

BỘ GIÁO DỤC VÀ ĐÀO TẠO

ĐẠI HỌC ĐÀ NẴNG

NGUYỄN THỊ TUYẾT HẰNG

LÝ THUYẾT GALOIS VÀ ỨNG DỤNG

Chuyên ngành: Phương pháp Toán sơ cấp

Mã số: 60 46 40

TÓM TẮT LUẬN VĂN THẠC SĨ KHOA HỌC

Đà Nẵng - 2011

Công trình được hoàn thành tại

ĐẠI HỌC ĐÀ NẴNG

Người hướng dẫn khoa học: TS. NGUYỄN NGỌC CHÂU

Phản biện 1 : TS. Lê Hoàng Trí

Phản biện 2 : PGS.TS. Nguyễn Gia Định

Luận văn được bảo vệ trước Hội đồng chấm Luận văn tốt nghiệp Thạc sĩ khoa học họp tại Đại học Đà Nẵng vào ngày 29 tháng 5 năm 2011.

** Có thể tìm hiểu luận văn tại :*

- Trung tâm Thông tin - Học liệu, Đại học Đà Nẵng
- Thư viện trường Đại học Sư phạm, Đại học Đà Nẵng.

MỞ ĐẦU

1. Lý do chọn đề tài.

Trong toán học, các phương trình dạng $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$, $a_n \neq 0$, trong đó x là ẩn số, và a_i , $i = 0, \dots, n$, là các số cho trước; được gọi là phương trình đại số bậc n .

Việc giải các phương trình đại số là một vấn đề kinh điển của toán học. Vào thế kỷ thứ 16, Tartaglia, Cardano và Ferrari tìm được cách giải các phương trình đại số bậc 3, bậc 4, với các công thức nghiệm là những biểu thức chỉ chứa các căn thức. Đến đầu thế kỷ thứ 19, Abel đã chứng tỏ rằng không thể tìm được một công thức tổng quát như vậy đối với các phương trình đại số bậc lớn hơn hoặc bằng 5. Và sau đó Galois đã đưa ra một tiêu chuẩn để một phương trình đại số có nghiệm là những biểu thức chứa căn thức. Phương pháp xét nghiệm của Galois sau này được gọi là ***“Lý thuyết Galois”***.

Lý thuyết Galois là một trong những nội dung cơ bản của đại số hiện đại, nó liên quan đến nhiều cấu trúc đại số khác như: nhóm, vành, trường, không gian vector... Lý thuyết Galois có nhiều ứng dụng trong những lĩnh vực khác nhau của toán học. Một trong những ứng dụng chủ yếu của Lý thuyết Galois là tìm nghiệm căn thức của các phương trình đại số, giải bài toán dựng hình bằng thước kẻ và compa. Với mong muốn tìm hiểu Lý thuyết Galois và những ứng dụng của nó, Tôi chọn đề tài luận văn Thạc sĩ của mình là: ***“Lý thuyết Galois và ứng dụng”***.

2. Mục đích nghiên cứu.

Mục đích của luận văn này là tìm hiểu và trình bày lý thuyết Galois cùng những ứng dụng của nó, cụ thể là:

- Giải những bài toán dựng hình bằng thước kẻ và compa
- Tìm nghiệm căn thức của những đa thức (còn gọi là tìm nghiệm căn thức của những phương trình đại số) .
- Xét xem khi nào thì một phương trình đại số giải được bằng căn thức.

3. Đối tượng và phạm vi nghiên cứu.

3.1. Đối tượng nghiên cứu:

- Trường số phức.
- Một số cấu trúc đại số như : nhóm, vành, trường, mở rộng trường...
- Phương trình đại số, định lý cơ bản của đại số.
- Bài toán dựng hình.
- Lý thuyết Galois.

3.2. Phạm vi nghiên cứu:

- Giải phương trình đại số bằng căn thức.
- Lý thuyết Galois và một số ứng dụng của nó.

4. Phương pháp nghiên cứu.

- Nghiên cứu các tài liệu về lý thuyết mở rộng trường, lý thuyết Galois và các kiến thức liên quan, như giáo trình, sách giáo khoa cùng một số tài liệu khác từ internet.
- Khảo sát, phân tích, tổng hợp và minh họa lý thuyết Galois cùng những ứng dụng của nó thông qua những ví dụ.

5. Cấu trúc của luận văn.

Luận văn gồm có hai chương:

Chương 1, Giới thiệu sơ lược về lý thuyết mở rộng trường và lý thuyết Galois.

Chương 2, là nội dung chính của luận văn, trình bày một số ứng dụng của lý thuyết Galois, bao gồm:

1. Giải những bài toán dựng hình cổ điển.
2. Tìm nghiệm căn thức của phương trình đại số có bậc nhỏ hơn 5, và giải bài toán:  khi nào một phương trình đại số giải được bằng căn thức”.
3. Chứng minh định lý cơ bản của đại số.

CHƯƠNG 1. MỞ RỘNG TRƯỜNG VÀ LÝ THUYẾT GALOIS

Chương này nhắc lại sơ lược về mở rộng trường và lý thuyết Galois để làm cơ sở cho chương sau.

1.1. MỞ RỘNG TRƯỜNG .

1.1.1. Định nghĩa [5]. Cho hai trường F và K , với F là một trường con của K . Khi đó K được gọi là mở rộng (trường) của F . Một mở rộng trường $F \subseteq K$ còn được ký hiệu là $K : F$. Nếu K là một mở rộng trường của F thì K là một F – Không gian vector.

