استخدام خواص حقول هلبرت في حل مسألة غالوا العكسية للزمر الدوارة

ديانا الرفاعي[1] و نور غازي[2]

تاريخ الإيداع 2014/06/15
قبل للنشر في 2014/10/16

الملخص

هدفنا من هذه الورقة البحثية هو تقديم طريقة جديدة لإثبات أنَّ كل زمرة دوارة تماثل زمرة غالوا فوق الحقل $\mathbb{Q}$، وذلك على مرحلتين:

المرحلة الأولى: إيجاد تمديد غالوا $E/\mathbb{Q}(x)$ من الدرجة n زمرة غالوا الموافقة له هي زمرة دوارة من المرتبة n (إذْ n عدد صحيح موجب).

المرحلة الثانية: بالإفادة من كون الحقل $\mathbb{Q}$ هو حقل هلبرت وبالإفادة من بعض خواص حقول هلبرت سننتقل إلى أنَّ تمديد غالوا فوق الحقل $\mathbb{Q}$ موافق للزمرة الدوارة.

الكلمات المفتاحية: تمديد غالوا، المسألة العكسية لغالوا، حقل هلبرت.

التصنيف الرياضياتي العالمي: 2010 *MSC* 12*F*12, 12*E*25

[1] طالبة ماجستير، [2] مدرسة، قسم الرياضيات، كلية العلوم، جامعة دمشق، سورية.

Use Hilbertian Field's Properties to Solve the Inverse Galois Problem for Cyclic Group

D. Alrifaii[(1)] and N. Ghazi[(2)]

Received 15/06/2014
Accepted 16/10/2014

ABSTRACT

Our aim of this paper is to prove that every cyclic group is isomorphic to Galois group over $\mathbb{Q}$. This will be done in two steps:

Step one: find Galois extension $E/\mathbb{Q}(x)$ of Galois group isomorphic to a cyclic group of degree n (with n positive integer) .

Step two: since $\mathbb{Q}$ is Hilbertian field, we will use some properties of Hilbertian field to prove that every cyclic group is Galois group over $\mathbb{Q}$.

Keywords: Galois extension, Inverse Galois Problem, Hilbertian field.

Mathematical Subject Classification: 2010 *MSC* 12*F*12, 12*E*25

[(1)]MCS., Student, [(2)]Assistant Professor, Department of Mathematics, Faculty of sciences, Damascus University, Syria.

1. المقدمة:

تتمحور دراستنا حول مسألة غالوا العكسية التي تنص على ما يأتي:

لأجل زمرة منتهية G وحقل معطى K فهل هناك إمكانية لإيجاد تمديد غالوا L/K بحيث $Gal(L/K) \cong G$؟ مع أنّ فكرة مسألة غالوا العكسية ترجع إلى العالم الفرنسي Evariste Galois إلا أنَّ أول من درس هذه المسألة بشكلٍ ملموس هو العالم الألماني David Hilbert وذلك بعد نحو سبعين سنة من ذلك التاريخ، ففي عام 1892 أثبت Hilbert مبرهنة عدم قابلية الاختزال وأوجد حل المسألة لأجل الزمر S_n, A_n [4] .

عام1937 حلَّ كلٌّ من Scholz وReichardt المسألة لأجل الزمر التي مراتبها قوة لعدد أولي فردي [4].

عام 1954 قام Shafarevich بحل المسألة لأجل الزمر القابلة للحل [3]. و في السنوات الأخيرة حدث تقدمٌ كبير في هذه المسألة إذْ قام كلٌّ من Matzat وMalle وFried بإثبات صحتها لأجل أغلب الزمر البسيطة [4],[5].

في هذه الورقة هدفنا إلى دراسة المسألة لأجل الزمر الدوارة. ونوهنا إلى أنَّ هذه المسألة حُلّتْ سابقاً، ولكننا اتّبعنا أسلوباً مختلفاً للحل بالإفادة من مبرهنة عدم قابلية الاختزال لهلبرت .

2. المفاهيم الأساسية:

تعريف 1.2 : [6]

ليكن K حقل و$f(x) \in K[x]$ حدودية غير ثابتة في حلقة الحدوديات بمتحول واحد x وبأمثال من K . عندئذٍ

- نقول عن الحدودية $f(x)$ إنّها **حدودية غير خزولة** $(irreducible\ polynomial)$ إذا لم نستطع كتابتها على شكل جداء لحدوديتين $g(x), h(x) \in K[x]$ درجتهما أصغر تماماً من درجة $f(x)$.

- ونقول عن f إنها **حدودية واحدية** $(monic\ polynomial)$ إذا كان معاملها القائد مساوياً الواحد .

- نقول عن الحدودية f إنها **قابلة للفصل** $(separable\ polynomial)$ فــوق K إذا لم يملك أيٌّ من عواملها غير الخزولة جذراً مضاعفاً (في حقل التفريق (1) يعرف لاحقاً).

