صفحة
مقدمة البحث
المحتويات
الفصل الأول : الحقول المنتهية
▪ مقدمة في البناء الجبري للحقول المنتهية
▪ البناء الضربي للحقول المنتهية
▪ طرق عد
الفصل الثاني : حول حلقات القسمة المنتهية
▪ كثيرات الحدود الدورية
▪ البرهان الأول لمبرهنة فدربرن
▪ البرهان الثاني لمبرهنة فدربرن
الفصل الثالث : حلقات القسمة الجبرية على حقل الأعداد االحقيقية
▪ تصنيف حلقات القسمة الجبرية على حقل الأعداد المركبة
▪ إحدى مبرهنات فروبينيس
الفصل الرابع : الرباعيات التامة ومبرهنة المربعات الأربعة
▪ حلقة الرباعيات الحقيقية
▪ حلقة هرفتز للرباعيات التامة
▪ مبرهنة المربعات الأربعة
المراجع

الفصل الأول

الحقول المنتهية

مقدمة في البناء الجبري للحقول المنتهية,

البناء الضربي للحقول المنتهية, طرق عد

(١-١)مقدمة في البناء الجبري للحقول المنتهية :

في هذا البند سوف نعطي مقدمة عن البناء الجبري للحقول التي تحوي عدداً منتهياً من العناصر وتدعى مثل هذه الحقول بالحقول المنتهية إن الحقول المنتهية موجودة ومثال على ذلك Z_p حقل الأعداد الصحيحة قياس العدد الأوليp . في هذا البند سوف نعين جميع الحقول المنتهية بالإضافة إلى العديد من الخواص التي تتمتع بها.

نبدأ بالتمهيدية التالية

تمهيدية(١-١-١):

ليكن Fحقلا منتهياً يحوي q من العناصر وافرض إن $F \subset K$ حيث K حقلا منتهياً . عندئذ K يحوي q^n من العناصر حيث $n = [K: F]$

البرهان :

باعتبار K فضاء متجهات على Fولكونه منتهياً فيجب أن يكون K منتهي البعد كفضاء متجهات على F وليكن $n = [K: F]$.بما أن Kفضاء منتهي البعد إذن له أساس على F وليكن $v_1, v_2, \dots, v_n$.

إذن أي عنصر في Kله تمثيل وحيد على الشكل :

$\alpha_1 v_1 + \alpha_2 v_2 + \cdots \alpha_n v_n$ حيث $\alpha_1, \alpha_2, \dots, \alpha_n$ في F

لذا عدد عناصر K هو عدد العناصر التي على الصيغة

$\alpha_1 v_1 + \alpha_2 v_2 + \cdots \alpha_n v_n$ حيث مجال تغيير

$\alpha_1, \alpha_2, \ldots, \alpha_n$ هو F وبما أن كل معامل يمكن أن يأخذ q من القيم فنستنتج من ذلك أن K يحوي q^n من العناصر.

نتيجة (١):

إذا كان F حقلا منتهياً فإن عدد عناصر F هو p^m حيث أن العدد الأولي p هو مميز F .

البرهان :

لما كان عدد عناصر F منتهياً فإن مميزه هو عدد أولي وليكن p

وعليه فإن F يحوي حقلا K يماثل $\mathbb{Z}_p$ أي أن $\mathbb{Z}_p \cong K < F$

وبما أن عدد عناصر K هو p فإنه من التمهيدية السابقة نجد أن عدد عناصر F هو p^m حيث $m = [K: F]$.

نتيجة(٢):

إذا كان عدد عناصر الحقل المنتهي F يساوي p^m فإنه لأي $a \in F$ يكون $a^{p^m} = a$

البرهان :

"نعلم أن مجموعة العناصر غير الصفرية لأي حقل تكون زمرة ضربية "

لذلك يكون مجموعة العناصر غير الصفرية في F زمرة ضربية و يكون عدد عناصرها هو $p^m - 1$ ومن نظرية الزمر يكون

$a^{p^m-1} = 1$ لكل $a \neq 0$ فإن $a^{p^m} = a$

أما في حالة كون $a=0$ فان ما تزعمه النتيجة صحيحة .

تمهيدية(١-١-٢):

إذا كان عدد عناصر الحقل المنتهي هو p^m فإن كثيرة الحدود $x^{p^m} - x$ في $F[x]$ فإنها تتحلل في $F[x]$ على النحو:

$$g(x) = x^{p^m} - x = \prod_{i=1}^{p^m} (x - \lambda_i)$$

البرهان:

نعلم أن عدد جذور كثيرة الحدود $g(x)$ في F لا يزيد عن p^m ولكن من نتيجة(٢) نجد أن جميع عناصر F هي جذور لكثيرة الحدود $g(x)$ ولتكن $F = \{\lambda_1, \lambda_2, \dots \lambda_{p^m}\}$ هي جميع جذور $g(x)$. نعلم من مبرهنة سابقه أن $(x - \lambda_i) | g(x)$ لكل $1 \le i \le p^m$ وعليه فإن :

$$g(x) = x^{p^m} - x = \prod_{i=1}^{p^m} (x - \lambda_i)$$

نتيجة (١):

إذا كان عدد عناصر F هو p^m فإن F هو حقل الإنشطار لكثيرة الحدود $g(x) = x^{p^m} - x$.

البرهان:

بما أن $g(x)$ تتحلل في F ،وعدد جميع جذور $g(x)$ هو p^m فإن $g(x)$ لا يمكن أن تتحلل في حقل اصغر من F لأن مثل هذا الحقل يجب أن يحوي جميع جذور $g(x)$ والتي عددها p^m وعليه فإن F هو حقل انشطار كثيرة الحدود .

تمهيدية(١-١-٣):

الحقلان المنتهيان الحاويان على العدد نفسه من العناصر متماثلان.

البرهان :

ليكن K وF حقلان يحويان على العدد نفسه من العناصر وليكن عدد عناصرهما هو p^m فإنه من النتيجة السابقة نجد أن كلاً من K وF حقلا انشطار لكثيرة الحدود $g(x) = x^{p^m} - x$ ، لكن من وحدانية حقول الانشطار نجد أن $F \cong K$.

تمهيدية(١-١-٤):

لكل عدد أولي p وكل عدد صحيح موجب m يوجد حقل وحيد يحوي p^m من العناصر.

البرهان :

لتكن $g(x) = x^{p^m} - x$ كثيرة حدود في $\mathbb{Z}_p[x]$ وليكن K حقل الانشطار لكثيرة الحدود هذه .

نعلم "أنه إذا كان $g'(a) = 0$ حيث a جذراً لكثيرة الحدود فإن a جذراً مكرراً لـ g " .

لذلك $g' = p^m x - 1 = -1 \neq 0$ وعليه فإنه لا يوجد تكرار في جذور g أي أن جميع جذورها مختلفة ، لذلك فان عدد جذورها هو p^m.

ليكن $F = \{\alpha_1, \alpha_2, \dots, \alpha_{p^m}\} = \{\alpha \in K | \alpha^{p^m} = \alpha\}$ هي جميع جذور g .

والآن نريد إثبات أن F حقل جزئي من K .

ليكن

$$a, b \in F \Longrightarrow a^{p^m} = a \wedge b^{p^m} = b \Longrightarrow a + b \in F$$

كذلك $(ab)^{p^m} = a^{p^m} b^{p^m} = ab$

$$\Longrightarrow ab \in F$$

وعليه فإن F حقل جزئي من K أي أنه حقل.

وعليه نكون قد أثبتنا أنه يوجد حقل F يحوي p^m من العناصر.

الآن لإثبات الوحدانية نفرض أن F' حقل آخر يحوي p^m من العناصر. من التمهيدية (١-١-٣) نجد F' وF متماثلان وبالتالي نكون قد أنهينا البرهان.

مثال :

أثبت وجود حقل رتبته1331 وأنه وحيد تحت سقف التماثل .

الحل:

نلاحظ أن $1331 = 11^3$وبالتالي فإن الحقل الذي رتبته 1331 هو حقل الانشطار لكثيرة الحدود $g(x) = x^{11^3} - x$ على $\mathbb{Z}_{11}$.

الآن ليكن F'وF حقلين رتبة كل منهما 11^3 فان $F \cong F'$ وذلك من التمهيدية (١-١-٣) وبالتالي فإن الحقل الذي يحوي 11^3 من العناصر هو حقل وحيد تحت سقف التماثل .

(١-٢) البناء الضربي للحقول المنتهية

نعود لبعض الوقت لنظرية الزمر . إن النتيجة التي ننشدها من نظرية الزمر تحدد بناء أي زمرة جزيئية من زمرة العناصر غير الصفرية في أي حقل بالنسبة لعملية الضرب ، وعلى وجه الخصوص تحدد البناء الضربي لأي حقل منتهي.

تمهيدية(١-٢-١)

لتكن Gزمرة إبدالية منتهية فيها تتحقق العلاقة$x^n = e$ لعدد من العناصر لا يزيد عن n وذلك لكل عدد صحيح موجب n . عندئذ G زمرة دورية .

البرهان :

سنتطرق في البرهان لحالتين :

الحالة الأولى : إذا كانت رتبة G قوى لعدد أولي

ليكن $a \in G$ عنصرا رتبته اكبر ما يمكن فإن هذه الرتبة يجب أن تكون q^r لعدد صحيح موجب r. إن العناصر $e, a, a^2, \dots a^{q^r-1}$ تعطينا q^r من الحلول المختلفة للمعادلة $x^{q^r} = e$ وحسب فرضيتنا تكون هذه العناصر هي جميع حلول تلك المعادلة .

الآن إذا كانت رتبة b في G هي q^s بحيث $s \leq r$ فإن
$b^{q^r} = (b^{q^s})^{q^{r-s}} = (e)^{q^{r-s}} = e$ ومما ذكرناه أعلاه فان هذا يجعل $b = a^i$ لعدد ما i مما يجعل G دورية .

الحالة الثانية : إذا كانت G زمرة إبدالية عامة فيمكن النظر إليها على النحو $G = S_{q_1} S_{q_2} \dots S_{q_k}$ بحيث S_{q_i} هي زمر سيلو الجزئية في G و q_i هي القواسم الأولية لرتبة G .

وبما أن G هي عبارة عن حاصل ضرب داخلي لزمر سيلو الجزئية فإنه يمكن كتابة كل عنصر g في G بصورة وحيده على الصورة :

$$g = s_1 s_2 \dots s_k$$

إن كل حل للمعادلة $x^n = e$ في S_{q_i} هو حل لذات المعادلة في G ، لذا فإن فرضيتنا على G تنطبق على S_{q_i} ،وحسب الحالة الأولى من البرهان نجد أن S_{q_i} زمرة دورية مولدة بعنصر نرمز له بـ a_i .

الآن ندعي أن $c = a_1 a_2 \dots a_k$ يولد G ، ومن أجل التحقق من ذلك ما علينا سوى بيان أن $|\langle c \rangle| \,\|\, |G|$ ولنرمز لرتبة c بـ m .