1.1.2. Định nghĩa [5]. Bậc của mở rộng trường $K : F$ là số chiều của F - không gian vector K , ký hiệu $[K : F]$. Nếu $[K : F]$ hữu hạn thì ta gọi $K : F$ là mở rộng hữu hạn. Nếu $[K : F]$ không hữu hạn thì ta gọi là mở rộng vô hạn.

1.1.3. Định nghĩa [2]. Cho $K : E$ là một mở rộng trường. Phần tử $u \in K$ được gọi là đại số trên E nếu nó là nghiệm của một đa thức khác 0 trong $E[x]$. Một phần tử $u \in K$ không đại số trên E được gọi là siêu việt trên E .

1.1.4. Định nghĩa. Mở rộng $K : F$ được gọi là mở rộng đại số nếu mọi phần tử của K đều đại số trên F .

1.1.5. Định nghĩa [2]. Một mở rộng trường $K : F$ là mở rộng đơn nếu tồn tại $u \in K$ sao cho $K = F(u)$. Phần tử u được gọi là phần tử nguyên thủy của mở rộng đơn. Một mở rộng đơn có thể có nhiều phần tử nguyên thủy khác nhau.

1.1.6. Định nghĩa. Cho $f \in F[x]$ và K là mở rộng trường của F . Ta nói f phân rã trong K hay K phân rã f nếu f có thể viết

được dưới dạng $f = (x - u_1)(x - u_2) \dots (x - u_n)$; với $a, u_i \in K$, $\forall i = \overline{1, n}$.

1.1.7. Định nghĩa. Cho $0 \neq f \in F[x]$. Một mở rộng K của F được gọi là trường phân rã của f trên F nếu K phân rã f và f không phân rã trong bất kỳ trường con thực sự nào của K .

1.1.8. Định nghĩa. Cho $K : F$ là mở rộng trường và $u \in K$ là phần tử đại số trên F . Đa thức có bậc nhỏ nhất $0 \neq f \in F[x]$ nhận u làm nghiệm và có hệ tử dẫn đầu bằng 1 được gọi là đa thức tối tiểu của u .

1.1.9. Định nghĩa. Một mở rộng đại số $E : F$ gọi là chuẩn tắc nếu đa thức tối tiểu của mọi phần tử thuộc E phân rã trong E .

1.1.10. Định nghĩa. Một đa thức $f \in F[x]$ gọi là tách được trên F nếu mọi nhân tử bất khả quy của f đều không có nghiệm bội. Một mở rộng đại số $E : F$ gọi là tách được nếu đa thức tối tiểu của mọi phần tử thuộc E đều tách được.

1.2. LÝ THUYẾT GALOIS

1.2.1. Định nghĩa [9]. Cho $E : F$ là một mở rộng trường. Các trường con của E chứa F gọi là các trường trung gian của mở rộng $E : F$. Ký hiệu $\mathcal{F}$ là tập tất cả các trường trung gian của $E : F$.

1.2.2. Bổ đề [9]. Cho $0 \neq H \subseteq \text{Aut}(E / F)$. Tập $\mathcal{J}(H) = \{ b \in E / \varphi(b) = b, \forall \varphi \in H \}$ là một trường trung gian của $E : F$, gọi là trường trung gian cố định bởi H .

1.2.3. Bổ đề [9]. Cho K là trường trung gian của mở rộng $E : F$. Khi đó $\text{Aut}(E / K)$ là một nhóm con của nhóm $\text{Aut}(E / F)$; gọi là nhóm con cố định K , ký hiệu $\mathcal{N}(K)$.

1.2.4. Định nghĩa [9]. Một mở rộng hữu hạn $E : F$ được gọi là mở rộng Galois nếu $F = \mathcal{J}(\mathcal{N}(F))$. Khi đó $\text{Aut}(E / F)$ gọi là nhóm Galois của mở rộng trường và ký hiệu là $\text{Gal}(E / F)$.

1.2.5. Định lý (tiêu chuẩn của mở rộng Galois) [9].

Cho mở rộng trường $E : F$. Các mệnh đề sau đây là tương đương:

- (i). E là trường phân rã của một đa thức tách được trên F .
- (ii). $[E : F] = (\text{Aut}(E / F) : 1) < \infty$.
- (iii). $E : F$ là mở rộng Galois.
- (iiii). $F = \mathcal{J}(G)$ với G là một nhóm con hữu hạn của $\text{Aut}(E/F)$.
- (iiiii). $E : F$ là mở rộng chuẩn tắc, tách được và hữu hạn trên F .

1.2.6. Định lý (Định lý cơ bản của lý thuyết Galois) [9].

Cho $E : F$ là mở rộng Galois với $G = \text{Gal}(E / F)$. Khi đó các tương ứng Galois $\mathcal{N} : \mathcal{F} \rightarrow \mathcal{H}$ và $\mathcal{J} : \mathcal{H} \rightarrow \mathcal{F}$ là các song ánh và là nghịch đảo của nhau. Hơn thế :

- (i). $H_1 \subset H_2 \Leftrightarrow \mathcal{J}(H_1) \supset \mathcal{J}(H_2), \forall H_1, H_2 \in \mathcal{H};$
- (ii). Chỉ số của nhóm bằng bậc của mở rộng trường, nghĩa là với mọi $H_1, H_2 \in \mathcal{H}$:

$$H_1 \subset H_2 \Rightarrow (H_2 : H_1) = [\mathcal{J}(H_1) : \mathcal{J}(H_2)];$$
- (iii). $\mathcal{J}(\sigma H \sigma^{-1}) = \sigma \mathcal{J}(H)$ và $\mathcal{N}(\sigma M) = \sigma \mathcal{N}(M) \sigma^{-1},$

$$\forall \sigma \in G \quad \forall H \in \mathcal{H}, \forall M \in \mathcal{F};$$

(iii). $H \trianglelefteq G$ khi và chỉ khi $\mathcal{F}(H) : F$ là mở rộng chuẩn tắc (do đó Galois) và $\text{Gal}(\mathcal{F}(H) / F) \cong G / H$.