تمهيدية 2.2: **[2]**

كل حدودية غير خزولة فوق حقل مميزه صفر هي حدودية قابلة للفصل.

معيار ايزنشتاين $(EISENTEN'S\ CRITERION)$ **3.2** : **[6]**

لتكن A حلقة تحليل $(factorial\ ring)$، و ليكن K حقــل القــسمة لهــا، و لنفرض أنَّ:

$f(x) = a_n\ x^n + \cdots + a_0 \in A[x]$ حدودية درجتها $n \geq 1$

عندئذٍ إذا وُجِد p أولي في A بحيث يحقق

- $a_i \equiv 0\ [mod\ p] \quad \forall\ i < n$
- $a_n \not\equiv 0\ [mod\ p]$
- $a_0 \not\equiv 0\ [mod\ p^2]$

فإن الحدودية $f(x)$ تكون غير خزولة في $K[x]$.

تعريف 4.2 : [1]

إذا كان E حقلاً وكان $F \subset E$ حقلاً جزئياً من E بمقصور العمليات المعرفة علــى E عندئذٍ F يسمى حقلاً جزئياً من E، وفي هذه الحالة نقول: إنَّ E هو **تمديد حقــل أو ممدد للحقل** F ونرمز لذلك بـِ $E\ /\ F$. وإذا كان E/F تمديد حقل عنــدها يمكننــا بسهولة النظر إلى F على أنه $E-$ فضاء شعاعي. ونعرف درجة التمديد كما يأتي:

تعريف *5.2* : [1]

ليكن E حقلاً ممدداً للحقل F عندئذٍ نعرف درجة التمديد $E\ /\ F$ بأنَّها بعد الفــضاء E $(dim_F E)$ كفضاء شعاعي فوق الحقل F. ونرمز للدرجة بالرمز $[E:F]$ نقــول عن التمديد $E\ /\ F$ إنَّه تمديد منتهٍ إذا كانت درجة التمديد $[E:F]$ منتهية.

تعريف *6.2* : [2]

نقول عن الحقل E الممدد للحقل F : إنّه حقل تفريق للحدودية $f(x) \in F[x]$ إذا كانت $f(x)$ يمكن تحليلها في $E[x]$، وهو أصغر حقل تتحلل فيه $f(x)$.

تعريف 7.2: [2]

نقول عن التمديد E/F: إنّه تمديد ناظمي $(normal\ extension)$ إذا كان حقل تفريق لأسرة من الحدوديات في $F[x]$.

تعريف *8.2*: [1]

ليكن E/F تمديد حقل و $a \in E$.عندئذٍ نقول عن العنصر a إنَّه قابل للفصل فوق F إذا كان a صفراً لحدودية قابلة للفصل. نقول عن التمديد E/F: إنّه تمديد قابل للفصل $(separable\ extension)$ إذا كان كل عنصر من E قابلاً للفصل فوق F .

تعريف 9.2: [2]

(1) الايزومورفيزم σ من K إلى نفسه يدعى أوتومورفيزم لـِ K .نرمز لمجموعة كل الأوتومورفيزمات لـِ K بـِ $Aut(K)$ وهي تشكل زمرة بالنسبة إلى عملية تركيب التطبيقات . إذا كان $\alpha \in K$ عندئذٍ نكتب $\sigma\alpha$ لأجل $\sigma(\alpha)$.

(2) نقول عن الأوتومورفيزم $\sigma \in Aut(K)$ إنه مثبت للعنصر $\alpha \in K$ إذا كان $\sigma\alpha = \alpha$.

(3) ليكن F حقلاً جزئياً من K عندئذٍ الأوتومورفيزم σ يدعى مثبتاً لـِ F إذا كان يثبت كل عنصر من F .

تعريف 10.2 : [2]

ليكن K/F تمديداً عندئذٍ $Aut(K/F)$ هي مجموعة كل الأوتومورفيزمات لـِ K التي تثبت F

$$Aut(K/F) = \{\alpha \in Aut(K) : \ \alpha(k) = k \quad \forall\, k \in F\}$$

وهي تشكل زمرة جزئية من الزمرة $Aut(K)$.

تعريف 11.2 : [2]

ليكن K/F تمديداً منتهياً، عندئذٍ نقول عن K : إنّه غالوا فوق F إذا كان $|Aut(K/F)| = [K:F]$ في هذه الحالة ندعو التمديد K/F تمديد غالوا و إذا كان K/F تمديد غالوا عندئذٍ ندعو زمرة الأوتومورفيزمات $Aut(K/F)$ زمرة غالوا لـِ K/F و يُرمز لها بـِ $Gal(K/F)$.

