندئذ توجد عناصر $c_i, d_i \in K$ بحيث:

$$-1 = \sum (c_i + d_i \sqrt{a})^2$$

ومنه يكون:

$$-1 = \sum (c_i^2 + 2\sqrt{a} \sum c_i \cdot d_i + \sum a \cdot d_i^2)$$

وبالتالي نجد أن:

$$-1 = \sum c_i^2 + 2\sqrt{a} \cdot (\sum c_i \cdot d_i) + \sum a \cdot d_i^2$$

$$-1 = \sum (c_i^2 + a \cdot d_i^2) + 2\sqrt{a} \cdot (\sum c_i \cdot d_i)$$

ولما كانت المجموعة $\{1, \sqrt{a}\}$ مستقلة خطياً نجد أن $-1 = \sum (c_i^2 + a \cdot d_i^2)$ ومنه فإن

$$-1 = \sum c_i^2 + a \cdot \sum d_i^2$$

$$-1 = \sum c_i^2 + \sum a_i^2 \cdot \sum d_i^2$$

وحسب التمهيدية (١٣-٢-١) فإن:

$$\sum a_i^2 \cdot \sum d_i^2 = \sum b_i^2$$

حيث $b_i \in K$ وهذا يبين أن $-1 = \sum c_i^2 + \sum b_i^2$ أي أن العنصر -1 هو مجموع مربعات لعناصر من الحقل K ، وحسب التعريف نجد أن الحقل K ليس حقيقياً مما يناقض الفرض، ومنه فإن الحقل $K(\sqrt{a})$ حقيقي.

٢ - لنفرض أن الحقل $K(\sqrt{a})$ ليس حقيقياً، عندئذ توجد عناصر $a_i, b_i \in K$ بحيث يكون $-1 = \sum (a_i + b_i \sqrt{a})^2$ ومنه نجد أن:

$$-1 = \sum (a_i^2 + 2a_i \cdot b_i \sqrt{a} + ab_i^2)$$

ولما كانت المجموعة $\{1, \sqrt{a}\}$ قاعدة للحقل $K(\sqrt{a})$ فوق K نجد أن:

$$-1 = \sum a_i^2 + a \sum b_i^2$$

ومنه نجد أن $-a = \frac{1 + \sum a_i^2}{\sum b_i^2}$ ومنه فإن العنصر $-a$ مجموع مربعات. ◊

المصطلحات العلمية

(إنكليزي - عربي)

algebraic	جبري
element	عنصر جبري
extension	تمديد جبري
relation	علاقة جبرية
Automorphism	تماثل
inner	تماثل ذاتي (داخلي)
between fields	تماثل حقول
binomial extension	تمديد ثنائي
irreducible	تمديد ثنائي غير قابل للتفريق
prime	تمديد ثنائي أولي
binomial polynomial,	حدودية ثنائية
Cauchy's theorem	مبرهنة كوشي
Characteristic of field	مميز الحقل
Classical Galois group	زمرة غالوا الكلاسيكية
Coefficient	أمثال
Conjugate root	صفر مرافق
Coset	مرافقة
Cyclotomic filed	حقل دوار
representatives	ممثل
cubic polynomial	حدودية مكعبة
cyclic	دائري
extension	تمديد دائري
(sub)group	زمرة دوارة
polynomial	حدودية دوارة
degree	درجة
of algebraic element	درجة العنصر
of extension	درجة التمديد
of polynomial	درجة الحدودية
Derivative of polynomial	مشتق حدودية
Divides	يقسم