لما كان رتبة c هي m ، فإن $c^m = e$ وعليه يكون

$a_1{}^m a_2{}^m \dots a_i{}^m = e$ ومن وحدانية تمثيل عناصر G كحاصل ضرب لعناصر في S_{q_i} نستنتج أن $a_i{}^m = e$ وعليه

$|S_{q_i}| \,\|\, m$ لكل i وعليه فان:

$$|G| = |S_{q_1}||S_{q_2}| \dots |S_{q_k}| \,\|\, m$$

ولكن $m \| G|$ لذا فان $m=|G|$.

وعليه فان G زمرة دورية .

إن لهذه التمهيدية استنتاج مهم وهو التمهيدية التالية:

تمهيدية (١-٢-٢) :

ليكن K حقلا وG زمرة جزئية منتهية من زمرة العناصر غير الصفرية في K بالنسبة لعملية الضرب . عندئذ فان G زمرة دورية .

البرهان :

لما كان K حقلا فإن عدد الجذور لكثيرة الحدود

$x^n - 1 \in K[x]$ لا يزيد عن n لكل عدد صحيح موجب n مما يجعل ذات الشيء ينطبق على G . وبهذا تكون فرضية التمهيدية السابقة قد تحققت وبالتالي فإن G زمرة دورية .

بالرغم من كون حالة الحقل المنتهي حالة خاصة من التمهيدية السابقة إلا إننا نفردها بسبب أهميتها .

مبرهنة(١-٢-١) :

زمرة العناصر غير الصفرية في حقل منته بالنسبة لعملية الضرب هي زمرة دورية .

البرهان :

ليكن F حقل منته ، فإنه بمجرد تطبيق التمهيدية السابقة على $K \equiv F$ وG زمرة العناصر غير الصفرية في F نحصل على المبرهنة .

(١-٣) طرق عد

نختتم هذا البند بتقديم طرق عد نبرهن منها على وجود حلول لمعادلات معينة في الحقل المنتهي . وسوف نحتاج هذا في البرهان الثاني لمبرهنة فدربرن .

تمهيدية (١-٣-١):

ليكن F حقلا منتهياً ، $\alpha \neq 0$ و $\beta \neq 0$ عنصرين في F فإنه يوجد عنصران a, b في F بحيث :

$$1 + \alpha a^2 + \beta b^2 = 0$$

البرهان :

بما أن F حقلا منتهياً فإن مميزه عدد أولي p .وفي البرهان سندرس في حالة كون $p = 2$ وفي حالة كون p عدد أولي فردي

الحالة الأولى " $p = 2$ " :

إذا كان مميز F يساوي2 ، فإن عدد عناصر F يساوي 2^n، أي عنصر x في F يحقق $x^{2^n} = x$ ، لذا فإن كل عنصر في F هو مربع لعنصر آخر. وعلى وجه الخصوص

$\beta^{-1} = b^2$ لعنصر $b \in F$ باستخدام هذا العنصر b و $a = 0$ نحصل على :

$$1 + \alpha a^2 + \beta b^2 = 1 + 0 + \beta\beta^{-1} = 1 + 1 = 0$$

وذلك لأن مميز F يساوي 2 .

الحالة الثانية :

إذا كان p عدد أولي فردي فإن عدد عناصر F يساوي p^n.

الآن دع $W_\alpha = \{1 + \alpha x^2 | x \in F\}$

لحساب عدد عناصر W_α نأخذ التطبيق $f : F^* \to F^*$ حيث $f(x) = x^2$
ومن السهل التحقق بأن هذا التطبيق تشاكل غامر. وعليه فإن
$F^*/\ker f \cong \operatorname{Im} f$.

$$\begin{aligned}\ker f &= \{x \mid f(x) = x^2 = 1\} \\ &= \{x \mid x = \pm 1\} = \{-1, 1\}\end{aligned}$$

لذا $F^*/\{-1,1\} \cong \operatorname{Im} f$ وعليه فإن $\left|F^*/\{-1,1\}\right| = \frac{p^n - 1}{2}$. بأخذ $S = \operatorname{Im} f$
والتطبيق $g : S^* \to F^*$ حيث $g(x) = 1 + \alpha x$ من السهل التحقق أنه أحادي
أي أنه يحافظ على عدد العناصر، بالتالي فإن عدد عناصر W_α هو :

$$1 + (p^n - 1)/2 = (p^n + 1)/2$$

وبطريقة مشابهة نستنتج أن عدد عناصر

$W_\beta = \{-\beta x^2 | x \in F\}$ هو $(p^n + 1)/2$

ولما كان عدد العناصر في كل من W_α وW_β يزيد على نصف عدد العناصر في F فلابد أن يكون تقاطعهما غير خال .

ليكن $c \in W_\beta \cap W_\alpha$ ، لما كان $c \in W_\alpha$ فإن $c = 1 + \alpha a^2$
لعنصر ما a في F.

وكذلك لكون $c \in W_\beta$ فإن $c = -\beta b^2$ لعنصر ما b في F .

وعليه فإن $-\beta b^2 = 1 + \alpha a^2$ وبنقل الطرف الأيسر للطرف الأيمن نحصل على المطلوب .

الفصل الثاني

حول حلقات القسمة المنتهية

كثيرات الحدود الدورية ، مبرهنة فدربرن

مقدمة:

في هذا البند سنقدم دراسة عن حلقات القسمة المنتهية حيث سنعرض مبرهنة فدربرن التي تعتبر الآن تقليدية وهي أن أية حلقة قسمة منتهية يجب أن تكون حقلاً . لقد حازت هذه النتيجة على اهتمام أغلب علماء الرياضيات لأنها غير متوقعة ، حيث إنها تربط بين شيئين يبدو أنه لا علاقة بينهما , وهما عدد العناصر في نظام جبري معين وعملية الضرب في ذلك النظام .

ولأهميتها لدينا سنعرض برهانين مختلفين لهذه النتيجة المهمة ، كما فعل جاوس في نتيجة التربيع التعاكسي فقد برهنها سبع مرات بطرق مختلفة مما يدل على أهمية النتيجة .

(٢-١) كثيرات الحدود الدورية

تعريف ١:

يقال عن عدد مركب θ أنه جذر بدائي للواحد من الرتبة n إذا كان $\theta^n = 1$ ولكن $\theta^m \neq 1$ لكل عدد صحيح موجب $m < n$.

تعريف٢:

تدعى كثيرة الحدود $\Phi_n(x) = \prod(x - \theta)$ بكثيرة حدود دورية إذا كان يشمل حاصل الضرب جميع الحدود التي فيها جذر بدائي للواحد من الرتبة n .

تعريف٣ :

ليكن $n \in Z^+$ فإننا نعرف دالة موبياس كالتالي :

$$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & p^2 \mid n \\ (-1)^k & n = p_1 p_2 \cdots p_k \end{cases}$$

مثال١:

١) $\mu(15) = \mu(3 \times 5) = (-1)^2 = 1$

٢) $\mu(16) = 0$ وذلك لأن $2^2 \mid 16$

مثال٢ :

$$\Phi_5(x) = \prod_{d \mid 5} (x^d - 1)^{\mu(5/d)}$$

بحيث μ هي دالة موبياس .

$$\Phi_5(x) = (x^5 - 1)(x - 1)^{-1}$$

$$= (x - 1)(x^4 + x^3 + x^2 + x + 1)(x - 1)^{-1}$$

$$= (x^4 + x^3 + x^2 + x + 1)$$

مثال٣ :

$$\Phi_6(x) = \prod_{d|6}(x^d - 1)^{\mu(6/d)}$$

$$\Phi_6(x) = (x-1)(x^2-1)^{-1}(x^3-1)^{-1}(x^6-1)$$

$$= (x+1)^{-1}(x^3+1) = x^2 - x + 1$$

نلاحظ في المثالين السابقين أن كثيرتي الحدود الدورية هما كثيرتي حدود واحديه معاملاتها أعداد صحيحة ، وهذا سيقودنا إلى أن نعمم الفكرة على $\Phi_n(x)$ لكل عدد صحيح n.

تمهيديه (٢-١-١)

إن $\Phi_n(x)$ كثيرة حدود واحديه جميع معاملاتها أعداد صحيحة .

البرهان :

لتكن $x^n - 1$ كثيرة حدود على حقل الأعداد المركبة □ ، بحيث $x^n - 1 = \prod(x - \lambda)$ حيث حاصل الضرب يشمل جميع الجذور البدائية للواحد من الرتبة n .

الآن نعيد تجميع عوامل $x^n - 1$ لنحصل على :

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

باستعمال الاستقراء الرياضي على n "المبدأ الثاني "

الخطوة الأولى : عندما n=1 فإن :

$$x - 1 = \Phi_1(x)$$

فرضية الاستقراء : نفرض صحة العبارة لكل $1 \leq d \leq n-1$،

ونريد إثباتها لـ n .

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

$\Phi_d(x)$ كثيرة حدود واحدية معاملاتها أعداد صحيحة لكل $d \neq n, d \mid n$

وعليه فانه:

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

$$= \Phi_n(x) g(x)$$

$$\Longrightarrow \Phi_n(x) = (x^n - 1) / g(x)$$

وبما أن $g(x), (x^n - 1)$ كثيرات حدود واحديه معاملاتها أعداد صحيحة ، فإن حاصل القسمة $\Phi_n(x)$ كذلك .

تمهيدية (٢-١-٢)

يوجد عدد صحيح موجب أكبر من الواحد يقسم

$(q^n - 1) / (q^m - 1)$ بحيث $m \mid n$ ولا يقسم $(q - 1)$.

البرهان :

لتكن $\Phi_n(x)$ كثيرة حدود دورية ولندعي أنه لأي قاسم m للعدد n بحيث $n \neq m$ أن : $\Phi_n(x) | (x^n - 1) / (x^m - 1)$

ولكي نثبت صحة ادعائنا نلاحظ أن :

$$x^m - 1 \equiv \prod_{k|m} \Phi_k(x)$$

وبما أن كل قاسم لـ m هو قاسم لـ n فبإعادة تجميع العوامل في الجهة اليمنى من

$$x^n - 1 = \prod_{m|n} \Phi_m(x)$$

فإننا نحصل على $x^m - 1$ في تلك الجهة .

ولكون $m<n$ فان $x^m - 1$ لا يشمل على $\Phi_n(x)$ إذا :

$$x^n - 1 = \Phi_n(x)(x^m - 1)f(x)$$

بحيث $f(x) \equiv \prod_{\substack{k|n, n\neq k \\ k\nmid m}} \Phi_k$.

