ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ THUỲ NINH

ĐA THỨC CHIA ĐƯỜNG TRÒN VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - Năm 2013

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ THUỲ NINH

ĐA THỨC CHIA ĐƯỜNG TRÒN VÀ ỨNG DỤNG

Chuyên ngành: **PHƯƠNG PHÁP TOÁN SƠ CẤP**
Mã số: **60460113**

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS.TS. LÊ THỊ THANH NHÀN

Thái Nguyên - Năm 2013

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 \Đa thức chia đường tròn" của tôi đã được hoàn thành. Có được kết quả này, đó là nhờ sự nhắc nhở, đôn đốc, dạy bảo hết sức tận tình và nghiêm khắc của Cô.

Tôi cũng xin gửi lời cảm ơn chân thành đến Ban Giám hiệu, Phòng Đào tạo-Khoa học-Quan hệ quốc tế 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 Phòng Giáo dục và Đào tạo Quận Lê Chân - thành phố Hải Phòng và Trường trung học cơ sở Nguyễn Bá Ngọc - 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 K5B (Khóa 2011-2013) đã quan tâm, tạo điều kiện, động viên cổ vũ để tôi có thể hoàn thành nhiệm vụ của mình.

LỜI NÓI ĐẦU

Ta biết rằng với mỗi số nguyên dương n, có đúng n căn bậc n của đơn vị: $\epsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, $k = 0, 1, \ldots, n-1$. Chú ý 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 $\epsilon_{k_1}, \ldots, \epsilon_{k_{\varphi(n)}}$ 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 $\Phi_n(x) = (x - \epsilon_{k_1}) \ldots (x - \epsilon_{k_{\varphi(n)}})$. Mục đích của luận văn này là trình bày một số kết quả về đa thức chia đường tròn, những ứng dụng của đa thức chia đường tròn trong một số bài toán sơ cấp, và chứng minh tính bất khả quy của đa thức chia đường tròn.

Luận văn gồm 3 chương. Các kiến thức chuẩn bị về số phức và đa thức được nhắc lại trong Chương 1. Phần đầu của Chương 2 dành để trình bày một số tính chất quan trọng của đa thức chia đường tròn. Chúng tôi chứng tỏ rằng $x^n - 1 = \prod_{d|n} \Phi_d(x)$ (Định lí 2.3.3), và từ đó ta suy ra $\Phi_n(x)$ có các hệ số đều nguyên (Hệ quả 2.3.5). Hơn nữa, nếu $x \in \mathbb{Z}$ và p là một ước nguyên tố của $\Phi_n(x)$ thì $p \equiv 1 \pmod{n}$ hoặc $p|n$ (Định lí 2.3.11). Phần cuối Chương 2 trình bày một số ứng dụng của đa thức chia đường tròn để chứng minh lại một Định lý của Dirichlet và giải quyết một số bài toán thi học sinh giỏi toán quốc tế liên quan đến phương trình nghiệm nguyên và đánh giá số ước của một số tự nhiên. Chương 3 trình bày một số phương pháp chứng minh tính bất khả quy trên $\mathbb{Q}$ của đa thức chia đường tròn.

Chú ý rằng đa thức bất khả quy đóng vai trò quan trọng giống như vai trò của số nguyên tố trong tập các số nguyên. Với n là số nguyên dương, đa thức chia đường tròn $\Phi_n(x)$ là một đa thức bất khả quy đặc biệt, nó là

một ước của $x^n - 1$ nhưng không là ước của $x^k - 1$ với mọi $k < n$. Khi p là số nguyên tố, tính bất khả quy của $\Phi_p(x)$ đã được giải quyết vào đầu Thế kỷ thứ 19, được chứng minh lần đầu tiên bởi C. F. Gauss 1801 [Gau] với cách chứng minh khá phức tạp và dài dòng. Sau đó chứng minh được đơn giản hoá đi nhiều bởi các nhà toán học L. Kronecker 1845 [K] và F. G. Eisenstein 1850 [E]. Còn việc chứng minh tính bất khả quy của $\Phi_n(x)$ với n tuỳ ý được giải quyết vào khoảng giữa Thế kỷ 19, được chứng minh lần đầu tiên bởi Kronecker 1854 [K2]. Sau đó, R. Dedekind 1857 [D] và một số nhà toán học khác đã đưa ra chứng minh đơn giản hơn.

