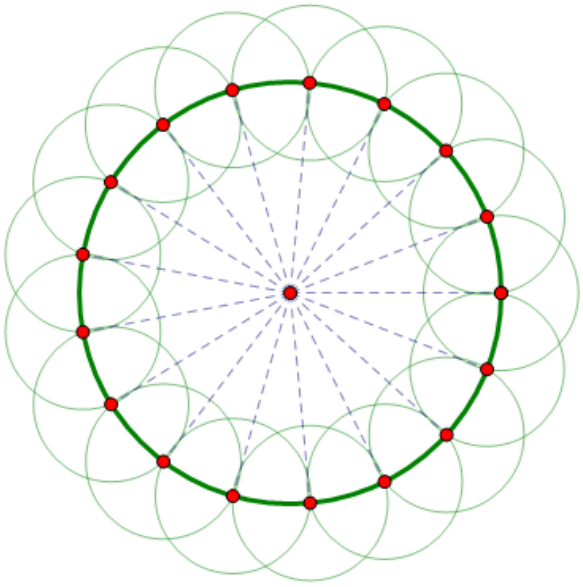
BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC QUY NHƠN

****

HÀ DUY NGHĨA

ỨNG DỤNG LÝ THUYẾT GALOA TRONG PHÉP DỰNG HÌNH



Quy nhơn, tháng 12 năm 2009

MỤC LỤC

LỜI MỞ ĐẦU

Lý thuyết Galoa là một trong những lý thuyết đẹp đẽ nhất của đại số, nó tập hợp nhiều kiến thức và phương pháp của các lĩnh vực toán học khác nhau nhằm giải quyết bài toán cổ điển và những vấn đề quan trọng khác của đại số hiện đại.

Một trong những ứng dụng chủ yếu đó là tìm nghiệm căn thức của phương trình đa thức, đặc biệt chỉ ra được phương trình bặc lớn hơn bốn không thể giải được bằng căn thức. Mặt khác, lý thuyết Galoa cho phép xác định đa giác đều n cạnh dựng được bằng thước kẻ và compa và lời giải cho bài toán dựng hình cổ điển.

Bài viết này tôi giới thiệu về ***Ứng dụng của lý thuyết Galoa trong phép dựng hình***, tiểu luận gồm 2 chương cùng với phần mở đầu, kết luận và danh mục các tài liệu tham khảo.

Chương 1: Giới thiệu một khái niệm về mở rộng Galoa, các định lý của mở rộng Galoa , trong đó mở rộng căn bậc hai là phần ứng dụng quan trọng cho lý thuyết dựng hình ở chương sau.

Chương 2: Là phần chính của tiểu luận, phần đầu của chương giới thiệu về điểm dựng được, số dựng được,chứng minh tập hợp các số dựng được lập thành một trường, và đặc biệt chứng minh định lý về điều kiện đủ về số dựng được. Phần sau của chương là áp dụng lý thuyết để giải quyết các bài toán dựng hình cổ điển và các bài toán dựng hình cụ thể. Kiến thức trong chương này được tham khảo từ tài liệu [1],[2].

Mặc dù bản thân đã rất cố gắng trong học tập, nghiên cứu và được sự hướng dẫn nhiệt tình của thầy giáo hướng dẫn, nhưng do năng lực của bản thân và thời gian còn hạn chế nên tiểu luận khó tránh khỏi những thiếu sót. Tôi rất mong nhận được sự góp ý của quý thầy cô và các bạn để tiểu luận được hoàn thiện hơn.

Cuối cùng tôi xin chân thành cảm ơn TS. Nguyễn Thái Hòa người đã tận tình giúp đỡ, cùng tập thể lớp cao học toán khoá 11 tạo điều kiện cho tôi hoàn thành tiểu luận này.

. *Tác giả*

Chương 1

KIẾN THỨC CƠ SỞ

1.1 Mở rộng Galoa

1.1.1 Khái niệm mở rộng Galoa và ví dụ

Định nghĩa 1.1.1. Mở rộng bậc hữu hạn F của trường K được gọi là mở rộng Galoa nếu nó là chuẩn tắc và tách được.

Ví dụ 1.1.2. 1) Trường chia đường tròn R_n trên $\mathbb{Q}$ là một mở rộng Galoa với nhóm Galoa đẳng cấu với nhóm nhân $\mathbb{Z}_n^*$ các lớp khả nghịch.

2) Trường hữu hạn $F_q, q = p^n$ là mở rộng Galoa trên trường con nguyên tố $\mathbb{Z}_p$. Nó có nhóm Galoa $G = G(F/\mathbb{Z}_p)$ là nhóm xyclic sinh bởi tự đẳng cấu $\psi : a \longrightarrow a^p$ với mọi $a \in F_q$

1.1.2 Các đặc trưng của mở rộng Galoa

Định lý 1.1.3. *Cho F là mở rộng bậc hữu hạn trên K với nhóm Galoa G. Khi đó các điều kiện sau tương đương:*

(i) F là mở rộng Galoa trên K.

(ii) $K = F^G$ (nghĩa là tập các phần tử của F bất biến dưới mọi tự đồng cấu của nhóm Galoa G đúng bằng K).

(iii) Cấp của nhóm Galoa G đúng bằng bậc của mở rộng $[F : K]$.

Chứng minh. $(i) \Rightarrow (ii)$ Nếu F là mở rộng Galoa trên K thì F là trường nghiệm của một đa thức tách được trên K ([1], Hệ quả 6.3). Khi đó theo ([1], Định lý 1.3) ta có (ii).

$(ii) \Leftrightarrow (iii)$ Giả sử cấp của G bằng n. Khi đó theo ([1], Mệnh đề 3.1.1),ta

có $n = \left[F : F^G\right]$. Bởi vậy nếu $F^G = K$ thì hiển nhiên $n = [F : K]$. Ngược lại, nếu $n = [F : K]$ thì $[F : K] = \left[F : F^G\right]$, do đó $K = F^G$ (vì $K \subset F^G$).

