

**UBND TỈNH QUẢNG NAM
TRƯỜNG ĐẠI HỌC QUẢNG NAM
KHOA TOÁN**



**KHÓA LUẬN
TỐT NGHIỆP ĐẠI HỌC**

Tên đề tài: PHÂN TÍCH ĐA THỨC TRÊN CÁC TRƯỜNG SỐ

Sinh viên thực hiện
NGUYỄN PHAN HOÀI LINH
MSSV: 2115010116
CHUYÊN NGÀNH: SƯ PHẠM TOÁN
KHÓA: 2015 – 2019

Cán bộ hướng dẫn
ThS. VÕ VĂN MINH

Quảng Nam, tháng 05 năm 2019

PHIẾU CHẤM ĐIỂM KHÓA LUẬN

PHẦN XÁC NHẬN CỦA TÁC GIẢ VÀ CÁN BỘ HƯỚNG DẪN	
<u>Sinh viên thực hiện đề tài</u> (ký và ghi rõ họ tên) Nguyễn Phan Hoài Linh	<u>Cán bộ hướng dẫn khóa luận</u> (ký và ghi rõ họ tên) ThS. Võ Văn Minh
PHẦN CHẤM ĐIỂM CỦA HỘI ĐỒNG BẢO VỆ KHÓA LUẬN	
- Điểm thống nhất bằng số: điểm - Điểm bằng chữ:	
<u>Cán bộ chấm 1</u> (ký và ghi rõ họ tên) ThS. Phạm Ngọc Hoàng	<u>Cán bộ chấm 2</u> (ký và ghi rõ họ tên) ThS. Hoàng Thị Hà My

LỜI CẢM ƠN

Trải qua bốn năm học tập và rèn luyện tại giảng đường trường ĐH Quảng Nam, dưới sự dìu dắt của quý Thầy Cô giáo, tôi đã tích lũy cho mình rất nhiều kiến thức và kinh nghiệm quý báu cả về chuyên môn và nghiệp vụ. Khóa luận này chính là thành quả quan trọng của cả quá trình đó.

Đầu tiên tôi xin gửi lòng biết ơn sâu sắc đến thầy giáo, ThS. Võ Văn Minh, người đã hướng dẫn và giúp đỡ tôi hoàn thành khóa luận này.

Tôi xin được gửi lòng biết ơn chân thành đến quý Thầy Cô đã giảng dạy lớp ĐHSP Toán K15 - 01 trường ĐH Quảng Nam, đặc biệt là toàn thể quý Thầy Cô Khoa Toán trường ĐH Quảng Nam, những người không những cho tôi kiến thức mà còn quan tâm động viên và nhiệt tình giúp đỡ tôi trong suốt quá trình học tập cũng như thời gian thực hiện khóa luận.

Cuối cùng, tôi xin được gửi lời cảm ơn đến tất cả người thân, bạn bè đã quan tâm động viên giúp đỡ tôi trong suốt thời gian qua.

Tam Kỳ, ngày 17 tháng 5 năm 2019

Sinh viên

NGUYỄN PHAN HOÀI LINH

MỤC LỤC

Phần 1. MỞ ĐẦU	1
1.1. Lý do chọn đề tài	1
1.2. Mục tiêu của đề tài.....	1
1.3. Đối tượng và phạm vi nghiên cứu	1
1.4. Phương pháp nghiên cứu	1
1.5 Lịch sử nghiên cứu.....	2
1.6 Đóng góp của đề tài	2
1.7 Cấu trúc đề tài	2
BẢNG KÝ HIỆU	3
Phần 2. NỘI DUNG NGHIÊN CỨU.....	4
Chương 1: KIẾN THỨC CHUẨN BỊ	4
1.1 Miền nguyên - Trường.....	4
1.1.1 Miền nguyên.....	4
1.1.2 Trường.....	4
1.2 Vành đa thức:.....	5
1.2.1 Vành đa thức một biến hệ số thực.....	5
1.2.2 Xây dựng vành đa thức một biến	5
1.2.3 Xây dựng vành đa thức nhiều biến	6
1.2.4 Đa thức đối xứng:.....	7
1.2.5 Bậc của đa thức	7
1.2.6 Phép chia có dư	8
1.2.7 Nghiệm của đa thức	9
1.3 Đa thức bất khả quy	9
Chương 2: PHÂN TÍCH ĐA THỨC TRÊN CÁC TRƯỜNG SỐ.....	10
2.1 Phân tích đa thức trên trường số thực và trường số phức.....	10
2.1.1 Phân tích đa thức trên trường số phức	10
2.1.2 Phân tích đa thức trên trường số thực	16
2.1.3 Bài tập vận dụng.....	18
2.2 Phân tích các đa thức nguyên và các đa thức hữu tỷ	27
2.2.1 Đa thức hệ số nguyên.....	27
2.2.2 Đa thức hệ số hữu tỷ	28

2.2.3 Bài tập vận dụng.....	32
2.3 Phân tích đa thức trên trường hữu hạn.....	41
2.3.1 Một số tính chất của trường hữu hạn	41
2.3.2. Đa thức bất khả quy trên trường hữu hạn	44
2.3.3. Phân tích đa thức trên trường hữu hạn.....	48
2.3.4 Bài tập vận dụng.....	51
Phần 3. KẾT LUẬN.....	56
Phần 4. TÀI LIỆU THAM KHẢO	56
Phần 5. PHỤ LỤC.....	56

Phần 1. MỞ ĐẦU

1.1. Lý do chọn đề tài

Toán học là một môn học cơ bản làm nền tảng cho các ngành khoa học khác. Môn Toán có tiềm năng to lớn trong việc khai thác và phát triển năng lực trí tuệ chung, rèn luyện các thao tác và tư duy của con người.

Đa thức là một đối tượng được nghiên cứu rất nhiều trong Toán học. Ngay từ THCS và THPT, đa thức đã được đề cập rất nhiều trong chương trình sách giáo khoa. Đa thức có vị trí quan trọng trong Toán học, không những là đối tượng nghiên cứu của Đại số mà còn là công cụ đắc lực của Giải tích, Lý thuyết số, Hình học,... Trong các cuộc thi học sinh giỏi quốc gia, Olympic Toán thì các bài toán về đa thức được đề cập rất nhiều, đây cũng là các dạng toán khó.

Tuy nhiên, tài liệu viết về sự phân tích đa thức còn rất ít nên việc nghiên cứu về đa thức còn gặp nhiều khó khăn. Xuất phát từ những lý do trên tôi quyết định chọn đề tài: **"Phân tích đa thức trên các trường số"**. Tôi mong rằng khóa luận này sẽ có ích cho những ai quan tâm đến đa thức, đặc biệt là sự phân tích đa thức trên các trường số.

1.2. Mục tiêu của đề tài

Thông qua việc nghiên cứu tài liệu tham khảo, khai thác và tìm hiểu các kiến thức chuyên sâu trong việc phân tích đa thức trên các trường số như trường số thực và phức, trường số nguyên và hữu tỷ, trường hữu hạn.

1.3. Đối tượng và phạm vi nghiên cứu

Các lý thuyết và bài tập có liên quan đến sự phân tích đa thức trên các trường số của đa thức một biến (nhiều biến).

1.4. Phương pháp nghiên cứu

- Phương pháp nghiên cứu lý luận:

Các phương pháp được sử dụng trong quá trình hoàn thành khóa luận là tham khảo, tổng hợp các nguồn tài liệu khác nhau như sách vở, giáo trình, nguồn thông tin từ internet,... để làm rõ nội dung lý thuyết, trao đổi thông tin từ thầy cô, bạn bè.

- Phương pháp nghiên cứu thực tiễn:

Phân tích, so sánh và hệ thống hóa các nội dung một cách rõ ràng.

Tham gia học hỏi và trau dồi những kinh nghiệm quý báu của các thầy cô giáo cũng như những ý kiến đóng góp của giảng viên hướng dẫn để làm tốt đề tài.

1.5 Lịch sử nghiên cứu

Nhận đề tài.

Sưu tầm tài liệu liên quan.

Lập đề cương chi tiết.

Làm rõ các vấn đề mà đề tài hướng tới hoặc có liên quan đến đề tài.

Trình bày các vấn đề đã làm được và thông qua giảng viên hướng dẫn.

Chỉnh sửa và hoàn thành khóa luận.

1.6 Đóng góp của đề tài

Khóa luận làm rõ các phân tích đa thức trên các trường số, tôi sẽ cố gắng nhiều để đạt được yêu cầu đặt ra, đây cũng là tài liệu tham khảo cho sinh viên các khóa sau.

1.7 Cấu trúc đề tài

Ngoài phần mở bài, kết luận và danh mục tài liệu tham khảo, phần nội dung được chia thành 2 chương:

- Chương 1: Kiến thức chuẩn bị.
- Chương 2: Phân tích đa thức trên các trường số.

BẢNG KÝ HIỆU

Ký hiệu	Ý nghĩa
$\mathbb{N}$	Tập hợp các số tự nhiên
$\mathbb{R}$	Tập hợp các số thực
$\mathbb{Z}$	Tập hợp các số nguyên
$\mathbb{Q}$	Tập hợp các số hữu tỷ
$\mathbb{C}$	Tập hợp các số phức
$m \mid n$	m là ước của n
$\mathbb{Z} \times \mathbb{Z}$	Tích Descartes của hai tập hợp $\mathbb{Z}$ và $\mathbb{Z}$
(y)	Idêan sinh bởi phần tử y
F_q^*	Nhóm nhân các phần tử khác không của F_q
$\gcd(f(x), g(x))$	Ước chung lớn nhất của $f(x)$ và $g(x)$
$\text{char} F$	Đặc số của vành (trường) F

Phần 2. NỘI DUNG NGHIÊN CỨU

Chương 1: KIẾN THỨC CHUẨN BỊ

1.1 Miền nguyên - Trường

1.1.1 Miền nguyên

Định nghĩa: Miền nguyên là vành giao hoán, có đơn vị, có nhiều hơn một phần tử và không có ước của không.

Ví dụ:

(1) Vành $\mathbb{Z}$ là một miền nguyên vì vành $\mathbb{Z}$ là vành giao hoán, có đơn vị là 1, có vô hạn phần tử.

$\forall a, b \in \mathbb{Z}, a \neq 0, b \neq 0$ suy ra $ab \neq 0$ nên vành $\mathbb{Z}$ không có ước của không.

(2) Vành $X = \mathbb{Z} \times \mathbb{Z}$ không là miền nguyên.

Thật vậy, lấy $(0,0) \neq (2,0) \in \mathbb{Z} \times \mathbb{Z}, (0,0) \neq (0,5) \in \mathbb{Z} \times \mathbb{Z}$. Khi đó:

$$(2,0) \cdot (0,5) = (2 \cdot 0, 0 \cdot 5) = (0,0) \Rightarrow X \text{ có ước của không.}$$

1.1.2 Trường

Định nghĩa: Trường là một miền nguyên, trong đó mọi phần tử khác 0 đều có nghịch đảo.

Ví dụ: Vành $\mathbb{Z}_5$ là một trường.

Thật vậy, ta có $\mathbb{Z}_5$ cùng với 2 phép toán cộng và nhân:

$$\forall \bar{a}, \bar{b} \in \mathbb{Z}_5, \bar{a} + \bar{b} = \overline{a+b}, \bar{a} \cdot \bar{b} = \overline{ab} \text{ là một vành giao hoán, có đơn vị là } \bar{1}.$$

Chứng minh: $\mathbb{Z}_5$ là miền nguyên, tức là $\mathbb{Z}_5$ không có ước của không.