مما يجعل معاملات $f(x)$ أعداد صحيحة إذنَ

$$(x^n - 1) / (x^m - 1) = \Phi_n(x) f(x)$$

$$\Longrightarrow \Phi_n(x) | (x^n - 1) / (x^m - 1)$$

الأمر الذي يعني أن خارج القسمة هو كثيرة حدود معاملاتها أعداد صحيحة وهذا يبرهن على صحة ادعائنا .

وعليه فإنه لكل عدد صحيح q يكون $\Phi_n(q)$ عدد صحيح ، بحيث

$\Phi_n(q)|(q^n-1)/(q^m-1)$ و $\Phi_n(q)|q^n-1$

الآن بقي إثبات أن $\Phi_n(q) \nmid q-1$ حيث $n>1$.

بما أن $\Phi_n(q)=\prod(q-\theta)$ حيث إن مجال θ هو جميع الجذور البدائية من الرتبة n.

وكذلك $|q-\theta|>q-1$ لكل $\theta \neq 1$ فإن :

$$|\Phi_n(q)|=\prod|(q-\theta)|>q-1$$

وعليه فإن $\Phi_n(q) \nmid q-1$.

تمهيدية (٢-١-٣)

لتكن D حلقة قسمة منتهية ، وليكن $a \in D$. فإن $N(a)$ حلقة قسمة جزئية في D .

البرهان :

$$N(a)=\{x \in D | ax=xa\}$$

$1 \in D$ $\Rightarrow a1=1a$

$\Rightarrow 1 \in N(a)$

$\Rightarrow N(a) \neq \varphi$

2\ $x, y \in N(a) \Rightarrow x = a^{-1}xa \wedge y = a^{-1}ya$

$$xy = (a^{-1}xa)(a^{-1}ya)$$

$$= a^{-1}x(aa^{-1})ya$$

$$= a^{-1}xy\,a$$

$$\Rightarrow xy \in N(a)$$

3\ $x, y \in N(a) \Rightarrow x - y = a^{-1}xa - a^{-1}ya$

$$= a^{-1}(x - y)a$$

$$\Rightarrow x - y \in N(a)$$

من 1,2,3 نجد أن $N(a)$ حلقة جزئية من D

وبما أن D حلقة قسمة منتهية فإن $N(a)$ حلقة قسمة جزئية منتهية من D .

(٢-٢)البرهان الأول لمبرهنة فدربرن

مبرهنة (فدربرن) :

إن كل حلقة قسمة منتهية هي حقل .

البرهان الأول :

لتكن K حلقة قسمة منتهية ، وليكن مركزها هو

$$Z = \{z \in K | zx = xz \quad \forall x \in K\}$$

نعلم أن Z حقل منتهي وكذلك $Z \subset K$.

فإذا كان عدد عناصر Z هو q ، فإن عدد عناصر K هو q^n حيث $n = [K:Z]$ "وفقا لتمهيدية (١-١-١)".

"إن الغاية هو برهان أن $Z=K$ أو أن $n=1$ " .

ليكن $a \in K$ بحيث

$$N(a) = \{x \in K | ax = xa\}$$

من التمهيدية السابقة نعلم أن $N(a)$ حلقة قسمة جزئية في K ، كذلك $Z \subset N(a)$. لذلك فإن $N(a)$ تحوي $q^{n(a)}$ من العناصر حيث $n(a)$ عدد صحيح موجب .

إن $n(a)|n$ وذلك لأن العناصر غير الصفرية في $N(a)$ تكون زمرة جزئية من زمرة العناصر غير الصفرية في K بالنسبة لعملية الضرب ، والتي عدد عناصرها $q^n - 1$ وبالتالي فإنه من مبرهنة لاجرانج والتي تنص على " إذا كانت G زمرة منتهية وكانت $H \leq G$ فإن $|H| \,|\, |G|$ "

يكون لدينا $q^{n(a)} - 1 | q^n - 1$ ومنه فإن $n(a)|n$.

من نظرية الزمر ، نعلم أن عدد العناصر المرافقة لـ a في زمرة العناصر غير الصفرية يساوي دليل منظم a في زمرة العناصر غير الصفرية في K . أي أن

$$c_a = (q^n - 1) / (q^{n(a)} - 1)$$

ومن مبرهنة سابقة في نظرية الزمر "يكون $n(a) = n \Leftrightarrow a \in Z$ " .

لذلك من معادلة الفصول يكون :

$$q^n - 1 = q - 1 + \sum_{\substack{n(a)|n \\ n(a)\neq n}} (q^n - 1) / (q^{n(a)} - 1)$$

الآن إذا كان $\Phi_n(q)|q^n - 1$ ، فإن

$\Phi_n(q)$ تقسم المجموع وتقسم $q - 1$ ولكن هذا يؤدي إلى تناقض مع التمهيدية (٢-١-٢) وبالتالي فانه لابد أن يكون $n(a) = n$ ، بالتالي

$a \in Z$. أي أن $K \subset Z$ ولكن $Z \subset K$ وعليه فإن :

$Z = K$ أي أن K حقل .

(٢-٣) البرهان الثاني لمبرهنة فدربرن

الآن قبل أن نطرح البرهان الثاني لمبرهنة فدربرن نحتاج إلى بعض التمهيديات التي ستساعدنا في البرهان .

تمهيدية (٢-٣-١)

لتكن R حلقة و $a \in R$ وليكن T_a التطبيق من R إلى نفسها والمعرف بـ $xT_a = xa - ax$ فإن :

$$xT_a^m = xa^m - maxa^{m-1} + \frac{m(m-1)}{2}a^2xa^{m-2} - \frac{m(m-1)(m-2)}{3!}a^3xa^{m-3} + \cdots$$

البرهان :

سنبرهن هذه التمهيدية باستخدام الاستقراء الرياضي :

الخطوة الأولى : عندما $m = 1$ فان :

$$xT_a = xa - ax$$

إذن المبرهنة صحيحة عند $m = 1$.

خطوة الاستقراء : نفرض صحة التمهيدية عند $m - 1$ ، أي أنه إذا كانت $xT_a = xa - ax$ فإن :

$$xT_a^{m-1} = xa^{m-1} - (m-1)axa^{m-2} + \frac{(m-1)(m-2)}{2}a^2xa^{m-3} - \frac{(m-1)(m-2)(m-3)}{3!}a^3xa^{m-4} + \cdots$$

ونريد إثباتها عند m.

$$xT_a^m = (xT_a^{m-1})T_a = \left[xa^m - (m-1)axa^{m-1} + \frac{(m-1)(m-2)}{2}a^2xa^{m-2} - \frac{(m-1)(m-2)(m-3)}{3!}a^3xa^{m-3} + \cdots\right] - \left[axa^{m-1} - (m-1)a^2xa^{m-2} + \frac{(m-1)(m-2)}{2}a^3xa^{m-3} - \cdots\right]$$

$$\Rightarrow xT_a^m = xa^m - maxa^{m-1} + \frac{m(m-1)}{2}a^2xa^{m-2} - \frac{m(m-1)(m-2)}{3!}a^3xa^{m-3} + \cdots$$

نتيجة (١)

إذا كانت R حلقة فيها $px = 0$ لكل x في R حيث p عدد أولي فان

$$xT_a^{p^m} = xa^{p^m} - a^{p^m}x$$

البرهان :

سندرس البرهان في حالة كون $p=2$ وفي حالة كون p عدد أولي فردي

أولا : إذا كان $p=2$:

فإنه استناداً إلى الصيغة في التمهيدية السابقة :

$$xT_a^2 = xa^2 - 2axa + a^2x$$

$$= xa^2 - a^2x$$

وذلك لأن $2axa = 0$ ومنه نستنتج :

$$xT_a^{2^2} = (xT_a^2)T_a^2 = (xa^2 - a^2x)a^2 - a^2(xa^2 - a^2x)$$

$$= x\,a^{2^2} - 2a^2xa^2 - a^{2^2}x$$

$$= x\,a^{2^2} - a^{2^2}x$$

أيضاً

$$xT_a^{2^3} = (xT_a^{2^2})T_a^{2^2} = (x\,a^{2^2} - a^{2^2}x)a^{2^2} - a^{2^2}(x\,a^{2^2} - a^{2^2}x)$$

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

وهكذا بالنسبة لـ $xT_a^{2^m}$.

ثانياً : إذا كان p عدد أولي فردي ، باستخدام صيغة التمهيدية السابقة مرة أخرى نحصل على :

$$xT_a^p = xa^p - paxa^{p-1} + \frac{p(p-1)}{2}a^2xa^{p-2} + \cdots - a^px$$

ولما كان :

$$p \left| \frac{p(p-1)\ldots(p-i+1)}{i!} \right.$$

وذلك لكل $i < p$. أي أن جميع الحدود الوسيطية تساوي صفر، فنستنتج أن :

$$xT_a^p = xa^p - a^px = xT_{a^p}$$

الآن

$$xT_a^{p^2} = x(T_{a^p})^p = xT_{a^{p^2}}$$

وهكذا بالنسبة للقوى العليا لـ p .

تمهيدية(٢-٣-٢)

لتكن D حلقة قسمة مميزها $p > 0$، مركزها Z وليكن

$P = \{0,1,\ldots,(p-1)\}$ الحقل الجزئي من المركز Z الذي يماثل Z_p .

لنفرض أن $a \in D$ و $a \notin Z$ بحيث $a^{p^n} = a$ لعدد ما $n \geq 1$ ، فإنه يوجد $x \in D$ بحيث :

١. $xax^{-1} = a^i \neq a$ لعدد صحيح i

٢. $xax^{-1} \in P(a)$ حيث $P(a)$ هو الحقل الذي نحصل عليه بضم a إلى p .

البرهان:

لنعرف التطبيق $T_a: D \longrightarrow D$ حيث $yT_a = ya - ay$ لكل $y \in D$.

بما أن a جبري على P، فان $P(a)$ حقل منتهي ولنفرض أن عدد عناصره هو p^m .

وفقا لنتيجة(٢) للتمهيدية(١-١-٢) فانه لأي $u \in P(a)$ يكون $u^{p^m} = u$.

ومن نتيجة التمهيدية السابقة نجد أن :

$$yT_a^{p^m} = ya^{p^m} - a^{p^m}y = ya - ay = yT_a$$

$$\Rightarrow T_a = T_a^{p^m}$$

الآن إذا كان $\lambda \in P(a)$ فإن :

$$(\lambda x)T_a = (\lambda x)a - a(\lambda x) = \lambda(xa) - \lambda(ax)$$
$$= \lambda(xa - ax) = \lambda(xT_a)$$

وذلك لأن λ تتبادل مع a .

لذا فإن التطبيق λI من D إلى نفسها والمعرف بـ $I\lambda: y \mapsto \lambda y$ يتبادل مع T_a لكل $\lambda \in P(a)$.

