

NHÓM GALOIS CỦA ĐA THỨC BẬC n

Ngô Quốc Hoàn

Khoa Toán và KHTN

Email: hoannq@dhhp.edu.vn

Ngày nhận bài: 23/9/2019

Ngày PB đánh giá: 20/11/2019

Ngày duyệt đăng: 27/12/2019

TÓM TẮT: Bài báo tổng hợp những kết quả về nhóm Galois của đa thức, một trong những vấn đề hấp dẫn nhất của lý thuyết Galois. Cụ thể, bài báo đã nêu ra những kết quả quan trọng nhất của nhóm Galois của đa thức một biến bậc n cũng như ứng dụng của vấn đề này trong việc vẽ hình bằng compa và thước kẻ và giải thích chúng bằng những ví dụ tính toán cụ thể. Đặc biệt, bài báo cũng đề cập tới thuật toán tính nhóm Galois, thứ cho phép xây dựng một chương trình tính nhóm Galois của đa thức dưới sự hỗ trợ của máy tính.

Từ khóa: Đa thức, Mở rộng trường, Nhóm Galois.

THE GALOIS'S GROUP OF POLYNOMIAL OF DEGREE n

ABSTRACT: This paper tells about the Galois's group of polynomial which is one of important problems of Galois's theory. We give some nice resultats of Galois's group of polynomial and explain them by the examples. Moreover, we also say about the algorithm which has been used to calculate the Galois's group under helping by a computer.

Keywords: Polynomial, Extension field, Galois's group.

I. GIỚI THIỆU

Lý thuyết Galois là một trong các phát minh quan trọng của Toán học nhằm giải quyết vấn đề tìm kiếm công thức nghiệm của phương trình đa thức, bài toán vẽ hình bằng thước kẻ và compa,....

Lý thuyết Galois nghiên cứu mối quan hệ giữa cấu trúc nghiệm của một đa thức với cấu trúc trường phân rã của đa thức đó⁽¹⁾. Sự đa dạng về đa thức trên một trường kéo theo sự đa dạng của trường phân rã. Lý thuyết Galois không chỉ nghiên cứu sự đa dạng đó mà còn chỉ ra dấu hiệu đặc trưng của trường phân rã để phương trình đa thức có thể giải được,.....

Thực tế, vấn đề này được đề cập đầu tiên bởi J. L. Lagrange, khi ông dùng các tính chất liên quan đến nhóm hoán vị trong việc giải phương trình đại số. Sau đó, các công trình của P. Ruffini và N. Abel đã bắt đầu sử dụng lý thuyết nhóm để xem xét tính giải được của phương trình đa thức [3,4].

(1) Cho đa thức $P(x)$ trên trường K . Trường phân rã của $P(x)$ trên K là trường mở rộng E của K chứa vừa đủ K và các nghiệm của đa thức $P(x)$.

E. Galois là người đầu tiên xây dựng một lý thuyết đầy đủ để chứng minh tính giải được của phương trình đa thức bằng cách áp dụng lý thuyết nhóm (xem [6]). Trong quá trình giải quyết vấn đề, E. Galois đã sáng tạo ra một khái niệm Toán học mới, kí hiệu là $Gal(F, K)$, ở đó K là trường còn F là mở rộng của K . Tập này bao gồm tất cả các tự đẳng cấu của F giữ nguyên các điểm của K . Galois cũng đã xây dựng một cấu trúc nhóm trên tập này, vì vậy ngày nay ta gọi tập này là nhóm Galois.

Ta biết rằng, một phương trình đa thức $P(x) = 0$ giải được bằng căn thức khi và chỉ khi nhóm Galois của đa thức đó được phân giải thành dãy $G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\}$, ở đó G_i là nhóm con chuẩn tắc của G_{i-1} và nhóm thương G_{i+1}/G_i là các nhóm giao hoán với mọi $i = 1, 2, 3, \dots$. Do đó, việc tính toán nhóm Galois là rất quan trọng trong quá trình nghiên cứu các vấn đề của Lý thuyết Galois. Bài viết này đề cập đến một số vấn đề về nhóm Galois của đa thức bậc n (xem [1, 2]), cũng như thuật toán tính nhóm này bằng máy tính (xem [8,9,10,11]) và một ứng dụng của nhóm Galois trong việc xác định tính vẽ được của một hình bằng compa và thước kẻ.

