ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

ĐỖ LAN HƯƠNG

ĐỊNH LÝ ZSIGMONDY VÀ TÍNH CHẤT SỐ HỌC CỦA ĐA THỨC

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2018

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

ĐỖ LAN HƯƠNG

ĐỊNH LÝ ZSIGMONDY VÀ TÍNH CHẤT SỐ HỌC CỦA ĐA THỨC

Chuyên ngành: Phương pháp Toán sơ cấp
Mã số : 84 60 113

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS.TS. ĐÀM VĂN NHỈ

THÁI NGUYÊN - 2018

Mục lục

Lời cảm ơn

Luận văn này được thực hiện tại Trường Đại học Khoa học - Đại học Thái Nguyên và hoàn thành với sự hướng dẫn của PGS.TS. Đàm Văn Nhỉ. Tác giả xin được bày tỏ lòng biết ơn chân thành và sâu sắc tới người hướng dẫn khoa học của mình, người đã đặt vấn đề nghiên cứu, dành nhiều thời gian hướng dẫn và tận tình giải đáp những thắc mắc của tác giả trong suốt quá trình làm luận văn.

Tác giả xin trân trọng cảm ơn Ban Giám hiệu Trường Đại học Khoa học - Đại học Thái Nguyên, Ban Chủ nhiệm Khoa Toán - Tin, cùng các giảng viên đã tham gia giảng dạy, đã tạo mọi điều kiện tốt nhất để tác giả học tập và nghiên cứu.

Tác giả muốn gửi những lời cảm ơn tốt đẹp nhất tới tập thể Lớp B, cao học Toán khóa 10 (2016 - 2018) đã động viên và giúp đỡ tác giả rất nhiều trong suốt quá trình học tập.

Nhân dịp này, tác giả cũng xin chân thành cảm ơn Sở Giáo dục và Đào tạo Hải Phòng, Ban Giám hiệu và các đồng nghiệp ở Trường THPT Lý Thường Kiệt, Huyện Thủy Nguyên, Thành phố Hải Phòng đã tạo điều kiện cho tác giả hoàn thành tốt nhiệm vụ học tập và công tác của mình.

Cuối cùng, tác giả muốn dành những lời cảm ơn đặc biệt nhất đến bố mẹ và đại gia đình đã luôn động viên và chia sẻ những khó khăn để tác giả hoàn thành tốt luận văn này.

Lời nói đầu

Đa thức có vị trí rất quan trọng trong Toán học vì nó không những là một đối tượng nghiên cứu trọng tâm của Đại số mà còn là một công cụ đắc lực của Giải tích trong lý thuyết xấp xỉ, lý thuyết biểu diễn, lý thuyết nội suy,... Ngoài ra, đa thức còn được sử dụng nhiều trong tính toán và ứng dụng. Trong các kì thi học sinh giỏi toán quốc gia và Olympic toán quốc tế thì các bài toán về đa thức cũng thường được đề cập đến và được xem như những bài toán khó của bậc phổ thông.

Đã có nhiều đề tài viết về đa thức nhưng trong luận văn của mình tôi muốn tập trung xét việc vận dụng đa thức trong số học.

Mục đích của luận văn này là giới thiệu Định lý Zsigmondy - một định lý rất mạnh trong xử lý các bài toán khó về số nguyên tố và giới thiệu tính chất đặc biệt của đa thức thuộc $\mathbb{Z}[x]$.

Luận văn gồm phần mở đầu, kết luận và hai chương.

Chương 1. Định lý Zsigmondy. Chương này gồm ba mục chính:

Mục 1.1 trình bày về một số tính chất cơ bản về đa thức và số phức.

Mục 1.2 trình bày về đa thức chia đường tròn.

Mục 1.3 trình bày về Định lý Zsigmondy và vận dụng Định lý Zsigmondy trong giải một số bài toán thi học sinh giỏi.

Chương 2. Tính chất số học của đa thức. Chương này được chia thành ba mục chính:

Mục 2.1 trình bày về tính chất đặc biệt của đa thức thuộc $\mathbb{Z}[x]$.

Mục 2.2 trình bày về đa thức Hilbert và biểu diễn Mahler.

Mục 2.3 trình bày về cách vận dụng đa thức Hilbert.

Chương 1

Định lý Zsigmondy

Trước khi giới thiệu về định lý Zsigmondy, phần đầu của chương này luận văn trình bày các kiến thức cơ sở về đa thức, trường số phức và đa thức chia đường tròn. Các kiến thức trong chương này được tham khảo từ tài liệu [1] và [3].