من تمهيدية (١-١-٢) فإن كثيرة الحدود $u^{p^m} - u$ تتحلل على $P(a)$ كما يلي :

$$u^{p^m} - u = \prod_{\lambda \in P(a)} (u - \lambda)$$

ولما كان T_a يتبادل مع $\mathrm{I}\lambda$ لكل $\lambda \in P(a)$ ولكون $T_a = T_a^{p^m}$ فإن :

$$0 = T_a - T_a^{p^m} = \prod_{\lambda \in P(a)} (T_a - \lambda \mathrm{I})$$

الآن نفرض جدلاً أنه لكل $0 \neq \lambda \in P(a)$ بحيث لأي عنصر غير صفري في D لا يعدم التطبيق $T_a - \lambda \mathrm{I}$

"أي أنه إذا كان $y(T_a - \lambda \mathrm{I}) = 0$ فان $y = 0$ " .

لما كان $T_a(T_a - \lambda_1 \mathrm{I}) \dots (T_a - \lambda_k \mathrm{I}) = 0$ بحيث $\lambda_1, \dots, \lambda_k$ عناصر غير صفرية في $P(a)$, ومنه نستنتج أن $T_a = 0$ أي أن :

$yT_a = ya - ay = 0$ لكل $y \in D$ وهذا يجعل $a \in \mathrm{Z}$ مما يناقض الفرض.

وعليه فانه يوجد $0 \neq \lambda \in P(a)$ و $0 \neq x \in D$ بحيث:

$$x(T_a - \lambda \mathrm{I}) = 0$$

$$\Rightarrow xa - ax - \lambda x = 0$$

$$\Rightarrow xa - (a + \lambda)x = 0$$

$$\Rightarrow xa = (a + \lambda)x$$

$$\Rightarrow xax^{-1} = (a + \lambda) \neq a \qquad \text{لان } 0 \neq \lambda \text{ ____}$$

وبما $\lambda, a \in P(a)$ فإن $xax^{-1} = (a + \lambda) \in P(a)$.

الآن لتكن رتبة a تساوي s ، فإنه في الحقل $P(a)$ جميع جذور $u^s - 1$ هي

$1, a, a^2, \dots, a^{s-1}$ وهي مختلفة عن بعضها لأن رتبة a تساوي s .

ولما كان $(xax^{-1})^s = xa^s a^{-1} = 1$ ولكون $xax^{-1} \in P(a)$ فإن:

xax^{-1} هو جذر في $P(a)$ لـ $u^s - 1$ لذلك فإن :

$$xax^{-1} = a^i \neq a$$

ملاحظة :

لتكن D حلقة قسمة منتهية ، مركزها Z فإنه بالاستقراء الرياضي يمكن الفرض أن أية حلقة قسمة عدد عناصرها أقل من عدد عناصر D هي حقل.

تمهيدية (٢-٣-٣) :

لتكن D حلقة قسمة منتهية ، مركزها Z وليكن $a, b \in D$ بحيث $b^t a = ab^t$ ولكن $ab \neq ba$ فإن $b^t \in Z$.

البرهان:

لنعتبر $N(b^t) = \{x \in D | b^t x = xb^t\}$ فإن $N(b^t)$ حلقة قسمة جزئية في D . إذا كانت $N(b^t) \neq D$ فإنه حسب الملاحظة السابقة فإن $N(b^t)$ ولكن كلاً من $a, b \in N(b^t)$ وهما لا يتبادلان . وعليه فإنه لابد أن تكون $N(b^t) = D$ فإن $b^t \in Z$.

تعريف :

لتكن D حلقة قسمة منتهية ، مركزها Z وليكن $a \in D$ فإننا نعرف رتبة a بالنسبة لـ Z بأنه أصغر عدد صحيح موجب $m(a)$ يحقق $a^{m(a)} \in Z$.

الآن أصبح لدينا كل ما نحتاجه لتقديم البرهان الثاني لمبرهنة فدربرن .

البرهان الثاني لمبرهنة فدربرن :

ليكن $a \in D$ و $a \notin Z$ بحيث تكون رتبة a بالنسبة لـ Z أصغر مايمكن ولنرمز لها بـ r فإن $a^r \in Z$.

الآن ندعي أن r عدد أولي .

لأنه لو كان $r = r_1 r_2$ حيث $1 < r_1 < r$ فإن $a^{r_1} \notin Z$ ولكن $(a^{r_1})^{r_2} = a^r \in Z$ وهذا يعني أن رتبة a^{r_1} بالنسبة لـ Z أصغر من رتبة a بالنسبة لـ Z ،وهذا يناقض كون رتبة a أصغر ما يمكن بالنسبة لـ Z وهذا يبرهن على صحة ادعائنا .

وفقا للتمهيدية (٢-٣-٢) يوجد $x \in D$ بحيث $xax^{-1} = a^i \neq a$ لذا:

$$x^2ax^{-2} = x(xax^{-1})x^{-1} = (xax^{-1})^i = a^{i^2}$$

وبصورة مشابهة نحصل على :

$$x^{(r-1)}ax^{-(r-1)} = a^{i^{(r-1)}}$$

وبما أن r عدد أولي فانه من مبرهنة فرما الصغرى نجد أن :

$$i^{r-1} \equiv 1 \ mod \ r$$

$$\Leftrightarrow i^{r-1} = 1 + ru_0$$

وعليه فإن :

$$a^{i^{(r-1)}} = a^{1+ru_0} = aa^{ru_0} = \lambda a$$

بحيث $\lambda = a^{ru_0}$ فإن $\lambda \in Z$.

لذا فإن

$$x^{(r-1)}ax^{-(r-1)} = \lambda a$$

$$\Rightarrow x^{(r-1)}a = \lambda a x^{(r-1)}$$

ولكون $x \notin Z$ فمن طبيعة اختيارنا لـ r فإن $x^{r-1} \notin Z$ ولما كان $xa \neq ax$ فإنه من التمهيدية السابقة $x^{(r-1)}a \neq ax^{(r-1)}$ أي أن $\lambda \neq 1$.

الآن دع $b = x^{r-1}$ فيصبح لدينا $bab^{-1} = \lambda a$ ونتيجة لذلك :

$$\lambda^r a^r = (bab^{-1})^r$$

$$= ba^r b^{-1}$$

$$= a^r \quad \text{لان } a^r \in Z$$

$$\therefore \lambda^r a^r = a^r \Longrightarrow \lambda^r = 1$$

إننا ندعي أنه إذا كان $y \in D$ وطالما كان $y^r = 1$ فإنه يجب أن يكون $y = \lambda^i$ لعدد ما i.

وذلك لأنه في الحقل $Z(y)$ يوجد على الأكثر r من الجذور لكثيرة الحدود $u^r - 1$. إن العناصر $1, \lambda, \lambda^2, \dots, \lambda^{r-1}$ مختلفة عن بعضها لأن رتبة λ هي العدد الأولي r وتعطينا هذه العناصر جميع جذور $u^r - 1$ في $Z(y)$ والتي عددها r وهذا يجعل $y = \lambda^i$.

لما كان $\lambda^r = 1$ فإن :

$$b^r = \lambda^r b^r = (a^{-1}ba)^r$$

$$= a^{-1}b^r a$$

$$\therefore ab^r = b^r a$$

وبما أن $ab \neq ba$ فإنه من التمهيدية السابقة $b^r \in Z$.

نعلم من مبرهنة(١-٢-١) أن زمرة العناصر غير الصفرية في Z بالنسبة لعملية الضرب زمرة دورية .وليكن γ في Z مولداً لهذه الزمرة .

لما كان $a^r, b^r \in Z$ فإنه يوجد k , j بحيث :

$$a^r = \gamma^j \ , \quad b^r = \gamma^k$$

الآن إذا كان $r|j$ فإن $j = rs$ فعليه :

$$a^r = \gamma^{rs} \implies a^r/\gamma^{rs} = 1$$
$$\implies (a/\gamma^s)^r = 1 \implies a/\gamma^s = \lambda^i$$

وهذا يجعل $a \in Z$ وهو مناقض لكون $a \notin Z$. إذن لابد أن يكون $r \nmid j$.

وبصورة مشابهة نثبت أن $r \nmid k$.

الآن دع $a_1 = a^k \quad , \quad b_1 = b^j$ إن حساباً مباشراً ابتداءً بـ $ba = \lambda a$ يبين أن $a_1 b_1 = \mu b_1 a_1$ بحيث $\mu = \lambda^{-jk}$.

ولما كان r عدد أولي والذي هو رتبة λ لايقسم j أو k ، فإن $\lambda^{jk} \neq 1$ إذن $\mu \neq 1$.

كذلك $\mu^r = (\lambda^{-jk})^r = (\lambda^r)^{-jk} = 1$.

الآن أوجدنا عنصرين a_1, b_1 بحيث :

١- $a_1^r = b_1^r = \alpha \in Z$.

٢- $a_1 b_1 = \mu b_1 a_1$ بحيث $\mu \neq 1$.

٣- $\mu^r = 1$.

الآن لنحسب $(a_1^{-1} b_1)^r$

$$(a_1^{-1}b_1)^2 = (a_1^{-1}b_1)(a_1^{-1}b_1) = a_1^{-1}(b_1 a_1^{-1})b_1$$

$$= a_1^{-1}(\mu a_1^{-1}b_1)b_1 = \mu a_1^{-2}b_1^2$$

$$(a_1^{-1}b_1)^3 = (\mu a_1^{-2}b_1^2)(a_1^{-1}b_1) = \mu a_1^{-2}(b_1^2 a_1^{-1})b_1$$

$$= \mu a_1^{-2}(\mu b_1 a_1^{-1}b_1)b_1 = \mu a_1^{-2}\mu(b_1 a_1^{-1})b_1^2$$

$$= \mu a_1^{-2}\mu(\mu a_1^{-1}b_1)b_1^2 = \mu^{1+2}a_1^{-3}b_1^3$$

إذن بالاستمرار نحصل على:

$$(a_1^{-1}b_1)^r = \mu^{1+2+\cdots+(r-1)}a_1^{-r}b_1^r = \mu^{1+2+\cdots+(r-1)}$$

$$= \mu^{r(r-1)/2}$$

هناك حالتان :

الحالة الأولى : إذا كان r عدد أولي فردي فإن :

$$\mu^{r(r-1)/2} = 1$$

وعليه $(a_1^{-1}b_1)^r = 1 \Longrightarrow a_1^{-1}b_1 = \lambda^i$

$$\Longrightarrow b_1 = a_1\lambda^i$$

ولكن حينئذ $\mu b_1 a_1 = a_1 b_1 = b_1 a_1$ وهذا يناقض كون $\mu \neq 1$

لذلك إذا كان r عدد أولي فردي فإننا نكون قد برهنا على المبرهنة .

الحالة الثانية : إذا كان $r=2$ في هذه الحالة يكون لدينا a_1, b_1 بحيث:

١ـ $a_1^2 = b_1^2 = \alpha \in Z$.

٢ـ $a_1 b_1 = \mu b_1 a_1$ بحيث $\mu \neq 1$.

٣ـ $\mu^2 = 1$.