Giả sử $\bar{a}, \bar{b} \in \mathbb{Z}_5$ và $\bar{a} \cdot \bar{b} = \bar{0}$ hay $\overline{ab} = \bar{0} \Rightarrow ab = 0 + 5x$, tức $ab : 5$ và do 5 là số nguyên tố.

$$\text{Suy ra } \begin{cases} a : 5 \\ b : 5 \end{cases} \Rightarrow \begin{cases} \bar{a} = \bar{0} \\ \bar{b} = \bar{0} \end{cases} \text{ tức là } \mathbb{Z}_5 \text{ không có ước của không.}$$

Vậy $\mathbb{Z}_5$ là miền nguyên.

Chứng minh $\mathbb{Z}_5$ khả nghịch:

Giả sử $\bar{0} \neq \bar{a} \in \mathbb{Z}_5$ suy ra a không chia hết cho 5 $\Rightarrow (a,5)=1$. Khi đó:

$$\exists u, v \in \mathbb{Z} : au + 5v = 1 \Rightarrow \overline{au + 5v} = \bar{1} \text{ hay } \bar{a} \cdot \bar{u} + \bar{5} \cdot \bar{v} = \bar{1}.$$

$$\Rightarrow \bar{a} \cdot \bar{u} = \bar{1} \text{ (vì trong } \mathbb{Z}_5 \text{ ta có } \bar{5} = 0)$$

Vậy $\mathbb{Z}_5$ khả nghịch.

1.2 Vành đa thức:

1.2.1 Vành đa thức một biến hệ số thực

Ta gọi tập các đa thức hệ số thực là $\mathbb{R}[x]$, trong đó:

$$f(x) = a_0 + a_1x + \dots + a_mx^m, a_i \in \mathbb{R}, i = \overline{0, m}$$

$$g(x) = b_0 + b_1x + \dots + b_nx^n, b_i \in \mathbb{R}, i = \overline{0, n}$$

Với $m \leq n$ ta có:

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_m + b_m)x^m + b_{m+1}x^{m+1} + b_nx^n.$$

$$f(x).g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \dots + (a_0b_k + a_1b_{k-1} + \dots + a_kb_0)x^k + \dots + a_mb_nx^{m+n}$$

Ta dễ dàng chứng minh $(\mathbb{R}[x], +, \cdot)$ lập thành một vành.

1.2.2 Xây dựng vành đa thức một biến

Cho A là vành giao hoán có đơn vị. Gọi P là tập các dãy vô hạn $(a_0, a_1, \dots, a_n, 0, \dots)$ với $a \in A, \forall i \in \mathbb{N}$, P chỉ chứa một số hữu hạn các phần tử khác 0.

Trên P ta định nghĩa phép cộng và phép nhân như sau:

- $(a_0, a_1, \dots, a_n, 0, \dots) + (b_0, b_1, \dots, b_n, 0, \dots) = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, 0, \dots)$
- $(a_0, a_1, \dots, a_n, 0, \dots) \cdot (b_0, b_1, \dots, b_n, 0, \dots) = (c_0, c_1, \dots, c_k, 0, \dots)$

$$\text{với } c_k = \sum_{i+j=k} a_ib_j, k = 0, 1, 2, \dots$$

Khi đó $(P, +, \cdot)$ lập thành một vành giao hoán, có đơn vị là $(1, 0, \dots)$

Xét dãy $x = (0, 1, 0, \dots)$

$$x^2 = (0, 0, 1, 0, \dots)$$

$\vdots$

$$x^n = \left(\underbrace{0, 0, 0, \dots, 0}_n, 1, 0, \dots \right)$$

Nếu $a \in A$, xét ánh xạ: $\varphi: A \rightarrow P$

$$a \mapsto \varphi(a) = (a, 0, \dots)$$

Khi đó φ là một đơn cấu vành.

Thật vậy, $\forall a, b \in A$, ta có:

$$\varphi(a+b) = (a+b, 0, \dots) = (a, 0, \dots) + (b, 0, \dots) = \varphi(a) + \varphi(b).$$

$$\varphi(ab) = (ab, 0, \dots) = (a, 0, \dots)(b, 0, \dots) = \varphi(a)\varphi(b).$$

Suy ra φ là đồng cấu vành.

$$\text{Ker } \varphi = \{a \in A \mid \varphi(a) = 0_p\} = \{a \in A \mid (a, 0, \dots) = (0, 0, \dots)\} = \{a \in A \mid a = 0\} = \{0\}.$$

Vậy φ là đơn cấu.

Ta gọi φ nhúng A vào P như một vành con, ta có thể đồng nhất

$$(a, p, \dots) \equiv a \in A.$$

Với dãy $(a_0, a_1, \dots, a_n, 0) \in P$ ta viết lại:

$$\begin{aligned} (a_0, a_1, \dots, a_n, 0, \dots) &= (a_0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0, 0, \dots, 0, a_n, 0, \dots) \\ &= (a_0, 0, \dots) + (a_1, 0, \dots)(0, 1, 0, \dots) + \dots + (a_n, 0, \dots)(0, 0, \dots, 1, 0, \dots) \\ &= a_0 + a_1x + \dots + a_nx^n = f(x). \end{aligned}$$

Vậy với mỗi dãy $(a_0, a_1, \dots, a_n, 0, \dots) \in P$, ta có thể viết được:

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \quad (a_n \neq 0)$$

Ký hiệu: $P = A[x]$.

1.2.3 Xây dựng vành đa thức nhiều biến

- Cho A là vành giao hoán có đơn vị 1. Xây dựng vành đa thức $A[x_1]$:

$$A[x_1] = \{f(x_1) = a_0 + a_1x_1 + a_2x_1^2 + \dots + a_nx_1^n \mid a_i \in A, \forall i \in \mathbb{N}\}.$$

- Vành $A[x_1]$ là vành giao hoán có đơn vị. Xác định vành đa thức $A[x_1, x_2]$:

$$A[x_1, x_2] = \{f(x_1, x_2) = a_0(x_1) + a_1(x_1)x_2 + \dots + a_n(x_1)x_2^n \mid a_i(x_1) \in A[x_1], \forall i \in \mathbb{N}\}$$

- Vành $A[x_1, x_2]$ là vành giao hoán có đơn vị. Xác định vành đa thức

$$A[x_1, x_2, x_3]:$$

$$\text{Phần tử } f(x_1, x_2, x_3) = C_0 + C_1x_1^{a_{11}}x_2^{a_{12}}x_3^{a_{13}} + \dots + C_mx_1^{a_{m1}}x_2^{a_{m2}}x_3^{a_{m3}}.$$

$$\text{Bằng phương pháp quy nạp: } A \subset A[x_1] \subset A[x_1, x_2] \subset \dots \subset A[x_1, x_2, \dots, x_n].$$

$$\text{Phần tử } f(x_1, x_2, \dots, x_n) = C_0 + C_1x_1^{a_{11}}x_2^{a_{12}} \dots x_n^{a_{1n}} + \dots + C_mx_1^{a_{m1}}x_2^{a_{m2}} \dots x_n^{a_{mn}}$$

trong đó: $C_i \in A, \forall i$; số mũ $a_{i1}, a_{i2}, \dots, a_{in}$ là các số tự nhiên.

C_i là hệ tử (hệ số).

$C_i x_1^{a_{i1}} x_2^{a_{i2}} \dots x_n^{a_{in}}$ là các hạng tử.

$f(x_1, x_2, \dots, x_n) = 0$ khi và chỉ khi các hệ số đều bằng 0.

1.2.4 Đa thức đối xứng:

Định nghĩa: $f(x_1, x_2, \dots, x_i, \dots, x_j, \dots, x_n) \in A[x_1, x_2, \dots, x_n]$ được gọi là đa thức đối xứng nếu nó không thay đổi khi ta thay đổi chỗ 2 vị trí x_i và x_j bất kỳ cho nhau.

$$f(x_1, x_2, \dots, x_i, \dots, x_j, \dots, x_n) = f(x_1, x_2, \dots, x_j, \dots, x_i, \dots, x_n)$$

Nhận xét: Các đa thức đối xứng:

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + \dots + x_n \\ \sigma_2 &= x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n \\ \sigma_3 &= x_1 x_2 \dots x_{n-1} + \dots + x_2 x_3 \dots x_n \\ &\vdots \\ \sigma_n &= x_1 x_2 \dots x_n\end{aligned}$$

Ta gọi $\sigma_1, \sigma_2, \dots, \sigma_n$ là các đa thức đối xứng cơ bản.

Ví dụ 3: Biểu diễn đa thức sau qua đa thức đối xứng cơ bản:

$$f(x_1, x_2, x_3) = x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_1 x_3^2 + x_2 x_3^2 + x_2^2 x_3.$$

Ta có: Hệ thống mũ: $(2, 1, 0), (1, 1, 1)$

Khi đó $\varphi(x_1^2 x_2) = \sigma_1 \sigma_2 + m_1 \sigma_3$.

Lập bảng tìm m_1 :

x_1	x_2	x_3	σ_1	σ_2	σ_3	f
1	1	1	3	3	1	$6 = 9 + m_1 \Rightarrow m_1 = -3$

Vậy $f(x_1, x_2, x_3) = \varphi(x_1^2 x_2) = \sigma_1 \sigma_2 - 3\sigma_3$.

1.2.5 Bậc của đa thức

a) Bậc của đa thức một biến:

Định nghĩa: Cho $f(x) = a_0 + a_1 x + \dots + a_n x^n \in A[x]$ với $a_n \neq 0, a_i \in \mathbb{R}, i = \overline{1, n}$.

- Ta gọi bậc đa thức $f(x)$ là số mũ của lũy thừa cao nhất mà hệ tử ứng với nó khác 0, ký hiệu: bậc $f(x)$ (hay $\deg f(x)$)

- Đa thức là hằng số khác 0 có bậc bằng 0.

- Đa thức 0 thì không có bậc.

Định lý 1: Cho $f(x), g(x) \neq 0$:

(i) Nếu bậc $f(x) \neq$ bậc $g(x)$ thì $f(x) + g(x) \neq 0$. Ta có:

$$\text{bậc}(f(x) + g(x)) = \max(\text{bậc } f(x), \text{bậc } g(x)).$$

Nếu bậc $f(x) =$ bậc $g(x)$ đồng thời $f(x) + g(x) \neq 0$ thì bậc $(f(x) + g(x)) \leq \max(\text{bậc } f(x), \text{bậc } g(x))$.

(ii) Nếu $f(x).g(x) \neq 0$ thì bậc $(f(x).g(x)) \leq \text{bậc } f(x) + \text{bậc } g(x)$.

Định lý 2: Nếu A là miền nguyên và $0 \neq f(x), g(x) \in A[x]$ thì:

$$\text{bậc}(f(x).g(x)) = \text{bậc } f(x) + \text{bậc } g(x)$$

Chứng minh: Giả sử $f(x) = a_0 + a_1x + \dots + a_nx^n$ ($a_n \neq 0$)

$$g(x) = b_0 + b_1x + \dots + b_mx^m$$
 ($b_m \neq 0$)

$$\text{Khi đó } f(x).g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \dots + a_nb_mx^{n+m}$$

Do $a_n \neq 0, b_m \neq 0 \Rightarrow a_nb_m \neq 0$ (vì A là miền nguyên nên không có ước của không).

$$\text{bậc}(f(x).g(x)) = n + m = \text{bậc } f(x) + \text{bậc } g(x)$$

Hệ quả: Nếu A là miền nguyên thì $A[x]$ cũng là miền nguyên.

b) Bậc của đa thức nhiều biến:

Cho $f(x_1, x_2, \dots, x_n) \in A[x_1, x_2, \dots, x_n]$.

- Bậc của f đối với ẩn x_i là số mũ của lũy thừa cao nhất trong các hạng tử của đa thức.

- Bậc của hạng tử $C_i x_1^{a_{i1}} x_2^{a_{i2}} \dots x_n^{a_{in}}$ bằng $a_{i1} + a_{i2} + \dots + a_{in}$.