II. Nội dung

1. Nhóm Galois của đa thức bậc n

Cho K là một trường có đặc số khác 2 và $f(x)$ là một đa thức bậc n trên K . Ta giả sử $x_1, \dots, x_n$ là các nghiệm của $f(x)$ trong một trường phân rã F của $f(x)$ trên K .

$$\text{Đặt } \Delta := \prod_{i < j} (x_i - x_j); D(f) := \Delta^2 = \prod_{i < j} (x_i - x_j)^2.$$

Biểu thức $D(f)$ được gọi là biệt thức của đa thức $f(x)$. Việc tính toán giá trị của biệt thức một đa thức, ta sử dụng hệ thức Viet.

Chẳng hạn, ta xét đa thức $f(x) = x^4 + bx^3 + cx^2 + dx + e$ trên trường K . Giả sử trên một mở rộng nào đó của K , đa thức $f(x)$ là tách được và có x_1, x_2, x_3, x_4 là các nghiệm của $f(x)$ (có thể trùng nhau). Đặt

$$A := x_1x_2 + x_3x_4;$$

$$B := x_1x_3 + x_2x_4;$$

$$C := x_1x_4 + x_2x_3.$$

$$\text{Bằng tính toán trực tiếp, ta thu được } (A-B)^2(B-C)^2(C-A)^2 = \prod_{1 \leq i < j \leq 4} (x_i - x_j)^2 = D(f).$$

Mặt khác, sử dụng hệ thức Viet ta có

$$\begin{cases} \delta_1 := x_2 + x_3 + x_4 = -b \\ \delta_2 := x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = c \\ \delta_3 := x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -d \\ \delta_4 := x_1x_2x_3x_4 = e \end{cases}.$$

Do đó, ta thu được

$$\begin{cases} A + B + C = c \\ AB + BC + CA = -4e + db \\ ABC = d^2 + b^2e - 4ce \end{cases}$$

Do đó A, B, C là nghiệm của đa thức $r(x) := x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2$. Vì vậy,

$$D(f) = (A - B)^2(B - C)^2(C - A)^2 = D(r).$$

Nhưng $r(x)$ là đa thức bậc 3, ta dễ dàng tính được¹

$$\begin{aligned} D(f) = D(r) &= c^2[(bd - 4e)^2 + 4c(4ce - b^2e - d^2)] - 4(bd - 4e)^3 \\ &\quad - 27(4ce - b^2e - d^2)^2 - 18c(bd - 4e)(4ce - b^2e - d^2). \end{aligned}$$

Đa thức $r(x)$ được gọi là *giải thức bậc 3* của $f(x)$.

Mệnh đề 1 [1,2]: Cho K là một trường có đặc số khác 2 và $f(x)$ là một đa thức bậc n trên K . Kí hiệu

$$\Delta := \prod_{i < j} (x_i - x_j); D(f) := \Delta^2 = \prod_{i < j} (x_i - x_j)^2,$$

ở đó $x_1, \dots, x_n$ là các nghiệm của $f(x)$ trong một trường phân rã F của $f(x)$ trên K . Ta có

1. $\delta \in \text{Gal}(F, K)$ là một phép thế chẵn nếu và chỉ nếu $\delta(\Delta) = \Delta$.
2. $\delta \in \text{Gal}(F, K)$ là một phép thế lẻ nếu và chỉ nếu $\delta(\Delta) = -\Delta$.

Từ mệnh đề 1, ta có thể thấy rằng $\text{Gal}(F, K) \subset A_n$ nếu và chỉ nếu $\Delta \in K$.