فإن $\mu = -1$ " لأن $\mu \neq 1$ " .

وعليه فإن $a_1 b_1 = -b_1 a_1 \neq b_1 a_1$.

نستنتج من ذلك أن مميز D لا يساوي 2.

واستناداً لتمهيدية سابقة يوجد $\xi, \eta \in Z$ بحيث :

$$1 + \xi^2 + \alpha\eta^2 = 0$$

الآن لنعتبر

$$(a_1 + \xi b_1 + \eta a_1 b_1)^2 = a_1^2 + \xi^2 b_1^2 + \eta^2 (a_1 b_1)^2$$

$$= \alpha + \xi^2\alpha + \eta^2\alpha^2 = \alpha(1 + \xi^2 + \eta^2\alpha) = 0$$

ولكوننا في حلقة قسمة نجد أن $a_1 + \xi b_1 + \eta a_1 b_1 = 0$

$$0 \neq 2a_1^2 = a_1(a_1 + \xi b_1 + \eta a_1 b_1) + a_1(a_1 + \xi b_1 + \eta a_1 b_1)$$
$$= 0$$

إن هذا التناقض ينهي برهان مبرهنة فدربرن .

(٢-٤)مبرهنة جيكوبسن

هناك بعض المميزات للبرهان الثاني لمبرهنة فدربرن منها أننا يمكن أن نستخدم بعض أجزائه لبرهان نتيجة رائعة لعالم الرياضيات جيكوبسن وهي

مبرهنة جيكوبسن :

لتكن D حلقة قسمة ، بحيث لكل عنصر a فيها يوجد عدد صحيح موجب $n(a) > 1$ معتمداً على a بحيث $a^{n(a)} = a$. عندئذ فإن D حقل.

البرهان :

إذا كان $a \neq 0$ في D فإن $a^n = a$ و $(2a)^m = 2a$ لعددين صحيحين $n, m>1$. دع $s=(n-1)(m-1)+1>1$.

إن $a^s = a^{(n-1)(m-1)}a = a$ وكذلك

$(2a)^s = (2a)^{(n-1)(m-1)}(2a) = 2a$ وذلك لأن

$$(2a)^{m-1} = 1 \quad , \quad a^{n-1} = 1$$

ولكن $(2a)^s = 2^s a^s = 2^s a$ وعليه :

$$2^s a = 2a \Rightarrow (2^s - 2)a = 0$$

لذا فإن مميز D هو $p>0$.

إذا كان P هو الحقل الذي يحوي p من العناصر محتوى داخل Z ، فلأن a جبري على P يكون P(a) حقلاً منتهياً عدد عناصره p^h لعدد صحيح موجب h. لذا فلكون a في P(a) يصبح $a^{p^h} = a$. إذن إذا كان $a \notin Z$

فإن جميع شروط التمهيدية (٢-٣-٢) متحققة وعليه يوجد $b \in D$ بحيث

$$bab^{-1} = a^{\mu} \neq a \qquad (١)$$

باستخدام الطريقة نفسها $b^{p^k} = b$ لعدد صحيح $k > 1$. دع

$$W = \{x \in D \mid x = \sum_{i=1}^{p^h} \sum_{j=1}^{p^k} p_{ij} a^i b^j \wedge p_{ij} \in P\}$$

إن W مجموعة منتهية مغلقة بالنسبة لعملية الجمع ، ومن (١) نرى أن W مغلقة بالنسبة لعملية الضرب . لذا فإن W حلقة منتهية، ولكونها حلقة جزئية من حلقة القسمة D ، فيجب أن تكون هي نفسها حلقة قسمة . إذن W حلقة قسمة منتهية وبالتالي من مبرهنة فدربرن فإنها إبدالية . ولكن $a,b \in W$ مما يجعل $ab = ba$ وهذا يناقض كون $a^{\mu}b = ba$ مما يثبت المبرهنة .

إن مبرهنة جيكوبسن في الحقيقة صحيحة لكل حلقة R تحقق $a^{n(a)} = a$ لكل a في R وليست مقتصرة على حلقات القسمة . إن الانتقال من حالة حلقة القسمة إلى الحالة العامة ليس صعباً ولكنه يتطلب استعمال مسلمة الاختيار والتي شرحها يخرجنا عن الإطار العام لموضوع بحثنا .

الفصل الثالث

حلقات القسمة الجبرية على حقل الأعداد الحقيقة

تصنيف حلقات القسمة الجبرية على حقل

الأعداد المركبة ,إحدى مبرهنات فروبينيس

(٣-١)تصنيف حلقات القسمة الجبرية على حقل الأعداد المركبة

في عام ١٨٧٧م صنف العالم الرياضي فروبينيس جميع حلقات القسمة التي تحوي حقل الأعداد الحقيقية في مركزها وتحقق شرطاً آخر نذكره أدناه .

قبل أن نبدأ نذكر بحقيقتين مهمتين عن حقل الأعداد المركبة وهما :

تمهيدية(٣-١-١)

جميع جذور كثيرة الحدود من الدرجة n على حقل الأعداد المركبة تقع في حقل الأعداد المركبة وعددها يساوي n .

البرهان :

لتكن $f(x) \in £[x]$ كثيرة حدود من الدرجة n على حقل الأعداد المركبة ، لما كان £ حقل مغلق جبرياً ، فإن أي كثيرة حدود عليه تكون مختزلة عليه وجميع جذورها تقع فيه .

تمهيدية(٣-١-٢)

إن كثيرات الحدود غير المختزلة على حقل الأعداد الحقيقية هي إما من الدرجة الأولى أو الثانية .

البرهان:

لتكن $f(x) \in ¡[x]$ كثيرة حدود غير مختزلة على ¡ ولنفرض جدلاً أن درجتها أكبر من اثنين . وليكن a جذراً لها فإن $f(x) = (x-a)g(x)$ ، لما كان درجة f أكبر من اثنين فإن درجة g أكبر من الواحد ، ولكن هذا يناقض كون f غير مختزلة وبالتالي لابد أن تكون درجة f أقل أو يساوي اثنين .

تعريف :

يقال عن جبر قسمة D إنه جبري على الحقل F إذا :

١. كان F محتوى في مركز D .

٢. كان كل $a \in D$ يحقق كثيرة حدود غير تافهة معاملاتها في F.

تمهيدية(٣-١-٣) :

ليكن £ حقل الأعداد المركبة ولنفرض أن حلقة القسمة D جبرية على £ . عندئذ $D = £$.

البرهان :

لنفرض أن $a \in D$.

لما كانت D جبرية على £فإن :

$$a^n + \alpha_1 a^{n-1} + \cdots + \alpha_{n-1} a + \alpha_n = 0$$

بحيث $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$

الآن كثيرة الحدود

$g(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1} x + \alpha_n$ في $£[x]$

استناداً للتمهيدية (٣-١-١) يمكن تحليلها في $£[x]$ إلى حاصل ضرب عوامل خطية أي $g(x) = (x - \lambda_1)(x - \lambda_2) \ldots (x - \lambda_n)$ حيث $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$

لما كان £ في مركز D فإن كل عنصر في £ يتبادل مع a لذا :

$$g(a) = (a - \lambda_1)(a - \lambda_2) \ldots (a - \lambda_n)$$

ولكن $g(a) = 0$ بالفرض , إذن $(a - \lambda_1)(a - \lambda_2) \ldots (a - \lambda_n) = 0$ ولما كان حاصل الضرب في حلقة قسمة يساوي الصفر إذا وفقط إذا كان أحد العوامل يساوي صفر, نستنتج أن $a - \lambda_k = 0$ لعدد ما $1 \le k \le n$ وعليه يكون $a = \lambda_k$. إذن $a \in £$ وعليه فإن :

$D \subset £$ ولكن $£ \subset D$ إذن $D = £$.

تمهيدية(٣-١-٤) :

لتكن D حلقة قسمة جبرية على حقل الأعداد الحقيقية ¡ وليكن $a \in D \quad , a \notin ¡$ فإنه يوجد $\alpha, \gamma \in ¡$ بحيث $[{(a-\alpha)}/{\gamma}]^2 = -1$.

البرهان :

بما أن D حلقة قسمة جبرية على ¡ فإن a يحقق كثيرة حدود غير مختزلة على ¡. ووفقا للتمهيدية(٣-١-٢) فإن a يحقق إما كثيرة حدود من الدرجة الأولى أو كثيرة حدود من الدرجة الثانية .

إذا كان a يحقق كثيرة حدود من الدرجة الأولى فإن $a - \alpha = 0$ بحيث $\alpha \in ¡$ وعليه فإن $a \in ¡$ وهذا مناقض للفرض .

إذن a يحقق كثيرة حدود تربيعية . فإنه يمكن الفرض أن $a^2 - 2\alpha a + \beta = 0$ بحيث $\alpha, \beta \in ¡$ لذا $(a-\alpha)^2 = \alpha^2 - \beta$.

لندعي أن $\alpha^2 - \beta < 0$ لأنه لو لم يكن كذلك لكان له جذر تربيعي حقيقي δ ونحصل على $a - \alpha = \pm\delta$ فيكون $a = \pm\delta - \alpha$ إذن $a = \pm\delta - \alpha$ وهذا مناقض للفرض مما يبرهن على صحة إدعاءنا .

ولكون $\alpha^2 - \beta < 0$ فإنه يمكن كتابته على الصيغة $-\gamma^2$ بحيث $\gamma \in ¡$ وعليه فإن :

$$[{(a-\alpha)}/{\gamma}]^2 = -1 \qquad \Leftarrow \qquad (a-\alpha)^2 = -\gamma^2$$

(٣-٢)إحدى مبرهنات فروبينيس

مبرهنة فروبينيس (٣-٢-١):

لتكن D حلقة قسمة جبرية على حقل الأعداد الحقيقية ¡. عندئذ D تماثل واحداً مما يلي :

١- حقل الأعداد الحقيقية . ٢- حقل الأعداد المركبة .

٣- حلقة الرباعيات الحقيقية .

البرهان :

إن البرهان يشتمل على ثلاثة أجزاء .

في الجزء الأول نثبت المبرهنة في حالة كون D إبدالية .

في الجزء الثاني نفرض أن D غير إبدالية وننشيء نموذجا مماثلا للرباعيات الحقيقية .

في الجزء الثالث نبرهن على أن هذا النموذج يحوي D .

إذا كانت D إبدالية فاختر $a \in D$, $a \notin ¡$ فإنه من التمهيدية السابقة يوجد $\alpha, \gamma \in ¡$ بحيث $[{}^{(a-\alpha)}\!/_{\gamma}]^2 = -1$.

اجعل $i = {}^{(a-\alpha)}\!/_{\gamma}$ ليكون $i^2 = -1$.

بما أن $a, \alpha, \gamma \in D$ فإن $i \in D$. ولكون $¡ \subset D$ فإن $¡(i) \subset D$ بحيث $¡(i)$ حقل يماثل حقل الأعداد المركبة .