Nội dung của luận văn được viết dựa theo cuốn sách \Lý thuyết Galois" của S. H. Weintraub [W1], bài báo \Elementary Properties of Cyclotomic Polynomials" của Y. Ge [Ge] và bài báo \Several proofs of the irreducibility of the cyclotomic polynomial" của S. H. Weintraub [W2]. Bên cạnh đó có tham khảo một số bài báo cổ điển của C.F. Gauss [Gau], F. G. Eisenstein [E], L. Kronecker [K] và R. Dedekind [D] về tính bất khả quy của $\Phi_n(x)$.

Chương 1

Kiến thức chuẩn bị

Trước khi trình bày các kết quả về đa thức chia đường tròn ở Chương 2, chúng ta nhắc lại kiến thức cơ sở về số phức và đa thức.

1.1 Số phức và các phép toán trên số phức

1.1.1 Định nghĩa. Số phức là một biểu thức có dạng $z = a + bi$ trong đó $a, b \in \mathbb{R}$ và $i^2 = -1$. Ta gọi a là *phần thực* và b là *phần ảo* của z. Số phức i được gọi là *đơn vị ảo*. Nếu $a = 0$ thì $z = bi$ được gọi là số *thuần ảo*. Nếu $b = 0$ thì $z = a$ là số thực. Tập các số phức được kí hiệu là $\mathbb{C}$. Số phức $\overline{z} = a - bi$ được gọi là số phức *liên hợp* của $z = a + bi$.

1.1.2 Chú ý. (i) Hai số phức bằng nhau nếu và chỉ nếu phần thực và phần ảo tương ứng bằng nhau: $a + bi = c + di \Leftrightarrow a = c, b = d$.

(ii) Nếu $z = a + bi$ thì $z\,\overline{z} = a^2 + b^2$ là một số thực.

(iii) Liên hợp của tổng (hiệu, tích, thương) bằng tổng (hiệu, tích, thương) của các liên hợp: $\overline{z \pm z'} = \overline{z} \pm \overline{z'}$, $\overline{z\ z'} = \overline{z}\ \overline{z'}$ và $\overline{\dfrac{z}{z'}} = \dfrac{\overline{z}}{\overline{z'}}$ với mọi $z' \neq 0$.

Biểu diễn số phức $z = a + bi$ được gọi là biểu diễn đại số của z. Các

phép toán trên số phức được thực hiện như sau:

$$(a+bi) \pm (c+di) = (a+c) \pm (b+d)i;$$
$$(a+bi)(c+di) = (ac-bd) + (bc+ad)i;$$
$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

Tập $\mathbb{C}$ các số phức với phép cộng và phép nhân là một trường chứa trường số thực $\mathbb{R}$, trong đó mỗi số thực a được đồng nhất với số phức $a+0i$.

1.1.3 Định nghĩa. Trong mặt phẳng P với hệ trục tọa độ vuông góc xOy, mỗi số phức $z = a+bi$ được đồng nhất với điểm $Z(a,b)$. Khi đó tập số phức lấp đầy P và ta gọi P là *mặt phẳng phức*. Xét góc α tạo bởi chiều dương trục hoành với véc tơ $\overrightarrow{OZ}$ và gọi r là độ dài của véc tơ $\overrightarrow{OZ}$, khi đó

$$z = a+bi = r(\cos\alpha + i\sin\alpha).$$

Biểu diễn $z = r(\cos\alpha + i\sin\alpha)$ được gọi là *biểu diễn lượng giác* của z. Ta gọi r là *môđun* của z và ký hiệu là $|z|$. Góc α được gọi là *argument* của z và kí hiệu là $\arg(z)$. Chú ý rằng môđun của một số phức là xác định duy nhất và argument của một số phức là xác định sai khác một bội nguyên lần của 2π, tức là $r(\cos\alpha + i\sin\alpha) = r'(\cos\alpha' + i\sin\alpha')$ nếu và chỉ nếu $r = r'$ và $\alpha = \alpha' + 2k\pi$ với $k \in \mathbb{Z}$.

Với mỗi số phức $z = a+bi$, rõ ràng $|z| = \sqrt{a^2+b^2} = |\overline{z}|$. Hơn nữa, với $z_1, z_2 \in \mathbb{C}$ ta có $|z_1|.|z_2| = |z_1|.|z_2|$ và $|z_1+z_2| \leqslant |z_1| + |z_2|$.

1.1.4 Chú ý. Cho $z = r(\cos\varphi + i\sin\varphi)$ và $z' = r'(\cos\varphi' + i\sin\varphi')$ là hai số phức. Khi đó $zz' = rr'\big(\cos(\varphi+\varphi') + i\sin(\varphi+\varphi')\big)$ và nếu $z' \neq 0$ thì $\frac{z}{z'} = \frac{r}{r'}\big(\cos(\varphi-\varphi') + i\sin(\varphi-\varphi')\big)$. Từ đây ta có thể nâng lên lũy thừa bằng công thức sau (gọi là công thức Moirve):

$$z^n = r^n(\cos n\varphi + i\sin n\varphi).$$

1.1.5 Định nghĩa. Số phức u là một *căn bậc* n của số phức z nếu $u^n = z$.