$(iii) \Rightarrow (i)$ Do F là mở rộng bậc hữu hạn trên K nên F đại số trên K. Giả sử α là phần tử tùy ý thuộc F. Ta sẽ xây dựng đa thức tối tiểu $p(x)$ của nó. Gọi $\alpha = \alpha_1, \alpha_2, ..., \alpha_m$ là tất cả các ảnh phân biệt của α bởi các tự đẳng cấu σ thuộc G.

Đặt $$\alpha_i = \sigma_i(\alpha) \text{ và } \sigma_1 = id_F$$

Khi đó $m \leq n$ (n là cấp của G và bằng $[F : K]$). Xét đa thức

$$p(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_m) \tag{1.1}$$

Các hệ tử của $p(x)$ là những đa thức đối xứng cơ bản của các α_i, vì vậy chúng là bất biến đối với các tự đẳng cấu $\sigma \in G$ (do mỗi σ cảm sinh một phép thế trên tập hợp $\{\alpha_1, \alpha_2, ..., \alpha_m\}$). Nghĩa là các hệ tử này thuộc K (do $(iii) \Leftrightarrow (ii)$). Vậy $p(x) \in K[x]$.

Nếu $g(x) \in K[x]$ là nhân tử bất khả quy của $p(x)$ nhận $\alpha = \alpha_1$ làm nghiệm thì $g(x)$ cũng nhận mọi phần tử liên hợp của nó $\alpha_i = \sigma_i(\alpha)$ làm nghiệm. Điều này chứng tỏ $p(x)$ chia hết $g(x)$ và do đó $p(x) = g(x)$ (vì $g(x)$ là bất khả quy).

Như vậy $p(x)$ là đa thức tối tiểu của α và điều đó chứng tỏ tính tách được của F trên K.Bây giờ giả sử $q(x)$ là đa thức bất khả quy trên K và có một nghiệm $\alpha \in F$. Theo chứng minh trên $p(x)$ chính là đa thức (1.1), nó phân rã hoàn toàn trong F. Điều này chứng tỏ tính chuẩn tắc của F trên K. □

Định lý 1.1.4. *Trường F là mở rộng Galoa trên trường K khi và chỉ khi F là trường nghiệm của đa thức tách được trên K.*

Chứng minh. Điều kiện cần chính là ([1],Hệ quả 2.62). Ngược lại, nếu F là trường nghiệm của đa thức tách được thì ([1], Định lý2.6.5) cấp của nhóm Galoa $G = G(F/K)$ bằng bậc của mở rộng $[F : K]$. Khi đó theo Định lý 1.1.3, F là mở rộng Galoa trên K. □

Nhận xét 1.1.5. Định lý trên cho ta một dấu hiệu tiện lợi để nhận biết một mở rộng Galoa . Nó cho thấy hầu hết những mở rộng trường mà chúng ta

thường gặp đều là những mở rộng Galoa. Chẳng hạn, mỗi đa thức $p(x)$ bất khả quy trên trường K có đặc số 0 đều là tách được do đó trường nghiệm của đa thức đó là một mở rộng Galoa trên K.

Nhận định trên có thể phát biểu trong hệ quả sau.

Hệ quả 1.1.6. *Nếu trường F là mở rộng của trường K có đặc số 0 thì các điều sau tương đương:*

(i) F là mở rộng Galoa.

(ii) F là mở rộng bậc hữu hạn và chuẩn tắc.

(iii) F là trường nghiệm của một đa thức nào đó trên K.

Chứng minh. $(i) \Leftrightarrow (ii)$ Nếu K có đặc số 0 thì mọi mở rộng chuẩn tắc đều là mở rộng tách được . Do đó ta có $(i) \Leftrightarrow (ii)$.
$(ii) \Leftrightarrow (iii)$ là nội dung của ([1],Định lý 2.6.1) □

Định lý 1.1.7 (**Về các phần tử liên hợp**). *Cho F là mở rộng Galoa trên K. Khi đó hai phần tử của F liên hợp trên K khi và chỉ khi tồn tại $K-$đẳng cấu biến một phần tử thành phần tử khác.*

Chứng minh. Giả sử c là phần tử tùy ý của mở rộng chuẩn tắc F trên K. Xét các phần tử

$$\varphi_1(c) = c, \varphi_2(c), ..., \varphi_n(c) \tag{1.2}$$

trong đó $\varphi_1 = id_F, \varphi_2, ..., \varphi_n$ là tất cả các tự đẳng cấu thuộc nhóm Galoa $G = G(F/K)$. Với mỗi tự đẳng cấu các phần tử của dãy (1.2) biến thành dãy

$$\varphi\varphi_1(c), \varphi\varphi_2(c), ..., \varphi\varphi_n(c)$$

tức là một hoán vị nào đó của dãy (1.2). Vì vậy các hệ tử của đa thức

$$g(x) = \prod_{i=1}^{n} (x - \varphi_i(c))$$

giữ bất động với mọi phần tử φ, do đó thuộc trường K.
Do $c = \varphi_1(c)$ nên đa thức $g(x)$ và đa thức tối tiểu $p(x)$ của c có nghiệm chung

(khi đó do đa thức $p(x)$ bất khả quy nên $g(x)$ chia hết cho $p(x)$). Mặt khác theo ([1],Bổ đề2.6.4) các phần tử $\varphi_1(c), \varphi_2(c), ..., \varphi_n(c)$ (có thể trùng nhau) liên hợp với c, nên cũng là nghiệm của $p(x)$. Bởi vậy mọi nghiệm của $g(x)$ đều là nghiệm của $p(x)$. Giả sử

$$g(x) = [p(x)]^k [q_1(x)]^{k_1} ... [q_r(x)]^{k_r}$$

Bởi vì mọi nghiệm của $g(x)$ là nghiệm của $p(x)$ và không một nghiệm nào của các đa thức $q_i(x)(i = 1, ..., r)$ có thể là nghiệm của $p(x)$ (do tính bất khả quy của mỗi đa thức này), nên các đa thức $q_i(x)(i = 1, ..., r)$ không thể có nghiệm, tức là $q_i(x) = 1$. Vậy

$$g(x) = [p(x)]^k$$

Từ đó đặc biệt suy ra rằng các phần tử

$$\varphi_1(c), \varphi_2(c), ..., \varphi_n(c)$$

vét cạn hết (có thể có sự lặp lại) tất cả các liên hợp của c. □

1.2 Mở rộng căn và mở rộng căn bậc hai

1.2.1 Mở rộng căn

Định nghĩa 1.2.1. Mở rộng F của trường cơ sở K gọi là mở rộng căn nếu tồn tại dãy mở rộng

$$K = K_0 \subset K_1 \subset ... \subset K_s = F \tag{1.3}$$

sao cho $K_i = K_{i-1}(\theta_i), \theta_i^{n_i} = a_i \in K_{i-1}$,

Lưu ý rằng trong dãy trên mỗi trường con K_i có thể không là mở rộng chuẩn tắc của trường con K_{i-1}, cũng như trường con F có thể không là chuẩn tắc trên K

