ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

-------ᘓ*ᘐ-------

NGÔ THỊ THÚY HẰNG

CĂN NGUYÊN THỦY, TRƯỜNG CHIA ĐƯỜNG TRÒN VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2015

Mục lục

LỜI CẢM ƠN

Trước hết, tôi xin gửi lời biết ơn chân thành và sâu sắc tới PGS.TS Lê Thị Thanh Nhàn. Cô đã dành nhiều thời gian và tâm huyết trong việc hướng dẫn. Sau quá trình nhận đề tài và nghiên cứu dưới sự hướng dẫn khoa học của Cô, luận văn "Căn nguyên thủy, trường chia đường tròn và ứng dụng" của tôi đã được hoàn thành. Có được kết quả này, đó là nhờ sự dạy bảo tận tình và nghiêm khắc của Cô.

Tôi cũng xin gửi lời cảm ơn chân thành đến Ban Giám hiệu, Phòng Đào tạo và Khoa Toán-Tin của Trường Đại học Khoa học - Đại học Thái Nguyên đã tạo điều kiện thuận lợi nhất trong suốt quá trình học tập tại trường cũng như thời gian tôi hoàn thành đề tài này. Sự giúp đỡ nhiệt tình và thái độ thân thiện của các cán bộ thuộc Phòng Đào tạo và Khoa Toán-Tin đã để lại trong lòng mỗi chúng tôi những ấn tượng hết sức tốt đẹp.

Tôi xin cảm ơn Sở Giáo dục - Đào tạo Quảng Ninh và trường trung học phổ thông Văn Lang - nơi tôi đang công tác đã tạo điều kiện cho tôi hoàn thành khóa học này.

Tôi xin cảm ơn gia đình, bạn bè đồng nghiệp và các thành viên trong lớp cao học Toán K7Q (Khóa 2013-2015) đã quan tâm, tạo điều kiện, động viên cổ vũ để tôi có thể hoàn thành nhiệm vụ của mình.

LỜI NÓI ĐẦU

Cho n là số nguyên dương. Khi đó có đúng n căn bậc n của đơn vị, đó là các số phức $\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$, $k = 0, 1, \ldots, n-1$. Ta biết rằng ε_k là căn nguyên thủy bậc n của đơn vị nếu và chỉ nếu $\gcd(k, n) = 1$. Vì thế có đúng $\varphi(n)$ căn nguyên thủy bậc n của đơn vị, trong đó φ là hàm Euler. Gọi $\varepsilon_{k_1}, \ldots, \varepsilon_{k_{\varphi(n)}}$ là các căn nguyên thủy bậc n của đơn vị. Khi đó *đa thức chia đường tròn* thứ n, kí hiệu là $\Phi_n(x)$, là đa thức bậc $\varphi(n)$ được cho bởi công thức $\Phi_n(x) = (x - \varepsilon_{k_1}) \ldots (x - \varepsilon_{k_{\varphi(n)}})$. Trường phân rã của đa thức $f(x) = x^n - 1$ trên trường $\mathbb{Q}$ gọi là *trường chia đường tròn thứ* n và được ký hiệu là $\mathbb{Q}_n$. Nếu ε là một căn nguyên thủy bậc n của đơn vị thì trường chia đường tròn $\mathbb{Q}_n$ chính là trường $\mathbb{Q}(\varepsilon)$. Chú ý rằng đa thức chia đường tròn $\Phi_n(x)$ là đa thức bất khả quy của ε, do đó trường chia đường tròn thứ n trên $\mathbb{Q}$ có bậc là $\varphi(n)$. Mục đích của luận văn này là trình bày một số kết quả về căn nguyên thủy, đa thức chia đường tròn, trường chia đường tròn và những ứng dụng trong một số bài toán sơ cấp.

Luận văn gồm 3 chương. Chương 1 trình bày các kiến thức về đa thức chia đường tròn, gồm căn nguyên thủy bậc n của đơn vị, đa thức chia đường tròn và tính bất khả quy của đa thức chia đường tròn. Một số kết quả quan trọng của đa thức chia đường tròn được chứng minh chi tiết như công thức $x^n - 1 = \prod_{d|n} \Phi_d(x)$ (xem Định lí 1.2.4), $\Phi_n(x)$ có các hệ số đều nguyên (xem Định lý 1.2.6), công thức tính $\Phi_n(x)$ dựa vào nghịch chuyển Mobius (xem Mệnh đề 1.2.10) và tính bất khả quy của $\Phi_n(x)$ (xem Định lý 1.3.4).