- Bậc tổng thể f là: $m = \max\{a_{i1} + a_{i2} + \dots + a_{in}\}$

1.2.6 Phép chia có dư

Định lý: Cho A là một trường, $f(x), g(x) \in A[x]$ với $g(x) \neq 0$ đều tồn tại duy nhất $q(x), r(x)$ với bậc $r(x) < \text{bậc } g(x)$ hoặc $r(x) = 0$ sao cho:

$$f(x) = g(x).q(x) + r(x)$$

trong đó $r(x)$: đa thức dư, $q(x)$: đa thức thương.

Hệ quả: $f(x) \vdots g(x) \Leftrightarrow r(x) = 0$.

1.2.7 Nghiệm của đa thức

a) Định nghĩa: Cho A là một trường, $c \in A$, $f(x) \in A[x]$ với

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (a_n \neq 0)$$

Ta gọi giá trị của $f(x)$ tại $x = c$ là $f(c) = a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0$.

Nếu $f(c) = 0$ thì c là nghiệm của đa thức $f(x)$.

b, Định lý Bezout: Cho A là một trường, $c \in A$, $f(x) \in A[x]$. Đa thức dư của phép chia $f(x)$ cho $x - c$ là $f(c)$.

Hệ quả: $f(x) \vdots (x - c) \Leftrightarrow f(c) = 0$ (hay c là nghiệm của $f(x)$).

Định nghĩa: (Nghiệm bội, nghiệm kép)

Cho A là một trường, $c \in A$ được gọi là nghiệm bội k của $f(x) \in A[x]$ nếu $f(x) \vdots (x - c)^k$ và $f(x) \nmid (x - c)^{k+1}$.

- Nếu $k = 1$ thì c là nghiệm đơn.

- Nếu $k = 2$ thì c là nghiệm kép.

1.3 Đa thức bất khả quy

Định nghĩa: Cho A là một trường, đa thức $f(x)$ trong vành $A[x]$ gọi là bất khả quy trên A nếu $f(x)$ có bậc là một số nguyên dương và từ điều kiện $f(x) = g(x)h(x)$, với $g(x), h(x) \in A[x]$ luôn suy ra $g(x)$ hoặc $h(x)$ là đa thức hằng.

Chương 2: PHÂN TÍCH ĐA THỨC TRÊN CÁC TRƯỜNG SỐ

2.1 Phân tích đa thức trên trường số thực và trường số phức

2.1.1 Phân tích đa thức trên trường số phức

Định lý 1. Nếu F là một trường và p là một đa thức bất khả quy của vành $F[x]$ với bậc p bằng n , tồn tại một trường K có các tính chất:

- i) K chứa F như một trường con;
- ii) K chứa một nghiệm u của đa thức p ;
- iii) Trường K được sinh bởi F và u và mọi phần tử của K có thể đặt dưới dạng một đa thức duy nhất theo u với hệ tử thuộc F và có bậc bé hơn hoặc bằng $n-1$.

Chứng minh:

i) Vì p là một đa thức bất khả quy của miền nguyên chính $F[x]$ nên $\text{idêan}(p)$ sinh bởi p của $F[x]$ là idêan tối đại. Do đó vành thương $K = F[x]/(p)$ là một trường.

Gọi $\pi : F[x] \rightarrow F[x]/(p) = K$

$$f \mapsto f + (p) \quad \text{là toàn cấu chính tắc}$$

Thu hẹp của π vào F là một đồng cấu trường $\pi' : F \rightarrow K$ cho nên π' là một đơn cấu và F đẳng cấu với trường con $\text{Im}\pi' = \pi(F)$ của trường K .

Đồng nhất F với $\text{Im}\pi'$ tức là đồng nhất mỗi $a \in F$ với $a + (p) \in K$, ta có K chứa F như một trường con.

ii) Ta có đồng cấu vành $\pi : F[x] \rightarrow F[x]/(p) = K$

Đặt $u = \pi(x) = x + (p) \in K$.

Vì $\pi(a) = \pi(a') = a$ với mọi $a \in F$ và $\pi(p) = (p) = 0 \in K$, nên trong K ta có:

$$\tilde{p}(u) = \tilde{p}(\pi(x)) = \pi(p) = 0 \in K$$

Nói cách khác u là một nghiệm của đa thức p trong K .

Ngoài ra, vì π là toàn cấu, mọi phần tử của K có dạng $\pi(f)$ với một đa thức $f \in F[x]$; hay $\pi(f) = \pi(f(x)) = f(\pi(x)) = f(u)$, tức là một đa thức theo u với hệ tử thuộc F .

Vậy $K = F[u]$, một vành đa thức theo biến $u \in K$ với hệ tử thuộc vành con F của K , nghĩa là K được sinh bởi F và u .

iii) Vì mọi đa thức $f \in F[x]$ có thể đặt dưới dạng $f = pq + r$ với một đa thức duy nhất $r \in F[x]$, nếu khác 0, có bậc $r < \text{bậc } p$ bằng n nên

$$\pi(f) = \pi(pq + r) = \pi(r) = r(u) \in F[u].$$

Điều này chứng tỏ mọi phần tử của $K = F[u]$ có thể viết thành một đa thức duy nhất $r(u)$ theo biến u với hệ tử thuộc F và nếu $r(u) \neq 0$ thì bậc $r \leq n-1$.

Định lý 2. Nếu F là một trường và f là một đa thức của vành $F[x]$ với bậc $f = n > 0$, thì tồn tại một trường K chứa F như một trường con, sao cho trong vành đa thức $K[x]$, f có dạng

$$f = a_n(x-u_1)\dots(x-u_n)g$$

trong đó $a_n, u_1, \dots, u_n$ là những hằng thuộc K và g là một đa thức của $K[x]$.

Chứng minh:

Trước hết đa thức $f \in F[x] \neq 0$ bậc n có hệ tử dẫn đầu $a_n \neq 0$ có thể viết với đa thức $0 \neq f_n \in F[x]$ có hệ tử dẫn đầu 1 và bậc $f_n = \deg f = n$.

Ta chứng minh định lý bằng quy nạp trên $n = \deg f$.

Với $n=1$, ta có $f = a_0 + a_1x \in F[x]$ ($a_1 \neq 0$) và có thể viết

$$f = a_1(x-u_1) \text{ với } u_1 = -\frac{a_0}{a_1},$$

Vậy trong trường hợp này trường K chính là F .

Với $n > 1$, giả sử định lý đúng với mọi đa thức khác 0 có bậc $\leq n-1$ của $F[x]$.

Vì $f = a_n f_n$ và f_n có một ước bất khả quy $p \in F[x]$, cho nên tồn tại một trường K_1 chứa F như một trường con và một nghiệm u_1 của p để trong vành đa thức $K_1[x]$, ta có $f_n = (x-u_1)g$ và $f = a_n(x-u_1)g$ với một đa thức $g \in K_1[x]$ có hệ tử dẫn đầu 1 và bậc $g = n-1$.

Theo giả thiết quy nạp, tồn tại một trường K chứa K_1 và F như những trường con sao cho trong vành đa thức $K[x]$, g có dạng $g = (x-u_2)\dots(x-u_n)$, do đó:

$$f = a_n(x-u_1)g = a_n(x-u_1)(x-u_2)\dots(x-u_n)g \text{ (đpcm)}.$$

Bổ đề 1. Mọi phần tử của $\mathbb{C}$ là bình phương của một phần tử của $\mathbb{C}$ và mọi đa thức bậc 2 của $\mathbb{C}[x]$ đều có nghiệm trong $\mathbb{C}$.

Chứng minh:

Cho số phức $a+bi \in \mathbb{C}$, ta chứng tỏ có một số phức $s+ti \in \mathbb{C}$ sao cho

$$(s+ti)^2 = a+bi \Leftrightarrow s^2 + 2sti - t^2 = a+bi \Leftrightarrow \begin{cases} s^2 - t^2 = a \\ 2st = b \end{cases}$$

$$\text{Suy ra: } (s^2 + t^2)^2 = a^2 + b^2$$

Gọi $c \geq 0$ là căn bậc hai của $a^2 + b^2 \geq 0$, ta có $c \geq |a|$, $c \geq |b|$ và $s^2 + t^2 = c$.

$$\text{Do đó, } s^2 = \frac{(c+a)}{2}, \quad t^2 = \frac{(c-a)}{2}.$$

Vì $c \geq |a|$ nên $c+a \geq 0$ và các đẳng thức trên cho định các số thực s và t .

Vậy số phức $a+bi$ là một bình phương.

Với $ax^2 + bx + c \in \mathbb{C}[x]$ với $a \neq 0$. Ta có

$$ax^2 + bx + c = a \left[\left(x + \frac{b}{2a} \right)^2 - \frac{b^2 - 4ac}{4a^2} \right].$$

Theo trên có số phức d sao cho $d^2 = \frac{b^2 - 4ac}{4a^2}$ nên đa thức bậc 2 đã cho có

$$\text{nghiệm } -\frac{b}{2a} \pm d \in \mathbb{C}.$$

Mệnh đề 1. Mọi đa thức bậc lớn hơn 0 của $\mathbb{R}[x]$ đều có nghiệm trong $\mathbb{C}$.

Chứng minh: Cho đa thức $g \in \mathbb{R}[x] \neq 0$ với bậc $g = n > 0$.

Với mọi số tự nhiên $n > 0$ đều có thể viết dưới dạng $n = 2^m q$ với số nguyên $m \geq 0$ và số nguyên q là số lẻ.

Vì mệnh đề đúng với $m = 0$, ta chứng minh bằng quy nạp trên m .

Không làm mất tính tổng quát của chứng minh, ta có thể giả sử hệ số dẫn đầu của g là $a_n = 1$, vì mọi đa thức có thể viết $f = a_n g$ với $\deg f = \deg g$ và g có hệ tử dẫn đầu bằng 1.

Theo định lý 2 có một trường K chứa $\mathbb{R}$ như một trường con sao cho trong $K[x]$ đa thức g có dạng nhân tử hóa như sau:

$$g = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

Dưới dạng khai triển: $g = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n$

trong đó $s_1, \dots, s_n$ là các đa thức đối xứng sơ cấp theo các nghiệm $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ của g .

Vì $g \in \mathbb{R}[x]$, dạng này cho thấy các hệ tử $s_1, \dots, s_n$ đều thuộc $\mathbb{R}$.

Với một số thực $b \in \mathbb{R}$, ta xét đa thức sau đây của $K[x]$:

$$G_b(x) = \prod_{1 \leq i < j \leq n} [x - (\alpha_i + \alpha_j + b\alpha_i\alpha_j)].$$

Đa thức này hiển nhiên có $\frac{1}{2}n(n-1)$ nghiệm $\beta_{ij} = \alpha_i + \alpha_j + b\alpha_i\alpha_j \in K$

cho nên các hệ tử của $G_b(x)$ là những đa thức đối xứng theo các β_{ij} với hệ số thuộc $\mathbb{R}$, do đó cũng là đa thức đối xứng theo $\alpha_1, \alpha_2, \dots, \alpha_n$ với hệ số thực.

Vì mỗi hệ tử của $G_b(x)$ là đa thức đối xứng của vành $\mathbb{R}[\alpha_1, \dots, \alpha_n]$, nên các hệ tử này biểu thị được như là đa thức theo $s_1, \dots, s_n$ và với hệ tử thuộc $\mathbb{R}$.

Nhưng vì $s_1, \dots, s_n \in \mathbb{R}$ theo trên, cho nên các hệ tử của $G_b(x)$ đều thuộc $\mathbb{R}$, hay $G_b(x) \in \mathbb{R}[x]$.

Mặt khác, ta có

$$\text{bậc } G_b(x) = \frac{1}{2}n(n-1) = 2^{m-1}q(2^m q - 1) = 2^{m-1}q'$$

(với $q' = q(2^m q - 1)$ là một số nguyên lẻ).