خاصة 12.2 : [2]

لتكن $H \leq Aut(K)$ زمرة جزئية من زمرة الأوتومورفيزمات لـِ K عندئذٍ المجموعة F المكونة من كل عناصر K المثبتة بواسطة كل عنصر من H

$$F = K^H = \{\alpha \in K : \ \sigma\alpha = \alpha \ \ \forall \sigma \in H\}$$

تشكل حقلاً جزئياً من K .

مبرهنة 13.2 : [5]

ليكن E/F تمديداً ما، عندئذٍ القضايا الآتية متكافئة:

(1) E حقل تفريق لحدودية قابلة للفصل $f \in F[x]$.

(2) $F = E^G$ لأجل زمرة ما منتهية G جزئية من زمرة الأوتومورفيزمات لـِ E.

(3) E ناظمي و قابل للفصل و من درجة منتهية فوق F .

(4) E غالوا فوق F .

تعريف 14.2 : [2]

ليكن لدينا التمديد E/F وليكن $\alpha \in E$ عندئذٍ فإنَّ الحقل $F(\alpha)$ هو أصغر حقل جزئي من E يحوي كلاً من F والعنصر α.

تعريف 15.2 : [1]

يسمى الحقل F حقلاً تاماً $(perfect)$ إذا كانت كل حدودية غير ثابتة في $F[x]$ هي حدودية قابلة للفصل فوق F (مثال الحقل $\mathbb{Q}$ حقل تام).

تمهيدية 16.2 : [1]

ليكن E/F تمديداً منتهياً بحيث إنَّ F حقل تام، عندئذٍ يوجد $\mu \in E$ إذْ $E = F(\mu)$.

مبرهنة 17.2 : [1]

كل حقل مميزه صفر هو حقل تام.

18.2 *CYCLOTOMIC FIELD* : [2]

لتكن $g(x)=x^n-1\in\mathbb{Q}[x]$ إذْ $n\geq 1$ عندئذٍ جذور هذه الحدودية هي الجـذور النونية للواحد $n^{th}\ roots\ of\ unity$.كما أنَّ مجموعة الجذور النونية للواحد تشكل زمرة دوارة بالنسبة إلى عملية الضرب (تماثل للزمرة $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^{\times}$) نرمز لها بـــ μ_n.

مُولد الزمرة الدوارة المؤلفة من كل الجذور النونية للواحد يسمى جذراً نونياً أولياً للواحد $primitive\ n^{th}\ root\ of\ unity$ ويُرمز له بالرمز ξ_n. الحقـل $\mathbf{E}=\mathbb{Q}(\xi_n)$ هو حقل تفريق للحدودية x^n-1 فوق $\mathbb{Q}$ ومن ثمَّ فهو تمديد غالوا على $\mathbb{Q}$ وندعو E حقلاً سيكلوتوميكاً $(cyclotomic\ field\ of\ n^{th}\ roots\ of\ unity)$.

تعريف 19.2 : [2]

نعرف الحدودية السيكلوتوميك من المرتبة n بأنها حدودية جـذورها هـي الجـذور الأولية للواحد، ونرمز لها بالرمز $\phi_n(x)$

$$\phi_n(x)=\prod_{\xi\ primitive\ \in\mu_n}(x-\xi)=\prod_{\substack{1\leq a\leq n\\(a,n)=1}}(x-\xi_n{}^a)$$

الحدودية السيكلوتوميك $\phi_n(x)$ هي حدودية واحدية غير خزولة في $\mathbb{Z}[x]$ مـن الدرجة $\varphi(n)$ وبذلك نجد أنَّ درجة تمديد الحقل السيكلوتوميك للجذور النونية الأوليـة للواحد فوق $\mathbb{Q}$ هي $\varphi(n)$ أي:

$$[\mathbb{Q}(\xi_n):\mathbb{Q}]=\varphi(n)$$

مبرهنة *20.2* : [2]

زمرة غالوا للتمديد $\mathbb{Q}(\xi_n)/\mathbb{Q}$ للجذور النونية للواحد تماثل الزمـرة الـضربية $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^{\times}$ ويعطى هذا التماثل بالتطبيق

$$\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^{\times} \longrightarrow Gal(\mathbb{Q}(\xi_n):\mathbb{Q})$$

$$\bar{a} = a\,(mod\,n) \longmapsto \sigma_a$$

إذْ σ_a أوتومورفيزم معرف بالشكل $\sigma_a(\xi_n) = {\xi_n}^a$.

صيغة سلاسل لورانس 21.2 : [8]

بفرض k حقلاً وبفرض Λ مجموعة المتتاليات $(a_i)_{i\in\mathbb{Z}}$ من عناصر k، وحيث كل عناصرها أصفار ما عدا عدد منته منها، أي إنَّه يوجد $N \in \mathbb{Z}$ يحقق $a_i = 0$ لأجل كل $i < N$. نعرف الجمع بالشكل

$$(a_i) + (b_i) = (a_i + b_i)$$

والضرب بالشكل:

$$(a_i)\,(b_j) = (c_n) \quad ; c_n = \sum_{i+j=n} a_i\, b_j$$

عندئذٍ المجموعة Λ تشكل حلقة تبديلية عنصرها الصفري هو المتتاليات الصفرية كلّها وعنصرها الواحدي هو المتتالية (a_i) إذْ كل عناصرها أصفار ما عدا $a_0 = 1$.