Chương 2 nghiên cứu về trường chia đường tròn gồm trường phân rã của đa thức và trường chia đường tròn. Chúng tôi chứng minh rằng với mỗi đa thức $f(x)$ với hệ số trên một trường K có bậc $n \geq 1$, tồn tại một trường phân rã của $f(x)$ trên K (xem Định lý 2.1.9). Trường chia đường tròn thứ n, kí hiệu là $\mathbb{Q}_n$, được hiểu là trường phân rã của đa thức chia đường tròn thứ n trên $\mathbb{Q}$. Chúng tôi chứng minh rằng bậc của mở rộng trường chia đường tròn thứ n là $\varphi(n)$ (xem Định lý 2.2.3). Một số mối quan hệ giữa các trường chia đường tròn cũng được trình bày trong chương này (xem Định lý 2.2.5 và Định lý 2.2.6).

Trong Chương 3, chúng tôi sử dụng các kết quả về căn nguyên thủy, đa thức chia đường tròn, trường chia đường tròn để giải một số bài toán sơ cấp. Chúng tôi chứng minh một số kết quả đã biết trong số học (xem Bài toán 3.1.1), trong hình học (xem Bài toán 3.1.3); tính giá trị $\cos\frac{2\pi}{n}$ và $\sin\frac{2\pi}{n}$ (xem Bài toán 3.2.1); phân tích đa thức thành nhân tử bất khả quy trên $\mathbb{Q}$ (xem Bài toán 3.2.2 và Bài toán 3.2.3); giải phương trình nghiệm nguyên (xem Bài toán 3.2.4). Đặc biệt, sử dụng trường chia đường tròn, chúng tôi đưa ra lời giải hai bài toán sơ cấp liên quan đến giá trị của đa thức tại $e^{\frac{2\pi}{n}}$ (xem Bài toán 3.3.1 và Bài toán 3.3.2).

Chương 1

Đa thức chia đường tròn

Trong suốt chương này, luôn kí hiệu $\mathbb{N} = \{0, 1, 2, \ldots\}$ là tập các số nguyên không âm và $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ là tập các số tự nhiên. Kí hiệu $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ lần lượt là trường số hữu tỷ, trường số thực và trường số phức.

1.1 Căn nguyên thủy bậc n của đơn vị

1.1.1 Định nghĩa. Cho $\varepsilon \in \mathbb{C}$ và $n \in \mathbb{N}^*$. Khi đó ε được gọi là một *căn bậc n của đơn vị* nếu $\varepsilon^n = 1$.

Chú ý rằng có đúng n căn bậc n của đơn vị, đó là

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0, 1, \ldots, n-1.$$

1.1.2 Định nghĩa. Cho n là một số nguyên dương và ε là một căn bậc n của đơn vị. Khi đó ε được gọi là *căn nguyên thủy* bậc n của đơn vị nếu ε không là căn bậc nhỏ hơn n của đơn vị.

Chú ý rằng số phức ε là căn nguyên thủy bậc n của đơn vị nếu và chỉ nếu n là số nguyên dương nhỏ nhất thỏa mãn $\varepsilon^n = 1$.

1.1.3 Ví dụ. a) Các căn bậc 3 của đơn vị là

$$\varepsilon_0 = 1, \varepsilon_1 = -\frac{1}{2} + \frac{i\sqrt{3}}{2}, \varepsilon_2 = -\frac{1}{2} - \frac{i\sqrt{3}}{2}.$$

Ta có $\varepsilon_0^1 = 1$, do đó ε_0 không là căn nguyên thủy bậc 3 của đơn vị. Ta có $\varepsilon_1 \neq 1$, $\varepsilon_1^2 = \varepsilon_2 \neq 1$ và $\varepsilon_1^3 = 1$. Vì thế ε_1 là căn nguyên thủy bậc 3 của đơn vị. Ta cũng kiểm tra được ε_2 là căn nguyên thủy bậc 3 của đơn vị.

b) Các căn bậc 4 của đơn vị là $1, i, -1, -i$. Số i là căn nguyên thủy bậc 4 của đơn vị vì $i^4 = 1$ và $i^n \neq 1$ với $n = 1, 2, 3$. Tương tự, $-i$ là căn nguyên thủy bậc 4 của đơn vị.

1.1.4 Mệnh đề. *(Tiêu chuẩn của căn nguyên thủy). Cho n là số nguyên dương. Kí hiệu*

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0, 1, \ldots, n-1.$$

Khi đó ε_k là một căn nguyên thủy bậc n của đơn vị nếu và chỉ nếu $\gcd(k, n) = 1$.

Chứng minh. Giả sử ε_k là một căn nguyên thủy bậc n của đơn vị. Khi đó n là số nguyên dương nhỏ nhất thỏa mãn $\varepsilon_k^n = 1$. Giả sử $\gcd(k, n) = d > 1$. Khi đó $n/d < n$. Ta có

$$\varepsilon_k^{\frac{n}{d}} = \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right)^{\frac{n}{d}} = \cos\frac{2k\pi}{d} + i\sin\frac{2k\pi}{d} = 1.$$

Điều này vô lí. Vậy $d = 1$, hay $\gcd(k, n) = 1$.

Ngược lại, cho $\gcd(k, n) = 1$. Chú ý rằng ε_k là một căn bậc n của đơn vị, nghĩa là $\varepsilon_k^n = 1$. Gọi t là số nguyên dương bé nhất thỏa mãn $\varepsilon_k^t = 1$. Ta có

$$\varepsilon_k^t = \cos\frac{2kt\pi}{n} + i\sin\frac{2kt\pi}{n} = 1.$$

Suy ra $\dfrac{2kt\pi}{n} = m2\pi$ với m là một số nguyên. Do đó kt là bội của n. Theo giả thiết, $\gcd(k, n) = 1$. Do đó t là bội của n. Suy ra $t = n$, tức là n là số nguyên dương nhỏ nhất thỏa mãn $\varepsilon_k^n = 1$. Vậy ε_k là căn nguyên thủy bậc n của đơn vị. $\square$

Từ đây đến hết luận văn, luôn kí hiệu

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0, 1, \ldots, n-1.$$

Kí hiệu $\varphi : \mathbb{N}^* \to \mathbb{N}$ là hàm Euler, tức là $\varphi(1) = 1$ và $\varphi(n)$ là số các số tự nhiên nhỏ hơn n và nguyên tố cùng nhau với n.

1.1.5 Nhận xét. i) Vì $\gcd(1, n) = 1$ nên theo Mệnh đề 1.1.4, ε_1 luôn là căn nguyên thủy bậc n của đơn vị.
ii) Từ định nghĩa hàm Euler, nếu n là số nguyên dương thì có đúng $\varphi(n)$ căn nguyên thủy bậc n của đơn vị.

1.1.6 Mệnh đề. *Nếu ε là một căn nguyên thủy bậc n của đơn vị thì $\varepsilon^a = \varepsilon^b$ nếu và chỉ nếu $a \equiv b \pmod{n}$.*

Chứng minh. Theo giả thiết ε là một căn nguyên thủy bậc n của đơn vị. Khi đó $\varepsilon^n = 1$ và $\varepsilon^m \neq 1, \forall m < n$. Không mất tính tổng quát giả sử $a > b$.
($\Rightarrow$) Giả sử $\varepsilon^a = \varepsilon^b$. Khi đó $\varepsilon^{a-b} = 1$. Chia $a-b$ cho n ta được $a-b = n.q+r$ với $0 \leq r < n$ suy ra $1 = \varepsilon^{a-b} = \varepsilon^{n.q+r} = \varepsilon^r$. Vì ε là căn nguyên thủy bậc n của đơn vị nên ta phải có $r = 0$ hay $a \equiv b \pmod{n}$.
($\Leftarrow$) Giả sử $a \equiv b \pmod{n}$. Khi đó $a - b \,\vdots\, n$ suy ra $a - b = tn$ với $t \in \mathbb{Z}$
Do đó $\varepsilon^{a-b} = \varepsilon^{tn} = (\varepsilon^n)^t = 1^t = 1$ hay $\varepsilon^a = \varepsilon^b$ □

Chú ý rằng nếu ε là căn bậc n của đơn vị thì $a \equiv b \pmod{n}$ kéo theo $\varepsilon^a = \varepsilon^b$, nhưng điều ngược lại không đúng. Chẳng hạn với $n = 4$ và $\varepsilon = -1$. Ta có $2 \not\equiv 0 (\mathrm{mod}\ 4)$ nhưng $\varepsilon^2 = 1 = \varepsilon^0$.