Bổ đề 1.2.2. *Giả sử K là trường tùy ý, E là mở rộng chuẩn tắc có bậc hữu hạn trên K và F là mở rộng chuẩn tắc có bậc hữu hạn trên E. Khi đó F là mở*

rộng chuẩn tắc trên K nếu và chỉ nếu F là trường nghiệm trên E của một đa thức trên K.

Chứng minh. ($\Rightarrow$) Nếu F là mở rộng chuẩn tắc trên K thì F là trường nghiệm của đa thức $f(x) \in K[x]$([1], Định lý 2.6.1) và vì vậy F là trường nghiệm của đa thức $f(x)$ trên E.

($\Leftarrow$) Ngược lại giả sử rằng $F = E(u_1, ..., u_n)$ trong đó $u_1, ..., u_n$ là mọi nghiệm của một đa thức $g(x) \in K[x]$,$E = K(v_1, ..., v_m)$ trong đó $v_1, ..., v_m$ là mọi nghiệm của $g(x)$. Khi đó

$$F = (v_1, .., v_m, u_1, ..., u_n)$$

nghĩa là F là trường nghiệm của đa thức $f(x).g(x) \in K[x]$ và do đó F chuẩn tắc trên K. □

Định lý 1.2.3. *Mọi mở rộng căn F của trường cơ sở K được chứa trong một mở rộng $\overline{F}$ đồng thời là mở rộng căn và chuẩn tắc trên K, khi đó ta nói rằng $\overline{F}$ là mở rộng căn và chuẩn tắc trên K*

Chứng minh. Chứng minh định lý bằng cách quy nạp theo độ dài của dãy(1.3)
Với s=1 ta có $F = K_1 = K(c), c^m = a \in K$.
Gọi ζ căn nguyên thủy bậc m và xét mở rộng $\overline{F} = K(c, \zeta)$, dễ thấy $\overline{F}$ là trường nghiệm của thức $x^m - a$, do đó $\overline{F}$ là chuẩn tắc trên K. Mặt khác$\overline{F}$ có dãy mở rộng căn

$$K \subset K(\zeta) \subset K(\zeta, c)$$

Vậy định lý đúng cho $s = 1$
Xét mở rộng căn F với dãy (1.3) có độ dài $s > 1$. Bởi vì $E = K_{s-1}$ là mở rộng căn của K với độ dài $s - 1$ nên theo giả thiết quy nạp tồn tại mở rộng căn $\overline{E}$ chuẩn tắc trên K và chứa E, $K \subset E \subset \overline{E}$.

Theo giả thiết $F = K_s$ là mở rộng căn đơn của tường $E = K_{s-1}$, tức là $F = E(\theta), \theta^n = u \in E$.

Xét đa thức tối tiểu $g(x)$ của u trên trường cơ sở K, do $\overline{E}$ chuẩn tắc và $u \in E \subset \overline{E}$ nên $\overline{E}$ chứa tất cả cá nghiệm $u - 1 = u, u_2, ..., u_r$ của $g(x)$. Đối với mỗi $i = 1, 2, ..., r$ ta xét phương $u^n - u_i = 0$. Giả sử c_i là nghiệm tùy ý của phương trình này, xét mở rộng $\overline{F} = \overline{E}(\zeta, c_1, ..., c_r)$ trong đó ζ là căn nguyên thủy bậc n của đơn vị. Do $c_1 = \theta$ nên $F \subset \overline{F}$, hơn thế nữa trên trường $\overline{E}, \overline{F}$ có dãy căn

$$\overline{E} = \overline{E} - 0 \subset \overline{E}_1 \subset ... \subset \overline{E}_{r+1} = \overline{F} \tag{1.4}$$

trong đó

$$\overline{E}_1 = \overline{E}_0(\zeta), \overline{E}_i = \overline{E}_{i-1}(c_i), i = 1, 2, ..., r + 1$$

theo giả thiết quy nạp $\overline{E}$ là mở rộng căn của K nên dãy căn bắt đầu từ K và kết thúc ở $\overline{E}$. Tiếp nối dãy này với dãy (1.4) ta được dãy căn bắt đầu từ K. Như vậy là $\overline{F}$ là mở rộng căn của K, Bây giờ ta chứng tỏ $\overline{F}$ là mở rộng chuẩn tắc trên K. Xét đa thức $G(x) = g(x^n)$. Thế thì $G(x) \in K[x]$. Do

$$G(x) = (x^n - u_1)...(x^n - u_n)$$

nên các phần tử $c_1, c_2, ..., c_r$ là nghiệm của đa thức $G(x)$. Mọi nghiệm còn lại của đa thức này nhận được từ phép nhân mỗi nghiệm $c_1, ..., c_r$ với các lũy thừa của ζ. Vì vậy $\overline{F}$ chứa trường nghiệm Q của $G(x)$ trên trường $\overline{E}$. Mặt khác

$$\overline{F} = \overline{E}(c_1, ..., c_r) \subset Q.$$

Vậy $\overline{F} = Q$, nghĩa là $\overline{F}$ là trường nghiệm trên $\overline{E}$ của đa thức $G(x) \in K[x]$ theo Bổ đề 1.2.2, $\overline{F}$ chuẩn tắc trên K. Định lý được chứng minh. □

1.2.2 Mở rộng căn bậc hai

Định nghĩa 1.2.4. Một mở rộng F của trường K được gọi là mở rộng bậc hai (Mở rộng Pythagore) nếu $F = K(u_{1,2}, ..., u_n)$, trong đó $u_1^2 \in K$ và $u_i^2 \in K(u_{1,2}, ..., u_{1-1}), (i = 2, .., n)$.