Do đó theo giả thiết quy nạp, đa thức $G_b(x)$ có một nghiệm $\beta_{ij} \in \mathbb{C}$, tức là có ít nhất một cặp chỉ số (i, j) sao cho:

$$\alpha_i + \alpha_j + b\alpha_i\alpha_j \in \mathbb{C} \text{ và } \alpha_i + \alpha_j + b'\alpha_i\alpha_j \in \mathbb{C} \text{ với } b \neq b'.$$

Từ đó suy ra $\alpha_i + \alpha_j \in \mathbb{C}$ và $\alpha_i\alpha_j \in \mathbb{C}$; hơn nữa vì:

$$(x - \alpha_i)(x - \alpha_j) = x^2 - (\alpha_i + \alpha_j)x + \alpha_i\alpha_j \in \mathbb{C}[x]$$

Ta có α_i và α_j là các nghiệm của một đa thức bậc 2 với hệ số phức, theo bổ đề 1, các nghiệm α_i và α_j thuộc $\mathbb{C}$. Điều này chứng tỏ đa thức $g \in \mathbb{R}[x]$ đã cho có ít nhất một nghiệm thuộc $\mathbb{C}$. (đpcm)

Định lý 3. Nếu $f(z)$ là một đa thức trong $\mathbb{C}[z]$ có bậc dương, thì $f(z)$ có nghiệm trong $\mathbb{C}$.

Chứng minh:

Phép chứng minh của định lý này là không thuần túy đại số, nên để chứng minh Định lý cơ bản của Đại số, ta có thể sử dụng định lý của E. Rouché.

Định lý Rouché: Cho miền $M \subseteq \mathbb{C}$ với biên của M là $B(M)$. Nếu $f(z)$ và $h(z)$ là các hàm giải tích trong và trên miền M sao cho $|h(z)| < |f(z)|$ trên biên $B(M)$ thì $f(z)$ và $f(z) + h(z)$ có cùng số nghiệm trên miền M .

Bây giờ ta chứng minh định lý 3.

Cho $f(z) = a_n z^n + \dots + a_1 z + a_0$ là một đa thức với hệ số phức bậc $n > 0$. Ta cần chứng minh $f(z)$ có nghiệm phức.

Đặt $p(z) = a_n z^n$ và $h(z) = f(z) - p(z) = a_{n-1} z^{n-1} + \dots + a_1 z + a_0$.

Lấy số thực $r > 0$. Trên đường tròn $|z| = r$ ta có

$$|p(z)| = |a_n z^n| = |a_n| |z|^n = |a_n| r^n$$

$$\text{và } |h(z)| = |a_{n-1} z^{n-1} + \dots + a_1 z + a_0| \leq |a_{n-1}| r^{n-1} + \dots + |a_1| r + |a_0|.$$

$$\text{Vì } |a_n| \neq 0 \text{ nên ta có thể đặt } K = \frac{|a_{n-1}| + \dots + |a_1| + |a_0|}{|a_n|}$$

Chọn $r > \max\{1, K\}$. Khi đó:

$$\begin{aligned} |h(z)| &\leq |a_{n-1}| r^{n-1} + \dots + |a_1| r + |a_0| \\ &\leq (|a_{n-1}| + \dots + |a_1| + |a_0|) r^{n-1} \\ &< (r |a_n|) r^{n-1} = |a_n| r^n = |p(z)|. \end{aligned}$$

Vì thế $|h(z)| < |p(z)|$ với mọi z nằm trên đường tròn tâm là gốc tọa độ, bán kính r .

Chú ý rằng đường tròn $|z| = r$ chính là biên của miền $M := \{z \in \mathbb{C} \mid |z| \leq r\}$.

Rõ ràng $p(z) = a_n z^n$ có n nghiệm phức (thực ra $p(z)$ có một nghiệm $z = 0$ với bội n).

Do đó, theo định lý Rouché, $f(z) = p(z) + h(z)$ có n nghiệm phức.

Định lý 4.

i) Nếu $z = a + bi$ là một nghiệm phức của đa thức $f(x) \in \mathbb{R}[x]$ thì liên hợp của nó $\bar{z} = a - bi$ cũng là một nghiệm. Do đó đa thức thực

$$(x - z)(x - \bar{z}) = x^2 - 2ax + (a^2 + b^2)$$

là một nhân tử của $f(x)$.

ii) Nếu $a, b, c \in \mathbb{Q}$ và $a + b\sqrt{c}$ là một nghiệm vô tỷ của đa thức hữu tỷ $f(x) \in \mathbb{Q}[x]$, thì $a - b\sqrt{c}$ cũng là một nghiệm, và đa thức hữu tỷ

$$x^2 - 2ax + (a^2 - b^2c)$$

là một nhân tử của $f(x)$.

Chứng minh:

i) Xét đa thức $g(x) = x^2 - 2ax + a^2 + b^2 = (x - z)(x - \bar{z})$.

Theo thuật toán chia trong $\mathbb{R}[x]$, tồn tại các đa thức thực $q(x)$ và $r(x)$ sao cho:

$$f(x) = q(x)g(x) + r(x), \text{ trong đó } r(x) = 0 \text{ hoặc } \deg r(x) < 2.$$

Do đó $r(x) = r_0 + r_1x$ trong đó $r_0, r_1 \in \mathbb{R}$.

Khi đó $z = a + bi$ là một nghiệm của $f(x), g(x)$; do đó nó cũng là một nghiệm của $r(x)$, nên $0 = r_0 + r_1(a + bi)$.

Cho phần thực và phần ảo bằng nhau, ta có $r_0 + r_1a = 0$ và $r_1b = 0$.

Nhưng khi đó $r(\bar{z}) = r(a - bi) = r_0 + r_1(a - bi) = r_0 + r_1a - r_1bi = 0$.

Do $\bar{z}$ là một nghiệm của $r(x)$ và $g(x)$, nó phải là nghiệm của $f(x)$.

Nếu z là số phức và không phải là số thực, thì $b \neq 0$. Trong trường hợp này $r_1 = 0$ và $r_0 = 0$.

Vậy $g(x) \mid f(x)$ hay $g(x)$ là một nhân tử của $f(x)$.

ii). Xét đa thức

$$h(x) = x^2 - 2ax + (a^2 - b^2c) = (x - a - b\sqrt{c})(x - a + b\sqrt{c}).$$

Theo thuật toán chia trong $\mathbb{Q}[x]$, tồn tại các đa thức thực $q(x)$ và $r(x)$ sao cho:

$$f(x) = q(x)h(x) + r(x), \text{ trong đó } r(x) = 0 \text{ hoặc } \deg r(x) < 2.$$

Do đó $r(x) = r_0 + r_1x$ trong đó $r_0, r_1 \in \mathbb{R}$.

Khi đó $a + b\sqrt{c}$ là một nghiệm của $f(x), h(x)$; do đó nó cũng là một nghiệm của $r(x)$, nên $0 = r_0 + r_1(a + b\sqrt{c})$. Cho $r_0 + r_1a = 0$ và $r_1b\sqrt{c} = 0$.

$$\text{Nhưng khi đó } r(a - b\sqrt{c}) = r_0 + r_1(a - b\sqrt{c}) = r_0 + r_1a - r_1b\sqrt{c} = 0.$$

Do $a - b\sqrt{c}$ là một nghiệm của $r(x)$ và $h(x)$, nên nó phải là nghiệm của $f(x)$.

Nếu a, b không đồng thời bằng 0 thì trong trường hợp này $r_1 = 0$ và $r_0 = 0$.

Vậy $h(x) \mid f(x)$ hay $h(x)$ là một nhân tử của $f(x)$.

Định lý 5. Các đa thức bất khả quy trong vành $\mathbb{C}[x]$ là các đa thức bậc 1.

Chứng minh:

Trong $\mathbb{C}[x]$, các đa thức bậc 0 là các phân tử khả nghịch.

Theo định lý 3, mỗi đa thức có bậc dương có một nghiệm trong $\mathbb{C}$.

Vậy tất cả các đa thức có bậc lớn hơn 1 khả quy và các đa thức bậc 1 là các đa thức bất khả quy trong vành $\mathbb{C}[x]$.

2.1.2 Phân tích đa thức trên trường số thực

Định lý 6. Các phân tử bất khả quy của miền nguyên $\mathbb{R}[x]$ chỉ là các đa thức bậc 1 có dạng $f(x) = ax + b$ ($a \neq 0$) hoặc bậc 2 có dạng $f(x) = ax^2 + bx + c$, (với $a \neq 0$) trong đó $b^2 - 4ac < 0$.

Chứng minh:

Hiển nhiên, nếu $f(x) \in \mathbb{R}[x]$ là đa thức bậc 1 hoặc tam thức bậc 2 với biệt thức $\Delta = b^2 - 4ac < 0$ thì $f(x)$ là bất khả quy trên $\mathbb{R}$. Ta chứng minh điều ngược lại.

Giả sử $f(x) \in \mathbb{R}[x]$ là một đa thức bất khả quy với $\deg f(x) \geq 1$.

- Trường hợp 1: $\deg f(x) = 1$ thì $f(x) = ax + b$ với $a \neq 0$.

- Trường hợp 2: $\deg f(x) = 2$, khi đó $f(x) = ax^2 + bx + c$ với $a \neq 0$.

Nếu $\Delta = b^2 - 4ac \geq 0$ thì $f(x)$ có hai nghiệm $\alpha_1, \alpha_2 \in \mathbb{R}$ và ta có

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \text{ (mâu thuẫn).}$$

Vậy $b^2 - 4ac < 0$.

- Trường hợp 3: $\deg f(x) > 2$.

Theo định lý 3 thì $f(x) = 0$ có nghiệm $\alpha = m + ni \in \mathbb{C}$.

Theo định lý 4 thì $f(x) = 0$ cũng có nghiệm $\bar{\alpha} = m - ni \in \mathbb{C}$.

Do đó trong $\mathbb{C}[x]$,

$f(x) = a(x - \alpha)(x - \bar{\alpha}) = a(x^2 - 2mx + m^2 + n^2) \in \mathbb{R}[x]$ hay $f(x)$ là khả quy (mâu thuẫn).

Vậy $f(x) \in \mathbb{R}[x]$ là một đa thức bất khả quy khi và chỉ khi hoặc $f(x) = ax + b$ ($a \neq 0$) hoặc $f(x) = ax^2 + bx + c$, (với $a \neq 0$) trong đó $b^2 - 4ac < 0$.

Định lý 7. Mọi đa thức $f(x) \in \mathbb{R}[x]$ khác 0 với bậc $f = n$ có dạng nhân tử hóa duy nhất

$$f(x) = a(x - b_1)^{n_1} \dots (x - b_s)^{n_s} (x^2 + c_1x + d_1)^{m_1} \dots (x^2 + c_tx + d_t)^{m_t}$$

trong đó $a \in \mathbb{R}^*$, các số thực $b_1, \dots, b_s$ phân biệt nhau, các đôi số thực $(c_1, d_1), \dots, (c_t, d_t)$ phân biệt nhau và sao cho $c_i^2 - 4d_i < 0$ ($i = 1, \dots, t$), còn $n_1, \dots, n_s$ và $m_1, \dots, m_t$ là những số nguyên ≥ 0 sao cho

$$n_1 + \dots + n_s + 2(m_1 + \dots + m_t) = n.$$

Chứng minh:

Ta biết rằng $\mathbb{R}[x]$ là một vành Euclide, nên $f(x)$ có thể phân tích được thành tích các nhân tử bất khả quy trong $\mathbb{R}[x]$.

Bằng cách viết $\alpha x + \beta = \alpha \left(x + \frac{\beta}{\alpha} \right)$ và $\alpha x^2 + \beta x + \gamma = \alpha \left(x^2 + \frac{\beta}{\alpha}x + \frac{\gamma}{\alpha} \right)$.

Khi đó ta có thể quy $f(x)$ về tích

$$f(x) = a(x - b_1)^{n_1} \dots (x - b_s)^{n_s} (x^2 + c_1x + d_1)^{m_1} \dots (x^2 + c_tx + d_t)^{m_t}$$

trong đó $b_1, \dots, b_s$ phân biệt nhau và $c_i^2 - 4d_i < 0$ ($i=1, \dots, t$), cùng với $(c_1, d_1), \dots, (c_t, d_t)$ phân biệt nhau.