1.1.7 Bổ đề. *Nếu ε là một căn nguyên thủy bậc n của đơn vị thì tập các căn bậc n của đơn vị là $\{1, \varepsilon^1, \varepsilon^2, \ldots, \varepsilon^{n-1}\}$.*

Chứng minh. Với mọi số dương k ta có $(\varepsilon^k)^n = 1$. Vì thế ε^k là một căn bậc n của đơn vị. Ta khẳng định nếu $0 \leqslant i < j \leqslant n$ là hai số nguyên dương thì $\varepsilon^i \neq \varepsilon^j$. Thật vậy, giả sử $\varepsilon^i = \varepsilon^j$. Khi đó $\varepsilon^{j-i} = 1$. Vì $j-i$ là số nguyên dương và ε là căn nguyên thủy bậc n của đơn vị nên ta có $j - i \geq n$, điều này là vô lí. Do đó khẳng định được chứng minh. Như vậy, các số $1, \varepsilon^1, \varepsilon^2, \ldots, \varepsilon^{n-1}$ là các căn bậc n của đơn vị và đôi một khác nhau. Chú ý rằng có đúng n căn bậc n của đơn vị. Vì thế bổ đề được chứng minh. $\square$

Nhắc lại rằng một tập G cùng với phép nhân làm thành một *nhóm* nếu phép nhân có tính kết hợp, trong G có phần tử đơn vị và mọi phần tử của G đều khả nghịch. Một nhóm G được gọi là *nhóm xyclic* nếu tồn tại một phần tử $u \in G$ sao cho $G = \{u^k \mid k \in \mathbb{Z}\}$. Trong trường hợp này ta cũng nói G là nhóm xyclic sinh bởi u.

1.1.8 Hệ quả. *Với mỗi số tự nhiên n, tập G_n các căn bậc n của đơn vị làm thành một nhóm xyclic với phép nhân thông thường.*

Chứng minh. Cho $u, v \in G_n$. Khi đó $u^n = v^n = 1$. Suy ra $(uv)^n = 1$. Vì thế $uv \in G_n$. Do đó phép nhân là đóng trong G_n. Rõ ràng phép nhân trong G_n có tính kết hợp. Phần tử $1 \in G_n$ đóng vai trò là đơn vị của G_n. Với $u \in G_n$ ta có $(1/u)^n = 1/u^n = 1$, do đó $1/u \in G_n$. Vì thế G_n là một nhóm với phép nhân. Lấy ε là một căn nguyên thủy bậc n của đơn vị. Từ Bổ đề 1.1.7 ta có

$$G_n = \{\varepsilon^k \mid k \in \mathbb{Z}\} = \{\varepsilon^k \mid k = 0, 1, \ldots, n-1\}.$$

Do đó G_n là nhóm xyclic sinh bởi ε. $\square$

1.2 Đa thức chia đường tròn

Mục tiêu của tiết này là trình bày khái niệm đa thức chia đường tròn thứ n, kí hiệu là $\Phi_n(x)$, và chứng minh một số kết quả quan trọng về đa thức chia đường tròn. Cụ thể, chúng tôi sẽ chứng minh:

(a) $\prod_{d|n} \Phi_d(x) = x^n - 1$ (xem Định lí 1.2.4).

(b) Các hệ số của $\Phi_n(x)$ đều là số nguyên (xem Định lí 1.2.6).

(c) $\Phi_n(x) = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}$, trong đó μ là hàm Mobius (xem Định lí 1.2.10).

Trong suốt tiết này, ta kí hiệu $\varepsilon_k = \cos \dfrac{2k\pi}{n} + i \sin \dfrac{2k\pi}{n}$ với $k = 0, 1, \ldots, n-1$ là các căn bậc n của đơn vị.

1.2.1 Định nghĩa. Cho n là số nguyên dương. *Đa thức chia đường tròn thứ* n, kí hiệu là $\Phi_n(x)$, được định nghĩa là tích của các đa thức tuyến tính $x - \varepsilon$, trong đó ε chạy trên các căn nguyên thủy bậc n của đơn vị.

Từ Mệnh đề 1.1.4, số phức ε_k là căn nguyên thủy bậc n của đơn vị nếu và chỉ nếu $\gcd(k, n) = 1$. Do đó ta có

$$\Phi_n(x) = \prod_{\substack{(k,n)=1 \\ k=1,\ldots,n-1}} (x - \varepsilon_k).$$

Rõ ràng đa thức chia đường tròn thứ n là đa thức dạng chuẩn (có hệ số cao nhất bằng 1) và có bậc là $\varphi(n)$.

1.2.2 Ví dụ. (i) Các căn nguyên thuỷ bậc 3 của đơn vị là $\varepsilon_1 = -\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$ và $\varepsilon_2 = -\dfrac{1}{2} - i\dfrac{\sqrt{3}}{2}$. Do đó đa thức chia đường tròn thứ 3 là

$$\Phi_3(x) = \left(x + \left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\right)\left(x + \left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\right) = x^2 + x + 1.$$

(ii) Các căn nguyên thuỷ bậc 4 của đơn vị là $\varepsilon_1 = i$ và $\varepsilon_3 = -i$. Đa thức chia đường tròn thứ 4 là

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1.$$