Division Algorithm

Quotient

remainder

divisor

Eisenstein's criterion

Element

algebraic

degree of algebraic

order of

primitive

transcendental

Euclidean Algorithm

Extension

algebraic

binomial

cyclic

degree of

finite

finitely generated

Galois

infinite

irreducible binomial

irreducible radical

prime radical

radical

separable

simple

normal

Unique

Fermat prime

Fermat's Little Theorem

Ferrari's formulas

field

between

cyclotomic

extension of

خوارزمية القسمة

ناتج القسمة

باق القسمة

قاسم

معيار أيزنشتاين

عنصر

عنصر جبري

مرتبة العنصر الجبري

مرتبة العنصر

عنصر أولي

عنصر غير جبري متسامي

خوارزمية القسمة

تمديد

تمديد جبري

تمديد ثنائي

تمديد دائري

درجة التمديد

تمديد منتهي

تمديد منتهي التوليد

تمديد غالوا

تمديد غير منتهي

تمديد ثنائي غير قابل للتفريق

تمديد جذري غير قابل للتفريق

تمديد أولي جذري

تمديد جذري

تمديد منفصل

تمديد بسيط

تمديد ناظمي

وحيد

أولي فيرما

مبرهنة فيرما الصغرى

علاقات فيراري

حق

حق بين حقليين

حق دوار

تمديد للحق

<i>finite</i>	حقل منتهي
<i>finitely generated</i>	حقل منتهي التوليد
<i>generated by</i>	حقل مولد بـ
<i>of fractions</i>	حقل التشوه
<i>splitting</i>	حقل التفريق
<i>subfield of</i>	حقل جزئي
<i>finite degree of extension</i>	تمديد درجته منتهية
<i>finitely generated extension</i>	تمديد منتهي التوليد
<i>Fundamental Theorem</i>	النظرية الأساسية في الجبر
<i>of Algebra</i>	
<i>of Galois Theory</i>	نظرية غالوا الأساسية
<i>on Symmetric Polynomials</i>	النظرية الأساسية للحدوديات المتناظرة
<i>Galois</i>	غالوا
<i>correspondence</i>	تمديد غالوا
<i>extension</i>	زمرة غالوا
<i>group</i>	اختبار غالوا
<i>Galois's criterion</i>	تمهيدية غاوص
<i>Gauss's lemma</i>	الحدودية العامة
<i>General polynomial</i>	الحدودية العامة التكعيبة
<i>cubic</i>	الحدودية العامة التربيعية
<i>quadratic</i>	مولد بـ
<i>Generated by</i>	مولد
<i>Generator</i>	قاسم مشترك أعظم
<i>Greatest common divisor</i>	زمرة
<i>Group</i>	تأثير زمرة
<i>action</i>	زمرة دوارة
<i>cyclic</i>	زمرة منتهية
<i>finite</i>	زمرة غالوا
<i>Galois</i>	مولد الزمرة الدوارة
<i>generator of cyclic</i>	زمرة غير منتهية
<i>infinite</i>	مرتبة الزمرة
<i>order of</i>	زمرة بسيطة
<i>simple</i>	زمرة قابلة للحل
<i>solvable</i>	زمرة تناظرية
<i>symmetric</i>	دليل الزمرة الجزئية
<i>index of subgroup</i>	واحد
<i>Identity</i>	

Image	صورة
Inner automorphism	تماثل ذاتي
Irreducibility	غير قابل للتفريق
Isomorphism Extension Theorem	نظرية تماثل التمديدات
Isomorphism Theorem	نظرية التماثل
First	نظرية التماثل الأولى
Second	نظرية التماثل الثانية
Third	نظرية التماثل الثالثة
Kernel	نواة
Lagrange's theorem	نظرية لاغرانج
Leading coefficient	معامل رئيسي
Minimal polynomial	حدودية أصغرية
Normal	ناظمي
extension	تمديد ناظمي
series	سلسلة ناظمية
Subgroup	زمرة جزئية
Orbit	مدار
Order	مرتبة
element	مرتبة العنصر
group	مرتبة الزمرة
Permutation	تبديل
Even	تبديل زوجي
Odd	تبديل فردي
Phi-function	التابع في (فربينوس)
Polynomial	حدودية
binomial	حدودية ثنائية
constant	حدودية ثابتة
cyclotomic	حدودية دوارة
degree	درجة الحدودية
derivative of	مشتق الحدودية
divisor of	قاسم حدودية
general	حدودية عامة
irreducible	حدودية غير قابلة للتفريق
minimal	حدودية أصغرية
monic	حدودية واحدة
of prime degree	حدودية درجتها أولية
primitive	حدودية أولية

<i>reducible</i>	حدودية قابلة للتفريق
<i>root of</i>	صفر للحدودية
<i>solvable by radicals</i>	حدودية قابلة للحل جذرياً
<i>splits</i>	حدودية قابلة للتفريق
<i>Prime</i>	أولي
<i>Root of unity</i>	جذر للواحد
<i>Radical</i>	جذر
<i>Radical extension</i>	تمديد جذري
<i>Rational function</i>	تابع كسري
<i>Relatively prime</i>	أوليّين نسبياً
<i>Remainder</i>	باق
<i>Ring</i>	حلقة
<i>generated by</i>	حلقة مولدة بـ
<i>of integers</i>	حلقة الأعداد الصحيحة
<i>of polynomials</i>	حلقة الحدوديات
<i>Root</i>	جذر
<i>conjugate</i>	جذر مرافق
<i>of polynomial</i>	صفر حدودية
<i>simple</i>	صفر بسيط
<i>root of unity</i>	جذر للواحد
<i>primitive</i>	جذر أولي
<i>Solvable</i>	قابل للحل
<i>by radicals</i>	قابل للحل جذرياً
<i>group</i>	زمرة قابلة للحل
<i>Splits</i>	تفريق
<i>Splitting field</i>	حقل تفريق