Ta thấy ngay sự phân tích này là duy nhất. (đpcm)

2.1.3 Bài tập vận dụng.

Bài tập 1. Trong vành $\mathbb{C}[x]$, chứng minh rằng đa thức $f(x)$ chia hết cho đa thức $g(x)$ khi và chỉ khi mọi nghiệm của $g(x)$ cũng là nghiệm của $f(x)$ và mọi nghiệm bội k của $g(x)$ cũng là nghiệm bội lớn hơn hoặc bằng k của $f(x)$.

Giải: Trong $\mathbb{C}[x]$, giả sử $f(x)$ chia hết cho $g(x)$.

Khi đó $\exists q(x) \in \mathbb{C}[x]$ sao cho $f(x) = g(x) \cdot q(x)$.

Giả sử $\alpha \in \mathbb{C}$ là một nghiệm của $g(x)$, từ $g(\alpha) = 0$ suy ra $f(\alpha) = 0$.

Nếu α là nghiệm bội cấp $k \geq 1$ của $g(x)$ thì ta có $\exists h(x) \in \mathbb{C}[x]$ sao cho $g(x) = (x - \alpha)^k h(x)$.

Khi đó $f(x) = (x - \alpha)^k \cdot h(x) \cdot q(x)$, tức là α là nghiệm bội lớn hơn hoặc bằng k của $f(x)$.

Ngược lại, nếu mọi nghiệm bội cấp $k_i \geq 1$ của $g(x)$ đều là nghiệm bội với cấp lớn hơn hoặc bằng k_i của $f(x)$ thì ta có:

$$\begin{aligned} g(x) &= a(x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} \dots (x - \alpha_n)^{k_n}, \\ f(x) &= b(x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} \dots (x - \alpha_n)^{k_n} q(x). \end{aligned}$$

Điều này chứng tỏ $f(x) = ba^{-1}g(x)q(x)$.

Vậy $f(x)$ chia hết cho $g(x)$.

Bài tập 2. Trong vành $\mathbb{Q}[x]$, chứng minh rằng đa thức:

$$f(x) = x^{3k} + x^{3l+1} + x^{3n+2} \quad (k, l, n \in \mathbb{N})$$

chia hết cho đa thức $g(x) = x^2 + x + 1$.

Giải: Ta có phương trình $x^2 + x + 1 = 0$ có 2 nghiệm là:

$$x_1 = \frac{-1}{2} + \frac{\sqrt{3}}{2}i; \quad x_2 = \frac{-1}{2} - \frac{\sqrt{3}}{2}i.$$

Ta thấy đa thức $g(x) = x^2 + x + 1$ là một đa thức bậc hai không có nghiệm hữu tỷ nên nó là đa thức bất khả quy trên $\mathbb{Q}[x]$.

Lại có: $x^3 - 1 = (x - 1)(x^2 + x + 1) = (x - 1)g(x)$, nên $g(x)$ có 2 nghiệm phức là $\varepsilon = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$; $\varepsilon^2 = \frac{-1}{2} - \frac{\sqrt{3}}{2}i$, là 2 căn nguyên thủy bậc ba của đơn vị.

Mặt khác ta có:

$$\begin{aligned} f\left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right) &= \left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)^{3k} + \left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)^{3l+1} + \left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)^{3n+2} \\ &= \left(\left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)^3\right)^k + \left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right) \cdot \left(\left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)^3\right)^l + \left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)^2 \cdot \left(\left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)^3\right)^n \\ &= 1^k + \left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right) \cdot 1^l + \left(\frac{-1}{2} + \frac{\sqrt{3}}{2}i\right)^2 \cdot 1^n \\ &= 1 + \frac{-1}{2} + \frac{\sqrt{3}}{2}i + \frac{-1}{2} - \frac{\sqrt{3}}{2}i = 0. \end{aligned}$$

Khi đó ta có thể nói $f(x) = x^{3k} + x^{3l+1} + x^{3n+2}$ cũng nhận ε và ε^2 làm nghiệm.

Theo bài tập 1, $\exists h(x) \in \mathbb{C}[x]$ sao cho $f(x) = g(x)h(x)$.

Nhưng $f(x)$ và $g(x) \in \mathbb{Q}[x]$ nên suy ra $h(x) \in \mathbb{Q}[x]$.

Vậy đa thức $f(x)$ chia hết cho đa thức $g(x)$.

Bài tập 3. Giả sử K là một trường, $f(x)$ và $g(x)$ là hai đa thức nguyên tố cùng nhau trong $K[x]$. Chứng minh rằng $yf(x) + g(x)$ là một đa thức bất khả quy trong $K[x, y]$.

Giải: Ta có K là một trường, $f(x)$ và $g(x)$ là hai đa thức nguyên tố cùng nhau.

Nên nếu xem $yf(x) + g(x)$ như một đa thức bậc nhất một ẩn đối với y thì $yf(x) + g(x)$ là đa thức nguyên bản, hay đa thức bất khả quy trên $K[x]$.

Suy ra $yf(x) + g(x)$ bất khả quy trong $K[x, y] = K[x][y]$.

Bài tập 4. Phân tích các đa thức sau thành nhân tử:

$$a, f(x, y) = 2x^4 + 7x^3y + 9x^2y^2 + 7xy^3 + 2y^4;$$

$$b, h(x, y) = 3x^4 - 8x^3y + 14x^2y^2 - 8xy^3 + 3y^4;$$

$$c, p(x, y, z) = 2x^2y^2 + 2y^2z^2 + 2z^2x^2 - x^4 - y^4 - z^4.$$

Giải:

$$\begin{aligned} a, f(x, y) &= 2x^4 + 7x^3y + 9x^2y^2 + 7xy^3 + 2y^4 \\ &= 2(x^4 + y^4) + 7xy(x^2 + y^2) + 9x^2y^2 \quad (*) \end{aligned}$$

Ta biểu diễn $f(x, y)$ qua đa thức đối xứng.

$$\text{Ta có: } x^4 + y^4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2$$

$$x^2 + y^2 = \sigma_1^2 - 2\sigma_2$$

Thay các kết quả vào (*) ta được:

$$\begin{aligned} f(x, y) &= 2(\sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2) + 7\sigma_2(\sigma_1^2 - 2\sigma_2) + 9\sigma_2^2 \\ &= 2\sigma_1^4 - \sigma_1^2\sigma_2 - \sigma_2^2 \end{aligned}$$

Ta có $f(x, y) = 2\sigma_1^4 - \sigma_1^2\sigma_2 - \sigma_2^2$ là tam thức bậc 2 theo σ_2 , suy ra $\sigma_2 = -2\sigma_1^2, \sigma_2 = \sigma_1^2$.

$$\begin{aligned} \text{Vậy } f(x, y) &= (2\sigma_1^2 + \sigma_2)(\sigma_1^2 - \sigma_2) \\ &= (2x^2 + 2y^2 + 5xy)(x^2 + y^2 + xy). \end{aligned}$$

$$\begin{aligned} b, h(x, y) &= 3x^4 - 8x^3y + 14x^2y^2 - 8xy^3 + 3y^4 \\ &= 3(x^4 + y^4) - 8xy(x^2 + y^2) + 14x^2y^2 \quad (*) \end{aligned}$$

Ta biểu diễn $h(x, y)$ qua đa thức đối xứng.

$$\text{Ta có: } x^4 + y^4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2$$

$$x^2 + y^2 = \sigma_1^2 - 2\sigma_2$$

Thay các kết quả trên vào (*) ta được:

$$\begin{aligned} h(x, y) &= 3(\sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2) - 8\sigma_2(\sigma_1^2 - 2\sigma_2) + 14\sigma_2^2 \\ &= 3\sigma_1^4 - 20\sigma_1^2\sigma_2 + 36\sigma_2^2 \end{aligned}$$

Ta có $h(x, y) = 3\sigma_1^4 - 20\sigma_1^2\sigma_2 + 36\sigma_2^2$ là tam thức bậc 2 theo σ_2 mà không có nghiệm thực. Do đó ta không thể phân tích thành nhị thức theo σ_2 .

Ta sử dụng hệ số bất định để phân tích. Ta có:

$$\begin{aligned} h(x, y) &= 3x^4 - 8x^3y + 14x^2y^2 - 8xy^3 + 3y^4 \\ &= (Ax^2 + Bxy + Cy^2)(Cx^2 + Bxy + Ay^2) \quad (**) \end{aligned}$$

Tìm A, B, C bằng cách sử dụng hệ số bất định.

$$\text{Với } x = y = 1, (A + B + C)^2 = 4 \Rightarrow A + B + C = \pm 2 \quad (1)$$

Nhận xét: Đẳng thức (**) không thay đổi khi ta thay đổi dấu của các hệ số A, B, C thành ngược lại. Để không mất tính tổng quát, ta cho $A + B + C = 2$.

$$\text{Với } x = 1, y = -1, (A - B + C)^2 = 36 \Rightarrow A - B + C = \pm 6 \quad (2)$$

$$\text{Với } x = 0, y = 1, AC = 3 \quad (3)$$

Từ (1), (2) và (3) ta có các hệ:

$$(I) \begin{cases} A + B + C = 2 \\ A - B + C = 6 \\ AC = 3 \end{cases} \quad \text{và} \quad (II) \begin{cases} A + B + C = 2 \\ A - B + C = -6 \\ AC = 3 \end{cases}$$

Hệ (I) cho ta nghiệm $A = 1, B = -2, C = 3$.

Hệ (II) không có nghiệm thực.

Vậy

$$h(x, y) = 3x^4 - 8x^3y + 14x^2y^2 - 8xy^3 + 3y^4 = (x^2 - 2xy + 3y^3)(3x^2 - 2xy + y^2)$$

$$\begin{aligned} c, p(x, y, z) &= 2x^2y^2 + 2y^2z^2 + 2z^2x^2 - x^4 - y^4 - z^4 \\ &= 2[(xy + yz + xz)^2 - 2xyz(x + y + z)] - (x^4 + y^4 + z^4) \end{aligned}$$

Ta biểu diễn $p(x, y)$ qua đa thức đối xứng.

$$\begin{aligned} p(x, y, z) &= 2(\sigma_2^2 - 2\sigma_1\sigma_3) - (\sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3) \\ &= -\sigma_1^4 + 4\sigma_1^2\sigma_2 - 8\sigma_1\sigma_3 \\ &= \sigma_1(-\sigma_1^3 + 4\sigma_1\sigma_2 - 8\sigma_3) \quad (*) \end{aligned}$$

Nhận thấy (*) chia hết cho $\sigma_1 = x + y + z$ và đa thức ban đầu là hàm số chẵn theo x, y, z . Do đó ta thay $x = -x$ (hoặc $y = -y$ hoặc $z = -z$) thì đa thức sẽ không đổi.

Do đó đa thức chia hết cho $x + y - z, -x + y + z, x - y + z$.

Khi đó $p(x, y, z) = (x + y + z)(x + y - z)(-x + y + z)(x - y + z) \cdot M$

Do $p(x)$ là đa thức bậc 4 nên M phải là hằng số. Sử dụng hệ số bất định, tìm M :

Cho $x = y = z = 1 \Rightarrow M = 1$.

Vậy $p(x, y, z) = (x + y + z)(x + y - z)(-x + y + z)(x - y + z)$.

Bài tập 5. Chứng minh rằng vành thương $\mathbb{Z}_2[x]/(\bar{1} + x + x^2)$ là một trường có 4 phần tử; lập bảng cộng và bảng nhân của trường này.

Giải: Đa thức $\bar{1} + x + x^2 \in \mathbb{Z}_2[x]$ không có nghiệm trong $\mathbb{Z}_2$ nên bất khả quy.