Chú ý rằng mỗi số phức $z = r(\cos\varphi + i\sin\varphi)$ khác 0 đều có đúng n căn bậc n, đó là

$$\omega_k = \sqrt[n]{r}(\cos\frac{\varphi + k2\pi}{n} + i\sin\frac{\varphi + k2\pi}{n}), k = 0, 1, \ldots, n-1.$$

Đặc biệt, có đúng n căn bậc n của đơn vị, đó là

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

1.2 Khái niệm đa thức

Trong suốt tiết này, luôn giả thiết K là một trong các trường $\mathbb{C}, \mathbb{R}, \mathbb{Q}$.

1.2.1 Định nghĩa. Một biểu thức dạng $f(x) = a_n x^n + \ldots + a_0$ trong đó $a_i \in K$ với mọi i được gọi là một *đa thức* của ẩn x (hay biến x) với hệ số trong K. Nếu $a_n \neq 0$ thì a_n được gọi là *hệ số cao nhất* của $f(x)$ và số tự nhiên n được gọi là *bậc* của $f(x)$, kí hiệu là $\deg f(x)$. Nếu $a_n = 1$ thì $f(x)$ được gọi là *đa thức dạng chuẩn* (monic polynomial).

Chú ý rằng hai đa thức $f(x) = \sum a_i x^i$ và $g(x) = \sum b_i x^i$ là bằng nhau nếu và chỉ nếu $a_i = b_i$ với mọi i. Ta chỉ định nghĩa bậc cho những đa thức khác 0, còn ta quy ước đa thức 0 là không có bậc. Kí hiệu $K[x]$ là tập các đa thức ẩn x với hệ số trong K. Với $f(x) = \sum a_i x^i$ và $g(x) = \sum b_i x^i$, định nghĩa $f(x) + g(x) = \sum(a_i + b_i)x^i$ và $f(x)g(x) = \sum c_k x^k$, trong đó $c_k = \sum_{i+j=k} a_i b_j$. Rõ ràng nếu $f(x) \neq 0$ và $f(x)g(x) = f(x)h(x)$ thì $g(x) = h(x)$. Hơn nữa ta có

$$\deg(f(x) + g(x)) \leqslant \max\{\deg f(x), \deg g(x)\}$$
$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

1.2.2 Định nghĩa. Cho $f(x), g(x) \in K[x]$. Nếu $f(x) = q(x)g(x)$ với $q(x) \in K[x]$ thì ta nói rằng $g(x)$ là *ước* của $f(x)$ hay $f(x)$ là *bội* của $g(x)$ và ta viết $g(x)|f(x)$. Tập các bội của $g(x)$ được kí hiệu là (g).

Ta có ngay các tính chất đơn giản sau đây.

1.2.3 Bổ đề. *Các phát biểu sau là đúng.*
(i) Với $a \in K$ và k là số tự nhiên ta có $(x-a)|(x^k - a^k)$.
(ii) Nếu $f(x) \in K[x]$ và $a \in K$ thì tồn tại $q(x) \in K[x]$ sao cho

$$f(x) = q(x)(x-a) + f(a).$$

Định lí sau đây, gọi là Định lí chia với dư, đóng một vai trò rất quan trọng trong lí thuyết đa thức.

1.2.4 Định lý. *Cho $f(x), g(x) \in K[x]$, trong đó $g(x) \neq 0$. Khi đó tồn tại duy nhất một cặp đa thức $q(x), r(x) \in K[x]$ sao cho*

$$f(x) = g(x)q(x) + r(x), \text{ với } r(x) = 0 \text{ hoặc } \deg r(x) < \deg g(x).$$

Chứng minh. Trước hết ta chứng minh tính duy nhất. Giả sử

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x),$$

trong đó $r(x), r_1(x)$ bằng 0 hoặc có bậc nhỏ hơn bậc của $g(x)$. Khi đó

$$g(x)(q(x) - q_1(x)) = r_1(x) - r(x).$$

Nếu $r(x) \neq r_1(x)$ thì

$$\deg(r - r_1) = \deg\big(g(q - q_1)\big) = \deg g + \deg(q - q_1).$$

Điều này mâu thuẫn vì

$$\deg(r - r_1) \leqslant \max\{\deg r, \deg r_1\} < \deg g \leqslant \deg g + \deg(q - q_1).$$