Hệ quả 1 [2]: Giả sử $f(x)$ là một đa thức bất khả quy tách được bậc 3 trên một trường K có đặc số khác 2 và G là nhóm Galois của $f(x)$. Khi đó,

1. $G = S_3$ nếu và chỉ nếu $\Delta \notin K$.
2. $G = A_3$ nếu và chỉ nếu $\Delta \in K$.

Hệ quả 2 [2]: Giả sử $f(x)$ là một đa thức bất khả quy tách được bậc 4 trên một trường K có đặc số khác 2 và G là nhóm Galois của $f(x)$. Gọi α, β, γ là các nghiệm của giải thức bậc ba của $f(x)$. Đặt $m = [K(\alpha, \beta, \gamma) : K]$. Khi đó m là một ước của 6. Hơn nữa

1. Nếu $m = 6$ thì $G = S_4$.
2. Nếu $m = 3$ thì $G = A_4$.
3. Nếu $m = 1$ thì $G = V$.
4. Nếu $m = 2$ thì
 - $G \cong D_4$ nếu và chỉ nếu $f(x)$ bất khả quy trên $K(\alpha, \beta, \gamma)$.
 - $G \cong \mathbb{Z}_4$ nếu và chỉ nếu $f(x)$ khả quy trên $K(\alpha, \beta, \gamma)$.

¹ Biệt thức của đa thức bậc ba $g(x) := x^3 + bx^2 + cx + d$ là $D(g) = b^2(c^2 - 4bd) - 4c^3 - 27d^2 + 18bcd$.

Chẳng hạn, ta có đa thức $f(x) = x^4 + 5x + 5$ là bất khả quy trên $\mathbb{Q}$ theo tiêu chuẩn Eisenstein. Dễ dàng chứng minh được $f(x)$ là tách được. Giải thức bậc 3 của $f(x)$ là

$$r(x) = x^3 - 20x - 25 = (x-5)\left(x + \frac{5+\sqrt{5}}{2}\right)\left(x + \frac{5-\sqrt{5}}{2}\right).$$

Vậy trường phân rã của $r(x)$ là $\mathbb{Q}(\sqrt{5})$ có bậc $m := [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$. Lại có $f(x)$ khả quy trên $\mathbb{Q}(\sqrt{5})$ vì $f(x) = x^4 + 5x + 5 = \left(x^2 - \sqrt{5}x + \frac{5+\sqrt{5}}{2}\right)\left(x^2 + \sqrt{5}x + \frac{5-\sqrt{5}}{2}\right)$.

Do đó nhóm Galois của $f(x) = x^4 + 5x + 5$ đẳng cấu với $\mathbb{Z}_4$.

2. Thuật toán tính nhóm Galois của đa thức bậc n

Ta sẽ bắt đầu bằng ví dụ tính nhóm Galois của đa thức $f(x) = x^4 - 7$. Đây là đa thức bậc 4 và trường phân rã là $F = \mathbb{Q}(i, \sqrt[4]{7})$. Mỗi phần tử $\delta \in \text{Gal}(F, \mathbb{Q})$ được xác định bởi ảnh của i và $\sqrt[4]{7}$. Hơn nữa, ta phải có rằng $\delta(i) \in \{-i, i\}; \delta(\sqrt[4]{7}) \in \{\sqrt[4]{7}, -\sqrt[4]{7}, i\sqrt[4]{7}, -i\sqrt[4]{7}\}$.

Do đó nhóm $\text{Gal}(F, \mathbb{Q})$ có tối đa 8 phần tử như sau:

δ	$\delta_1 = Id$	δ_2	δ_3	δ_4	δ_5	δ_6	δ_7	δ_8
$\delta(i)$	i	I	i	i	$-i$	$-i$	$-i$	$-i$
$\delta(\sqrt[4]{2})$	$\sqrt[4]{7}$	$i\sqrt[4]{7}$	$-\sqrt[4]{7}$	$-i\sqrt[4]{7}$	$\sqrt[4]{7}$	$i\sqrt[4]{7}$	$-\sqrt[4]{7}$	$-i\sqrt[4]{7}$

Nhưng ta lại có rằng $|\text{Gal}(F, \mathbb{Q})| = [F : \mathbb{Q}] = 8$. Vì vậy nhóm $\text{Gal}(F, \mathbb{Q})$ có đúng 8 phần tử xác định như ở bảng trên.