Do đó vành thương $\mathbb{Z}_2[x]/(\bar{1} + x + x^2)$ là một trường đẳng cấu với trường $\mathbb{Z}_2(u)$, với $\bar{1} + u + u^2 = 0$, và trường này có 4 phần tử là $\bar{0}, \bar{1}, u, \bar{1} + u$.

Lập bảng:

(+)	$\bar{0}$	$\bar{1}$	u	$\bar{1} + u$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{0} + u$	$\bar{1} + u$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{1} + u$	$\bar{0} + u$
u	$\bar{0} + u$	$\bar{1} + u$	$2u$	$\bar{1} + 2u$
$\bar{1} + u$	$\bar{1} + u$	$\bar{0} + u$	$\bar{1} + 2u$	$\bar{0} + 2u$

(x)	$\bar{0}$	$\bar{1}$	u	$\bar{1} + u$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{1}u$	$\bar{1} + \bar{1}u$
u	$\bar{0}$	$\bar{1}u$	u^2	$\bar{1}u + u^2$
$\bar{1} + u$	$\bar{0}$	$\bar{1} + \bar{1}u$	$\bar{1}u + u^2$	$\bar{1} + u^2$

Bài tập 6. Tìm dạng nhân tử hóa của đa thức trong $\mathbb{R}[x]$:

$$f(x) = 1 + x + 3x^2 + 2x^3 + 3x^4 + x^5 + x^6$$

Giải: Ta thấy $x = 0$ không là nghiệm của phương trình $f(x) = 0$ (1), nên ta chia cả 2 vế của phương trình (1) cho x^3 , phương trình trở thành:

$$\begin{aligned}
 & \frac{1}{x^3} + \frac{1}{x^2} + \frac{3}{x} + 2 + 3x + x^2 + x^3 = 0 \\
 \Leftrightarrow & \left(x^3 + \frac{1}{x^3}\right) + \left(x^2 + \frac{1}{x^2}\right) + 3\left(x + \frac{1}{x}\right) + 2 = 0 \\
 \Leftrightarrow & \left(x + \frac{1}{x}\right)^3 - 3\left(x + \frac{1}{x}\right) + \left(x + \frac{1}{x}\right)^2 - 2 + 3\left(x + \frac{1}{x}\right) + 2 = 0 \\
 \Leftrightarrow & \left(x + \frac{1}{x}\right)^3 + \left(x + \frac{1}{x}\right)^2 = 0 \\
 \Leftrightarrow & \left(x + \frac{1}{x}\right)^2 \left(x + \frac{1}{x} + 1\right) = 0.
 \end{aligned}$$

Bài tập 7. Biết rằng đa thức có hệ số phức sau đây

$$f(x) = 1 - 3i + 9ix - (5 + 6i)x^2 + 2x^3$$

có một nghiệm số thực. Tìm dạng nhân tử hóa của $f(x)$ trong $\mathbb{C}[x]$.

Giải: Dễ dàng kiểm tra $f(x)$ có một nghiệm số thực là $x = \frac{1}{2}$.

- Dùng Hoocne:

	2	$-(5 + 6i)$	$9i$	$-3i + 1$
$x = \frac{1}{2}$	2	$-4 - 6i$	$-2 + 6i$	0

Suy ra $f(x) = 2\left(x - \frac{1}{2}\right)(x^2 - (2 + 3i)x - 1 + 3i)$.

- Xét $g(x) = x^2 - (2 + 3i)x - 1 + 3i$

Lập $\Delta = [-(2 + 3i)]^2 - 4(-1 + 3i) = -1 = i^2$.

Khi đó $g(x)$ có 2 nghiệm là $\begin{cases} x_1 = 1 + 2i \\ x_2 = 1 + i \end{cases}$

Vậy dạng nhân tử hóa của $f(x)$ trong $\mathbb{C}[x]$ là:

$$f(x) = 2\left(x - \frac{1}{2}\right)(x - 1 - 2i)(x - 1 - i).$$

Bài tập 8. Tìm dạng nhân tử hóa của các đa thức sau đây trong $\mathbb{C}[x]$:

a) $1 + i + x + x^2$;

b) $1 + x - x^3 - x^4$;

c) $x^2 + i$;

$$d) x^2 - 4i + 3;$$

$$e) x^5 + 1.$$

Giải:

$$\begin{aligned} a) 1+i+x+x^2 &= (1+x^2)+(i+x) = (x-i)(x+i)+(i+x) \\ &= (x+i)(x+1-i). \end{aligned}$$

$$\begin{aligned} b) 1+x-x^3-x^4 &= (x+1)-x^3(x+1) = (x+1)(1-x^3) \\ &= (x+1)(1-x)(x^2+x+1) = (x+1)(x-1)\left(x+\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\left(x+\frac{1}{2}-\frac{\sqrt{3}}{2}i\right). \end{aligned}$$

$$\begin{aligned} c) x^2+i &= x^2-(-i) = x^2-\frac{1}{2}(-2i) = x^2-\frac{1}{2}(1-i)^2 \\ &= x^2-\left(\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i\right)^2 = \left(x-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right)\left(x+\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i\right). \end{aligned}$$

$$\begin{aligned} d) x^2-4i+3 &= x^2-(-4+4i+1) = x^2-\left[(2i)^2+4i+1\right] \\ &= x^2-(2i+1)^2 = (x-2i-1)(x+2i+1). \end{aligned}$$

$$e) x^5+1 = (x+1)(x^4-x^3+x^2-x+1)$$

$$\text{Xét } f(x) = x^4 - x^3 + x^2 - x + 1$$

Ta thấy $x=0$ không là nghiệm của $f(x)=0$, nên ta chia cả 2 vế của phương trình cho x^2 , ta được phương trình sau:

$$\begin{aligned} x^2-x+1-\frac{1}{x}+\frac{1}{x^2} &= 0 \quad \Leftrightarrow \left(x^2+\frac{1}{x^2}\right)-\left(x+\frac{1}{x}\right)+1=0 \\ \Leftrightarrow \left(x+\frac{1}{x}\right)^2-2-\left(x+\frac{1}{x}\right)+1 &= 0 \Leftrightarrow \left(x+\frac{1}{x}\right)^2-\left(x+\frac{1}{x}\right)-1=0 \\ \Leftrightarrow \begin{cases} x+\frac{1}{x} = \frac{1+\sqrt{5}}{2} \\ x+\frac{1}{x} = \frac{1-\sqrt{5}}{2} \end{cases} \end{aligned}$$

$$\text{Vậy } x^5+1 = (x+1)\left(x^2-\frac{1+\sqrt{5}}{2}x+1\right)\left(x^2-\frac{1-\sqrt{5}}{2}x+1\right).$$

Bài tập 9. Tìm dạng nhân tử hóa của các đa thức sau đây trong $\mathbb{R}[x]$:

a, $x^4 + 16$;

b, $1 + x^8$;

c, $1 + x^4 + x^8$;

d, $1 + 4x + 8x^2 + 4x^3 + x^4$.

Giải:

a, $x^4 + 16 = x^4 + 8x^2 + 16 - 8x^2$

$$= (x^2 + 4)^2 - 8x^2$$

$$= (x^2 - 2\sqrt{2}x + 4)(x^2 + 2\sqrt{2}x + 4).$$

b, $1 + x^8 = 1 + 2x^4 + x^8 - 2x^4 = (1 + x^4)^2 - 2x^4$

$$= (1 - x^2\sqrt{2} + x^4)(1 + x^2\sqrt{2} + x^4).$$

c, $1 + x^4 + x^8 = 1 + 2x^4 + x^8 - x^4 = (1 + x^4)^2 - x^4$

$$= (1 + x^2 + x^4)(1 - x^2 + x^4)$$

$$= (1 + 2x^2 + x^4 - x^2)(1 + 2x^2 + x^4 - 3x^2)$$

$$= \left[(1 + x^2)^2 - x^2 \right] \left[(1 + x^2)^2 - 3x^2 \right]$$

$$= (1 - x + x^2)(1 + x + x^2)(1 - x\sqrt{3} + x^2)(1 + x\sqrt{3} + x^2).$$

d, Giả sử

$$1 + 4x + 8x^2 + 4x^3 + x^4 = (x^2 + Ax + B)(x^2 + Cx + D)$$

$$= x^4 + (A + C)x^3 + (D + AC + B)x^2 + (AD + BC)x + BD(*)$$

(với

$$0 \neq A, B, C, D \in \mathbb{R})$$

Khi đó ta có:

$$\begin{cases} A + C = 4 \\ D + AC + B = 8 \\ AD + BC = 4 \\ BD = 1 \end{cases} \Leftrightarrow \begin{cases} C = 4 - A & (1) \\ \frac{1}{B} + A(4 - A) + B = 8 & (2) \\ \frac{A}{B} + B(4 - A) = 4 & (3) \\ D = \frac{1}{B} & (4) \end{cases}$$

Giải phương trình (2), ta được:

$$\frac{1}{B} + A(4 - A) + B = 8 \Leftrightarrow 1 + AB(4 - B) + B^2 - 8B = 0 \quad (5)$$

Giải phương trình (3), ta được:

$$\begin{aligned} \frac{A}{B} + B(4 - A) = 4 &\Leftrightarrow A + B^2(4 - A) - 4B = 0 \\ &\Leftrightarrow A + 4B^2 - AB^2 - 4B = 0 \\ &\Leftrightarrow A(1 - B^2) - 4B(1 - B) = 0 \end{aligned} \quad (6)$$

Dễ dàng kiểm tra được $B = 1$ không phải là nghiệm của hệ phương trình.

Với $B \neq 1$ ta được:

$$\begin{aligned} (6) &\Leftrightarrow A(1 + B) - 4B = 0 \\ &\Leftrightarrow A = \frac{4B}{1 + B} \quad (B \neq -1) \end{aligned} \quad (7)$$

Thay (7) vào (5) ta được:

$$\begin{aligned}
 & 1 + \frac{16B^2}{1+B} - \frac{16B^3}{(1+B)^2} + B^2 - 8B = 0 \\
 \Leftrightarrow & (1+B)^2 + 16B^2(1+B) - 16B^3 + B^2(1+B)^2 - 8B(1+B)^2 = 0 \\
 \Leftrightarrow & 1 + 2B + B^2 + 16B^2 + 16B^3 - 16B^3 + B^2 + 2B^3 + B^4 - 8B - 16B^2 - 8B^3 = 0 \\
 \Leftrightarrow & B^4 - 6B^3 + 2B^2 - 6B + 1 = 0 \\
 \Leftrightarrow & B^2 \left(B^2 - 6B + 2 - \frac{6}{B} + \frac{1}{B^2} \right) = 0 \\
 \Leftrightarrow & \left(B^2 + \frac{1}{B^2} \right) - 6 \left(B + \frac{1}{B} \right) + 2 = 0 \quad (B \neq 0) \\
 \Leftrightarrow & \left(B + \frac{1}{B} \right)^2 - 6 \left(B + \frac{1}{B} \right) = 0 \\
 \Leftrightarrow & \left(B + \frac{1}{B} \right) \left(B + \frac{1}{B} - 6 \right) = 0 \\
 \Leftrightarrow & \begin{cases} B + \frac{1}{B} = 0 \\ B + \frac{1}{B} - 6 = 0 \end{cases} \Leftrightarrow \begin{cases} B^2 + 1 = 0 & (\text{VN}) \\ B^2 - 6B + 1 = 0 \end{cases} \Leftrightarrow \begin{cases} B = 3 + 2\sqrt{2} \\ B = 3 - 2\sqrt{2} \end{cases}
 \end{aligned}$$

Suy ra ta có các bộ nghiệm sau:

$$\begin{cases} A = 2 + \sqrt{2} \\ B = 3 + 2\sqrt{2} \\ C = 2 - \sqrt{2} \\ D = 3 - 2\sqrt{2} \end{cases} \quad \text{hoặc} \quad \begin{cases} A = 2 + \sqrt{2} \\ B = 3 - 2\sqrt{2} \\ C = 2 + \sqrt{2} \\ D = 3 + 2\sqrt{2} \end{cases}$$

Nhận xét: Đẳng thức (*) không thay đổi khi ta thay đổi vị trí của A và C; B và D.