ولما كانت D إبدالية و جبرية على ¡ ، فإنها حتما جبرية على $¡(i)$ ومن التمهيدية السابقة فإن $¡(i) = D$. إذن إذا كانت D إبدالية فهي إما ¡ أو $¡(i)$.

الآن نفرض أن D غير إبدالية .

لندعي أن مركز D يجب أن يساوي ¡. لأنه لو لم يكن كذلك فإنه يوجد a في مركز D وليس في ¡. ومن التمهيدية السابقة يوجد $\alpha, \gamma \in ¡$ بحيث $[{}^{(a-\alpha)}\!/_{\gamma}]^2 = -1$ مما يجعل المركز يحوي حقلا مماثلا لحقل الأعداد

المركبة ، لكن من تمهيدية سابقة إذا كان حقل الأعداد المركبة (أو حقل مماثل له) موجودا داخل مركز D فإن $D = £$ مما يجعل D إبدالية وهذا يناقض الفرض مما يبرهن على صحة ادعاءنا .

الآن ليكن $a \notin ¡$, $a \in D$ و $i = (a-\alpha)/\gamma$ ، حيث $\alpha, \gamma \in ¡$ و $i^2 = -1$.

لما كان $i \notin ¡$ فإن i ليس في المركز لذا فإنه يوجد $b \in D$ بحيث $c = bi - ib \neq 0$.

الآن لنحسب $ic + ci$

$$\begin{aligned} ic + ci &= i(bi - ib) + (bi - ib)i \\ &= ibi + b - b - ibi = 0 \\ &\Rightarrow ic + ci = 0 \quad \Rightarrow ic = -ci \neq ci \end{aligned}$$

لذا فإن c ليست في مركز D ومن هذا نحصل على :

$$ic^2 = (ic)c = (-ci)c = -c(ic) = -c(-ci) = c^2 i$$

لذا فإن c^2 تتبادل مع i .

إن c يحقق معادلة تربيعية على ¡ على النحو $c^2 + \lambda c + \mu = 0$ ، حيث $\lambda, \mu \in ¡$. ولما كان c^2 و μ يتبادلان مع i فإن λc يتبادل مع i أي أن

$$\begin{aligned} &\lambda ci = i\lambda c = \lambda ic = -\lambda ci \\ &\Rightarrow \quad 2\lambda ci = 0 \end{aligned}$$

ولما كان $2ci \neq 0$ فإن $\lambda = 0$ وعليه فإن $c^2 = -\mu$.

ولما كان $c \notin ¡$ و $c^2 < 0$ فإنه يمكن كتابته على الصيغة $-v^2$ ، حيث $v \in ¡$ إذن $-\mu = -v^2$ فعليه :

$$c^2 = -v^2 \Rightarrow (\frac{c}{v})^2 = -1$$

خذ $j = \frac{c}{v}$ فإن j يحقق:

١- $j^2 = (\frac{c}{v})^2 = -1$.

٢- $ji + ij = \frac{c}{v} i + i \frac{c}{v} = \frac{ci - ci}{v} = 0$.

ضع $k = ij$ ، إن العناصر i, j, k التي أنشأناها تحقق خواص مثيلاتها في الرباعيات .

لذا: $T = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_i \in ¡ \}$ تكون حلقة قسمة جزئية في D مماثلة للرباعيات الحقيقية .

الآن بقي إثبات أن T=D .

ملاحظة: إذا كان $r \in D$ يحقق $r^2 = -1$ فدع $N(r) = \{x \in D \mid xr = rx\}$.

إن N(r) حلقة قسمة جزئية في D ، لذلك فإن r وبالأحرى جميع العناصر $\alpha_0 + \alpha_1 r$ حيث $\alpha_0, \alpha_1 \in ¡$ تقع في مركز N(r) واستناداً إلى تمهيدية سابقة فإن $N(r) = \{\alpha_0 + \alpha_1 r \mid \alpha_0, \alpha_1 \in ¡ \}$. لذا إذا كان $xr = rx$ فإن $x = \alpha_0 + \alpha_1 r$.

الآن نعود إلى البرهان ولنفرض أن $u \in D \quad , u \notin ¡$ فإنه من التمهيدية السابقة يوجد $\alpha, \beta \in ¡$ بحيث $w^2 = [(u - \alpha)/\beta]^2 = -1$.

إننا ندعي أن $wi + iw$ يتبادل مع كلا من w, i وذلك لأن :

$$i(wi + iw) = iwi + i^2 w = iwi + wi^2 = (iw + wi)i \quad \text{لأن } i^2 = -1$$

وبصورة مشابهة $w(wi + iw) = (iw + wi)w$ إذن من الملاحظة أعلاه نجد أن :

$$wi + iw = \alpha_0 + \alpha_1 i = \alpha_0' + \alpha_1' w$$

حيث $\alpha_l, \alpha_l' \in ¡$.

إذا كان $w \notin T$ فإن $\alpha_1 = 0$ (لأنه لو لم يكن كذلك لكان يمكننا كتابة w بدلالة i) لذا $wi + iw = \alpha_0 \in ¡$ ، وبصورة مشابهة

$$wj + jw = \beta_0 \in ¡ \quad و \quad wk + kw = \gamma_0 \in ¡$$

الآن دع $z = w + \frac{\alpha_0}{2} i + \frac{\beta_0}{2} j + \frac{\gamma_0}{2} k$ عندئذ :

$$\begin{aligned} zi + iz &= wi + iw + \frac{\alpha_0}{2}(i^2 + i^2) + \frac{\beta_0}{2}(ji + ij) + \frac{\gamma_0}{2}(ki + ik) \\ &= \alpha_0 - \alpha_0 = 0 \end{aligned}$$

وبصورة مشابهة $zk + kz = 0 \quad \wedge \quad zj + jz = 0$.

ولندعي أن العلاقة $zk + kz = 0$ تجعل $z = 0$ لأن :

$$0 = zk + kz = zij + ijz = (zi + iz)j + i(jz - zj) = i(jz - zj)$$

ولكن $i \neq 0$ فإن $jz - zj = 0$ وعليه $zj = jz$ ،غير أن $zj + jz = 0$ إذن $2jz = 0$
ولما كان $2j \neq 0$ فإن $z = 0$ ، بالرجوع إلى تعبير z نحصل على :

$$w + \frac{\alpha_0}{2} i + \frac{\beta_0}{2} j + \frac{\gamma_0}{2} k = 0 \Rightarrow w = -\frac{\alpha_0}{2} i - \frac{\beta_0}{2} j - \frac{\gamma_0}{2} k$$

مما يجعل $w \in T$ وهذا مناقض لـ $w \notin T$ نستنتج أن W حقاً في T . وحيث إن $w = {(u - \alpha)}/{\beta}$ فإن $u = \beta w + \alpha$ مما يجعل $u \in T$.

لقد برهنا الآن على أن $D \subset T$ ، وبما أن $T \subset D$ فإن $T = D$.

ولما كانت T تماثل حلقة الرباعيات الحقيقية فنحصل على أن D تماثل حلقة الرباعيات الحقيقية مما ينهي برهان المبرهنة .

الفصل الرابع

الرباعيات التامة ومبرهنة المربعات الأربعة

حلقة الرباعيات الحقيقية ,حلقة هرفتز,

مبرهنة المربعات الأربعة

مقدمة:

درسنا في نظرية الحلقات نوعاً خاصاً من الحلقات التامة يسمى الحلقات الإقليدية .

أما الآن فسنعتبر حلقة خاصة من حلقة الرباعيات والتي تشابه في جميع أوجهها الحلقة الإقليدية سوى كونها غير إبدالية . لهذا السبب سيكون من الممكن تمييز جميع مثالياتها اليسرى ، مما يقودنا بسرعة إلى برهان المبرهنة التقليدية للاجرانج والتي تنص على أن كل عدد صحيح موجب هو حاصل جمع أربعة مربعات . إن هذه المبرهنة تعتبر نقطة البداية لمجال واسع في نظرية الأعداد والذي يسمى مسألة وورينج ، هذه المسألة تسأل عما إذا كان عدد صحيح موجب يساوي مجموع عدد معين من الأعداد مرفوعة للقوة k . فعلى سبيل المثال يمكن برهان أن كل عدد صحيح هو حاصل جمع تسعة مكعبات لكننا لن نتطرق إلى هذه المسائل

لأنها ستحيد بنا عن موضوع البحث ، لذلك سنكتفي بمبرهنة لاجرانج التقليدية .

(٤-١) حلقة الرباعيات الحقيقية

تعريف :

لتكن $Q = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \mid \alpha_i \in ¡ \}$ حلقة الرباعيات الحقيقية . إذا كان $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ في Q فنعرف قرين x ونرمز له بالرمز x^* على أنه $x^* = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$.

تمهيدية(٤-١-١) :

إن القرين في Q يحقق ما يلي :

١- $x^{**} = x$.

٢- $(\delta x + \alpha y)^* = \delta x^* + \alpha y^*$.

٣- $(xy)^* = y^* x^*$.

لكل $x, y \in Q$ وكل الأعداد الحقيقية δ و α.

البرهان :

إذا كان $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ فإن $x^* = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$ وحينئذ :

$$\begin{aligned} x^{**} &= (x^*)^* = (\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k)^* \\ &= \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k = x \end{aligned}$$

وهذا يبرهن ١ .

دع $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ و $y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$ في Q وليكن δ, γ عددين صحيحين اختيارين عندئذ :

$$\delta x + \gamma y = (\delta\alpha_0 + \gamma\beta_0) + (\delta\alpha_1 + \gamma\beta_1)i + (\delta\alpha_2 + \gamma\beta_2)j + (\delta\alpha_3 + \gamma\beta_3)k$$

ومن تعريف * يكون :

$$(\delta x + \gamma y)^* = (\delta\alpha_0 + \gamma\beta_0) - (\delta\alpha_1 + \gamma\beta_1)i - (\delta\alpha_2 + \gamma\beta_2)j - (\delta\alpha_3 + \gamma\beta_3)k$$

$$= \delta(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) + \gamma(\beta_0 - \beta_1 i - \beta_2 j - \beta_3 k)$$
$$= \delta x^* + \gamma y^*$$

وهذا يبرهن٢.

في ضوء ما أثبتناه في (٢) فإنه يكفي لبرهان الجزء (٣) أن نثبت لأساس لـ Q على الأعداد الحقيقية وسنفعل هذا للأساس 1,i,j,k .

الآن $i = jk$ لذا

$$i^* = (jk)^* = -jk = kj = (-k)(-j) = k^* j^*$$

بصورة مشابهة $(ki)^* = i^* k^*$ و $(ij)^* = j^* i^*$.