1.3. NHÓM GALOIS CỦA ĐA THỨC.

1.3.1. Định nghĩa [2]. Cho một trường K , một đa thức $0 \neq f \in K[x]$ bậc n và $N = K(u_1, \dots, u_n)$ là trường nghiệm của f ; nhóm $\text{Gal}(N / K)$ được gọi là nhóm Galois của đa thức f (hay nhóm Galois của phương trình $f(x) = 0$).

1.3.2. Định nghĩa. Nhóm Galois của một đa thức tách được $f \in F[x]$ là nhóm Galois của trường phân rã của f .

1.3.3. Biệt thức. Cho $f = x^n + a_1x^{n-1} + \dots + a_0 \in F[x]$ là một đa thức tách được, với $n \geq 2$. Gọi $\alpha_1, \alpha_2, \dots, \alpha_n$ là tất cả các nghiệm của f . Đặt $D_f = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$, gọi là biệt thức của f .

Rõ ràng, $D_f \neq 0$ khi và chỉ khi f không có nghiệm bội. Ta ký hiệu G_f là nhóm Galois của f trên F , và xem G_f là nhóm con của nhóm đối xứng S_n .

Sau đây sẽ trình bày nhóm Galois của đa thức bậc 2, bậc 3, bậc 4 và để đơn giản trong biện luận, ta giả thiết F có đặc số khác 2, 3. Khi đó mọi đa thức bậc 2, 3, 4 trên F đều tách được.

1.3.4. Nhóm Galois của đa thức bậc hai.

Cho đa thức bậc hai $f = x^2 + bx + c \in F[x]$ tách được. Gọi x_1, x_2 là hai nghiệm của f . Ta có :

$$D_f = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4c.$$

Biệt thức $D_f = 0$ khi và chỉ khi f có nghiệm kép. Nhóm Galois G_f đẳng cấu với nhóm con của S_2 .

Nếu D_f chính phương trong F thì $G_f = 1 = A_2$;

Nếu D_f không chính phương trong F thì $G_f = S_2$.

1.3.5. Nhóm Galois của đa thức bậc ba.

1.3.5.1. Bài toán [9]. Xác định nhóm Galois của đa thức bậc ba

$$f = x^3 + ax^2 + bx + c \in F[x].$$

1.3.5.2. Giải . Đặt $x = y - \frac{a}{3}$, ta có đa thức theo y

$$g = y^3 + py + q \in F[y] \quad (1.1)$$

$$\text{với } p = \frac{1}{3} (3b - a^2), \quad q = \frac{1}{27} (2a^3 - 9ab + 27c) .$$

Ở đây dễ thấy trường phân rã của f và g trên F là như nhau và biệt thức của chúng cũng trùng nhau. Gọi $\alpha_1, \alpha_2, \alpha_3$ là ba nghiệm của g . Ta có: $g = (y - \alpha_1)(y - \alpha_2)(y - \alpha_3)$

Đạo hàm hình thức của g là

$$g' = (y - \alpha_1)(y - \alpha_2) + (y - \alpha_2)(y - \alpha_3) + (y - \alpha_1)(y - \alpha_3)$$

$$\text{Do đó} \quad g'(\alpha_1) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3);$$

$$g'(\alpha_2) = (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3);$$

$$g'(\alpha_3) = (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2).$$

$$\begin{aligned} \text{Suy ra } D_g &= [(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)]^2 \\ &= -g'(\alpha_1)g'(\alpha_2)g'(\alpha_3). \end{aligned}$$

Mặt khác từ (1.1) ta có $g' = 3y^2 + p$. Do đó

$$D_g = - (3a_1^2 + p) (3a_2^2 + p) = - [27a_1^2 a_2^2 a_3^2 + 9p(a_1^2 a_2^2 + a_1^2 a_3^2 + a_2^2 a_3^2) + 3p^2 (a_1^2 + a_2^2 + a_3^2) + p^3].$$

Biểu diễn D_g qua các đa thức đối xứng sơ cấp S_1, S_2, S_3 của a_1, a_2, a_3 với chú ý rằng $S_1 = 0, S_2 = p, S_3 = -q$; ta có

$$D_g = -4p^3 - 27q^2.$$

Do D_g cũng là biệt thức của f , biểu diễn D_g theo các hệ tử của f ta có: $D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$.

Nếu f khả quy trên F thì nhóm Galois của nó trùng với nhóm Galois của một đa thức bậc hai của F . Ta chỉ cần xét khi f bất khả quy. Khi đó $(G_f : 1) \geq 3$, do đó G_f đẳng cấu với A_3 hoặc với S_3 . Nếu D_f chính phương trong F thì do $G_f \subset A_3$, suy ra $G_f = A_3$. Khi đó trường phân rã $E_g = F(a_i)$ với $i \in \{1, 2, 3\}$. Nếu D_f không chính phương trong F thì $G_f = S_3$ và $E_f = F(a_i, \sqrt{D_f})$ với $i \in \{1, 2, 3\}$.

1.3.6. Nhóm Galois của đa thức bậc bốn.

1.3.6.1. Bài toán [9]. Xác định nhóm Galois của đa thức bậc bốn

$$f = x^4 + ax^3 + bx^2 + cx + d \in F[x].$$

1.3.6.2. Giải.

Đặt $x = y - \frac{a}{4}$, ta có đa thức theo y

$$g = y^4 + py^2 + r \in F[y];$$

$$\text{với } p = \frac{1}{8}(-3a^2 + 8b); \quad q = \frac{1}{8}(a^3 - 4ab + 8c);$$

$$r = \frac{1}{256}(-3a^4 + 16a^2b - 64ac + 256d).$$

Gọi các nghiệm của g là $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Gọi G là nhóm Galois của g (cũng là của f). Nếu g là tích của một đa thức bậc 1 và bậc 3 trên F thì nhóm G đẳng cấu với nhóm Galois của một đa thức bậc ba đã xác định ở trên. Nếu g là tích của hai đa thức bất khả quy bậc hai trên F thì trường phân rã E_g của g trên F là $F(\sqrt{d_1}, \sqrt{d_2})$ với $d_1, d_2 \in F^*$. Nếu $d_1 = a^2 d_2$ với $a \in F$ thì E_g là mở rộng bậc hai trên F và $G \cong \mathbb{Z}_2$. Nếu không thì $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Ta xét trường hợp g bất khả quy trên F . Khi đó, ta biết rằng với hai nghiệm tùy ý α_i, α_j cho trước của g , tồn tại một phần tử $\sigma \in G$ biến α_i thành α_j . Những nhóm con của S_4 thỏa mãn tính chất đó là:

S_4 ; A_4 ;

$$D_8 = \{1, (1324), (12)(34), (1423), (13)(24), (14)(23), (12)(34)\}$$

và các nhóm con liên hợp $\sigma^{-1}D_8\sigma$ của D_8 ;

$$K_4 = \{1, (12)(34), (13)(24), (14)(23)\};$$

$C_4 = \{1, (1234), (13)(24), (1423)\}$ và các nhóm con liên hợp $\sigma^{-1}C_4\sigma$ của C_4 .

Nhóm Galois G sẽ đẳng cấu với một trong các nhóm trên.

$$\text{Đặt } \theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4); \quad \theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4);$$

$$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).$$

Ta có $\theta_1 + \theta_2 + \theta_3 = 2p$; $\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = p^2 - 4r$;
 $\theta_1\theta_2\theta_3 = -q^2$. Suy ra θ_1, θ_2 và θ_3 là ba nghiệm của

$$h(X) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2 \quad (1.2)$$

Đa thức (1.2) là giải thức bậc ba của g . Ta thấy rằng

$$\theta_1 - \theta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 = -(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3).$$

$$\text{Tương tự ta có: } \theta_1 - \theta_3 = -(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4),$$

$$\theta_2 - \theta_3 = -(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4).$$

Suy ra biệt thức của giải thức (1.2) trùng với biệt thức của g (do đó cũng trùng với biệt thức của f). Từ công thức tính biệt thức $D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$, ta có biệt thức của giải thức (1.2) là

$$D_h = 16p^4r - 128p^2r^2 + 256r^3 - 4p^3q^2 - 27q^4 + 144pq^2r \quad (1.3)$$

Thay các giá trị của p, q, r trong (1.3), ta có

$$\begin{aligned} D_f = & -6a^2c^2d + b^2a^2c^2 + 144a^2bd^2 - 4a^2b^3d + 144bdc^2 \\ & + 18abc^2 - 192acd^2 + 16b^4d - 128b^2d^2 - 80b^2acd + 18a^3bcd \\ & - 27a^4d^2 + 256d^3 - 4a^3c^3 - 4b^3c^2 - 27c^4. \end{aligned}$$

Trường phân rã của giải thức $h(X)$ chứa trong trường phân rã của f . Do đó nhóm Galois của h là nhóm thương của G . Ta có các trường hợp :

1. Nếu h bất khả quy và D_f không chính phương trong F . Khi đó G không chứa trong A_4 và nhóm Galois của h đẳng cấu với S_3 . Do đó cấp của G chia hết cho 6. Suy ra $G = S_4$.

2. Nếu h bất khả quy và D_f chính phương trong F . Khi đó $G \subseteq A_4$ và nhóm Galois của h đẳng cấu với A_3 . Suy ra G có cấp chia hết cho 3. Suy ra $G = A_4$.

3. Nếu h khả quy và phân rã thành ba nhân tử tuyến tính trong $F[x]$. Khi đó $\theta_1, \theta_2, \theta_3$ thuộc F . Do đó mọi phần tử G phải cố định chúng. Suy ra $G \subseteq K_4$. Vì g bất khả quy nên $G = K_4$.

4. Nếu h được phân tích thành một đa thức bậc hai và một đa thức bậc một trong $F[X]$. Khi đó có đúng một phần tử trong $\{\theta_1, \theta_2, \theta_3\}$ thuộc F . Ta có thể giả thiết θ_1 thuộc F . Như thế mọi phần tử của G cố định θ_1 nhưng không cố định θ_2 và θ_3 . Suy ra $G \subseteq D_8$ và $G \not\subseteq K_4$. Vậy $G = D_8$ hoặc $G = C_4$.

Chú ý rằng $F(\sqrt{D_f})$ là trường cố định bởi $G \cap A_4$. Ta có $D_8 \cap A_4 = K_4$ và $C_4 \cap A_4 = \{1, (13)(24)\}$. Với chú ý rằng $G \cap A_4$ là nhóm Galois của g trên $F(\sqrt{D_f})$ thì $G \cap A_4$ có cấp không nhỏ hơn 4, do đó $G = D_8$. Ngược lại, nếu g khả quy trên $F(\sqrt{D_f})$ thì $G = C_4$.

1.4. ĐA THỨC TỔNG QUÁT

1.4.1. Định nghĩa. Cho F là một trường và $s_1, \dots, s_n$ là các phần tử độc lập đại số trên F . Đa thức $g = t^n - s_1 t^{n-1} + \dots + (-1)^n s_n \in F(s_1, \dots, s_n)[t]$ gọi là đa thức tổng quát bậc n trên F .

1.4.2. Định lý [9]. Cho F là một trường và g là đa thức tổng quát trên F . Gọi E_g là trường phân rã của g trên $F(s_1, \dots, s_n)$. Khi đó các nghiệm $t_1, \dots, t_n$ của g độc lập đại số trên F và nhóm Galois của $E_g : F(s_1, \dots, s_n)$ là S_n .

1.5. MỘT SỐ BÀI TOÁN MINH HỌA

Bài 1 [4]. Hãy định xem mỗi số thực hoặc phức sau đây

$\sqrt{7}$, $\sqrt[3]{5}$, π^2 , $e + 3$, $3 + i$, $\sqrt{2} + i$ là đại số hay siêu việt trên trường $\mathbb{Q}$ các số hữu tỷ.

Giải. $\sqrt{7}$, $\sqrt[3]{5}$, $3 + i$, $\sqrt{2} + i$ là đại số trên $\mathbb{Q}$ theo thứ tự là nghiệm của các đa thức có hệ số hữu tỷ: $x^2 - 7$, $x^3 - 5$, $(x - 3)^2 + 1$ và $(x^2 - 3)^2 + 4x^2$. Các số π^2 , $e + 3$ là siêu việt trên $\mathbb{Q}$ vì π và e siêu việt trên $\mathbb{Q}$.

Bài 2 [2]. Chứng minh rằng mọi mở rộng hữu hạn của trường $\mathbb{R}$ các số thực hoặc là chính $\mathbb{R}$ hoặc là một trường đẳng cấu với trường $\mathbb{C}$ các số phức.

Giải. Cho F là một mở rộng hữu hạn của $\mathbb{R}$. Mọi $u \in F$ là đại số trên $\mathbb{R}$ và có đa thức tối thiểu $q_u \in \mathbb{R}[x]$ sao cho có đẳng cấu trường $\mathbb{R}[x]/q(u) \cong \mathbb{R}[u]$. Nhưng đa thức bất khả quy $q_u \in \mathbb{R}[x]$ có bậc 1 hoặc bậc 2.

Nếu q_u bậc 1, ta có u thuộc $\mathbb{R}$ nên thuộc $\mathbb{R}[u] = \mathbb{R}$. Nếu q_u bậc 2 (vì q_u có biệt số thực âm), thì thuộc $\mathbb{R}[x]/q_u \cong \mathbb{C} \cong \mathbb{R}[u]$.

Trong trường hợp F có một phần tử u sao cho $\mathbb{C} \cong \mathbb{R}[u] \subset F$, thì với mọi $r \in F$ vì đại số trên $\mathbb{R}$ nên cũng đại số trên $\mathbb{C}$ và có đa thức bất khả quy tối thiểu $q_r \in \mathbb{C}[x]$ và đẳng cấu trường $\mathbb{C}[x]/(q_r) \cong \mathbb{C}[u]$; nhưng vì mọi đa thức bất khả quy $q_r \in \mathbb{C}[x]$ phải là đa thức bậc 1; hơn nữa vì u là nghiệm của q_r ta suy ra $u \in \mathbb{C}$, trong trường hợp này $F \subset \mathbb{C}$.

Vậy, mọi mở rộng hữu hạn của $\mathbb{R}$, nếu phân biệt với $\mathbb{R}$, thì đẳng cấu với $\mathbb{C}$.

CHƯƠNG 2. ỨNG DỤNG CỦA LÝ THUYẾT GALOIS

Chương này là nội dung chính của luận văn, trình bày một số ứng dụng của lý thuyết Galois.

2.1. DỰNG HÌNH BẰNG THƯỚC KẼ VÀ COMPA.

Trước tiên ta có thể quy giả thiết của mọi bài toán dựng hình về việc cho trước một số điểm nào đấy. Ví dụ như biết một độ dài có nghĩa là cho trước hai điểm sao cho đoạn thẳng nối hai điểm đó có độ dài đã cho; cho trước một đường tròn có nghĩa là cho trước hai điểm sao cho một điểm là tâm đường tròn và đoạn thẳng nối hai điểm đó là bán kính; cho trước một góc nghĩa là cho trước ba điểm mà tam giác của chúng có một góc bằng góc đã cho. Cũng tương tự như vậy, một hình sẽ được coi là dựng được nếu ta dựng được những điểm xác định hình đó.

2.1.1. Định nghĩa [9]. Trong mặt phẳng $\mathbb{R}^2$, cho hai điểm $P_0 = (0; 0)$, $P_1 = (1; 0)$. Một điểm $P \in \mathbb{R}^2$ được gọi là dựng được (bằng thước kẻ và compa) nếu tồn tại dãy hữu hạn $P_0, P_1, \dots, P_n$ sao cho $P = P_n$ và với mọi $j \geq 2$, điểm P_j xác định từ $S_{j-1} := \{P_0, P_1, \dots, P_{j-1}\}$ bởi một trong ba “phép dựng” sau:

1. Giao của hai đường thẳng phân biệt, trong đó mỗi đường thẳng đi qua hai điểm bất kỳ của S_{j-1} .

2. Giao của một đường thẳng qua hai điểm của S_{j-1} và một đường tròn có tâm tại một điểm của S_{j-1} và có bán kính bằng khoảng cách giữa hai điểm trong S_{j-1} .