Vậy $1 + 4x + 8x^2 + 4x^3 + x^4 = \left[x^2 + (2 + \sqrt{2})x + 3 + 2\sqrt{2} \right] \left[x^2 + (2 - \sqrt{2})x + 3 - 2\sqrt{2} \right]$.

2.2 Phân tích các đa thức nguyên và các đa thức hữu tỷ

2.2.1 Đa thức hệ số nguyên

Định nghĩa. Nếu đa thức $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $a_n \neq 0$ có các hệ số $a_i \in \mathbb{Z}$, $i = \overline{0, n}$ thì ta nói $f(x)$ là đa thức hệ số nguyên.

Ta kí hiệu tập hợp các đa thức hệ số nguyên là $\mathbb{Z}[x]$.

Định lý 8. Nếu đa thức $f(x)$ có nghiệm nguyên $x = \alpha$ thì $f(x) = (x - \alpha)g(x)$ với $g(x)$ là đa thức hệ số nguyên.

Định lý 9. Cho $f(x)$ là đa thức hệ số nguyên:

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (a_i \in \mathbb{Z}; i = \overline{0, n})$, a, b là hai số nguyên khác nhau. Khi đó: $f(a) - f(b) : (a - b)$.

Chứng minh:

Ta có:
$$f(a) = a_n a^n + a_{n-1} a^{n-1} + \dots + a_1 a + a_0$$

$$f(b) = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0$$

Suy ra $f(a) - f(b) = a_n (a^n - b^n) + a_{n-1} (a^{n-1} - b^{n-1}) + \dots + a_1 (a - b)$

Mặt khác, $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \dots + b^{k-1}) : (a - b)$ (với $\forall k \in \mathbb{N}$)

Nên $f(a) - f(b) : (a - b)$ (đpcm).

2.2.2 Đa thức hệ số hữu tỷ

Định lý 10. Cho đa thức hệ số nguyên

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x].$$

Nếu $x = \frac{p}{q}$, với $\text{UCLN}(p, q) = 1$, $q \neq 0$ là nghiệm hữu tỷ của $f(x)$ thì $p \mid a_0$

và $q \mid a_n$.

Chứng minh:

Giả sử phân số tối giản $\frac{p}{q}$ là nghiệm của đa thức $f(x)$. Khi đó ta có:

$$\begin{aligned} f\left(\frac{p}{q}\right) = 0 &\Leftrightarrow a_n \cdot \frac{p^n}{q^n} + a_{n-1} \cdot \frac{p^{n-1}}{q^{n-1}} + \dots + a_1 \cdot \frac{p}{q} + a_0 = 0 \\ &\Leftrightarrow a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0 \end{aligned} \quad (1)$$

Từ (1) ta có:

$$a_n p^n = -q(a_{n-1} p^{n-1} + \dots + a_1 p q^{n-2} + a_0 q^{n-1}) \quad (2)$$

và $a_0 q^n = -p(a_n p^{n-1} + a_{n-1} p^{n-2} q + \dots + a_1 q^{n-1}) \quad (3)$

Từ (2) suy ra $a_n p^n : q$ mà $(p^n, q) = 1$ nên $a_n : q$.

Từ (3) suy ra $a_0 q^n : p$ mà $(p^n, q) = 1$ nên $a_0 : p$. (đpcm)

Ví dụ: Phân tích $f(x) = 2x^3 + 3x^2 - 1$ trong $\mathbb{Q}[x]$.

Giải: Nếu $f\left(\frac{p}{q}\right) = 0$ thì $p \mid (-1)$ và $q \mid 2$.

Do đó $p = \pm 1$ và $q = \pm 1$ hoặc ± 2 . Khi đó $\frac{p}{q} \in \left\{ \pm 1; \pm \frac{1}{2} \right\}$

Do $f(1) = 4$, $f(-1) = 0$ nên $f(x) \vdots x+1$.

Thực hiện phép chia ta được $f(x) = (x+1)(2x^2 + x - 1)$

Tam thức bậc hai $2x^2 + x - 1$ có hai nghiệm là $x = -1$ và $x = \frac{1}{2}$ nên ta có:

$$f(x) = (x+1)^2 (2x-1).$$

Trong định lý trên nếu $a_n = 1$ ta có hệ quả sau:

Hệ quả 1. Cho đa thức $p(x) \in \mathbb{Z}[x]$ với hệ tử cao nhất bằng 1. Khi đó nghiệm hữu tỷ (nếu có) của $f(x)$ là nghiệm nguyên và hệ số nguyên này là ước của số hạng tự do.

Định lý 11. Nếu phân số tối giản $\frac{p}{q}$ là nghiệm của đa thức

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x] \text{ và } m \in \mathbb{Z} \text{ thì } p - mq \mid f(m).$$

Chứng minh: Giả sử $\frac{p}{q}$ là nghiệm của $f(x)$, tức là $f\left(\frac{p}{q}\right) = 0$.

Giá trị $f(x)$ tại $x = m$ là:

$$\begin{aligned} f(m) &= a_n m^n + a_{n-1} m^{n-1} + \dots + a_1 m + a_0 - f\left(\frac{p}{q}\right) \\ &= a_n \left(m^n - \frac{p^n}{q^n} \right) + a_{n-1} \left(\frac{m^{n-1} q^{n-1} - p^{n-1}}{q^{n-1}} \right) + \dots + a_1 \left(\frac{mq - p}{q} \right) \\ &= (mq - p) \left(a_n \frac{A_n}{q^n} + \frac{a_{n-1} A_{n-1}}{q^{n-1}} + \dots + \frac{a_1}{q} \right) \end{aligned}$$

$$\Rightarrow q^n \cdot f(m) = (mq - p) \cdot A \quad (*)$$

Do $(p, q) = 1$ nên $(mq - p, q) = 1 \Rightarrow (mq - p, q^n) = 1$.

Từ (*) suy ra $f(m) \vdots mq - p$ hay $p - mq \mid f(m)$ (đpcm).

Định lý 12. (Bổ đề Gauss). Cho đa thức với hệ số nguyên

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x].$$

Nếu $f(x)$ có thể phân tích được trong $\mathbb{Q}[x]$ thành $f(x) = g(x)h(x)$ với $g(x), h(x) \in \mathbb{Q}[x]$ thì $f(x)$ cũng phân tích được trong $\mathbb{Z}[x]$.

Một cách tương đương, nếu đa thức $f(x) \in \mathbb{Z}[x]$, bậc $n > 1$, bất khả quy trên $\mathbb{Z}$ thì cũng bất khả quy trên $\mathbb{Q}$.

Chứng minh:

* **Nhận xét:** Một đa thức $f(x) \in \mathbb{Q}[x]$ luôn luôn viết được dưới dạng tích của một phân số tối giản và một đa thức có các hệ số nguyên tố cùng nhau. Một đa thức như vậy được gọi là đa thức nguyên bản.

Thật vậy, giả sử:

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \dots + \frac{a_n}{b_n}x^n, \quad a_i, b_i \in \mathbb{Z} \text{ trong đó các hệ số hữu tỷ của } f(x) \text{ ở}$$

dạng phân số tối giản.

Đặt $q = b_0 b_1 \dots b_n$ ta có $f(x) = \frac{1}{q} g(x)$, $g(x) \in \mathbb{Z}[x]$.

Gọi p là ước chung lớn nhất của các hệ tử của $g(x)$ ta được $g(x) = pf^*(x)$,
với $f^*(x)$ là đa thức nguyên bản. Từ đó $f(x) = \frac{p}{q} f^*(x)$.

Giả sử $f(x) = g(x)h(x)$ là sự phân tích trong $\mathbb{Q}[x]$. Theo nhận xét trên ta có:

$$f = \frac{s}{u} g^*(x) \frac{t}{v} h^*(x) = \frac{st}{uv} g^*(x) h^*(x), \text{ trong đó } g^*(x), h^*(x) \text{ là những đa thức}$$

nguyên bản.

Để chứng minh định lý, ta chứng minh rằng $uv \mid st$ bằng cách chứng minh rằng không có ước nguyên tố p của uv có thể chia hết cho mọi hệ số của $g^*(x)h^*(x)$.

Thật vậy, giả sử

$$\begin{aligned} g^*(x) &= b_0 + \dots + b_k x^k, \\ h^*(x) &= c_0 + \dots + c_l x^l. \end{aligned}$$

Chọn một ước nguyên tố p của uv . Do $g^*(x)h^*(x)$ là nguyên bản nên phải có những hệ số đầu tiên b_r, c_s không chia hết cho p . Hệ số của x^{r+s} của tích $g^*(x)h^*(x)$ là

$$(b_0 c_{r+s} + \dots + b_{r-1} c_{s+1}) + b_r c_s + (b_{r+1} c_{r-1} + \dots + b_{r+s} c_0).$$

Các tổng ở hai dấu ngoặc đều chia hết cho p , nhưng $b_r c_s$ không chia hết cho p nên hệ số của x^{r+s} không chia hết cho p . Điều này chứng tỏ p không là ước chung của các hệ số của tích $g^*(x)h^*(x)$. Bởi vậy, p phải là ước của st .

Suy ra $uv \mid st$, và do đó $f(x)$ phân tích được trong $\mathbb{Z}[x]$.

Mệnh đề 2. Một đa thức bậc 2:

$$ax^2 + bx + c \in \mathbb{Z}[x], \quad a \neq 0$$

với biệt số $b^2 - 4ac < 0$ là bất khả quy trong $\mathbb{Q}[x]$.

Chứng minh:

Thật vậy $ax^2 + bx + c \in \mathbb{Z}[x]$, $a \neq 0$ là khả quy trong $\mathbb{Q}[x]$ nếu và chỉ nếu nó có nghiệm số hữu tỷ, tức là có các số nguyên $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ sao cho

$$ax^2 + bx + c = (\alpha x + \beta)(\gamma x + \delta) = \alpha\gamma x^2 + (\alpha\delta + \beta\gamma)x + \beta\delta.$$

$$\text{Khi đó, } b^2 - 4ac = (\alpha\delta + \beta\gamma)^2 - 4\alpha\gamma\beta\delta = (\alpha\delta - \beta\gamma)^2 \geq 0.$$

Đối với những đa thức có hệ số nguyên với bậc $n > 1$ bất kì, trong một số trường hợp, ta có thể sử dụng tiêu chuẩn bất khả quy trong $\mathbb{Q}[x]$ sau đây, gọi là *Tiêu chuẩn Eisenstein*.

Định lý 13. (Tiêu chuẩn Eisenstein). Đa thức với các hệ số nguyên $f(x) = a_0 + a_1x + \dots + a_nx^n$, ($n > 1$) là đa thức bất khả quy trong vành đa thức hệ số hữu tỷ $\mathbb{Q}[x]$ nếu tồn tại số nguyên tố p thỏa mãn đồng thời:

$$i) p \mid a_i \quad (i = 0, \overline{n-1})$$

$$ii) p \nmid a_n$$

$$iii) p^2 \nmid a_0$$

Chứng minh:

Giả sử $f(x)$ khả quy trên $\mathbb{Q}$. Khi đó theo định lý 12 nó cũng khả quy trên $\mathbb{Z}$,

$$f(x) = g(x)h(x)$$

$$g(x) = b_0 + b_1x + \dots + b_rx^r, \quad 0 < r < n, \quad b_i \in \mathbb{Z}$$

$$h(x) = c_0 + c_1x + \dots + c_sx^s, \quad 0 < s < n, \quad c_i \in \mathbb{Z}$$

Theo giả thiết, p chia hết cho $a_0 = b_0c_0$. Tuy nhiên, vì $p^2 \nmid a_0$ nên chỉ có một trong hai số b_0, c_0 chia hết cho p , chẳng hạn $b_0 \vdots p$.