1.1 Đa thức và số phức

1.1.1 Khái niệm đa thức, phép toán

Mục này tập trung nghiên cứu vành các đa thức một biến trên một trường. Trường K có thể là trường $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Ký hiệu tập đa thức trên K

$$K[x] = \{a_0 + a_1x + \cdots + a_nx^n | a_i \in K, n \in \mathbb{N}\} = \Big\{ \sum_{i=0}^{n} a_ix^i \mid a_i \in K \Big\}.$$

Mỗi phần tử thuộc $K[x]$ được viết là $f(x)$ hoặc đơn giản f. Phần tử $f = \sum_{i=0}^{n} a_ix^i$ với quy ước $x^0 = 1$, được gọi là *một đa thức* của biến x với các hệ tử thuộc K. Khi $a_n \neq 0$ và n là số tự nhiên thì n được gọi là bậc của đa thức f và được ký hiệu $n = \deg f$; a_n được gọi là *hệ tử cao nhất*; a_0 được gọi là *hệ tử tự do* hay số hạng *tự do*. Trường hợp $f = a \neq 0, a \in K$, được gọi là đa thức *bậc 0*. Đặc biệt, khi $f = 0$ thì đa thức này được quy ước có bậc -1 hoặc $-\infty$, tùy theo việc sử dụng bậc vào lĩnh vực nào. Đa thức dạng $f = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ được gọi là *đa thức monic*. Các phép toán trong $K[x]$: Với $f = \sum_{i=0}^{n} a_ix^i, g = \sum_{i=0}^{m} b_ix^i \in K[x]$

ta định nghĩa

$$f = g \text{ khi và chỉ khi } \begin{cases} m = n \\ a_i = b_i, i = 0, 1, \ldots, n \end{cases}$$

$$f + g = \sum_{i=0}(a_i + b_i)x^i,\ fg = \sum_{i=0}^{m+n}\Big(\sum_{j=0}^{i} a_{i-j}b_j\Big)x^i.$$

Mệnh đề 1.1. *Với các phép toán trên, $K[x]$ lập thành một vành giao hoán có đơn vị.*

Mệnh đề 1.2. *Với hai đa thức $f, g \in K[x]$ ta có các kết quả về bậc:*

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

(2) $\deg(fg) = \deg f.\deg g$.

Chứng minh. (1) Giả sử $f = \sum_{i=0}^{n} a_i x^i$ và $g = \sum_{i=0}^{m} b_i x^i$. Không hạn chế có thể coi $m \leqslant n$. Nếu $m < n$ thì $\deg(f + g) = n \leqslant \max\{n, m\}$. Nếu $m = n$ và $a_n + b_n \neq 0$ thì $\deg(f + g) = n = \max\{n, n\}$. Nếu $m = n$ và $a_n + b_n = 0$ thì $\deg(f + g) < n = \max\{n, n\}$. Tóm lại, ta luôn có $\deg(f + g) \leqslant \max\{\deg f, \deg g\}$.
(2) Vì $a_n, b_m \neq 0$ nên $a_n.b_m \neq 0$. Do vậy $\deg(fg) = m.n = \deg f.\deg g$. □

1.1.2 Thuật toán Euclid

Cho hai đa thức $f(x)$ và $g(x)$ với bậc $n = \deg f(x)$ và $m = \deg g(x)$. Giả thiết $m > 0$. Nếu có đa thức $h(x)$ để $f(x) = h(x)g(x)$ thì ta nói rằng $f(x)$ *chia hết cho* $g(x)$ với *thương* $h(x)$. Nếu không có đa thức $h(x)$ nào để $f(x) = h(x)g(x)$ thì ta nói rằng đa thức $f(x)$ *không chia hết cho* $g(x)$. Ta có hai đa thức duy nhất $h(x)$, $r(x)$ để

$$f(x) = h(x)g(x) + r(x), \deg r(x) < m.$$

Đa thức $r(x)$ được gọi là đa thức *dư* trong phép chia đa thức $f(x)$ cho đa thức $g(x)$.

Định lý 1.1. *Với các đa thức $f(x), g(x)$ thuộc vành $K[x]$ và $g(x) \neq 0$ có hai đa thức duy nhất $q(x), r(x)$ sao cho $f(x) = q(x)g(x) + r(x)$, trong đó* $\deg r(x) < \deg g(x)$.

Chứng minh. Sự tồn tại: Giả sử $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ và $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$.
Nếu $n < m$ thì chọn $q(x) = 0, r(x) = f(x)$.
Nếu $n \geqslant m$ thì ta xét hiệu $f_1(x) = f(x) - \dfrac{a_n}{b_m}x^{n-m}g(x)$. Khi đó $n_1 = \deg f_1(x) \leqslant n-1$. Nếu $n_1 < m$ thì chọn $q(x) = \dfrac{a_n}{b_m}x^{n-m}$ và $r(x) = f_1(x)$.
Nếu $n_1 \geqslant m$ ta tiếp tục quá trình trên. Sau một số hữu hạn bước, ta đạt được $q(x)$ và $r(x)$ thỏa mãn các yêu cầu đặt ra.
Tính duy nhất: Giả sử có các đa thức $q_1(x), q_2(x), r_1(x), r_2(x)$ thỏa mãn $q_1(x)g(x)+r_1(x) = f(x) = q_2(x)g(x)+r_2(x)$ với $\deg r_1(x), \deg r_2(x) < m$. Từ đây suy ra

$$[q_1(x) - q_2(x)]g(x) = r_1(x) - r_2(x).$$

Nếu $q_1(x)-q_2(x) \neq 0$ thì $\deg[q_1(x)-q_2(x)]g(x) \geqslant m > \deg[r_1(x)-r_2(x)]$, vô lý. Từ đó suy ra $q_1(x) = q_2(x)$ và $r_1(x) = r_2(x)$. □

Định nghĩa 1.1. Đa thức $d(x)$ được gọi là *nhân tử chung* của hai đa thức $f(x)$ và $g(x)$ nếu $f(x)$ và $g(x)$ cùng chia hết cho đa thức $d(x)$. Hai đa thức $f(x)$ và $g(x)$ được gọi là *nguyên tố cùng nhau* nếu chúng chỉ có ước chung là các đa thức bậc 0.

Định lý 1.2. [Bézout] *Hai đa thức $f(x)$ và $g(x)$ nguyên tố cùng nhau khi và chỉ khi có hai đa thức $p(x)$, $q(x)$ để $p(x)f(x) + q(x)g(x) = 1$.*

Định lý 1.3. *Vành $K[x]$ là một vành chính và nó là vành nhân tử hóa.*

1.1.3 Xây dựng trường số phức $\mathbb{C}$

Xét tích $\mathrm{T} = \mathbb{R}\mathrm{x}\mathbb{R} = \{(a, b) \,|a, b \in \mathbb{R}\}$. Với kí hiệu $\mathrm{i} \notin \mathbb{R}$ ta đồng nhất cặp (a, b) với $a + bi$ và tích Carte $\mathrm{T} = \mathbb{R}\mathrm{x}\mathbb{R}$ được coi như tập

$\mathbb{T} = \{(a+bi)\,|a,b \in \mathbb{R}\}$. Định nghĩa các phép toán trong T:

$$a+bi = c+di \text{ khi và chỉ khi } a=c, b=d$$

$$(a+bi)+(c+di) = (a+c)+(b+d)i$$

$$(a+bi).(c+di) = (ac-bd)+(ad+bc)i$$

$$a = a+0i, i = 0+bi, bi = ib.$$

Để đơn giản, ta quy ước viết $(a+bi)(c+di)$ thay cho $(a+bi).(c+di)$
Từ định nghĩa, ta có :
(1) Với $i = 0+1i \in \mathbb{T}$ có $i^2 = (0+1i)(0+1i) = -1+0i = -1$
(2) $(a+bi)(1+0i) = a+bi = (1+0i)(a+bi)$.
Ký hiệu $\mathbb{C}$ là tập T cùng với các phép toán đã nêu ra ở trên. Ta có:

Bổ đề 1.1. *Ánh xạ $\phi : \mathbb{R} \to \mathbb{C}, a \mapsto (a,0)$, là một đơn ánh và nó thỏa mãn $\phi(a+a') = \phi(a)+\phi(a'), \phi(aa') = \phi(a)\phi(a')$ với mọi $a, a' \in \mathbb{R}$.*

Đồng nhất $(a,0) \in \mathbb{C}$ với $a \in \mathbb{R}$. Khi đó ta có thể viết

$$(a,b) = (a,0)+(b,0)(0,1) = a+bi \text{ với } i^2 = (-1,0) = -1.$$

Do đó i hay a hoặc a+ bi là bình đẳng trong $\mathbb{C}$.
Như vậy $\mathbb{C} = \left\{(a+bi)\,|a,b \in \mathbb{R}, \mathrm{i}^2 = -1\right\}$ và trong $\mathbb{C}$ ta có các kết quả:

$$a+bi = c+di \text{ khi và chỉ khi } a=c, b=d$$

$$a+bi+c+di = a+c+(b+d)i$$

$$(a+bi)(c+di) = ac-bd+(ad+bc)i.$$

Mỗi phần tử $z = a+bi \in \mathbb{C}$ được gọi là một số phức với phần thực a, ký hiệu $Re(z)$, và phần ảo b, ký hiệu $Im(z)$; còn i được gọi là đơn vị ảo. Số phức $a-bi$ được gọi là số phức liên hợp của của $z = a+bi$ và được ký hiệu là $\overline{z} = \overline{a+bi}$. Ta có $z\overline{z} = (a+bi)(a-bi) = a^2+b^2, \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$ và gọi $|z| = \sqrt{z\overline{z}}$ là mô-đun của z. Số đối của $z' = c+di$ là $-z' = -c-di$ và hiệu $z-z' = (a+bi)-(c+di) = a-c+(b-d)i$.
Xét mặt phẳng tọa độ (Oxy). Mỗi số phức $z = a+bi$ ta cho tương ứng với điểm M (a;b). Tương ứng này là một song ánh:

$$\mathbb{C} \to \mathbb{R} \times \mathbb{R}, z = a+bi \to M(a;b).$$

Khi đồng nhất $\mathbb{C}$ với (Oxy) qua việc đồng nhất z với M, mặt phẳng tọa độ biểu diễn số phức như thế gọi là *mặt phẳng phức* hay mặt phẳng *Gauss*, ghi công C. F. Gauss-người đầu tiên đưa ra biểu diễn.

Mệnh đề 1.3. *C là trường chứa trường R như một trường con.*

Chứng minh. Dễ dàng kiểm tra $\mathbb{C}$ là một vành giao hoán với đơn vị 1. Giả sử $z = a + bi \neq 0$. Khi đó $\mathrm{a}^2 + b^2 > 0$. Giả sử $z' = x + yi \in \mathbb{C}$ thỏa mãn zz'=1 hay $\begin{cases} \mathrm{ax} - by = 1 \\ bx + ay = 0 \end{cases}$. Giải hệ ta được $\begin{cases} x = \dfrac{a}{a^2+b^2} \\ y = -\dfrac{b}{a^2+b^2} \end{cases}$

Vậy $z' = \dfrac{a}{a^2+b^2} - \dfrac{b}{a^2+b^2}i$ là nghịch đảo của z, ký hiệu là $\mathrm{z}^{-1} = \dfrac{1}{z}$.
Như vậy $\mathbb{C}$ là một trường . Tương ứng $\mathrm{C} \to \mathrm{C}, \mathrm{z} \to \overline{z}$, là một tự đẳng cấu liên hợp. Đồng nhất $a \in \mathbb{R}$ với $\mathrm{a} + 0\mathrm{i} \in \mathbb{C}$ và coi $\mathbb{R}$ như là một trường con của $\mathbb{C}$ hay $\mathbb{R} \subset \mathbb{C}$. □

Chú ý, nghịch đảo của $\mathrm{z} \neq 0$ là $z^{-1} = \dfrac{\overline{z}}{|z|^2}$ và $\dfrac{z'}{z} = z'z^{-1} = \dfrac{z'\overline{z}}{|z|^2}$.

Định nghĩa 1.2. *Cho số phức $z \neq 0$. Giả sử M là điểm trong mặt phẳng phức biểu diễn số phức z. Số đo (rađian) của mỗi góc lượng giác tia đầu Ox và tia cuối OM được gọi là một Argument của z và được ký hiệu là Arg(z). Góc $\alpha = \widehat{xOM}$, $-\pi \leq \alpha \leq \pi$, được gọi là argument của z và được ký hiệu bởi argz. Argument của số phức 0 là không định nghĩa.*
Chú ý, nếu α là một argument của z thì mọi argument của z đều có dạng α+k2.π với $\mathrm{k} \in \mathrm{Z}$. Với $z \neq 0$, ký hiệu α+k.2π là argument của z. Ký hiệu $\mathrm{r} = \sqrt{z\overline{z}}$. Khi đó số phức $z = a + bi$ có $\mathrm{a} = \mathrm{r}\cos\alpha, b = r\sin\alpha$. Vậy khi $\mathrm{z} \neq 0$ thì có thể biểu diễn $\mathrm{z} = \mathrm{r}(\cos\alpha + i\sin\alpha)$ và biểu diễn này được gọi là dạng lượng giác của z.

Ví dụ 1.1. *Với* $\mathrm{a} + \mathrm{bi} = (x+iy)^n$ *có* $\mathrm{a}^2 + b^2 = \left(x^2+y^2\right)^n$.

Bài giải. Từ $a + bi = \left(x+iy\right)^n$ suy ra $a - bi = \left(x-iy\right)^n$. Như vậy $a^2 + b^2 = \left(x^2+y^2\right)^n$. □