أيضاً $(i^2)^* = (-1)^* = -1 = (i^*)^2$ وكذلك بالنسبة لـ k,j . لما كان الجزء (٣) صحيح بالنسبة لعناصر الأساس ، ولكون الجزء (٢) صحيح فإن الجزء (٣) يكون صحيح لجميع التركيبات الخطية من عناصر الأساس بمعاملات من الأعداد الحقيقية . وعليه يصبح (٣) صحيح لأي عنصرين اختيارين x و y في Q .

تعريف :

إذا كان $x \in Q$ فنعرف معيار x ونرمز له بـ N(x) على النحو التالي $N(x) = xx^*$.

ملاحظات :

١- $N(x)$ هو عدد حقيقي موجب لكل $x \neq 0$ في Q وذلك لأنه إذا كان :

$x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ فإن :

$$N(x) = xx^* = (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k)$$

$$= \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$$

فعليه $N(0) = 0$.وعلى وجه الخصوص لكل عدد حقيقي α يكون $N(\alpha) = \alpha^2$.

2- إذا كان $x \neq 0$ فإن $x^{-1} = \frac{1}{N(x)} x^*$.

تمهيدية(٤-١-٢) :

لكل $x, y \in Q$ فإن $N(xy) = N(x)N(y)$.

البرهان :

من تعريف المعيار_____ $N(xy) = (xy)(xy)^*$

$$= (xy)(y^* x^*)$$

$$= x(yy^*)x^*$$

$$= xN(y)x^*$$

ولما كان $N(y)$ عدد حقيقي ، فإنه في مركز Q وعلى وجه الخصوص فإن هذا العدد يتبادل مع x^* فنستنتج أن :

$$N(xy) = xx^* N(y) = N(x)N(y)$$

كاستنتاج مباشر من التمهيدية السابقة نحصل على ما يلي .

تمهيدية(٤-١-٣) متطابقة لاجرانج

إذا كانت $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ و $\beta_0, \beta_1, \beta_2, \beta_3$ أعداد حقيقية فإن :

$$(\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2)(\beta_0^2+\beta_1^2+\beta_2^2+\beta_3^2)=(\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3)^2+(\alpha_0\beta_1+\alpha_1\beta_0+\alpha_2\beta_3-\alpha_3\beta_2)^2$$
$$+(\alpha_0\beta_2-\alpha_1\beta_3+\alpha_2\beta_0+\alpha_3\beta_1)^2+(\alpha_0\beta_3+\alpha_1\beta_2-\alpha_2\beta_1+\alpha_3\beta_0)^2$$

البرهان :

بالطبع يوجد برهان واضح لهذه النتيجة وهو أن نفتح الأقواس ونقارن الحدود . لكن ثمة طريقة أبسط من ناحية أنها تنشيء المتطابقة وفي الوقت نفسه نبرهنها .

ليكن $x=\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ و $y=\beta_0+\beta_1 i+\beta_2 j+\beta_3 k$ في Q .

نلاحظ أن الجهة اليسرى من المتطابقة هي $N(x)N(y)$ بينما الجهة اليمنى هي $N(xy)$. ومن التمهيدية السابقة نعلم أن $N(xy)=N(x)N(y)$ مما يبرهن متطابقة لاجرانج .

(٤-٢)حلقة هرفتز للرباعيات التامة

إن متطابقة لاجرانج تنص على أن حاصل ضرب مجموع أربعة مربعات مع مجموع أربعة مربعات هو مجموع أربعة مربعات .

هناك نتيجة غريبة لـ" أدلف هرفتز" تنص على أنه إذا كان حاصل ضرب مجموع n من المربعات بمجموع n من المربعات هو أيضاً مجموع n من المربعات ، بحيث أن حدود المجموع الأخيرة حُسبت بطريقة خطية ثنائية من حدود المجموعين الآخرين . في الحقيقة توجد متطابقة لحاصل ضرب مجموعي ثمانية مربعات ولكننا لن نكتبها هنا لأنها مطوّلة وشائكة.

تعريف :

نعرف حلقة هرفتز للرباعيات التامة على أنها المجموعة

$$H=\{m_0\zeta+m_1 i+m_2 j+m_3 k \mid m_0,m_1,m_2,m_3\in\mathbf{Z}\wedge\zeta=\frac{1}{2}(1+i+j+k)\}$$

تمهيدية (٤-٢-١)

إذا كان $x\in H$ فإن $x^*\in H$ و N(x) عدد صحيح موجب لكل $x\neq 0$.

البرهان :

ليكن $x = m_0\zeta + m_1 i + m_2 j + m_3 k$ فإن $x^* = m_0\zeta^* - m_1 i - m_2 j - m_3 k$ حيث

$\zeta^* = \frac{1}{2}(1 - i - j - k)$. الآن

$$N(x) = xx^* = (m_0\zeta + m_1 i + m_2 j + m_3 k)(m_0\zeta^* - m_1 i - m_2 j - m_3 k)$$
$$= m_0^2 + m_1^2 + m_2^2 + m_3^2 + m_0 m_1 (i\zeta^* - \zeta i) + m_0 m_2 (j\zeta^* - \zeta j) + m_0 m_3 (k\zeta^* - \zeta k)$$

لأن $\zeta\zeta^* = 1$ و $i^2 = j^2 = k^2 = -1$

وكذلك $jk = -kj$, $ki = -ik$, $j = -ji$.

لنحسب $(i\zeta^* - \zeta i)$

$$(i\zeta^* - \zeta i) = \frac{1}{2}(1 + i + j - k + 1 - i - j + k) = 1$$

وبصورة مشابهة $(j\zeta^* - \zeta j) = 1$ و $(k\zeta^* - \zeta k) = 1$ إذن :

$$N(x) = m_0^2 + m_1^2 + m_2^2 + m_3^2 + m_0(m_1 + m_2 + m_3) > 0$$

قد تبدو الحلقة H لأول وهلة أنها مبتدعة فلماذا نستخدم الرباعي ζ؟ لماذا لا نعتبر الحلقة الأكثر ألفة Q_0 حيث

$Q_0 = \{m_0 + m_1 i + m_2 j + m_3 k \mid m_0, m_1, m_2, m_3 \in \mathbf{Z}\}$؟

إن الجواب على ذلك أن Q_0 ليست كبيرة بالحد الكافي على النقيض من H وذلك لفرض أن تكون التمهيدية التالية صحيحة . ولكننا نحتاج إلى أن تكون التمهيدية التالية صحيحة في الحلقة التي نتعامل معها لأنها تجعلنا نميز مثالياتها اليسرى . وهذا قد يوضح السبب الذي جعلنا (أو بالأحرى هرفتز) نختار العمل في الحلقة H بدلاً من Q_0.

تمهيدية(٤-٢-٢) (خوارزم القسم الأيسر):

ليكن $a, b \in H$ حيث $b \neq 0$ فإنه يوجد عنصران $c, d \in H$ بحيث $a = cb + d$ و $N(d) < N(b)$.

البرهان :

لغرض برهان التمهيدية فإننا سنثبت أولاً حالة خاصة جداً وهي التي فيها a عنصر اختياري في H ولكن b عدد صحيح موجب . لنفرض أن $a = t_0\zeta + t_1 i + t_2 j + t_3 k$ حيث t_0, t_1, t_2, t_3 أعداد صحيحة و $b = n$ ، حيث n عدد صحيح موجب . دع $c = x_0\zeta + x_1 i + x_2 j + x_3 k$ ، حيث x_0, x_1, x_2, x_3 أعداد صحيحة تُعين أدناه . إننا نريد تعيين هذه الأعداد بحيث يكون $N(a - cn) < N(n) = n^2$ ولكن

$$a - cn = (t_0(\frac{1+i+j+k}{2}) + t_1 i + t_2 j + t_3 k) - nx_0(\frac{1+i+j+k}{2}) - nx_1 i - nx_2 j - nx_3 k$$

$$= \frac{1}{2}(t_0 - nx_0) + \frac{1}{2}(t_0 + 2t_1 - n(x_0 + 2x_1))i + \frac{1}{2}(t_0 + 2t_2 - n(x_0 + 2x_2))j + \frac{1}{2}(t_0 + 2t_3 - n(x_0 + 2x_3))k$$

إذا أمكننا اختيار الأعداد الصحيحة x_0, x_1, x_2, x_3 بحيث يكون

$$|t_0 - nx_0| \le \frac{1}{2}n \quad , \quad |t_0 + 2t_1 - n(x_0 + 2x_1)| \le n$$

$$|t_0 + 2t_2 - n(x_0 + 2x_2)| \le n \quad , \quad |t_0 + 2t_3 - n(x_0 + 2x_3)| \le n$$

فينتج عن ذلك أن :

$$N(a - cn) = \frac{(t_0 - nx_0)^2}{4} + \frac{(t_0 + 2t_1 - n(x_0 + 2x_1))^2}{4} + \frac{(t_0 + 2t_2 - n(x_0 + 2x_2))^2}{4} + \frac{(t_0 + 2t_3 - n(x_0 + 2x_3))^2}{4}$$

$$\le \frac{1}{16}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2 < n^2 = N(n)$$

الآن يمكننا تعيين الأعداد الصحيحة x_0, x_1, x_2, x_3 :

١) يوجد عدد صحيح x_0 بحيث $t_0 = nx_0 + r$ حيث $-\frac{1}{2}n \le r \le \frac{1}{2}n$ لهذا العدد x_0 يكون $|t_0 - nx_0| = |r| \le \frac{1}{2}n$.

٢) يوجد عدد صحيح k بحيث $t_0 + 2t_1 = kn + r$ و $0 \le r \le n$.

إذا كان $k - x_0$ عدداً زوجياً فاجعل $2x_1 = k - x_0$ حينئذ $t_0 + 2t_1 = (2x_1 + x_0)n + r$ وعليه $|t_0 + 2t_1 - n(x_0 + 2x_1)| = |r| \le n$.

من ناحية أخرى إذا كان $k-x_0$ عدداً فردياً فاجعل $2x_1=k-x_0+1$ لذا:

$$t_0+2t_1=(2x_1+x_0-1)n+r=(2x_1+x_0)n+r-n$$

$$\Rightarrow t_0+2t_1-(2x_1+x_0)n=r-n$$

وعليه

$$|t_0+2t_1-(2x_1+x_0)n|=|r-n|\le n$$

وذلك لأن $0\le r<n$. إذن يمكننا إيجاد عدد صحيح x_1 بحيث يحقق :

$$|t_0+2t_1-(2x_1+x_0)n|\le n$$

٣) كذلك بنفس الطريقة في (٢) يمكننا إيجاد عددين صحيحين x_1,x_2 يحققان :

$$|t_0+2t_2-(2x_2+x_0)n|\le n \quad , \quad |t_0+2t_3-(2x_3+x_0)n|\le n$$

الآن في الحالة الخاصة والتي فيها a عنصر اختياري في H و b عدد صحيح موجب قد بيننا أن التمهيدية صحيحة .

الآن نريد إثبات التمهيدية في الحالة العامة ، أي عندما يكون كلاً من a,b عنصرين اختيارين من H و $b\neq 0$.