لنتحقق أنَّ الحلقة Λ تشكل حقلاً. لأجل متتالية غير صفرية (a_i) في Λ يوجد $N \in \mathbb{Z}$ إذْ $a_i = 0$ لأجل $i < N$ و $a_N \neq 0$. نُعرف $b_j = 0$ لأجل $j < -N$ و $b_{-N} = {a_N}^{-1}$. لأنَّ المعادلات:

$$\sum_{i+j=n} a_i\, b_j = 0 \qquad n = 1,2,\ldots\ldots$$

يمكن أن تحل تدريجياً لأجل b_j إذْ $j = -N+1\,,-N+2\,,\ldots\ldots$. المتتالية الناتجة (b_j) هي عكس (a_i) و بهذا نكون قد أثبتنا أنَّ Λ حقل.

وضوحاً k يُثبت كحقل جزئي من Λ وفقاً للتطبيق الذي يرسل $a \in k$ إلى المتتالية (a_i) إذْ $a_0 = a$ و $a_i = 0$ خلاف ذلك. فضلاً عن ذلك، لتكن t المتتالية (a_i) إذْ

$a_1 = 1$ و$a_i = 0$ خلاف ذلك. عندئذٍ الحلقة الجزئية $k[t]$ من Λ المولدة بـــ k وt هي حلقة حدوديات بمتغير واحد فوق k :

$$\sum_{i=0}^{M} a_i\, t^i = (a_i)$$

إذْ $a_i = 0$ عندما $i < 0$ أو $i > M$. بشكل عام نكتب:

$$\sum_{i=N}^{\infty} a_i\, t^i = (a_i)$$

إذْ $a_i = 0$ إذا كانت $i < N$.

إنَّ عمليات الحقل في Λ تقابل صيغة الجمع و الضرب لسلاسل لورانس، وبهـــذا Λ يدعى حقلاً لصيغة سلاسل لورانس فوق k عناصره من الشكل:

$$\sum_{i=N}^{\infty} a_i\, t^i$$

ونرمز لهذا الحقل بالرمز $k((t))$.

المجموعة الجزئية من Λ المؤلفة من العناصر كلّها من الشكل:

$$\sum_{i=0}^{\infty} a_i\, t^i$$

تشكل حلقة وتدعى حلقة صيغة سلاسل القوى فوق k و نرمز لها بالرمز $k[[t]]$.

تعريف 22.2:

لتكن G زمرة عنصرها الحيادي e ولتكن S مجموعة. عندئذٍ نعرف تأثير الزمرة G في المجموعة S بأنه التطبيق:

$$G \times S \longrightarrow S$$
$$(x, s) \to xs$$

إذْ يحقق الخاصتين

$$\forall\, x, y \in G\ , s \in S;\ \ (1)\ x(ys) = (xy)s$$

$$(2)\ es = s$$

لنوضح كيف تؤثر زمرة غالوا في حقل سلاسل لورانس: ليكن E/F تمديد زمـــرة غالوا ولنرمز G لزمرة غالوا الموافقة له. عندئذٍ نعرف تأثير زمرة غالوا في الحقــل E بالشكل:

$$G \times E \longrightarrow E$$

$$(\sigma, \alpha) \mapsto \sigma_\alpha(a) := \sigma(\alpha) \quad ; \ a \in E$$

لنأخذ $L = \mathbb{Q}(\xi_n)$ و لنأخــذ الحقــل $L((x))$ و لــتكن $G = Gal(L/\mathbb{Q})$ عندئذٍ G تؤثر في $L((x))$ بالتأثير في معاملات سلاسل لورانس كما يأتي:

$$*: G \times L((x)) \longrightarrow L((x))$$

$$\sigma * \sum_{i=m}^{\infty} a_i x^i \mapsto \sum_{i=m}^{\infty} \sigma(a_i) x^i \quad ; \ a_i \in L$$