Từ ví dụ trên ta thấy rằng việc tính toán nhóm Galois của một đa thức bậc n khi n đủ lớn là không dễ dàng. Với sự hỗ trợ của máy tính, việc tính toán sẽ trở lên dễ dàng hơn. Điều quan trọng là ta phải mô hình hóa các kết quả ở trên dưới dạng thuật toán. Chẳng hạn, đối với đa thức $p(x)$ bậc 4, ta kí hiệu H_i là các nhóm con của nhóm Galois của $p(x)$ với mọi i . Hơn nữa, với mỗi hàm $f(x)$, ta kí hiệu $R(f, p)$ là tính giải được của p và của f . Với mỗi nhân tử giải được, ta kí hiệu I là tập liên kết, δ_k là tính giải được của $\delta_k, \dots$. Thuật toán ta có thể sử dụng để tính nhóm Galois của $p(x)$ như sau:

Input: p là một đa thức một biến bậc 4

Output: G là nhóm Galois của p

Tính toán biệt thức của p

Nếu biệt thức của p là bình phương thì G là chẵn, nếu không G là lẻ

Nhân tử hóa p

Nếu $I = (4)$ thì G là Bốn cầu

Nếu $I=(1,3)$ và G là lẻ thì $G = H_4$

Nếu $I = (1,3)$ và G là chẵn thì $G = H_8$

Nếu $I = (2^2)$ và G là lẻ thì $G = H_7$

Nếu $I = (2^2)$ và G là chẵn thì $G = H_9$

Nếu $I = (1^2, 2)$ thì $G = H_{10}$

Nếu $I = (1^4)$ thì $G = H_{11}$

Khi G là nhân tử bậc cầu $R(b, p)$

Nếu $I = (3)$ và G là lẻ thì $G = H_1$

Nếu $I = (3)$ và G là chẵn thì $G = H_2$

Nếu $I = (1^3)$ thì $G = H_6$

Nếu $I = (1, 2)$ thì nhân tử hóa được và $R(\delta_3, p)$ (hay $R(\delta_2, p)$)

Nếu $I = (8)$ thì $G = H_3$

Nếu $I = (4^2)$ thì $G = H_5$

Với thuật toán này, dưới sự hỗ trợ của mở rộng SYM của MAXIMA, ta có thể tính được nhóm Galois của các đa thức một biến bậc 4 (xem [5]):

	Biểu diễn	Phần tử sinh	Cấp	
H1	S_4	$[(1,4), (2,4), (3,4)]$	G_1	24
H2	A_4	$[(1,2)(3,4), (1,3)(2,4), (2,3,4)]$	G_2	12
H3	D_4	$[(3,4), (1,2)(3,4), (1,3)(2,4)]$	G_3	8
H4	$\text{Id} \times S_3$	$[(2,3,4), (3,4)]$		6
H5	$\mathbb{Z}_4$	$[(1,2)(3,4), (1,3,2,4)]$	G_4	4
H6	V_4	$[(1,2)(3,4), (1,3)(2,4)]$	G_5	4
H7	$S_2 \times S_2$	$[(3,4), (1,2)]$		4
H8	$A_3 \times S_1$	$[(1,2,3)]$		3
H9		$[(1,2), (3,4)]$		2
H10	$S_1 \times S_1 \times S_2$	$[(3,4)]$		2
H11	Id_4	$[\]$		1

Thực tế, với cách làm tương tự, máy tính có thể giúp ta tính nhóm Galois của đa thức có bậc cao hơn (xem [6,7,8]).