3. Giao của hai đường tròn phân biệt, trong đó mỗi đường tròn có tâm tại một điểm của S_{j-1} và có bán kính bằng khoảng cách giữa hai điểm trong S_{j-1} .

2.1.2. Định lý [9]. Cho $\alpha \in E \subset \mathbb{H}$ với E là mở rộng Galois của $\mathbb{Q}$. α dựng được bằng thước kẻ và compa khi và chỉ khi $[E : \mathbb{Q}] = 2^r$ với $r \in \mathbb{N}$.

2.1.3. Hệ quả [9]. Không thể chia ba góc $\frac{\pi}{3}$ bằng thước kẻ và compa.

2.1.4. Hệ quả [9]. Không thể dựng được điểm $(\sqrt[3]{2}, 0)$. Nói cách khác không thể gấp đôi hình lập phương có cạnh bằng 1.

2.1.5. Hệ quả [9]. Không thể dựng được điểm $(\sqrt{x}, 0)$. Nói cách khác không thể dựng được hình vuông có diện tích bằng diện tích hình tròn bán kính bằng 1.

2.1.6. Định lý [10]. Đa giác đều n cạnh dựng được khi và chỉ khi $n = 2^r p_1 \dots p_s$, với $p_1, \dots, p_s$ là các số nguyên tố Fermat khác nhau.

Từ đây về sau việc tìm nghiệm của một phương trình đại số được xem như tìm nghiệm của một đa thức.

2.2. TIÊU CHUẨN GIẢI ĐƯỢC BẰNG CĂN THỨC CỦA ĐA THỨC

2.2.1. Định nghĩa [9]. Một mở rộng $E : F$ gọi là mở rộng căn nếu $E = F(\alpha_1, \dots, \alpha_m)$ sao cho với mọi $i = 1, \dots, m$ tồn tại $n_i : \alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$. Khi đó ta cũng nói E là một mở rộng căn của F . Ta nói các phần tử α_i tạo ra một chuỗi căn cho mở rộng $E : F$.

2.2.2. Định nghĩa [9]. Một phần tử α thuộc vào một mở rộng căn $E : F$ thì được gọi là biểu diễn được bằng căn thức (trên F). Một đa thức f trên F được gọi là giải được bằng căn thức (trên F) nếu trường phân rã của f nằm trong một mở rộng căn của F .

2.2.3. Định nghĩa [10]. Cho một dãy lồng nhau các nhóm con

$$G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\}. \quad (2.1)$$

(2.1) được gọi là tháp chuẩn tắc nếu G_i là nhóm con chuẩn tắc của G_{i-1} , với $i = 1, \dots, n$.

(2.1) được gọi là tháp aben (cyclic) nếu nó là một tháp chuẩn tắc đồng thời G_{i-1}/G_i là một nhóm aben (cyclic) với $i = 1, \dots, n$.

Nhóm G được gọi là *giải được* nếu tồn tại một tháp aben (2.1) cho G .

2.2.4. Định lý [10]. Với $n \leq 4$ thì S_n giải được.

2.2.5. Định lý [8]. Mọi nhóm hữu hạn có cấp là lũy thừa của một số nguyên tố là nhóm giải được.

2.2.6. Định lý [9]. Nếu nhóm Galois của đa thức f trên trường có đặc số 0 giải được thì f giải được bằng căn thức trên F .

2.2.7. Hệ quả [9]. Cho F là trường có đặc số 0. Đa thức tổng quát $g = t^n - s_1 t^{n-1} + \dots + (-1)^n s_n$ không giải được bằng căn thức trên $F(s_1, \dots, s_n)$ khi và chỉ khi $n \geq 5$.

2.3. TÍNH KHÔNG GIẢI ĐƯỢC CỦA ĐA THỨC CÓ BẬC LỚN HƠN 4

2.3.1. Mệnh đề. Cho một đa thức $f \in \mathbb{Q}[x]$ bất khả quy có bậc p nguyên tố. Nếu f có đúng hai nghiệm không thực trong $\mathbb{C}$ thì nhóm Galois của f là nhóm đối xứng S_p .

2.3.2. Định lý [10]. Với $n \geq 5$ thì S_n không giải được.

2.4. NGHIỆM CĂN THỨC CỦA CÁC ĐA THỨC TỔNG QUÁT CÓ BẬC KHÔNG QUÁ 4

2.4.1. Đa thức tổng quát bậc hai.

Cho $g = t^2 - s_1 t + s_2$ có nhóm Galois trên $F(s_1, s_2)$ là $S_2 = \{1, (12)\}$. Phần tử $(1, 2)$ hoán vị t_1, t_2 nên có định $(t_1 - t_2)^2$. Do đó $(t_1 - t_2)^2 \in F(s_1, s_2)$. Cụ thể $(t_1 - t_2)^2 = s_1^2 - 4s_2$. Kí hiệu $\sqrt{s_1^2 - 4s_2}$ là một nghiệm của $x^2 - (s_1^2 - 4s_2)$, ta có $t_1 - t_2 = \sqrt{s_1^2 - 4s_2}$ và $t_1 + t_2 = s_1$. Suy ra công thức nghiệm quen thuộc

$$\begin{cases} t_1 = \frac{1}{2} \left(s_1 + \sqrt{s_1^2 - 4s_2} \right) \\ t_2 = \frac{1}{2} \left(s_1 - \sqrt{s_1^2 - 4s_2} \right) \end{cases}$$

2.4.2. Đa thức tổng quát bậc ba.