Mệnh đề 1.2.5. *Bậc $[F : K]$ của mở rộng căn bậc hai là luỹ thừa của 2, tức là bằng 2^n.*

Chứng minh. Thật vậy nếu $u^2 \in E$ và $u \notin E$ thì u là nghiệm của đa thức bất khả quy $x^2 - a \in E[x]$ và do đó

$$[E(u) : E] = 2.$$

Từ đó, nếu là mở rộng căn bậc hai của K thì dễ dàng chứng minh được đẳng thức $[F : K] = 2^n$. □

Mệnh đề 1.2.6. *Giả sử F là mở rộng chuẩn tắc trên K có bậc $[F : K] = 2^n$, khi đó F là mở rộng căn bậc hai trên K*

Chứng minh. Theo giả thiết F là mở rộng Galoa trên K với nhóm Galoa $G = G(F/K)$ có cấp 2^n, ta thừa nhận rằng mọi nhóm có cấp là lũy thừa của số nguyên tố là giải được. Như vậy nhóm Galoa G là giải được với với dãy giải được

$$G = H_0 \supset H_1 \supset ...H_n = \{e\}$$

mà các thương H_{i-1}/H_i là nhóm xiclic cấp 2. Giả sử

$$K = K_0 \subset K_1 \subset K_n = F$$

là dãy trường con tương ứng của trường F ta có

$$[K_i : K_{i-1}] = 2 \Rightarrow K_i = K_{i-1}(u_i).$$

với u_i là nghiệm của đa thức $x^2 - a \in Ki - 1[x]$ điều này chứng tỏ F là mở rộng căn bậc hai trên K. □

Mệnh đề 1.2.7. *Mọi mở rộng căn bậc hai F trên K chứa trong một mở rộng căn bậc hai chuẩn tắc*

Chứng minh. Giả sử F là mở rộng căn bậc hai chuẩn tắc trên K, khi đó theo Mệnh đề 1.2.5

$$[F : K] = 2^n.$$

Bây giờ ta chứng minh mệnh đề quy nạp theo n.

Với $n = 1$ thì $F = K(u)$ với $u^2 = K$. Rõ ràng F là trường nghiệm của đa thức $x^2 - a \in K[x]$ nên F chuẩn tắc trên K.

Với $n > 1$, giả sử $F = K(u_1, u_2, ..., u_n)$với $u_1^2 \in K$ và $u_i^2 \in K(u_1, u_2, ..., u_{i-1}), i = 1, 2..., n$. Khi đó đặt $u = u_n$ ta có $F = E(u), E = K(u_1, u_2, ..., u_{n-1}), u^2 \in E$. Theo giả thiết quy nạp, E chứa trong mở rộng căn bậc hai chuẩn tắc $\overline{E}$, Xét đa thức tối tiểu $f(x)$ của u^2 trên trường K, do $u^2 \in \overline{E}$ và $\overline{E}$ chuẩn tắc trên K nên trong $\overline{E}$ có sự phân tích

$$f(x) = (x - c_1)...(x - c_m)$$

trong đó $c_1 = u^2$,Đặt $g(x) = f(x^2)$ thế thì $g(u) = 0$. Gọi $\overline{F}$ là trường nghiệm của $g(x)$ trên $\overline{E}$. Do $g(x) \in K[x]$ nên theo Bổ đề 1.2.2 ta có $\overline{F}$ là chuẩn tắc trên K, ngoài ra

$$F \subset \overline{F}, (F = E(u))$$

Sau cùng ta có

$$\overline{F} = \overline{E}(\gamma_1, ..., \gamma_m)$$

trong đó $\gamma_i^2 = c_i$ Do $\gamma_i^2 \in \overline{E}$ nên $\gamma^2 \in \overline{E}(\gamma_1, ..., \gamma_{i-1})$.

Như vậy $\overline{F}$ là mở rộng căn bậc hai của$\overline{E}$ và do đó là mở rộng căn bậc hai của K. □

Chương 2

ÁP DỤNG LÝ THUYẾT GALOA TRONG PHÉP DỰNG HÌNH

Trong chương này, chúng tôi sử dụng lý thuyết mở rộng trường để tìm ra câu trả lời cho 3 bài toán dựng hình xuất hiện thời Hy Lạp cổ đại và xét bài toán dựng đa giác đều n-cạnh bằng thước kẻ và compa.

Ba bài toán dựng hình cổ điển đó là:

• Bài toán *chia ba một góc*: Chia một góc thành ba phần bằng nhau.

• Bài toán *gấp đôi hình lập phương*: Dựng một hình lập phương có thể tích gấp hai lần thể tích một hình lập phương cho trước.

• Bài toán*cầu phương đường tròn*: Dựng một hình vuông có diện tích bằng diện tích một hình tròn cho trước.

2.1 Khái niệm và tính chất về điểm và số dựng được

Định nghĩa 2.1.1. Trong mặt phẳng $\mathbb{R}^2$ cho 2 điểm $P_0(0;0), P_1(1;0)$. Một điểm $P \in \mathbb{R}^2$ gọi là dựng được bằng thước kẻ và compa nếu tồn tai dãy hữu hạn $P_0, P_1, ..., P_n$ sao cho $P = P_n$ và với mọi $j \geq 2$ điểm P_j xác định từ $S_{j-1} = \{P_0, P_1, ..., P_{j_1}\}$ bởi một trong ba phép dựng sau.

Giao của hai đường thẳng phân biệt, trong đó mỗi đường thẳng qua 2 điểm bất kỳ của S_{j-1}

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

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

Định nghĩa 2.1.2. Một đường thẳng gọi là dựng được nếu nó đi qua hai điểm dựng được, một đoạn thẳng gọi là dựng được nếu nó đi qua hai điểm dựng được, một đường tròn gọi là dựng được nếu nó có tâm là một điểm dựng được và có bán kính bằng khoảng cách giữa hai điểm dựng được.