3. Bài toán dựng hình bằng compa và thước kẻ

Ta sẽ bắt đầu bằng bài toán dựng đa giác đều 17 cạnh bằng compa và thước kẻ được Gauss thực hiện năm 1832. Thực chất bài toán này là việc chia đường tròn thành 17 phần

bằng nhau và vì vậy chính là bài toán dựng góc $\frac{2\pi}{17}$ hoặc dựng $\cos \frac{2\pi}{17}$.

$$\text{Đặt } \omega := \cos \frac{2\pi}{17} + i \sin \frac{2\pi}{17},$$

thì tập các căn nguyên thủy bậc 17 của đơn vị là $\{\omega^k \mid k = 1, 2, \dots, 16\}$.

Hiển nhiên ta suy ra các căn này, trong đó có ω , là nghiệm của đa thức

$$\phi_{17}(x) := \frac{x^{17} - 1}{x - 1} = 1 + x + x^2 + \dots + x^{16}.$$

Bây giờ ta đặt

$$\begin{cases} a_1 = (\omega + \omega^{16}) + (\omega^2 + \omega^{15}) + (\omega^4 + \omega^{13}) + (\omega^8 + \omega^9) \\ a_2 = (\omega^3 + \omega^{14}) + (\omega^5 + \omega^{12}) + (\omega^6 + \omega^{11}) + (\omega^7 + \omega^{10}) \end{cases}.$$

Từ $\omega^{17-k} = \omega^{-k}, \forall k = 1, \dots, 16$, ta suy ra

$$\begin{cases} a_1 + a_2 = -1 \\ a_1 a_2 = 4(a_1 + a_2) = -4 \end{cases}.$$

$$\text{Do đó ta có } a_1 = \frac{1}{2}(-1 + \sqrt{17}); a_2 = \frac{1}{2}(-1 - \sqrt{17}).$$

Đặt

$$\begin{cases} b_1 = (\omega + \omega^{16}) + (\omega^4 + \omega^{13}) \\ b_2 = (\omega^5 + \omega^{12}) + (\omega^8 + \omega^9) \\ b_3 = (\omega^3 + \omega^{14}) + (\omega^5 + \omega^{12}) \\ b_4 = (\omega^6 + \omega^{11}) + (\omega^7 + \omega^{10}) \end{cases},$$

thì

$$\begin{cases} b_1 + b_2 = a_1 \\ b_1 b_2 = a_1 + a_2 = -1 \\ b_3 + b_4 = a_2 \\ b_3 b_4 = a_1 + a_2 = -1 \end{cases}.$$

Từ tính toán trực tiếp, ta có

$$\begin{aligned} b_1 &= \frac{1}{2}(a_1 + \sqrt{4 + a_1^2}); b_2 = \frac{1}{2}(a_1 - \sqrt{4 + a_1^2}); \\ b_3 &= \frac{1}{2}(a_2 + \sqrt{4 + a_2^2}); b_4 = \frac{1}{2}(a_2 - \sqrt{4 + a_2^2}). \end{aligned}$$

$$\text{Đặt } c_1 = \omega + \omega^{16}; c_2 = \omega^4 + \omega^{13}, \text{ ta có } c_1 = \frac{1}{2}(b_1 + \sqrt{b_1^2 - 4b_3}); c_2 = \frac{1}{2}(b_1 - \sqrt{b_1^2 - 4b_3}).$$

Vì vậy, ta thu được

$$16 \cos \frac{2\pi}{17} = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} + 2(-1 + \sqrt{17})\sqrt{34 - 2\sqrt{17}}} - 16\sqrt{34 + 2\sqrt{17}}.$$

Nhắc lại rằng, một số phức α được gọi là dựng được thông qua một bước dựng hình nếu như α là nghiệm của một đa thức bậc dương không vượt quá 2 với các hệ số phức đã được coi là dựng được bằng thước kẻ và compa. Từ biểu thức trên, ta suy ra $\cos \frac{2\pi}{17}$ là dựng được bằng thước kẻ và compa vì chỉ chứa căn bậc 2.

Thực tế, ta có thể dựng góc $\frac{2\pi}{17}$ như sau:

- Đầu tiên dựng đường tròn tâm O bán kính 1, giao với Ox tại điểm A(1,0), giao với Ox' tại điểm A, giao với Oy tại điểm B(0,1).