ونظراً إلى أنَّ G زمرة غالوا فإنَّ $\sigma(a_i)$ تبقى في L و هذا ما يبرهن أنَّ المـــستقر هو $L((x))$. سنوضح التأثير لأجل $n = 3$. نعلم أنَّ الشكل العام لعناصر الحقــل $\mathbb{Q}(\xi_3)$ (ونرمز له باختصار $\mathbb{Q}(\xi)$) هو

$$a + b\,\xi + c\,\xi^2 \quad ; \quad a, b, c \in \mathbb{Q}$$

عندئذٍ

$$\sigma * \sum_{i=m}^{\infty} a_i x^i = \sum_{i=m}^{\infty} \sigma(a_i) x^i$$

$$= \sigma(a_m)x^m + \sigma(a_{m+1})x^{m+1} + \sigma(a_{m+2})x^{m+2} + \cdots$$

$$= \sigma(a'_m + b'_m\xi + c'_m\xi^2)x^m + \sigma(a'_{m+1} + b'_{m+1}\xi + c'_{m+1}\xi^2)x^{m+1} + \sigma(a'_{m+2} + b'_{m+2}\xi + c'_{m+2}\xi^2)x^{m+2} + \cdots$$

$$= \big(\sigma(a'_m) + \sigma(b'_m\xi) + \sigma(c'_m\xi^2)\big)x^m + \big(\sigma(a'_{m+1}) + \sigma(b'_{m+1}\xi) + \sigma(c'_{m+1}\xi^2)\big)x^{m+1} + \big(\sigma(a'_{m+2}) + \sigma(b'_{m+2}\xi) + \sigma(c'_{m+2}\xi^2)\big)x^{m+2} + \cdots$$

$$= (\theta_m + \vartheta_m + \mu_m)x^m + (\theta_{m+1} + \vartheta_{m+1} + \mu_{m+1})x^{m+1} + (\theta_{m+2} + \vartheta_{m+2} + \mu_{m+2})x^{m+2} + \cdots$$

بحيث $\theta_i = \sigma(a_i')$ و $\vartheta_i = \sigma(b_i'\xi) = b_i'\,\sigma(\xi)$ و $\mu_i = \sigma(c_i'\xi^2) = c_i'\,\sigma(\xi^2)$ كون $\sigma \in Gal(L/\mathbb{Q})$ ومن ثمَّ فهي تثبت عناصر $\mathbb{Q}$ و تأخذ كل ξ إلى إحدى مرافقاتها التي هي $1, \xi, \xi^2$. ومنه

$$= \sum_{i=m}^{\infty} \theta_i\, x^i + \sum_{i=m}^{\infty} \vartheta_i x^i + \sum_{i=m}^{\infty} \mu_i\, x^i \in \mathbb{Q}(\xi)((x)) = L((x))$$

و بشكلٍ مشابه نعرف تأثير زمرة غالوا في الحقل $L(x)$.

3. دراسة الزمرة الدوارة كزمرة غالوا:

سنورد في هذا المقطع تمهيديتين أساسيتين وبعض المفاهيم في حقول هلبرت تفيدنا في برهان المبرهنة الأساسية في هذا البحث.

تعريف 1.3:

لتكن $f(x,y) \in K[x,y]$ حدودية بالمتحولين x و y فوق الحقل K عندئذٍ ندعو الحدودية $f(b,y)$ بالحدودية المخصصة لـِ $f(x,y)$، وذلك بعد تعويض كل x في الحدودية $f(x,y)$ بالعنصر $b \in K$.

تمهيدية 2.3 : [8]

لتكن $F(x,y) \in K[[x]][y]$ حدودية واحدية. ولتكن الحدودية المخصصة $F(0,y) = F_0 \in K[y]$ تتحلل إلى جداء حدوديتين في $K[y]$ بالشكل :

$$F_0 = g(y)\,h(y)$$

إذْ $g(y), h(y)$ حدوديتان في $K[y]$ واحدية أولية فيما بينهما (أي $gcd(g,h) = 1$)، عندئذٍ يمكن تحليل الحدودية F إلى جداء حدوديتين بالشكل:

$$F = G.H$$

إذْ أنَّ $G(x,y), H(x,y)$ حدوديتان واحديتان في y مع معاملات من $K[[x]]$ وتحقق

$$G(0,y) = G_0 = g \quad , \quad H(0,y) = H_0 = h$$

تمهيدية 3.3 :

لتكن $p(x,y) \in K[x][y]$ حدودية من الدرجة $n > 1$ بالمتحول y عندئذٍ إذا كانت الحدودية المخصصة $p(0,y)$ لها درجة الحدودية نفسها $p(x,y)$ بالنسبة إلى المتحول y وكانت $p(0,y)$ تملك صفراً بسيطاً α عندئذٍ توجد سلسلة وحيدة $y_\alpha(x) \in K[[x]]$ بحيث تحقق ما يأتي:

1) $p\big(x, y_\alpha(x)\big) = 0$

2) $y_\alpha(0) = \alpha$

البرهان:

لدينا الحدودية $p(0,y)$ لها صفر بسيط α ومن ثمَّ توجد حدودية $q(y) \in K[y]$ بحيث:

$$p(0,y) = (y-\alpha)\, q(y) \quad ; \quad q(\alpha) \neq 0$$

بحسب التمهيدية (*2.3*) السابقة يوجد $H(x,y), G(x,y) \in K[[x]][y]$ بحيث $p = G\,H$ و $H(0,y) = y - \alpha \quad , \quad G(0,y) = q(y)$

ومن ثمَّ فإنَّ $H(x,y)$ لها الشكل $y - y_\alpha(x)$. مما سبق نجد أنه توجد حدودية $y_\alpha(x)$ بحيث $y_\alpha(0) = \alpha$ و$y_\alpha(x)$ جذر للحدودية $p(x,y)$. وبهذا نكون قد أثبتنا الوجود وبقي علينا إثبات الوحدانية.