Một số thực x được gọi là dựng được (bằng thước kẻ và compa) nếu $(x;0) \in \mathbb{R}^2$ dựng được, Khi đó độ dài của đoạn thẳng dựng được là số thực dựng được.

Một góc β gọi là đựng được nếu $cos\beta$ là số thực dựng được.

Mệnh đề 2.1.3. *Điểm (a,b) dựng được khi và chỉ khi a,b dựng được.*

Chứng minh. Nếu a,b dựng được, tức là các điểm $(a,0),(b,0)$ dựng được, suy ra $(0,b)$ dựng được. Điểm (a,b) dựng được vì nó là điểm thứ 4 của hình bình hành có 3 điểm $(0,0),(a,0),(0,b)$ dựng được.

Ngược lại nếu (a,b) là điểm dựng được, xét hai đường tròn tâm $(0,0)$ và $(1,0)$ đi qua (a,b). Giao điểm của chúng là (a,b) và $(a,-b)$, đường thẳng qua hai điểm này cắt trục hoành tại (a,0) nên (a,0) không dựng được. Điểm (0,b) dựng được vì nó là đỉnh thứ 4 của hình bình hành có 3 điểm $(0,0),(a,0),(a,b)$ dựng được, suy ra $(b,0)$ dựng được. □

Định lý 2.1.4. *Tập tất cả các số dựng được là trường con của trường $\mathbb{R}$, Hơn nữa, nếu c dựng được và $c>0$ thì $\sqrt{c}$ dựng được.*

Chứng minh. Gọi E là tập tất cả các số dựng được, cho $a,b \in E$ ta có $-a \in E$, ngoài ra do $(a,0)$ và $(b,0)$ dựng được, điểm giữa $Q=(\frac{a+b}{2},0)$ dựng được. Giao điểm của trục hoành và đường tròn tâm Q qua $(0,0)$ là $(a+b,0)$ do đó $a+b$ dựng được.

Để chứng minh $ab \in E$, ta chỉ cần xét trường hợp $ab \neq 0$ và $b \neq 1$. Do $(b-1)$ dựng được nên điểm $(0,b-1)$ dựng được, do đó $(a,b-1)$ dụng được. Giao điểm của đường thẳng qua $(0,b)$ và $(a,b-1)$ với trục hoành là điểm $(ab,0)$. Vậy (ab) dựng được.

Ta chứng minh rằng $a^{-1} \in E$, nếu $a \neq 0$. Do $a \in E$ ta có $1-a \in E$, hay

điểm $(0, 1-a)$ dựng được, do đó điểm (1,1-a) dựng được. Đường thẳng qua $(0,1)$ và $(1, 1-a)$ cắt trục hoành tại $(a^{-1}, 0)$. Vậy $a^{-1} \in E$.

Điều này suy ra E là một trường.

Cho $c \in E$ và $c > 0$, do $\frac{1}{2}(1-c)$ là dựng được, điểm $Q(0, \frac{1-c}{2})$ dựng được. Đường tròn tâm Q qua (0,1) cắt trục hoành tại hai điểm có tọa độ $(u, 0)$ và $(-u, 0)$ với $u > 0$. Theo định lý Pythagore, ta có $u^2 + \frac{1}{4}(1-c)^2 = \frac{1}{4}(1+c)^2$, suy ra $u^2 = c$ do đó $u = \sqrt{c}$, vậy $\sqrt{c}$ dựng được. □

Định lý 2.1.5. *Cho $P = (\alpha, \beta) \in \mathbb{R}^2$, là điểm dựng được, khi đó $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^r$, với $r \in \mathbb{N}$*

Chứng minh. Cho$P_0, P_1, ..., P_n$ là dãy hữu hạn các điểm dựng được. Đặt $K_0 = K_1 = \mathbb{Q}$ và $K_j = K_{j-1}(\alpha_j, \beta_j)$, với $2 \leq j \leq n$ và $P_j = (\alpha_j, \beta_j)$. Dễ dàng thấy được rằng các số thực α_j, β_j là nghiệm của đa thức bậc 1 hoặc bậc 2 có hệ tử trongK_{j-1}. Do đó $[K_j : K_{j-1}] = 2^t$ với $t \in \mathbb{N}$ suy ra $[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\alpha, \beta)][\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^m$,với $m \in \mathbb{N}$, Do đó $\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^r, n \in N$ □

Hệ quả 2.1.6. *Nghiệm của đa thức $p(x)$ bất khả quy trên trường K là dựng được bằng thước và compa khi và chỉ khi bậc của trường nghiệm E của đa thức $p(x)$ trên K là lũy thừa của 2.*

Chứng minh. Thật vậy, nếu nghiệm x_0 của $p(x)$ là dựng được bằng thước và compa thì nó chứa trong mở rộng căn bậc hai F của K và do đó chứa trong mở rộng căn bậc hai chuẩn tắc $\overline{F}$. vì trường nghiệm E chưa trong $\overline{F}$ và $[\overline{F} : K] = 2^n$ nên $[E : K] = 2^m$. Điều ngược lại hiển nhiên. □

2.2 Một số bài toán áp dụng

2.2.1 Bài toán 1: *Chia ba một góc*

Cho góc α, hãy dựng góc $\frac{\alpha}{3}$.

Giải

Đặt $a = \cos\alpha$ và ta có u là nghiệm của phương trình $4x^3 - 3x = a$. Đặt $x = \frac{z}{2}$ ta đưa phương trình trên về dạng

$$f(x) = z^3 - 3z - 1$$

là bất khả quy trên $\mathbb{Q} = \mathbb{Q}(1)$.

Giả sử $f(z)$ bất khả quy trên $\mathbb{Q}(a)$. Gọi v là một nghiệm của $f(z)$ và F là trường nghiệm của nó ta có dãy mở rộng trường

$$\mathbb{Q}(a) \subset \mathbb{Q}(a, v) \subset F$$

Từ đó

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(a, v)][\mathbb{Q}(a, v) : \mathbb{Q}(a)].$$

Bởi vì $[\mathbb{Q}(a)(v) : \mathbb{Q}(a)] = 3$ nên

$$[F : \mathbb{Q}(a)] \neq 2^m$$

Do đó $\cos\frac{\alpha}{3}$ là không dựng được , nghĩa là $\frac{\alpha}{3}$ là không dựng được .