- Dựng điểm $C\left(-\frac{1}{4}, 0\right)$.

- Dựng đường tròn tâm C bán kính BC, cắt Ox tại D, cắt Ox' tại E.

- Dựng đường tròn tâm D bán kính BD, cắt Ox tại điểm F.

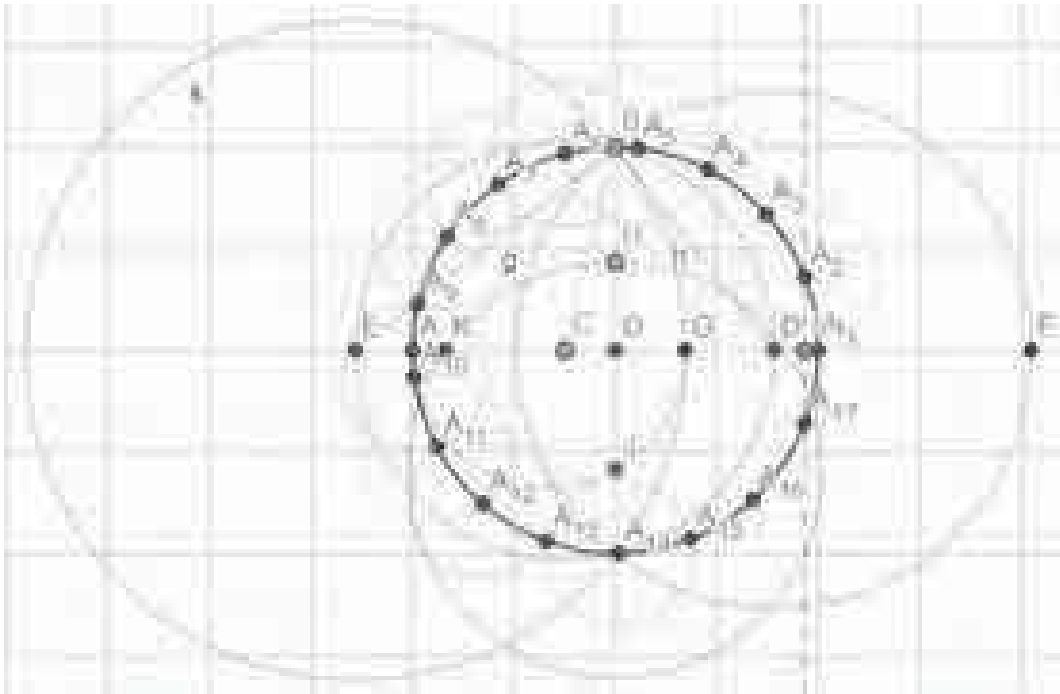
- Dựng đường tròn tâm E bán kính EB, cắt Ox tại G.

- Dựng đường tròn đường kính AG, cắt Oy' tại J.

- Dựng đường tròn tâm J bán kính $\frac{1}{2}OF$, cắt Ox' tại điểm K. Bằng tính toán ta thu được $OK + \frac{1}{2}OF = \frac{b_1}{2} + \frac{1}{2}\sqrt{b_1^2 - 4b_3} = 2\cos\frac{2\pi}{17}$.

Từ đó dựng điểm M trên Ox sao cho $OM = \cos\frac{2\pi}{17}$. Qua M kẻ đường thẳng song song với Oy, giao với đường tròn đơn vị tại hai điểm A_2, A_{17} . Ta có $A_1OA_2 = \frac{2\pi}{17}$. Như vậy ta có các đỉnh là A_1, A_2, A_{17} .

- Các điểm còn lại ta có thể dùng compa như sau : vẽ đường tròn tâm A_2 bán kính A_2A_1 cắt đường tròn đơn vị tại A_3 ; vẽ đường tròn tâm A_3 bán kính A_3A_2 cắt đường tròn đơn vị tại A_4 ;



Hình 1: Hình mô phỏng vẽ đa giác đều 17 cạnh bằng phần mềm GeoGebra

Thực tế, nếu các số phức $\alpha_1, \dots, \alpha_n$ dựng được bằng thước kẻ và compa thì các số của trường $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ với $\mathbb{Q}$ là trường các số hữu tỉ, cũng dựng được bằng thước kẻ và compa.