لنفرض وجود سلسلتين مختلفتين $y_1(x)\,,\, y_2(x)$ تحققان شروط المبرهنة، عندئذٍ يوجد $G_1, G_2 \in K[[x]][y]$ بحيث

$$p(x,y) = \big(y - y_1(x)\big)\; G_1(x,y)$$
$$p(x,y) = \big(y - y_2(x)\big)\; G_2(x,y)$$

ومنه $(y-y_2)$ يقسم G_1 . عندئذٍ توجد حدودية ما $T(x,y) \in K[[x]][y]$ بحيث

$$p(x,y) = \big(y, y_1(x)\big)\,\big(y - y_2(x)\big)\,T(x,y)$$

ومنه نجد أنَّ a جذر مضاعف لـِ $p(0,y)$ و هذا يناقض الفرض.

حقول هلبرت :

ترميز 4.3 : في الأفكار التي تخص حقل هلبرت سوف نرمز بـِ k لحقل مميزه صفر و $x_1, x_2, \dots$ عناصر مستقلة فوق k.عندئذٍ $k[x_1, \dots, x_m]$ ترمز لحلقة الحدوديات بالمتحولات $x_1, \dots, x_m$ و $k(x_1, \dots, x_m)$ لحقل الدوال العادية فوق الحقل k في $x_1, \dots, x_m$.

مبرهنة 5.3 : [8]

ليكن k حقلاً عندها الشروط الثلاثة الآتية متكافئة:

(1) لأجل كل حدودية غير خزولة $f(x,y) \in k[x,y]$ بمتحولين فوق k من درجة ≤ 1 يوجد عدد غير منتهٍ من العناصر $b \in k$ بحيث إنَّ الحدودية المخصصة $f(b,y) \in k[y]$ غير خزولة على k .

(2) لأجل تمديد منتهٍ معطى L/k وحدوديات $h_1(x,y), \dots, h_2(x,y) \in L[x][y]$ غير خزولة بالنسبة إلى المتحول y فوق الحقل $L(x)$ يوجد عدد غير منتهٍ من العناصر $b \in k$ بحيث إنّ الحدوديات المخصصة $h_1(b,y), \dots, h_2(b,y)$ غير خزولة في $L[y]$.

(3) لأجل أي $p_1(x,y), \dots, p_2(x,y) \in k[x][y]$ غير خزولة و من درجة أكبر من الواحد كحدوديات بالنسبة إلى المتحول y فوق الحقل $k(x)$ يوجد عدد غير منتهٍ من العناصر $b \in k$ بحيث إنَّه ولا أيّ من الحدوديات المخصصة $p_1(b,y), \dots, p_2(b,y)$ تملك جذراً في k.

تعريف 6.3 : [8]

نقول عن k: إنَّه حقل هلبرت $(Hilbertian\ field)$ إذا حقق أحد الشروط الثلاثة الواردة في المبرهنة 5.3 .

مبرهنة 7.3 : **[8]**

لنفرض k حقل هلبرت. عندئذٍ إذا كانت G زمرة غالوا للتمديد $k(x_1, \dots, x_m)$ فإنَّ G هي أيضاً زمرة غالوا فوق k .

مبرهنة 8.3 : [8]

الحقل $\mathbb{Q}$ هو حقل هلبرت .

المبرهنة الأساسية 9.3 :

كل زمرة دوارة هي زمرة غالوا فوق $\mathbb{Q}$.

البرهان:

سنأخذ البرهان على مرحلتين: سنقوم في المرحلة الأولى ببرهان أنه يوجد تمديد غالوا $E/\mathbb{Q}(x)$ زمرته $\mathbb{Z}/_{n\mathbb{Z}}$ أمّا المرحلة الثانية فنستخدم هلبرت للوصول إلى النتيجة الأساسية.