2.2.2 Bài toán 2: *Gấp đôi một hình lập phương*

Hãy dựng cạnh của hình lập phương có thể tích gấp đôi thể tích hình lập phương đơn vị.

Giải

Gọi a là cạnh của hình lập phương cần dựng. Thế thì a là nghiệm của đa thức $x^3 - 2$. Đa thức này bất khả quy trên $\mathbb{Q}$. Gọi α là một nghiệm, còn F là trường nghiệm của đa thức này ta có dãy mở rộng trường

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset F$$

Từ đó

$$[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Bởi vì $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ nên

$$[F : \mathbb{Q}] \neq 2^m$$

Điều này chứng tỏ bài toán không giải được .

2.2.3 Bài toán 3: *Cầu phương đường tròn*

Dựng hình vuông có diện tích bằng diện tích hình tròn có bán kính 1(Nói cách khác là dựng điểm $(\sqrt{\pi}, 0)$ *trong* $\mathbb{R}^2$*)*

Giải

Vì ($\sqrt{\pi}$ là siêu việt trên $\mathbb{Q}$ nên $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$, do đó áp dụng Định lý 2.1.5 ta suy ra không dựng được điểm $(\sqrt{\pi}, 0)$ trong $\mathbb{R}^2$.

Vậy không thể dựng được hình vuông có diện tích bằng hình tròn có bán kính cho trước.

2.2.4 Bài toán 4: *Chia đường tròn thành* n *phần bằng nhau*

Để giải quyết bài toán này trước hết ta chứng minh bổ đề sau.

Bổ đề 2.2.1. *Nếu* $n = p.q, (p, q) = 1$ *thì đường tròn chia được thành* n *phần bằng nhau khi và chỉ khi nó chia được thành* p, q *phần bằng nhau.*

Chứng minh. ($\Rightarrow$) Giả sử chia được đường tròn thành n phần bằng nhau, tức là dựng được cung $\frac{2\pi R}{n}$. Khi đó ta có thể viết

$$\frac{1}{p} = q\frac{1}{n} \text{ và } \frac{1}{q} = p\frac{1}{n}$$

và vì vậy các cung $\frac{2\pi R}{p}, \frac{2\pi R}{q}$ là dựng được .

($\Leftarrow$) Giả sử đường tròn chia được thành p, q phần bằng nhau. Do p và q nguyên tố cùng nhau nên tồn tại các số nguyên u, v sao cho

$$up + vq = 1$$

Từ đó chia cả hai vế của đẳng thức ta được

$$\frac{1}{n} = u\frac{1}{q} + v\frac{1}{p}$$

Điều này chứng tỏ cung $\frac{2\pi R}{n}$ là dựng được . □

Trở lại bài toán, không làm mất tính tổng quát ta giả sử đường tròn có bán kính $R = 1$. Để chia đường tròn thành n phần bằng nhau ta cần dựng $\cos\frac{2\pi}{n}$

thay cho góc $\frac{2\pi}{n}$. Gọi ζ là căn nguyên thủy bậc n của đơn vị ta có

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

$$\zeta^{-1} = \cos\frac{2\pi}{n} - i\sin\frac{2\pi}{n}$$

Từ đó

$$\cos\frac{2\pi}{n} = \frac{1}{2}(\zeta + \zeta^{-1}) \in \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}_0$$

Bởi vậy theo Mệnh đề 1.2.5 ta có $\cos\frac{2\pi}{n}$ dựng được khi và chỉ khi

$$[\mathbb{Q}_0 : \mathbb{Q}] = 2^r$$

Mặt khác ta có

$$[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$$

vì ζ và ζ^{-1} là các nghiệm của đa thức trên $\mathbb{Q}(\zeta + \zeta^{-1})$:

$$x^2 - (\zeta + \zeta^{-1})x + 1$$

Do đó

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2[\mathbb{Q}(\zeta) : \mathbb{Q}_0]$$

Do nhận định vừa nêu trên ta thấy đẳng thức

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^m$$

là điều cần và đủ để dựng được $\cos\frac{2\pi}{n}$.

Với những khảo sát trên ta có thể chứng minh mệnh đề sau:

Mệnh đề 2.2.2. *Đường tròn có thể chia được thành n phần bằng nhau bởi thước kẻ và compa nếu và chi nếu n có dạng*

$$n = 2^k q_1 ... q_s$$

trong đó k là số tự nhiên, còn q_i là những số nguyên tố lẻ dạng $2^{2^r} + 1$ (số nguyên tố Phecma).

Chứng minh. Theo bổ đề ta chỉ cần xét trường hợp $n = q^k$.
Xét trường hợp chia đường tròn $R_n = \mathbb{Q}(\zeta)$, $\zeta^n = 1$, ta có

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = q^{k-1}(q-1).$$

Mặt khác theo nhận định trên bài toán là giải được khi và chỉ khi

$$q^{k-1}(q-1) = 2^m.$$

Nếu $q \neq 2$ thì đẳng thức trên xảy ra khi $k = 1$ và $q = 2^m + 1$. Nếu $m = ab$,b lẻ thì

$$q = (2^a)^b + 1 = (2^a + 1).M, M > 1$$

Điều này trái với giả thiết q nguyên tố. Vậy $m = 2^r$ và do đó $q = 2^{2^r} + 1$. □

2.3 Một vài phép dựng hình cụ thể

2.3.1 Dựng đa giác đều 5 cạnh

Bài toán cũng có nghĩa là chia đường tròn thành năm phần bằng nhau. Để làm điều đó ta cần dựng đoạn thẳng có dộ dài bằng $\cos\frac{2\pi}{5}$ thay cho góc $\frac{2\pi}{5}$. Gọi ζ là căn nguyên thủy bậc 5 của đơn vị ta có

$$\zeta = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}, i^2 = -1.$$

và

$$\cos\frac{2\pi}{5} = \frac{1}{2}\left(\zeta + \zeta^{-1}\right)$$

Ta cần tìm mở rộng căn bậc hai chứa $\cos\frac{2\pi}{5}$. Xét dãy các mở rộng trường

$$\mathbb{Q} \subset \mathbb{Q}\left(\zeta + \zeta^{-1}\right) \subset \mathbb{Q}\left(\zeta\right) = \mathbb{R}_5$$