Mệnh đề 2 [1,2]: Từ các đại lượng phức cho trước $\alpha_1, \dots, \alpha_n$ coi như đã dựng được tạo nên trường $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ với $\mathbb{Q}$ là trường các số hữu tỉ. Khi đó một số phức α dựng được bằng thước kẻ và compa nếu và chỉ nếu $\alpha \in F$ với F là một trường phân rã của một đa thức trên K có $[F : K]$ là một lũy thừa của 2.

Từ mệnh đề trên ta suy ra rằng một số phức α dựng được bằng thước kẻ và compa. Khi đó α là nghiệm của một đa thức bất khả quy có bậc 2^m trên trường số hữu tỉ $\mathbb{Q}$.

Chú ý rằng, mỗi số phức thực chất đều tương ứng với một điểm trên mặt phẳng tọa độ. Do đó, việc dựng một hình, tức là dựng một tập hợp điểm trên mặt phẳng tọa độ, cũng chính là việc dựng một tập hợp các số phức tương ứng với hình đó. Chẳng hạn, một đa giác đều n cạnh dựng được nếu và chỉ nếu các nghiệm phức của phương trình $x^n - 1 = 0$ dựng được. Nhưng do đa thức $x^n - 1$ là tách được trên $\mathbb{Q}$ nên các phần tử của trường phân rã F dựng được khi và chỉ khi $[F : \mathbb{Q}]$ là một lũy thừa của 2. Chú ý rằng $[F : \mathbb{Q}] = \varphi(n)$, nên một đa giác đều n cạnh dựng được nếu và chỉ nếu $\varphi(n)$ là một lũy thừa của 2.

III. KẾT LUẬN

Bài báo phân tích những kết quả quan trọng về nhóm Galois của đa thức bậc n và giải thích những kết quả đó bằng những ví dụ tính toán cụ thể. Bài báo cũng đề cập đến việc đưa việc tính nhóm Galois của đa thức dưới dạng thuật toán để áp dụng cho máy tính. Cuối cùng, bài báo giới thiệu một ứng dụng quan trọng của lý thuyết nhóm Galois của đa thức, bài toán vẽ hình bằng thước kẻ và compas.

TÀI LIỆU THAM KHẢO

1. Ngô Việt Trung (2006), *Lý thuyết Galois*, NXB Đại học Quốc gia Hà Nội.
2. Dương Quốc Việt (chủ biên) (2015), Lê Văn Chua, *Cơ sở lý thuyết Galois*, NXB Đại học Sư phạm.
3. N. Abel (1824), *Mémoire sur les équations algébriques, ou l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré*, trong Sylow, Ludwig; Lie, Sophus.
4. N. Abel (1826), *Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré*, trong Sylow, Ludwig; Lie, Sophus.
5. G. Cardano, *Artis magnae, sive de regulis algebraicis* (also known as *Ars magna*), Nuremberg, 1545 (on algebra).
6. E. Galois (1989), Sophie Lie, *Oeuvres mathématiques*, Éditions Jacques Gabay.
7. Francis Borceux (2001), George Janelidze, *Galois Theories*, Cambridge University Press.
8. J.M. Arnaudiès (1994), A. Valibouze, *Groupes de Galois de polynômes en degré 4 à 6*, Rapport interne LITP 94.48, Juillet.
9. J.M. Arnaudiès (1994), A. Valibouze, *Groupes de Galois de polynômes en degré 8*, Rapport interne LITP 94.25, Mars.
10. J.M. Arnaudiès (1994), A. Valibouze, *Groupes de Galois de polynômes en degré 9*, Rapport interne LITP 94.30, Mai.
11. J.M. Arnaudiès, A. Valibouze, *Groupes de Galois de polynômes en degré 10 et 11*, (manuscrit).