ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

TRẦN ĐỨC THỌ

VÀNH ĐA THỨC
VÀ MỘT SỐ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

Chuyên ngành : PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số : 60 .46 .40

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

THÁI NGUYÊN - 2012

Mục lục

MỞ ĐẦU

Vành đa thức là một phần rất quan trọng trong nhiều lĩnh vực của Toán học, chẳng hạn: Đại số, Giải tích, Hình học, Toán rời rạc...vv. Trong chương trình toán phổ thông, phần đa thức chủ yếu được đưa vào bộ môn Đại số và Giải tích. Đặc biệt trong các kỳ thi đại học, học sinh giỏi quốc gia và quốc tế đều có những bài toán liên quan đến đa thức. Chính vì vậy mà chuyên đề về vành đa thức rất thiết thực với những ai muốn tìm hiểu sâu về toán sơ cấp.

Từ các kết quả đạt được trong vành đa thức chúng ta có thể vận dụng giải một số bài toán về hình học rất phức tạp, giải hệ phương trình và xây dựng một số kết quả về Tổ hợp, Số học. Khi xét đa thức ta thường quan tâm đến nghiệm, tính bất khả quy và việc biểu diễn thành tích các nhân tử bậc nhỏ hơn. Nội dung của luận văn nhằm giải quyết hai vấn đề chính:

Vấn đề 1: Chứng minh lại một số kết quả cơ bản của vành đa thức mà các kết quả ấy gắn liền với tên tuổi của những nhà toán học lỗi lạc. Vận dụng các kết quả đạt được để giải quyết một số bài toán đã được đặt ra.

Vấn đề 2: Đưa ra một số chặn nghiệm của một đa thức, tiêu chuẩn chia hết của một vài đa thức đặc biệt, ước chung của dãy số từ đa thức, phương pháp biểu diễn đa thức đối xứng qua các đa thức đối xứng cơ bản.

Luận văn được chia làm hai chương.

Chương I: Vành đa thức.

Nội dung chương I trình bày một số khái niệm về vành đa thức, một vài tiêu chuẩn bất khả quy, tính đóng đại số của trường $\mathbb{C}$, đa thức đối xứng.

Chương II: Một số ứng dụng của vành đa thức.

Nội dung chương II trình bày về chặn nghiệm, tính chất chia hết của một vài đa thức đặc biệt, phương pháp biểu diễn đa thức đối xứng qua đa thức đối xứng sơ cấp. Trong chương này chúng tôi còn trình bày ứng dụng lý thuyết đa thức đối xứng vào đại số sơ cấp và đã xây dựng được đa thức bậc ba với nghiệm là đại lượng liên quan đến tam giác.

Dù đã rất cố gắng, nhưng chắc chắn nội dung được trình bày trong luận văn không tránh khỏi thiếu sót nhất định, em rất mong nhận được sự góp ý của các thầy cô giáo và các bạn.

Luận văn này được hoàn thành dưới sự hướng dẫn khoa học của PGS.TS Đàm Văn Nhỉ. Em xin được tỏ lòng cảm ơn chân thành nhất tới thầy về sự giúp đỡ nhiệt tình từ khi xây dựng đề cương, viết và hoàn thành luận văn. Tiếp theo em xin chân thành cảm ơn các thầy cô giáo phản biện đã đọc và góp ý để em hoàn thiện luận văn của mình. Em xin được cảm ơn chân thành nhất tới Trường Đại học Khoa học - Đại học Thái Nguyên, nơi em đã nhận được một học vấn sau đại học căn bản. Xin cảm ơn gia đình, đồng nghiệp đã cảm thông, chia sẻ, ủng hộ và giúp đỡ trong thời gian em học cao học và viết luận văn. Lời cuối em xin chúc sức khỏe các thầy cô giáo và đồng nghiệp.

Em xin chân thành cảm ơn!

Hà Nội, ngày 20 tháng 7 năm 2012

Người thực hiện

Trần Đức Thọ

Chương 1

VÀNH ĐA THỨC

1.1 Vành đa thức một biến

Khái niệm vành đa thức một biến trên $\mathbb{R}$

Giả sử V là một vành giao hoán và A là một vành con của nó. Giả sử $v \in V$. Mọi vành con của V chứa A và v đều chứa các phần tử có dạng

$$a_0 + a_1v + a_2v^2 + ... + a_nv^n$$

trong đó $a_i \in A, n \in \mathbb{N}$. Một phần tử như thế gọi là một đa thức của V với các hệ tử a_i trong A, $i = 1, 2, ..., n$.
Nếu $b_0 + b_1v + b_2v^2 + ... + b_mv^m$ cũng là một đa thức của v, và $m \geq n$ thì:

$$(a_0 + a_1v + a_2v^2 + ... + a_nv^n) + (b_0 + b_1v + b_2v^2 + ... + b_mv^m)$$

$$= (a_0+b_0)+(a_1+b_1)v+(a_2+b_2)v^2+...+(a_n+b_m)v^m+a_{m+1}v^{m+1}+...+a_nv^n$$

$$(a_0 + a_1v + a_2v^2 + ... + a_nv^n).(b_0 + b_1v + b_2v^2 + ... + b_mv^m)$$

$$= (a_0.b_0) + (a_1b_0 + a_0b_1)v + ... + \sum_{j+k=i} a_jb_kv^i + ... + (a_n.b_m)v^{n+m}.$$

Vậy tổng và tích của hai đa thức của $\mathbb{R}$ lại là một đa thức của $\mathbb{R}$.
Mặt khác 1 dĩ nhiên cũng là đa thức thuộc $\mathbb{R}$.
Vậy tập hợp các đa thức của v với hệ tử trong A lập thành một vành con của V. Dĩ nhiên đó là vành con nhỏ nhất của V chứa A và v.
Kí hiệu vành con đó qua vành $A[v]$. Nếu tồn tại một hệ thức đa thức

$$d_0 + d_1v + d_2v^2 + ... + d_nv^n = 0(d_i \in A)m \geq 1$$

với ít nhất một $d_i \neq 0$, thì hai đa thức của v có dạng khác nhau có thể trùng nhau. Thí dụ, nếu V=R, A=Q, $v = \sqrt{2}$ là nghiệm của $2 - v^2 = 0$, thì ta có chẳng hạn: $0 + 2v = 0 + 0v + 0v^2 + v^3$.
Nhưng nếu một hệ thức có dạng: $d_0 + d_1 v + d_2 v^2 + ... + d_n v^n = 0 (d_i \in A)$ chỉ xảy ra khi tất cả các $d_i = 0$, thì hai đa thức $\sum\limits_{i=0}^{n} a_i v^i$ và $\sum\limits_{j=0}^{m} b_i v^j$ sẽ chỉ bằng nhau khi các hệ tử tương ứng với a_i và b_j bằng nhau. Thật vậy nếu $n \geq m$ và

$$\sum_{i=0}^{n} a_i v^i = \sum_{j=0}^{m} b_j v^j$$

thì

$$(a_0 - b_0) + (a_1 - b_1)v + (a_2 - b_2)v^2 + ... + (a_m - b_m)v^m + a_{m+1}v^{m+1} + ... + a_n v^n.$$

Từ đó $a_i = b_i (i = 0, ..., n)$ và $a_{m+1} = ... = a_n = 0$.
Như vậy để xác định cấu trúc của vành đa thức, ta cần có sẵn các vành dạng $A[x]$, trong đó mọi hệ thức $\sum\limits_{i=0}^{m} d_i X^i = 0$ đều kéo theo $\forall d_i = 0$. Ta chú ý rằng trong trường hợp này, một đa thức của X có dạng

$$a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$$

xác định một dãy con duy nhất $(a_0, a_1, a_2, ...)$ với tính chất là $a_i = 0$ với i đủ lớn.
Các nhận xét trên đưa ta đến cách dựng sau đây của vành $A[x]$

Vành đa thức một biến

Giả sử A là vành giao hoán đã cho và B là tập hợp các dãy vô hạn:

$$(a_0, a_1, a_2, ...) với\ 0 = (a, 0, ..., 0)$$

Với chỉ một số hữu hạn hạng tử $a_i \neq 0$.
Hai phần tử $(a_0, a_1, a_2, ...)$ và $(b_0, b_1, b_2, ...)$ của B được xem là bằng nhau nếu và chỉ nếu $a_i = b_i, \forall i$

Phép cộng trong B được định nghĩa bởi

$$(a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...).$$

Vế phải là một phần tử của B vì tất cả các số hạng bắt đầu từ một điểm nào đó đều bằng 0.

(B,+) rõ ràng là một nhóm Aben. Phần tử không là 0=(a, 0, 0, ...) và phần tử đối của $(a_0, a_1, a_2, ...)$ là $(-a_0, -a_1, -a_2, ...)$
Phép nhân trong B được định nghĩa bởi

$$(a_0, a_1, a_2, ...).(b_0, b_1, b_2, ...) = (p_0, p_1, p_2, ...)$$

trong đó p_i được cho bởi

$$p_i = \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j+k=i} a_j b_k.$$

Nếu $a_i = 0$ với i > n và $b_j = 0$ với j > m thì $p_k = 0$ với k > n + m. Vậy vế phải của tích trên là một phần tử của B.
Nếu $a = (a_0, a_1, a_2, ...), b = (b_0, b_1, b_2, ...)$ và $c = (c_0, c_1, c_2, ...)$ thì hạng tử với chỉ số i trong (ab)c là

$$\sum_{m+l=i} \left(\sum_{j+k=m} a_j b_k \right) c_l = \sum_{j+k+l=i} a_j b_k c_l.$$

Tương tự hạng tử tương ứng của a(bc) là:

$$\sum_{m+j=i} a_j \left(\sum_{k+l=m} b_k c_l \right) = \sum_{j+k+l=i} a_j b_k c_l.$$

Vậy (ab)c=a(bc). Mặt khác rõ ràng ta có ab=ba. Dãy 1=(1,0,0,...) đóng vai trò đơn vị. Vậy (B,.,1) là một vị nhóm giao hoán.
Phép nhân phân phối đối với phép cộng, vì ta có

$$\sum_{j+k=i} (a_j + b_j) c_k = \sum_{j+k=l} a_j c_k + \sum_{j+k=i} b_j c_k.$$

Vế trái là hạng tử thứ i của (a+b)c, còn vế phải là hạng tử thứ i của ac+bc. Như vậy B là một vành giao hoán.
Ánh xạ f xác định bởi:

$$f : \underset{a}{A} \underset{\mapsto}{\rightarrow} \underset{(a,0,...)}{B}$$

Vậy nếu ta đồng nhất hóa A với f(A) đẳng cấu với nó, thì ta có thể xem A là một vành con của vành B.

Ta kí hiệu (0,1,0,0, ...) là X và gọi nó là một ẩn trên A.
Ta có $X = (0, 1, 0, 0, ...)$

$$X^2 = (0, 0, 1^2, 0, ...)$$
$$X^k = (0, 0, ..., 1^{k+1}, 0, ...).$$

Ngoài ra ta còn bao hàm thức $A \subseteq B$ ta có

$$(0, 0, ..., a, 0, 0, ...) = aX^k = X^k a$$

Phần tử tổng quát $(a_0, a_1, a_2, ...a_n, 0, 0, ...)$ của B bây giờ có thể viết theo các kí hiệu mới như sau:

$$a_0 + a_1 X + a_2 X^2 + ... + a_n X^n.$$

Vậy B=A[X]. Nếu $a_0 + a_1 X + ... + a_n X^n = 0$ thì $(a_0, a_1, ...a_n, 0, ...) = 0$. Do đó $a_i = 0 \forall i$.
Vành B = A[X] xác định như trên gọi là vành đa thức của ẩn X trên A. Các phần tử của nó gọi là các đa thức của X.
Ta thường viết $f(X) = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$
hoặc $f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$.
Hệ tử a_0 gọi là hằng hạng tử hoặc hạng tử tự do. Nếu $a_n \neq 0$ thì a_n gọi là hệ tử cao nhất và n gọi là bậc của đa thức đó và được kí hiệu là $n = degf(X)$. Ta gán cho đa thức không bậc là $-\infty$. Ta có $-\infty + (-\infty) = -\infty$, $-\infty + n = -\infty$ và $-\infty < n, \forall n \in \mathbb{N}$. các đa thức bậc 1 còn gọi là tuyến tính.
Từ định nghĩa của phép cộng và phép nhân trong A[X] , ta suy ra rằng

$$deg(f(X) + g(X)) \leq max(degf(X), degg(X)).$$
$$deg(f(X)g(X)) \leq degf(X) + degg(X).$$

Bất đẳng thức thứ hai được thay thế bởi đẳng thức

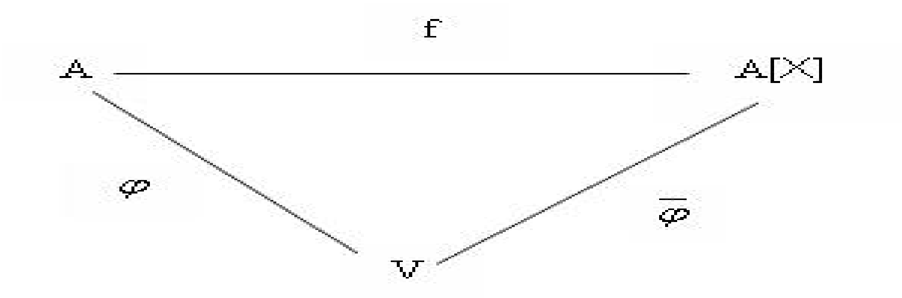
$$deg(f(X)g(X)) = degf(X) + degg(X).$$

Mỗi khi tích $a_n b_m$ của các hệ tử cao nhất của f(X) và g(X) khác không, vì

$$f(X).g(X) = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + ... + a_n b_m X^{n+m}.$$

Như vậy, nếu A là một miền nguyên vẹn thì vành A(X) cũng là miền nguyên vẹn.

Định lý 1.1.1. [Tính chất dộc xạ của vành $A[X]$] *Giả sử A là một vành giao hoán, A[X] là vành đa thức của ẩn X trên A, $f : A \to A[X]$ là phép nhúng A vào ttrong A[X]. Khi đó với mọi vành giao hoán V và mọi đồng cấu φ từ vành A tới vành V, tồn tại duy nhất một đồng cấu $\overline{\varphi}$ từ vành A[X] tới vành V sao cho $\overline{\varphi}(X) = v$, trong đó v là một phần tử tùy ý của V và sao cho biểu đồ sau giao hoán.*



Hình 1.1: Tính chất dộc xạ của vành $A[X]$

Chứng minh. Trước hết ta giả thiết rằng một đồng cấu $\overline{\varphi}$ như thế tồn tại. Ta có $\overline{\varphi}(X^k) = (\overline{\varphi}(X))^k = v^k$. Mặt khác $\overline{\varphi}f(a) = \overline{\varphi}(a) = \varphi(a)$.
Vậy $\varphi(a_0 + a_1X + ... + a_nX^n) = \varphi(a_0) + \varphi(a_1)v^1 + ... + \varphi(a_n)v^n$.
Vì $\overline{\varphi}(a_0 + a_1X + ... + a_nX^n)$ là duy nhất xác định bởi φ và v, nên nếu φ tồn tại thì nó là duy nhất.
Đảo lại, ta hãy xác định ánh xạ $\overline{\varphi} : A[X] \to V$. Bởi công thức.
$\overline{\varphi}(a_0 + a_1X + ... + a_nX^n) = \varphi(a_0) + \varphi(a_1)v + ... + \varphi(a_n)v^n$.
Ta có $\overline{\varphi}(X) = v$ và $\overline{\varphi}(a_0) = \varphi(a_0) = \varphi f(a_0), \forall a_0 \in V$.
Vậy $\overline{\varphi} = \varphi f$, tức là biểu đồ đã cho là giao hoán.
Mặt khác ta có

$$\overline{\varphi}[(a_0+a_1X+...+a_nX^n)+(b_0+b_1X+...+b_mX^m+OX^{m+1}+...+OX^n)] =$$

$$= \overline{\varphi}\left[\sum_{i=0}^{n}(a_i+b_i)X^i\right] = \sum_{i=0}^{n}\varphi(a_i+b_i)X^i = \sum_{i=0}^{m}(\varphi(a_i)+\varphi(b_i))X^i$$

$$= \sum_{i=0}^{m}\varphi(a_i)X^i + \sum_{i=0}^{m}\varphi(b_i)X^i = \overline{\varphi}\left(\sum_{i=0}^{m}(a_i)X^i\right) + \overline{\varphi}\left(\sum_{i=0}^{m}(b_i)X^i\right)$$

$$\overline{\varphi}(\sum_{i=0}^{n}a_iX^i)(\sum_{j=0}^{m}b_jX^j) = \overline{\varphi}\sum_{i=0}^{n+m}(\sum_{j+k=i}a_jb_k)X^{j+k}$$

$$= \sum_{i=0}^{n+m} \left(\sum_{j+k=i} \varphi(a_j)\varphi(b_k) \right) v^{i+j} = \left(\sum_{i=0}^{n} (a_i) v^i \right) \left(\sum_{j=o}^{m} (b_j) v^j \right)$$

$$= \overline{\varphi} \left(\sum_{i=0}^{n} a_i X^i \right) \overline{\varphi} \left(\sum_{j=o}^{m} b_j X^j \right)$$

$$\overline{\varphi}(1) = \varphi(1) = 1$$

Vậy $\overline{\varphi}$ là một đồng cấu vành A[X] tới vành V, và nó thỏa mãn tất cả các yêu cầu đã đề ra. □

Hệ quả 1.1.2. *Giả sử A là một vành con của một vành giao hoán B và φ là phép nhúng chính tắc. Khi đó ta có thể phát biểu tính chất trên dưới dạng sau:*
Giả sử vành giao hoán V chứa vành A làm một vành con. Khi đó với mỗi phần tử $v \in V$ tồn tại duy nhất một đồng cấu vành.

$$\overline{\varphi} : A[x] \to V$$

sao cho $\overline{\varphi}(a) = a \forall a \in A, \overline{\varphi}(X) = V$.
Trong trường hợp này ta có

$$\overline{\varphi}(a_0 + a_1 X + ... + a_n X^n) = a_0 + a_1 v + ... + a_n v^n.$$

Vế phải của đẳng thức trên gọi là giá trị của đa thức

$$f(X) = a_0 + a_1 X + ... + a_n X^n$$

tại X=v. Nó cũng được kí hiệu là f(v).

Định nghĩa 1.1.3. Một phần tử $v \in V$ gọi là đại số trên A nếu và chỉ nếu ta có $\overline{\varphi}(f(X)) = f(v) = 0$, với một đa thức f(X) nào đó của vành A[X].
Còn nếu: $\overline{\varphi} : A[x] \to V$ là một đơn cấu tức là
$\overline{\varphi}(f(X)) = 0 <=> f(X) = 0 <=> f(v) = 0$ nếu và chỉ nếu tất cả các hệ tử của f đều bằng 0, thì v gọi là phần tử siêu việt trên A.
Trong trường hợp A=Q và V=C thì ta gọi tắt là những số *đại số* hoặc *siêu việt*. Thí dụ $\sqrt{2}, \sqrt{2} + \sqrt{3}$ là những số đại số, e, π là những số siêu