Đa thức xác định của ζ trên $\mathbb{Q}$ là

$$F_5(x) = x^4 + x^3 + x^2 + x + 1$$

Từ đó $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ và do đó

$$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = 2$$

Như vậy $\zeta + \zeta^{-1}$ có đa thức xác định bậc hai, ta tìm đa thức đó. Bởi vì ζ thỏa mãn phương trình $F_5(x) = 0$ và $\zeta^{-1} = \zeta^4$ nên

$$\begin{aligned}(\zeta + \zeta^{-1})^2 &= \zeta^2 + 2 + \zeta^3 \\ &= (-1 - \zeta - \zeta^4) + 2 \\ \zeta + \zeta^{-1} &= -1 - (\zeta + \zeta^{-1})\end{aligned}$$

Từ đó suy ra $\zeta + \zeta^{-1}$ là nghiệm của phương trình

$$x^2 + x - 1 = 0$$

Bởi vậy ta có được biểu thức cần tìm

$$2\cos\frac{2\pi}{5} = \zeta + \zeta^{-1} = \frac{-1 + \sqrt{5}}{2}$$

Biểu thức trên đây cho phép dựng $\cos\frac{2\pi}{5}$ như sau:
Trước hết dựng đường tròn $(O, R = 1)$ rồi tiếp đó thực hiện các phép dựng:
Dựng

$$\frac{\sqrt{5}}{2} = \sqrt{1^2 + \left(\frac{1}{2}\right)^2}$$

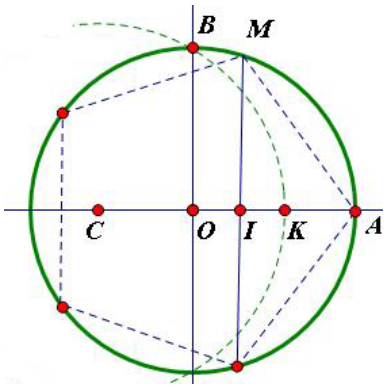
Dựng đường tròn (C, BC). Khi đó $OK = \frac{-1+\sqrt{5}}{2}$. Chia đôi OK ta được $OI = \cos\frac{2\pi}{5}$. Cung $\overset{\frown}{AM}$ là cung cần dựng.

2.3.2 Dựng đa giác đều 15 cạnh

Bài toán cũng có nghĩa là chia đường tròn thành 15 phần bằng nhau.
Ta có $15 = 3 \times 5$. Khi đó $1 = 2 \times 3 - 5$ và do đó

$$\frac{1}{15} = \frac{2}{5} - \frac{1}{3}$$

Đẳng thức này cho phép ta dựng cung $\frac{2\pi}{15}$ theo các cung $\frac{2\pi}{5}$ và $\frac{2\pi}{3}$.



Hình 2.1: Chia đường tròn thành 5 phần bằng nhau

2.3.3 Dựng đa giác đều 17 cạnh

Bài toán cũng có nghĩa là chia đường tròn thành 17 phần bằng nhau. Ta phải dựng $\cos\frac{2\pi}{17} = \frac{1}{2}(\zeta + \zeta^{-1})$ với $\zeta = e^{\frac{2\pi i}{17}}$. Ta cần tìm mở rộng căn bậc hai chứa $\cos\frac{2\pi}{5}$. Xét dãy các mở rộng trường

$$\mathbb{Q} \subset \mathbb{Q}\left(\zeta + \zeta^{-1}\right) \subset \mathbb{Q}\left(\zeta\right) = \mathbb{R}_{17}$$

Ta có $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$ vì ζ là nghiệm của phương trình

$$x^2 - (\zeta + \zeta^{-1})x + 1 = 0$$

Bây giờ ta hãy xét các mở rộng trường trung gian giữa $\mathbb{Q}$ và $\mathbb{Q}(\zeta + \zeta^{-1})$. Nhóm Galois của R_{17} trên $\mathbb{Q}$ là nhóm xyclic cấp 16:

$$G = \langle\sigma\rangle_{16} \simeq (\mathbb{Z}_{17})^* = \left\langle\overline{3}\right\rangle_{16}$$

Trong G có dãy giải được

$$G \supset G_1 = \left\langle\sigma^2\right\rangle_8 \supset G_2 = \left\langle\sigma^4\right\rangle_4 \supset G_3 = \left\langle\sigma^8\right\rangle_2 \supset E$$

Dãy trường tương ứng là

$$\mathbb{Q} \subset K_1 = \mathbb{Q}(\alpha) \subset K_2 = \mathbb{Q}(\beta) \subset K_3 = \mathbb{Q}(\gamma) \subset R_{17}$$

Để tìm các phần tử nguyên thủy α, β, γ ta xét bảng sau:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$3^i(\text{mod}17)$	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6
$\zeta_i = \zeta^{3^i}$	ζ^1	ζ^3	ζ^9	ζ^{10}	ζ^{13}	ζ^5	ζ^{15}	ζ^{11}	ζ^{16}	ζ^{14}	ζ^8	ζ^7	ζ^4	ζ^{12}	ζ^2	ζ^6

Các chu kì Gaoxơ tám hạng tử là

$$\alpha_0 = \zeta^1 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2$$
$$\alpha_1 = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$$

Bởi vì $\alpha_0 + \alpha_1 = -1$ và $\alpha_0\alpha_1 = -4$ nên α_0 và α_1 là các nghiệm của đa thức

$$x^2 + x - 4 \in \mathbb{Q}[x].$$

Suy ra $\alpha_0 = -\frac{1}{2} + \frac{\sqrt{17}}{2}; \alpha_1 = -\frac{1}{2} - \frac{\sqrt{17}}{2}$.