أولاً: ليكن n عدداً صحيحاً موجباً عندها فإنَّ $\mathbb{Q}(\xi_n)/\mathbb{Q}$ تمديد غالوا زمرته $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^{\times}$ إذْ إنَّ ξ_n جذر نوني أولي للواحد. أكثر من ذلك لدينا التماثل

$$\tau: \left(\mathbb{Z}/_{n\mathbb{Z}}\right)^{\times} \longrightarrow Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$$
$$a \longmapsto \sigma_a$$

بحيث

$$\sigma_a: \mathbb{Q}(\xi_n) \longrightarrow \mathbb{Q}(\xi_n)$$
$$\xi_n \longmapsto \xi_n{}^a$$

عندئذٍ لدينا التطبيق

$$\chi: G \longrightarrow \{1,2,\dots,n-1\}$$
$$\sigma(\xi_n) \longmapsto \xi_n{}^{\chi(\sigma)}$$

عندئذٍ فإنه $\forall\, \sigma,\tau \in G$

$$\chi(\sigma\tau) \equiv \chi(\sigma)\chi(\tau)\ mod\, n$$

كما أنَّ:

$$\chi(\tau\,\tau^{-1}) \equiv \chi(\tau)\chi(\tau^{-1}) \equiv 1\ mod\, n$$

ليكن $L = \mathbb{Q}(\xi_n)$ ولتكن $G = Gal(L/\mathbb{Q})$ عندئذٍ بحسب تأثير زمرة غـــالوا في $L((x))$ الموضح سابقاً نجد أنَّ $L((x))$ تمديد غالوا لـِ $\mathbb{Q}((x))$ زمرة غالوا الموافقة له تماثل G إذْ $L((x)) \cong \mathbb{Q}((x))(\xi_n)$ ومنه:

$$Gal(L/\mathbb{Q}) \cong Gal(\, L((x))/\mathbb{Q}((x))\,) \cong Gal(L(x)/\mathbb{Q}(x))$$

نفرض وجود $g(x) \in L[x]$ من الشكل $g(x) = (x-a)\,\overline{g}(x)$ بحيـــث $\overline{g}(a) \neq 0$ و $a \in L$. عندئذٍ $z^n - g(x)$ حدودية بـــالمتحول z فـــوق $L(x)$ وهي حدودية غير خزولة بحسب معيار ايزنشتاين كما أنها قابلة للفصل بحسب التمهيديـــة (2.2).

إنَّ L حقلاً يحوي كل جذور الواحد من المرتبة n لذلك يمكننا أن نحصل على تمديد غالوا لـِ $L(x)$ من المرتبة n وذلك بإضافة u إذْ $u^n = g(x)$. وعنـــدها تكـــون زمرة غالوا الموافقة لهذا التمديد زمرة دوارة مولدة بالعنصر ω إذْ $\omega(\theta) = \xi_n\, u$.

اختيار $g(x)$: كون $\mathbb{Q}$ حقلاً تاماً عندها يوجد $c \neq 0$ عنـــصر مـــن L بحيـــث $L = \mathbb{Q}(c)$ (بحسب التمهيدية 16.2 و المبرهنة 17.2)، لنفرض

$$g(x) = \prod_{\mu \in G} (1 + \mu(c)x)^{x(\mu^{-1})}$$

إنَّ $g(x)$ حدودية من $L(x)$.

لنأخذ $y \in L[[x]]$ بحيث يحقق $y^n = 1 + cx$. لنفرض

$$u = \prod_{\mu \in G} \mu(y)^{x(\mu^{-1})} \in L((x))$$

سنثبت الآن أنَّ u يحقق $u^n = g(x)$ (أي إنَّه جذر للمعادلة $y^n - g(x)$)

$$u^n = \prod_{\mu \in G} \left(\mu(y)^{x(\mu^{-1})}\right)^n = \prod_{\mu \in G} \mu(y^n)^{x(\mu^{-1})}$$

$$= \prod_{\mu \in G} (1 + \mu(c)x)^{x(\mu^{-1})} = g(x)$$

ومن ثمَّ نجد أنَّ $u^n = g(x)$.

و بهذا فإنّ الحقل $L(x)(u)$ وهو تمديد غالوا للحقل $L(x)$ من الدرجة n زمرته تماثل الزمرة الدوارة $\langle\omega\rangle$ بحيث $\omega(u) = \xi_n\, u$ (لأنَّ L يحوي جذور الواحد من المرتبة n). لأجل أي $\tau \in G$ لدينا

$$\tau(u) = \tau\left(\prod_{\mu\in G}\mu(y)^{\chi(\mu^{-1})}\right) =$$

$$\prod_{\mu\in G}\tau\mu(y)^{\chi(\mu^{-1})} = \prod_{\mu\in G}\tau\mu(y)^{\chi(\tau\tau^{-1}\mu^{-1})}$$

$$= \prod_{\mu\in G}\tau\mu(y)^{\chi(\tau)\chi(\tau^{-1}\mu^{-1})\, mod\, n} =$$

$$\prod_{\mu\in G}\left(\tau\mu(y)^{\chi(\tau^{-1}\mu^{-1})}\right)^{\chi(\tau)}\tau\mu(y)^{kn} \quad ; k \in \mathbb{Z}^+$$

$$= u^{\chi(\tau)}\prod_{\mu\in G}\tau\mu(1+cx)^k$$

$$= u^{\chi(\tau)}\, f_\tau(x) \in L(x)(u)$$

إذْ $f_\tau(x) = \prod\tau\mu(1+cx)^k \in L(x)$

وهذا يعني أنَّ G تصور كل عنصر من $L(x)(u)$ بعنصر من الحقل نفسه.