2.4.2.1. Bài toán [9]. Tìm nghiệm căn thức của đa thức

$$g = t^3 - s_1 t^2 - s_2 t - s_3 \in F(s_1, s_2, s_3)[t].$$

2.4.2.2 Giải.

a. Cách 1. Đa thức $g = t^3 - s_1 t^2 - s_2 t - s_3$ có nhóm Galois trên $F(s_1, s_2, s_3)$ là S_3 . Ta có dãy các nhóm con chuẩn tắc $1 \triangleleft A_3 \triangleleft S_3$ có thương là nhóm cyclic.

Đặt $\omega = e^{\frac{2\pi i}{3}}$ và $y = t_1 + \omega t_2 + \omega^2 t_3$, với t_1, t_2, t_3 là các nghiệm của g . Với mọi $\sigma \in A_3$, tồn tại $0 \leq i \leq 2$ sao cho $\sigma(y) = \omega^i y$, nên $\sigma(y^3) = y^3$.

Tương tự, đặt $z = t_1 + \omega^2 t_2 + \omega t_3$ thì ta có $\sigma(z^3) = z^3$, $\forall \sigma \in A_3$. Mặt khác với σ là một phép thế lẻ thì $\sigma(y^3) = z^3$.

Nói cách khác, các phân tử $y^3 + z^3$ và $y^3 z^3$ bất biến với S_3 . Do đó $y^3 + z^3$ và $y^3 z^3$ thuộc $F(s_1, s_2, s_3)$. Như thế y^3 và z^3 là nghiệm của cùng một đa thức bậc hai trên $F(s_1, s_2, s_3)$. Mặt khác, ta thấy rằng

$$\begin{cases} t_1 = \frac{1}{3}(s_1 + y + z) \\ t_2 = \frac{1}{3}(s_1 + \omega^2 y + \omega z) \\ t_3 = \frac{1}{3}(s_1 + \omega y + \omega^2 z) \end{cases}$$

Do đó khi giải được y^3 và z^3 , ta có nghiệm của g . Ở đây ta có thể tính trực tiếp

$$yz = s_1^2 - 3s_2 \quad \text{và} \quad y^3 + z^3 = 2s_1^3 - 9s_1 s_2 + 27s_3.$$

b. Cách 2 (thường dùng trong thực hành).

Đặt $u = t - \frac{s_1}{3}$. Khi đó ta có đa thức bậc ba theo u là

$f = u^3 + pu + q$ với $p = s_2 - \frac{1}{3}s_1^2$; $q = -\frac{2}{27}s_1^3 + \frac{1}{3}s_1 s_2 - s_3 \in F(s_1, s_2, s_3)$. Do đó $y^3 + z^3 = -27q$, $y^3 z^3 = -27p^3$. Khi đó y^3 và z^3 là hai nghiệm của $x^2 + 27qx - 27p^3 = 0$. Từ đó

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

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

sao cho $yz = -3p$. Ta nhận được công thức nghiệm Cardano

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

và 3 nghiệm của f cho bởi

$$\begin{cases} u_1 = \frac{1}{3}(y+z) \\ u_2 = \frac{1}{3}(\omega^2 y + \omega z) \\ u_3 = \frac{1}{3}(\omega y + \omega^2 z) \end{cases}$$

2.4.3. Đa thức tổng quát bậc 4.

2.4.3.1. Bài toán. Tìm nghiệm căn thức của đa thức

$$g = t^4 - s_1 t^3 + s_2 t^2 - s_3 t + s_4 \in F(s_1, s_2, s_3, s_4).$$

2.4.3.2. Giải.

a. Cách 1. Nhóm Galois S_4 của g có dãy nhóm con chuẩn tắc $1 \triangleleft K_4 \triangleleft A_4 \triangleleft S_4$.

$$K_4 = \{1, (12)(34), (13)(24), (14)(23)\}.$$

Đặt

$$y_1 = (t_1 + t_2)(t_3 + t_4); \quad y_2 = (t_1 + t_3)(t_2 + t_4);$$

$$y_3 = (t_1 + t_4)(t_2 + t_3).$$

Vì các đa thức đối xứng sơ cấp của y_1, y_2, y_3 thuộc $F(s_1, s_2, s_3, s_4)$ nên y_1, y_2, y_3 là các nghiệm của một đa thức bậc ba trên $F(s_1, s_2, s_3, s_4)$, gọi là giải thức bậc ba của g.

Khi đã giải được y_1, y_2, y_3 cùng với $t_1 + t_2 + t_3 + t_4 = s_1$, suy ra các cặp $(t_1 + t_2 + t_3 + t_4); (t_1 + t_3, t_2 + t_4); (t_1 + t_4, t_2 + t_3)$ là

nghiệm của các đa thức bậc hai có hệ tử trong $F(s_1, s_2, s_3, s_4, y_1, y_2, y_3)$. Từ đó giải được t_1, t_2, t_3, t_4 .

b. Cách 2 (Thường dùng trong thực hành). Đặt $u = t - 1/4 s_1$ thì ta phải có một đa thức bậc 4 theo u $uf = u^4 + pu^2 + qu + r$. Từ đó tính được $y_1 + y_2 + y_3 = 2p$; $y_1y_2 + y_1y_3 + y_2y_3 = p^2 - 4r$; $y_1y_2y_3 = -q^2$.