Các chu kì Gaoxơ bốn hạng tử là

$$\beta_0 = \zeta + \zeta^{13} + \zeta^{16} + \zeta^4$$
$$\beta_1 = \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12}$$
$$\beta_2 = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2$$
$$\beta_3 = \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6$$

Ta có $\begin{cases} \beta_0 + \beta_2 = \alpha_0 \\ \beta_0\beta_2 = -1 \end{cases}$ và $\begin{cases} \beta_1 + \beta_3 = \alpha_1 \\ \beta_1\beta_3 = -1 \end{cases}$

Suy ra β_0, β_2 (tương ứngβ_1, β_3) là nghiệm của đa thức

$$x^2 - \alpha_0 x - 1 \in K_1[x]$$

(tương ứng $x^2 - \alpha_0 x - 1 \in K_1[x]$).

Vậy

$$\beta_{0,2} = \frac{\alpha_0}{2} \pm \frac{1}{2}\sqrt{\alpha_0^2 + 4}$$
$$\beta_{1,3} = \frac{\alpha_1}{2} \pm \frac{1}{2}\sqrt{\alpha_1^2 + 4}$$

Cuối cùng các chu kì Gaoxơ hai hạng tử là:

$$\gamma_0 = \zeta + \zeta^{16} = \zeta + \zeta^{-1} = 2\cos\tfrac{2\pi}{17}$$
$$\gamma_1 = \zeta^{13} + \zeta^4$$

Và do $\gamma_0 + \gamma_1 = \beta_0$ $\gamma_0 - \gamma_1 = \beta_1$ nên γ_0 và γ_1 là nghiệm của đa thức

$$x^2 - \beta_0 x + \beta_1 \in K_2[x]$$

$$\gamma_{0,1} = \frac{\beta_0}{2} \pm \frac{1}{2}\sqrt{\beta_0^2 - 4\beta_1}$$

Từ đó ta suy ra cách dựng $\cos\frac{2\pi}{17}$ như sau:

- Dựng đường tròn $(O, OB = 1)$;

- Dựng $BC = \sqrt{1^2 + (\frac{1}{4})^2}$ - Dựng đường tròn (C, BC). Khi đó $OD = \frac{\alpha_0}{2}$, $OE = \frac{\alpha_1}{2}$ và

- Dựng đường tròn (D, DB) ta được $OF = \beta_0$

- Dựng đường tròn (E, EB) ta được $OG = \beta_1$

Vì $\frac{1}{2}\sqrt{\beta_0^2 - 4\beta_1} = \sqrt{\left(\frac{\beta_0}{2}\right)^2 - \left(\sqrt{\beta_1}\right)^2}$, nên ta dựng như sau:

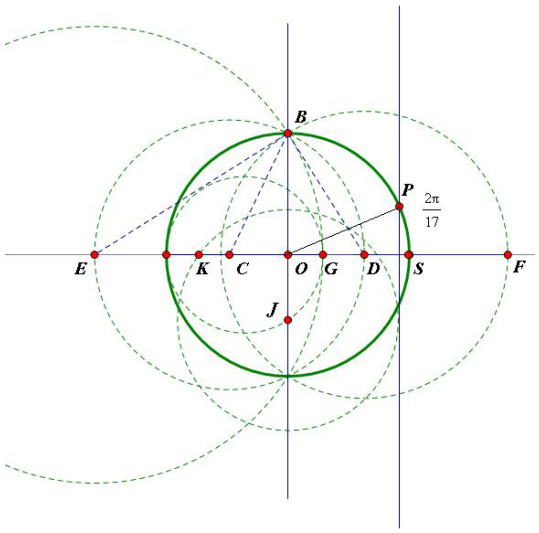
- Dựng đường tròn đường kính AG ta được $OJ = \sqrt{\beta_1}$;

- Dựng đường tròn $\left(J, \frac{OF}{2}\right)$ ta được $OK = \frac{1}{2}\sqrt{\beta_0^2 - 4\beta_1}$.

Từ đó dựng được

$$2\cos\frac{2\pi}{17} = \zeta + \zeta^{-1} = \gamma_0 = \frac{\beta_0}{2} + \frac{1}{2}\sqrt{\beta_0^2 - 4\beta_1}$$

Từ đó ta có thể dựng được cung $\overset{\frown}{SP} = \frac{2\pi}{17}$ như hình vẽ.



Hình 2.2: Hình chia đường tròn thành 17 phần bằng nhau

KẾT LUẬN

Trong tiểu luận "Ứng dụng của lý thuyết Galoa trong phép dựng hình" tác giả đã học tập, nghiên cứu và trình bày các vấn đề sau:

1.Trình bày ứng dụng của lý thuyết Galoa trong phép dựng hình, cụ thể chứng minh định lý về điều kiện đủ cho đường việc chia đường tròn thành n phần bằng nhau.

2.Áp dụng để giải các bài toán dựng hình cổ điển như không thể chia góc thành 3 phần bằng nhau bởi thước kẻ và compa, dựng hình vuông có cùng diện tích với hình tròn,...Đặc biệt đã nêu phương pháp dựng cụ thể chia đường tròn thành 5,15,17 phần bằng nhau bàng thước kẻ và compa.

Trong khuôn khổ một tiểu luận và hạn chế về thời gian cũng trình độ nên một vài vấn đề chưa được trình bày, như chia đường tròn thành n phần bằng nhau với $n = 20, 24, ...$trong thời gian đến tôi sẽ tiếp tục nghiên cứu để bổ sung. Mặc dù thật cố gắng nhưng sẽ không tránh khỏi những thiếu sót, rất mong được lượng thứ, chỉ bảo của Thầy cô giáo và các bạn để bài tiểu luận hoàn thiện hơn.

TÀI LIỆU THAM KHẢO

1. Nguyễn Tiến Quang *Cơ sở lý thuyết trường và lý thuyết Galoa* . Nhà xuất bản Đại học sư phạm, Hà nội, 2007

2. Nguyễn Chánh Tú *Lý thuyết mở rộng trường và Galoa* , Huế, 2006.

3. Nguyễn Tiến Quang *Đại số và số học - Tập 3*, Nhà xuất bản giáo dục, 1987