ليكن $\tau \in G$ ولنضع $m = \chi(\tau)$ عندئذ

$$\tau\omega(u) = \tau(\xi_n u) = \xi_n{}^m\, u^m\, f_\tau(x) = \omega(u)^m\, f_\tau(x)$$

$$= \omega\left(u^m\, f_\tau(x)\right) = \omega\tau(u)$$

ومن ثمَّ نجد أنَّ $\tau\omega = \omega\tau$ وبهذا نجد أنَّ الزمرتين G وَ $\langle\omega\rangle$ تتبادلان فيما بينهما. (i)

الآن أصبح لدينا الزمرة G تثبت الحقل $\mathbb{Q}$ الجزئي من L (ii)

$$\begin{matrix} L \\ G\left\{ \right. \\ \mathbb{Q} \end{matrix}$$

كما أنَّ الزمرة $\langle\omega\rangle$ تثبت الحقل $L(x)$ الجزئي من $L(x)(u)$ (iii)

$$\begin{matrix} L(x)(u) \\ \langle\omega\rangle\left\{ \right. \\ L(x) \end{matrix}$$

ومن ثمَّ من $(i),(ii),(iii)$ نجد أنَّ $G\,.\langle\omega\rangle$ تثبت الحقل $\mathbb{Q}(x)$.

$$\begin{matrix} L(x)(u) \\ G\,.\langle\omega\rangle\left\{ \right. \\ \mathbb{Q}(x) \end{matrix}$$

لنفرض الحقل E هو الحقل الجزئي من $L(x)(u)$ المثبت بواسطة الزمرة G (أي $E = \left(L(x)(u)\right)^G$) عندئذٍ

$$\left\{ \quad \right\}$$

ومن ثمَّ نجد أنَّ $E/\mathbb{Q}(x)$ تمديد غالوا زمرة غالوا الموافقة له هي

$$Gal(E/\mathbb{Q}(x)) = \frac{G.\langle\omega\rangle}{G} \cong \langle\omega\rangle \cong \mathbb{Z}/_{n\mathbb{Z}}$$

ثانياً : الانتقال من $\mathbb{Q}(x)$ إلى $\mathbb{Q}$

أثبتنا أنَّ $E/\mathbb{Q}(x)$ تمديد غالوا منتهٍ زمرته $Gal(E/\mathbb{Q}(x)) \cong \mathbb{Z}/_{n\mathbb{Z}}$. من التمهيدية 16.2 يوجد $\alpha \in E$ بحيث $E = \mathbb{Q}(x)(\alpha)$. لتكن $p(x,y)$ الحدوديـــة الأصغرية لـِ α فوق $\mathbb{Q}(x)$

$$p(x,y) = y^n + a_{n-1}\, y^{n-1} + \cdots + a_0 \in \mathbb{Q}(x)[y]$$

نظراً إلى أنَّ $\mathbb{Q}$ حقل هلبرت عندئذٍ يوجد عدد غير منتهٍ من العناصر $b \in \mathbb{Q}$ بحيث تحقق $p(b,y) := g(y) \in \mathbb{Q}[y]$ غير خزولة في $\mathbb{Q}[y]$ و لذلك فـــإنَّ الحقـــل $E_1 = \mathbb{Q}[y]/_{(y_b)}$ غالوا فوق $\mathbb{Q}$ زمرته G_1 بحيث:

$$G_1 \cong Gal(E/\mathbb{Q}(x)) \cong \mathbb{Z}/_{n\mathbb{Z}}$$

REFERENCES

[1]Carstensen C., Fine B. and Rosenberger G. 2011. Abstract Algebra applications to galois group, algebraic to geometry and cryptography Walter de Gruyter GmbH & Co. KG, Berlin/NewYork.

[2]Dummit D. S and Foote R. M. 2004. Abstract Algebra, 3rd Edition, John Wiley and sons.

[3]Jensen C., Ledet A., and Yui N. 2011. Generic Polynomials, Cambridge , University press.

[4]Malle G. and Matzat B. H. 2001. Inverse Galois Theory, volume 53 of Cambridge studies in Advanced Mathematics. Springer, New York.

[5] Milne J.S. 2013. Fields and Galois theory , New Zealand.

[6] Lang S. 2002. Algebra, Third Edition, springer – Verlag new york.

[7]Serre J. P, 2008. Topics in Galois Theory, volume 1 of Research Notes in Mathematics, A K Peters, Ltd., Massachusettes.

[8] Volklein H. 1996. Groups as Galois groups, Cambridge University Press.