المراجع العلمية

- [1] – Artin E. *Galois Theory*, 2nd ed. (University of Notre Dame Press, Notre Dame, 1944).
- [2] – Bastida J. R. *Field Extensions and Galois Theory*. (Addison-Wesley, Menlo Park, CA, 1984).
- [3] – Bowersdorff J. *Galois Theory for Beginners: A Historical Perspective*. (Amer. Math. Soc, Providence, RI, 2006).
- [4] – Chambert-Loir A. *A Field Guide to Algebra*. (Springer, New York, 2005).
- [5] – Clark A. *Elements of Abstract Algebra*. (Wadsworth, Belmont, CA, 1971).
- [6] – Cooke R. *Classical Algebra: Its Nature, Origins, and Uses*. (John Wiley & Sons, Inc., Hoboken, NJ, 2008).
- [7] – Cox D. A. *Galois Theory*, 2nd ed. (John Wiley & Sons, Inc., Hoboken, NJ, 2012).
- [8] – Dehn E. *Algebraic Equations: An Introduction to the Theories of Lagrange and Galois*. (Dover, Mineola, NY, 1960).
- [9] – Dummit D. S. and Foote R. M. *Abstract Algebra*, 3rd ed. (John Wiley & Sons, Inc., Hoboken, NJ, 2004).
- [10] – Edwards H. M. *Galois Theory*. (Springer-Verlag, New York, 1984).
- [11] – Escofier J.-P. *Galois Theory*. (Springer, New York, 2001).
- [12] – Fenrick M. H. *Introduction to the Galois Correspondence*. (Birkhäuser, Boston, MA, 1992).
- [13] – Gaal L. *Classical Galois Theory with Examples*, 4th ed. (Chelsea, New York, 1988).
- [14] – Howie J. M. *Fields and Galois Theory*. (Springer, London, 2006).
- [15] – Jacobson N. *Basic Algebra 1*, 2nd ed. (W. H. Freeman & Company, New York, 1985).

- [16] – King R. B. *Beyond the Quartic Equation*. (Birkhäuser, Boston, MA, 1996).
- [17] – Lang S. *Algebra*, 3rd ed. (Addison-Wesley, Reading, MA, 1993).
- [18] – Lorenz F. *Algebra: Fields and Galois Theory*, Volume I. (Springer, New York, 2006).
- [19] – Morandi P. *Field Theory and Galois Theory*. (Springer, New York, 1996).
- [20] – Roman S. *Field Theory*. (Springer-Verlag, New York, 1995).
- [21] – Rotman J. *Galois Theory*, 2nd ed. (Springer, 1990).
- [22] – Stewart I. *Galois Theory*, 3rd ed. (Chapman & Hall/CRC, Boca Raton, FL, 2004).
- [23] – Swallow J. *Exploratory Galois Theory*. (Cambridge University Press, Cambridge, 2004).
- [24] – Tignol J.-P. *Galois' Theory of Algebraic Equations*. (World Scientific, Singapore, 2001).
- [25] – van der Waerden B. L. *Algebra*, 7th ed., Volume I. (Springer Verlag, New York, 1991).
- [26] – Weintraub S. H. *Galois Theory*. (Springer, New York, 2006).

اللجنة العلمية

الأستاذ الدكتور يوسف الوادي	قسم الرياضيات جامعة دمشق.
الأستاذ الدكتور عبد الباسط الخطيب	قسم الرياضيات جامعة البعث.
الأستاذ المساعد الدكتور إيلي قدسي	قسم الرياضيات جامعة دمشق.

المدقق اللغوي

الدكتور حمود يونس

حقوق الطباعة والترجمة والنشر محفوظة لمديرية الكتب والمطبوعات



DAMASCUS UNIVERSITY
FACULTY OF SCIENCE
DEPARTEMENT OF MATHEMATICS

EXTENSION OF FIELDS

HAKMI HAMZE IBRAHIM

NOUR MOWAFK GHAZI

DEPARTEMENT OF MATHEMATICS

All right reserved
DAMASCUS UNIVERSITY

سعر المبيع للطالب: