

Ideal trên vành đa thức - Định lý Nullstellensatz

Trương Phước Nhân, 27/02/2018

Trong bài viết “Ứng dụng của định lý Combinatorial Nullstellensatz” ta đã đề cập đến một kết quả rất đẹp và có nhiều ứng dụng độc đáo của lý thuyết đa thức hiện đại, trong bài viết này ta sẽ chứng minh lại kết quả gốc tổng quát của định lý không điểm tổ hợp nêu trên dưới góc độ đại số.

Kết quả 1: (Định lý Nullstellensatz) Cho $f, f_1, \dots, f_r \in \mathbb{C}[x_1, \dots, x_n]$, trong đó f bị triệt tiêu trên tập các không điểm chung của các đa thức $f_1, \dots, f_r$.

Khi đó, với một số nguyên dương q nào đó, đa thức f^q sẽ nằm trong ideal sinh bởi các đa thức $f_1, \dots, f_r$, hay có nghĩa là $f^q = g_1 f_1 + \dots + g_r f_r$ trong đó $g_1, \dots, g_r \in \mathbb{C}[x_1, x_2, \dots, x_n]$

Đầu tiên ta sẽ chứng minh trường hợp suy biến của định lý Nullstellensatz và sau đó sử dụng kết quả này để giải quyết vấn đề trong trường hợp tổng quát.

Kết quả 2: Cho $f_1, \dots, f_r \in \mathbb{C}[x_1, \dots, x_n]$ không có chung các không điểm.

Khi đó, tồn tại các đa thức $g_1, \dots, g_r \in \mathbb{C}[x_1, x_2, \dots, x_n]$ sao cho $g_1 f_1 + \dots + g_r f_r = 1$

Chứng minh: Kí hiệu $I(f_1, \dots, f_r)$ là ideal trong vành $K = \mathbb{C}[x_1, \dots, x_n]$ sinh bởi các đa thức $f_1, \dots, f_r$. Giả sử rằng không tồn tại các đa thức $g_1, \dots, g_r$ sao cho $g_1 f_1 + \dots + g_r f_r = 1$. Khi đó $I(f_1, \dots, f_r) \neq K$.

Khẳng định 1:

Cho I là một ideal cực đại của K sao cho $I(f_1, \dots, f_r) \subset I$. Khi đó vành $A = K/I$ là một trường

Chứng minh khẳng định 1: Ta chỉ cần chỉ ra rằng mọi phần tử khác không của K/I đều có phần tử khả nghịch. Nếu $f \notin I$ thì $I + fK$ là một ideal thực sự chứa I nên $I + fK = K$. Điều đó có nghĩa là, trong trường hợp riêng, tồn tại các đa thức $a \in I$ và $b \in K$ sao cho $a + bf = 1$. Khi đó lớp $\bar{b} \in K/I$ là nghịch đảo của $\bar{f} \in K/I$.

Gọi α_i là ảnh của x_i qua phép chiếu chính tắc $p: \mathbb{C}[x_1, x_2, \dots, x_n] \rightarrow \mathbb{C}[x_1, x_2, \dots, x_n]/I = A$.

Khi đó $A = \mathbb{C}[\alpha_1, \alpha_2, \dots, \alpha_n]$.

Khẳng định 2: Nếu một đại số hữu hạn sinh $A = \mathbb{C}[\alpha_1, \alpha_2, \dots, \alpha_n]$ trên $\mathbb{C}$ là một trường thì A có thể được đồng nhất với $\mathbb{C}$.

Ta cần đến một kết quả phụ sau

Bổ đề: Trong $A = \mathbb{C}[\alpha_1, \alpha_2, \dots, \alpha_n]$ tồn tại các phần tử $y_1, y_2, \dots, y_k$ độc lập đại số trên $\mathbb{C}$ sao cho với mọi phần tử $a \in A$ đều thỏa mãn một phương trình đại số chuẩn tắc trên $\mathbb{C}[y_1, y_2, \dots, y_k]$, có nghĩa là

$a^l + b_1 a^{l-1} + \dots + b_l = 0$, trong đó $b_1, \dots, b_l \in \mathbb{C}[y_1, y_2, \dots, y_k]$.

Chứng minh bổ đề: Ta chứng minh bằng quy nạp toán học theo n . Nếu các phần tử $\alpha_1, \alpha_2, \dots, \alpha_n$ là độc lập đại số thì khẳng định của bài toán là hiển nhiên. Gọi $f(\alpha_1, \alpha_2, \dots, \alpha_n) = 0$ là một liên hệ đại số giữa chúng.

Nếu f là một đa thức bậc m trong đó hệ số của x_n^m không bị triệt tiêu thì ta có $\alpha_n^m + b_1 \alpha_n^{m-1} + \dots + b_m = 0$, $b_1, b_2, \dots, b_m \in \mathbb{C}[\alpha_1, \alpha_2, \dots, \alpha_{n-1}]$. Áp dụng giả thiết quy nạp ta suy ra kết luận của bài toán.

Nếu hệ số của x_n^m bằng không, ta thực hiện phép đổi biến $x_n = \zeta_n$ và $x_i = \zeta_i + a_i \zeta_n$ với $i = 1, \dots, n-1$.

Chúng ta cố gắng chọn các số $a_i \in \mathbb{C}$ sao cho đa thức

$g(\zeta_1, \dots, \zeta_{n-1}, \zeta_n) = f(x_1, \dots, x_n) = f(\zeta_1 + a_1 \zeta_n, \dots, \zeta_{n-1} + a_{n-1} \zeta_n, \zeta_n)$ có hệ số ζ_n^m không bị triệt tiêu. Hệ số này chính là $g_m(0, \dots, 0, 1) = f_m(a_1, \dots, a_{n-1}, 1)$, trong đó f_m và g_m lần lượt là các thành phần thuần nhất của bậc cao nhất của các đa thức f và g . Hiển nhiên, đa thức thuần nhất $f_m(x_1, \dots, x_n)$ là không đồng nhất bằng không với $x_n = 1$.

Bây giờ ta thực hiện phép chứng minh A đồng nhất với $\mathbb{C}$. Chọn các phần tử $y_1, y_2, \dots, y_k \in A$ như trong khẳng định của bổ đề. Ta sẽ chứng minh rằng một phần tử khác không x bất kì trong $B = \mathbb{C}[y_1, \dots, y_k]$ đều khả nghịch, hay nói cách khác B là một trường. Theo giả thiết A là một trường nên x khả nghịch trong A . Tuy nhiên theo bổ đề ta suy ra phần tử x^{-1} sẽ thỏa mãn phương trình

$$(x^{-1})^l + b_1(x^{-1})^{l-1} + \dots + b_l = 0, \quad b_1, \dots, b_l \in B.$$

Bằng cách nhân hai vế của phương trình trên cho x^{l-1} ta thu được

$$x^{-1} = -b_1 - b_2x - \dots - b_lx^{l-1} \in B$$

Trường $B = \mathbb{C}[y_1, \dots, y_k]$ là một vành các đa thức theo k biến trên $\mathbb{C}$, nhưng với $k \neq 0$ ta đã biết vành đa thức không thể là một trường. Do đó $B = \mathbb{C}$. Một phần tử phân kì của trường A đều là nghiệm của một đa thức $(x^{-1})^l + b_1(x^{-1})^{l-1} + \dots + b_l = 0$. Như vậy $A = \mathbb{C}$.

Khẳng định 3: Các đa thức $f_1, \dots, f_r$ triệt tiêu tại điểm $(\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{C}^n$

Chứng minh khẳng định 3: Thật vậy, qua phép chiếu chính tắc

$$p: \mathbb{C}[x_1, x_2, \dots, x_n] \rightarrow \mathbb{C}[x_1, x_2, \dots, x_n] / I = A = \mathbb{C}$$

phần tử x_i biến thành $\alpha_i \in \mathbb{C}$ nên đa thức $\varphi(x_1, \dots, x_n)$ biến thành $\varphi(\alpha_1, \dots, \alpha_n)$, trong khi các đa thức $f_1, \dots, f_r$ đều nằm trong ideal I nên ta suy ra ngay kết luận vừa nêu.

Ta đây ta thấy được sự mâu thuẫn, bởi vì theo giả thiết đầu bài $f_1, \dots, f_r$ không có nghiệm chung. Từ đây ta suy ra khẳng định cần chứng minh.

Sau cùng ta sẽ chỉ ra tính đúng đắn của định lý Nullstellensatz. Với $f = 0$, khẳng định là hiển nhiên.

Giả sử $f \neq 0$, bằng cách bổ sung thêm vào $x_1, x_2, \dots, x_n$ một biến mới $x_{n+1} = z$ và xét các đa thức

$f_1, \dots, f_r, 1 - zf$. Các đa thức này không có không điểm chung nên

$$1 = h_1 f_1 + \dots + h_r f_r + h(1 - zf)$$

trong đó $h_1, \dots, h_r, h$ là một số đa thức theo các biến $x_1, \dots, x_n, z$ nào đó. Đặt $z = \frac{1}{f}$, sau khi thực hiện việc

quy đồng mẫu biểu thức trên ta thu được $f^q = g_1 f_1 + \dots + g_r f_r$, trong đó $g_1, g_2, \dots, g_r$ là một số đa thức theo các biến $x_1, x_2, \dots, x_n$ nào đó. Từ đây ta có điều phải chứng minh.

Tài liệu tham khảo:

[1]. Victor V. Prasolov, Polynomials, Second Edition

[2]. Trương Phước Nhân, Ideal trên vành đa thức – Định lý cơ bản Hilbert, 29/08/2017

[3]. Trương Phước Nhân, Định lý không điểm tổng hợp, 30/07/2017