من تمهيدية (٤-٢-١) نعلم أن $N(b)=bb^*=n$ ، حيث أن n عدد صحيح موجب . بما أن $ab^*\in H$ و n عدد صحيح موجب ، فإنه باستخدام ما أثبتناه في الحالة الخاصة يوجد عنصران $c,d_1\in H$ بحيث $ab^*=cn+d_1$ حيث $N(d_1)<N(n)$. لذلك فإن $N(ab^*-cn)<N(n)$ ، لكن $bb^*=n$ حينئذ نحصل على :

$$N(ab^*-cbb^*)<N(n)$$

$$\Rightarrow N((a-cb)b^*)<N(n)$$

$$\Rightarrow N(a-cb)N(b^*)<N(n)$$

ولما كان $N(n)=N(bb^*)=N(b)N(b^*)$ "من تمهيدية (٤-١-٢)" ولكون $N(b^*)>0$ فإن :

$$N(a-cb)<N(b)\Rightarrow N(d)<N(b)$$

وذلك بجعل $d=a-cb$ فيكون لدينا $a=cb+d$.

تمهيدية (٤-٢-٣)

ليكن L مثالياً أيسر في H. عندئذ يوجد عنصر u في L بحيث لكل x في L يكون $x=cu$ حيث c في H .

البرهان :

إذا كان L=(0) ، فإنه كل ما يجب أن نفعله هو فرض $u=0$.

لذا نفرض أن $L\neq(0)$. بما أن معيار أي عنصر غير صفري في L هو عدد صحيح موجب ، لذا يوجد $0\neq u\in L$ بحيث يكون $N(u)<N(l)$ ، لكل $0\neq l\in L$. إذا كان $x\in L$ فإنه من التمهيدية السابقة يوجد عنصران $c,d\in H$ بحيث $x=cu+d$ و $N(d)<N(u)$. إذن $d=x-cu$ ولما كان $u\in L$ ، فإنه من خاصية المغناطيس $cu\in L$ وعليه $d\in L$ فإن $N(d)=0$ مما يجعل $d=0$ وعليه $x=cu$.

تمهيدية(٤-٢-٤)

إذا كان $a\in H$ فإن $a^{-1}\in H$ إذا وفقط إذا كان $N(a)=1$.

البرهان :

$\Leftarrow$) ليكن $a\in H$ و $a^{-1}\in H$ فإنه استناداً لتمهيدية سابقة يكون كل من $N(a)$ و $N(a^{-1})$ أعداد صحيحة موجبة . ولكن $aa^{-1}=1$ لذا فإن

$$N(a)N(a^{-1})=N(aa^{-1})=N(1)=1$$

وهذا يجعل $N(a)=1$.

$\Rightarrow$) ليكن $a \in H$ و $N(a)=1$ فإن $aa^* = N(a) = 1$ وعليه فإن

$a^* = a^{-1}$. لكن من تمهيدية سابقة يكون $a^* \in H$ وذلك لأن $a \in H$ وعليه يصبح $a^{-1} \in H$.

(٤-٣)مبرهنة المربعات الأربعة للاجرانج

قبل أن نقدم مبرهنة المربعات الأربعة سنعرض إحدى الحيل القديمة لـ أويلر

تمهيدية (٤-٣-١)

إذا كان $2a = x_0^2 + x_1^2 + x_2^2 + x_3^2$ ، حيث x_0, x_1, x_2, x_3 أعداد صحيحة فإن $a = y_0^2 + y_1^2 + y_2^2 + y_3^2$ ، حيث y_0, y_1, y_2, y_3 أعداد صحيحة .

البرهان :

نلاحظ أن $2a$ عدداً زوجياً ، أي أن الأعداد x_0, x_1, x_2, x_3 إما جميعها زوجية، أو جميعها فردية أو اثنان منهما زوجيين واثنان زوجيين .

في جميع الحالات يمكننا إعادة ترقيم هذه الأعداد وتجميعها في أزواج بحيث يكون كل زوج يحوي عددين زوجيين أو عددين فرديين

الآن دع

$$y_0 = \frac{x_0 + x_1}{2} \quad , \quad y_1 = \frac{x_0 - x_1}{2}$$
$$y_2 = \frac{x_2 + x_3}{2} \quad , \quad y_3 = \frac{x_2 - x_3}{2}$$

أي أن y_0, y_1, y_2, y_3 أعداد صحيحة .

ولكن

$$y_0^2+y_1^2+y_2^2+y_3^2=(\frac{x_0+x_1}{2})^2+(\frac{x_0-x_1}{2})^2+(\frac{x_2+x_3}{2})^2+(\frac{x_2-x_3}{2})^2$$
$$=\frac{1}{2}(\frac{2(x_0+x_1+x_2+x_3)}{2})$$
$$=\frac{1}{2}(x_0+x_1+x_2+x_3)$$
$$=\frac{1}{2}(2a)=a$$

وبذلك نكون برهنا على صحة حيلة أويلر .

مبرهنة المربعات الأربعة (٤-٣-١)

يمكن كتابة أي عدد صحيح موجب كمجموع أربعة مربعات.

البرهان :

ليكن n عدد صحيح موجب ، فإنه يمكن كتابته كحاصل ضرب أعداد أولية $p_1,p_2,...,p_m$ أي أن $n=p_1p_2...p_m$. لما كان كل عدد أولي هو حاصل جمع لأربعة مربعات أي أن $p_i=y_0^2+y_1^2+y_2^2+y_3^2$ لكل $1\le i\le m$. فإنه من متطابقة لاجرانج " تمهيدية (٤-١-٣) " يصبح كل عدد صحيح موجب هو مجموع أربعة مربعات فيصبح $n=x_0^2+x_1^2+x_2^2+x_3^2$.

بهذا نكون قد اختصرنا البرهان إلى الأعداد الأولية فقط .

نلاحظ أن العدد الأولي 2 يمكن كتابته على النحو $2=1^2+1^2+0^2+0^2$. إذن دون المساس بعمومية البرهان يمكننا الفرض أن n عدد أولي فردي والذي عادة يرمز له بالرمز p .

لنعتبر الرباعيات W_p على Z_p مجموعة الأعداد الصحيحة قياس p .

$$W_p=\{\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k \mid \alpha_0,\alpha_1,\alpha_2,\alpha_3\in Z_p\}$$

إن W_p حلقة منتهية وبالإضافة إلى ذلك أنها غير إبدالية لأن $ij=-ji\neq ji$ حيث $p\neq 2$ لذا من مبرهنة فدربرن لا يمكن لـ W_p أن تكون حلقة قسمة. بأخذ المكافيء العكسي للعبارة " إذا كانت R حلقة بعنصر وحدة ليس بالضروري إبدالية وكان المثاليين الأيمنين الوحيدين فيها هما (0),R فإن R

حلقة قسمة " . فإن W_p يجب أن تحوي مثالياً أيسر لا يساوي كلاً من (0) و W_p .

لندعي أن المثالي ثنائي الجانب V في H والمعرف بـ

$$V = \{x_0\zeta + x_1 i + x_2 j + x_3 k \mid x_l \,|\, p \ \forall\, 0 \le l \le 3\}$$

أنه لا يمكن أن يكون مثالياً أيسراً أعظمياً في H لأن $H/V \cong W_p$ ولأنه لو كان V مثالياً أيسراً أعظمياً في H لكان H/V ومن ثم W_p لا يمكن أن تحوي مثاليات يسرى عدا (0) و H/V وهذا يناقض لما بيناه أعلاه مما يبرهن على صحة ادعائنا .

ولما كان V ليس أعظمياً فإنه يوجد مثالي أيسر L في H بحيث $L \neq V, H \neq L$ و $V \subset L$. وفقاً لتمهيدية (٤-٢-٣) يوجد عنصر U في L بحيث كل عنصر في L هو مضاعف أيسر لـ U .

لما كان $p \in v$ فإن $p \in L$ وعليه $p = cu$ لعنصر C في H . ولما كان $u \notin V$ فإنه لا يوجد معكوس لـ C في H لأنه حينئذ سيكون $u = c^{-1}p \in V$. لذلك فإنه من تمهيدية (٤-٢-٤) يكون $N(c) > 1$. ولما كان $H \neq L$ فإنه لا يوجد معكوس لـ U في H مما يجعل $N(u) > 1$.

ولكون $p = cu$ فإن $p^2 = N(p) = N(cu) = N(c)N(u)$ ولكن $N(u) > 1, N(c) > 1$ بحيث كلا من $N(u), N(c)$ عددان صحيحان لأن $c, u \in H$ وفقاً لتمهيدية(٤-٢-١) وبما أن كلا من $N(u), N(c)$ يقسم p^2 فإنه لابد أن يكون $N(c) = N(u) = p$.

لما كان $u \in H$ فإن $u = m_0\zeta + m_1 i + m_2 j + m_3 k$ ، حيث m_0, m_1, m_2, m_3 أعداد صحيحة لذا :

$$\begin{aligned} 2u &= 2m_0\zeta + 2m_1 i + 2m_2 j + 2m_3 k \\ &= (m_0 + m_1 i + m_2 j + m_3 k) + 2m_1 i + 2m_2 j + 2m_3 k \\ &= m_0 + (m_0 + 2m_1)i + (m_0 + 2m_2)j + (m_0 + 2m_3)k \end{aligned}$$

إذن $N(2u)=m_0^2+(m_0+2m_1)^2+(m_0+2m_2)^2+(m_0+2m_3)^2$. لكن $N(2u)=4p$

وعليه $4p=m_0^2+(m_0+2m_1)^2+(m_0+2m_2)^2+(m_0+2m_3)^2$.

ولما كان $4p$ يساوي مجموع أربعة مربعات ، فإنه وفقاً للتمهيدية السابقة يكون $2p$ أيضاً كذلك . ولكون $2p$ يساوي مجموع أربعة مربعات فإن p يكون كذلك أيضاً . لذا $p=a_0^2+a_1^2+a_2^2+a_3^2$ حيث a_0,a_1,a_2,a_3 أعداد صحيحة .

وبهذا نكون قد انتهينا من برهان مبرهنة لاجرانج .

وخير خاتمة لهذا البحث المتواضع بالصلاة على خاتم الأنبياء والمرسلين سيدنا محمد وعلى آله وصحبه أجمعين .

المراجع

- مواضيع في الجبر ، أي .إن . هيرستين، ترجمة الدكتور فوزي بن أحمد الذكير والدكتور علي السحيباني ، الطبعة الثانية ، الرياض ، جامعة الملك سعود النشر العلمي والمطابع١٤٢٠هـ - ١٩٩٤ م .
- نظرية الحلقات وامتداد الحقول ، يوسف عبد الله الخميس ، الطبعة الثانية ، النشر العلمي والمطابع ، جامعة الملك سعود ١٤٢٦هـ - ٢٠٠٥م .