Suy ra giải thức $f(u)$ là : $x^3 - 2px^2 + (p^2 - 4r)x + q^2$. Các nghiệm của f cho bởi

$$\begin{cases} u_1 = \frac{1}{2}(\sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3}) \\ u_2 = \frac{1}{2}(\sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3}) \\ u_3 = \frac{1}{2}(-\sqrt{-y_1} + \sqrt{-y_2} - \sqrt{-y_3}) \\ u_4 = \frac{1}{2}(-\sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3}) \end{cases}$$

với các căn thức được chọn sao cho $\sqrt{-y_1} \cdot \sqrt{-y_2} \cdot \sqrt{-y_3} = -q$.

2.5. CHỨNG MINH ĐỊNH LÝ CƠ BẢN CỦA ĐẠI SỐ.

2.5.1. Bổ đề [9]. Mọi đa thức hệ số thực có bậc lẻ đều có một nghiệm thực. Suy ra $\mathbb{R}$ không có một mở rộng thực sự bậc lẻ.

2.5.2. Bổ đề [9]. Mọi đa thức bậc hai trên $\mathbb{C}$ có nghiệm trong $\mathbb{C}$.

2.5.3. Định lý [9]. Mọi đa thức bậc lớn hơn 0 trên trường số phức $\mathbb{C}$ có một nghiệm trong $\mathbb{C}$.

2.6. MỘT SỐ BÀI TOÁN MINH HỌA.

Bài 1 [9]. Chứng minh không thể dựng được đa giác đều 18 cạnh bằng thước kẻ và compa.

Giải. Ta chứng minh $\cos \frac{2\pi}{18}$ hay $\cos \frac{\pi}{9}$ dựng được. Ta có

$$\cos \frac{\pi}{3} = \cos\left(3 \frac{\pi}{9}\right) = 4 \cos^3 \frac{\pi}{9} - 3 \cos \frac{\pi}{9}$$

$$\Leftrightarrow \frac{1}{2} = 4 \cos^3 \frac{\pi}{9} - 3 \cos \frac{\pi}{9} \Leftrightarrow 4 \cos^3 \frac{\pi}{9} - 3 \cos \frac{\pi}{9} - \frac{1}{2} = 0$$

Đặt $u = \cos \frac{\pi}{9}$, ta có $4u^3 - 3u - \frac{1}{2} = 0 \Leftrightarrow 8u^3 - 6u - 1 = 0$.

Đa thức này bất khả quy trên $\mathbb{Q}$ (đặt $u = y - 1$, ta được đa thức theo ẩn y là $8y^3 - 24y^2 + 18y - 3$, bất khả quy theo tiêu chuẩn Eisenstein cho $p = 3$).

Vậy $[Q(u) : Q] = 3 \neq 2^r$ nên theo định lý 1.13, $\cos \frac{\pi}{9}$

không dựng được bằng thước kẻ và compa.

Bài 2 [9]. Tìm nghiệm căn thức của đa thức $f = t^4 + 4t + 2$.

Giải. Đa thức f có giải thức bậc 3 là $h = x^3 - 8x + 16$. Biệt thức $D_h = -4864 = -2^8 \cdot 19$. Nghiệm của giải thức h là

$$\begin{cases} x_1 = \sqrt[3]{-8 + \frac{32}{9}\sqrt{57}} + \sqrt[3]{-8 - \frac{32}{9}\sqrt{57}} \\ x_2 = \omega \sqrt[3]{-8 + \frac{32}{9}\sqrt{57}} + \omega^2 \sqrt[3]{-8 - \frac{32}{9}\sqrt{57}} \\ x_3 = \omega^2 \sqrt[3]{-8 + \frac{32}{9}\sqrt{57}} + \omega \sqrt[3]{-8 - \frac{32}{9}\sqrt{57}} \end{cases}$$

Vậy nghiệm căn thức t_1, t_2, t_3, t_4 của f là

$$\left\{ \begin{array}{lcl} t_1 & = & \frac{1}{2} (\sqrt{-x_1} + \sqrt{-x_2} + \sqrt{-x_3}) \\ t_2 & = & \frac{1}{2} (\sqrt{-x_1} - \sqrt{-x_2} - \sqrt{-x_3}) \\ t_3 & = & \frac{1}{2} (-\sqrt{-x_1} + \sqrt{-x_2} - \sqrt{-x_3}) \\ t_4 & = & \frac{1}{2} (-\sqrt{-x_1} - \sqrt{-x_2} - \sqrt{-x_3}) \end{array} \right.$$

KẾT LUẬN

Luận văn “ *Lý thuyết Galois và ứng dụng*” đã thực hiện được những vấn đề sau:

1. Trình bày mở rộng trường và lý thuyết Galois, minh họa các khái niệm bằng những bài toán cụ thể.
2. Trình bày những ứng dụng của lý thuyết Galois, cụ thể:
 - Giải những bài toán dựng hình cổ điển.
 - Khảo sát bài toán: Khi nào một phương trình đại số giải được bằng căn thức.
 - Tìm nghiệm căn thức của các phương trình đại số bậc 2, 3, 4.
 - Chứng minh định lý cơ bản của đại số.

Hy vọng rằng nội dung của luận văn sẽ được tiếp tục mở rộng và hoàn thiện hơn, nhằm có thể làm tài liệu tham khảo cho những ai quan tâm đến Lý thuyết Galois.