Do p không chia hết cho $a_n = b_rc_s$ nên $p \nmid b_r$.

Giả sử b_k là hệ số đầu tiên của $g(x)$ không chia hết cho p . Khi đó từ đẳng thức $a_k = (b_0 c_k + b_1 c_{k-1} + \dots + b_{k-1} c_1) + b_k c_0$ ta suy ra $b_k c_0 \equiv p$ vì a_k và tổng trong dấu ngoặc chia hết cho p .

Vì $c_0 \not\equiv p$ nên $b_k \equiv p$, điều này trái với giả thiết về b_k .

Mệnh đề 3. (Tiêu chuẩn bất khả quy thu gọn). Cho p là một số nguyên tố và đa thức $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$, có đa thức $\bar{f}(x)$ tương ứng

$$\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \dots + \bar{a}_n x^n \in \mathbb{Z}_p[x]$$

sao cho $\bar{f}(x) \neq 0$ và bậc của $\bar{f}(x)$ bằng bậc của $f(x)$. Khi đó, nếu $\bar{f}(x)$ là đa thức bất khả quy trong $\mathbb{Z}_p[x]$ thì $f(x)$ bất khả quy trong $\mathbb{Q}[x]$.

Chứng minh:

Giả sử $f(x) = u(x)v(x)$, $u(x), v(x) \in \mathbb{Z}[x]$.

Khi đó $\bar{f}(x) = \bar{u}(x)\bar{v}(x)$, $\bar{u}(x), \bar{v}(x) \in \mathbb{Z}_p[x]$.

Do $\deg f = \deg \bar{f}$ nên $\deg u = \deg \bar{u}$ và $\deg v = \deg \bar{v}$.

Nếu $\bar{f}(x)$ bất khả quy trong $\mathbb{Z}_p[x]$ thì $\bar{u}(x)$ hoặc $\bar{v}(x)$ là phân tử khả nghịch trong $\mathbb{Z}_p[x]$, chẳng hạn $\bar{u}(x) \in \mathbb{Z}_p[x]$, $\bar{u}(x) \neq 0$.

Vì thế $\deg \bar{u}(x) = \deg u(x) = 0$, nghĩa là $u(x) \in \mathbb{Z}^*$ và khả nghịch trong $\mathbb{Q}$.

Vậy $f(x)$ bất khả quy trên $\mathbb{Q}$.

2.2.3 Bài tập vận dụng.

Bài tập 1. Nếu $\frac{r}{s}$ là một nghiệm hữu tỷ, ở dạng tối giản, của một đa thức $p(x)$ với hệ số nguyên, chứng minh rằng $p(x) = (sx - r)g(x)$ với một đa thức $g(x)$ nào đó với hệ số nguyên.

Giải: Do $\frac{r}{s}, (r, s) = 1$, là một nghiệm hữu tỷ của đa thức $p(x)$ với hệ số nguyên nên ta có: $p(x) = \left(x - \frac{r}{s}\right)q(x)$.

Giả sử $q(x) = b_{n-1}x^{n-1} + \dots + b_1x + b_0$ trong đó $b_i \in \mathbb{Q}$. Khi đó:

$$p(x) = \left(b_{n-2} + \frac{r}{s}b_{n-1}\right)x^{n-1} + \dots + \left(b_0 - \frac{r}{s}b_1\right)x + \frac{r}{s}b_0$$

Do $p(x)$ là các đa thức với hệ số nguyên nên ta có: $\frac{r}{s}b_0 \in \mathbb{Z}$.

Mà $(r, s) = 1$ nên $s \mid b_0$.

Lại do $b_0 - \frac{r}{s}b_1 \in \mathbb{Z}$, mà $b_0 \in \mathbb{Z}$ nên $\frac{r}{s}b_1 \in \mathbb{Z}$ suy ra $s \mid b_1$.

Tiếp tục lập luận như vậy ta được $s \mid b_i$ với mọi $i = 0, 1, \dots, n-1$.

Do đó $p(x)$ có thể viết lại được dưới dạng:

$$p(x) = (sx - r)g(x)$$

với $g(x)$ là đa thức thu được từ $q(x)$ bằng cách chia các hệ số b_i của $q(x)$ cho s .

Bài tập 2. Chứng minh rằng $\frac{r}{s}$ ở dạng tối giản, không thể là một nghiệm của đa thức nguyên $p(x)$ trừ khi $(s-r) \mid p(1)$. Điều này có thể được sử dụng để rút ngắn danh sách các nghiệm hữu tỷ có thể có của một đa thức nguyên.

Giải: Nếu $\frac{r}{s}, (r, s) = 1$, là một nghiệm hữu tỷ của đa thức $p(x)$ thì theo Bài tập 1, $p(x)$ được viết dưới dạng $p(x) = (sx - r)q(x)$, trong đó $q(x)$ là đa thức với hệ số nguyên.

Thay $x = 1$ vào đẳng thức trên ta được $p(1) = (s-r)q(1)$, trong đó $q(1) \in \mathbb{Z}$.

Do đó $(r-s) \mid p(1)$. Như vậy, phân số tối giản $\frac{r}{s}$ không thể là một nghiệm của đa thức nguyên $p(x)$ trừ khi $(r-s) \mid p(1)$.

Do đó để tìm nghiệm hữu tỷ của một đa thức nguyên, ta chỉ cần kiểm tra các phân số tối giản $\frac{r}{s}$, trong đó r là ước của hệ tử tự do, s là ước của hệ tử cao nhất thỏa mãn $(r-s) \mid p(1)$.

Bài tập 3. Chứng minh rằng đa thức $f(x)$ với hệ số nguyên không có nghiệm nguyên nếu $f(0)$ và $f(1)$ đều là những số lẻ.

Giải: Giả sử ngược lại rằng đa thức $f(x) \in \mathbb{Z}[x]$ có nghiệm nguyên là a trong khi $f(0)$ và $f(1)$ là những số lẻ.

Do $f(0)$ là số hạng tự do nên a là ước của $f(0)$ phải là số lẻ.

Lại theo điều kiện cần trong Bài tập 2 thì $a - 1$ phải là ước của $f(1)$.

Song $a - 1$ là số chẵn, $f(1)$ là số lẻ nên điều này là vô lý.

Vậy $f(x)$ không có nghiệm nguyên.

Bài tập 4. Chứng minh rằng:

a, $\sqrt[5]{2}$ là số vô tỷ.

b, $\frac{\sqrt{2}}{\sqrt[3]{5}}$ là số vô tỷ.

Giải: a, Ta thấy $\sqrt[5]{2}$ là một nghiệm của phương trình $x^5 - 2 = 0$.

Nếu đa thức này có một nghiệm hữu tỷ c thì theo hệ quả 1, c là một số nguyên ước của 2.

Do đó các nghiệm hữu tỷ chỉ có thể là $\pm 1, \pm 2$.

Lập bảng giá trị

x	-2	-1	1	2
$x^5 - 2$	-34	-3	-1	30

Từ bảng trên ta thấy $\pm 1, \pm 2$ không phải là nghiệm hữu tỷ của đa thức.

Nên tất cả các nghiệm của đa thức $x^5 - 2$ phải là các số vô tỷ.

Vậy $\sqrt[5]{2}$ là số vô tỷ. (đpcm)

b, Ta có $\frac{\sqrt{2}}{\sqrt[3]{5}}$ là một nghiệm của phương trình $25x^6 - 8 = 0$.

Nếu đa thức này có một nghiệm hữu tỷ $\frac{p}{q}$ thì $p|8$ và $q|25$.

Do đó các nghiệm hữu tỷ (nếu có) của đa thức này chỉ có thể là

$$\pm 1, \pm 2, \pm 4, \pm 8, \pm \frac{1}{5}, \pm \frac{1}{25}, \pm \frac{2}{5}, \pm \frac{4}{5}, \pm \frac{4}{25}, \pm \frac{8}{5}, \pm \frac{8}{25}.$$

Dễ dàng kiểm tra các giá trị này không phải là nghiệm của đa thức $25x^6 - 8$.

Nên tất cả các nghiệm của đa thức $25x^6 - 8$ phải là các số vô tỷ.

Vậy $\frac{\sqrt{2}}{\sqrt[3]{5}}$ là số vô tỷ. (đpcm)

Bài tập 5. Chứng minh rằng nếu đa thức

$$f(x) = ax^2 + bx + c \in \mathbb{Z}[x], (a \neq 0)$$

có nghiệm hữu tỷ thì ít nhất một trong ba số a, b, c chẵn.

Giải: Giả sử x_1 là nghiệm hữu tỷ của $f(x)$.

$$\text{Khi đó } ax_1^2 + bx_1 + c = 0.$$

Do đó $(ax_1)^2 + b(ax_1) + ac = 0$, nghĩa là $y_1 = ax_1$ là nghiệm hữu tỷ của tam thức bậc hai $g(y) = y^2 + by + ac$.

Hiển nhiên nghiệm hữu tỷ y_1 là nghiệm nguyên và $g(y)$ còn có nghiệm thứ hai y_2 . Ta có $y_1 + y_2 = -b$ và $y_1 y_2 = ac$.

$$\text{Do } b, y_1 \in \mathbb{Z} \text{ nên } y_2 = -b - y_1 \in \mathbb{Z}.$$

$$\text{Do đó } abc = -y_1 y_2 (y_1 + y_2).$$

Vì trong ba số nguyên $y_1, y_2, y_1 + y_2$ có ít nhất một số chẵn nên abc chẵn và vì vậy có ít nhất một trong ba số a, b, c chẵn.

Bài tập 6. Trong vành $\mathbb{Q}[x]$ chứng minh rằng đa thức

$$f(x) = x^3 - 3n^2x + n^3,$$

với n là một số tự nhiên khác không, là một đa thức bất khả quy.

Giải: Đa thức $f(x) = x^3 - 3n^2x + n^3$ có bậc 3 nên $f(x)$ bất khả quy trong $\mathbb{Q}[x]$ khi và chỉ khi $f(x)$ không có nghiệm hữu tỷ.

$$\text{Ta có } n \neq 0 \text{ nên } f(x) = n^3 \left(\frac{x^3}{n^3} - 3\frac{x}{n} + 1 \right).$$

$$\text{Đặt } y = \frac{x}{n} \text{ khi đó } f(y) = n^3 (y^3 - 3y + 1).$$

$$\text{Đặt } y = z - 1 \text{ khi đó: } f(y) = n^3 (z^3 - 3z^2 + 3) = n^3 f(z)$$

Sử dụng tiêu chuẩn Eisenstein với $p = 3$ là số nguyên tố ta có:

$$\begin{cases} 3 \mid (3, 0, 3) \\ 3 \nmid 1 = a_3 \\ 9 \nmid 3 = a_0 \end{cases}$$

Vậy $f(x)$ bất khả quy trong $\mathbb{Q}[x]$.

Bài tập 7. Tìm điều kiện cần và đủ để đa thức $f(x) = x^4 + px^2 + q$ là bất khả quy trong $\mathbb{Q}[x]$.

Giải: Giả sử $f(x) = x^4 + px^2 + q$ có thể phân tích được thành tích được thành tích của hai đa thức bậc hai:

$$x^4 + px^2 + q = (x^2 + ax + m)(x^2 + bx + n).$$

Khi đó so sánh hệ số ở hai vế ta được:

$$\begin{cases} a + b = 0 \\ m + n + ab = p \\ an + bm = 0 \\ mn = q \end{cases}$$

$$\text{Nếu } a = 0 \text{ thì } b = 0 \text{ và } \begin{cases} m + n = p \\ mn = q \end{cases}$$

Khi đó m và n là nghiệm của phương trình $X^2 - pX + q = 0$.

Phương trình này có nghiệm hữu tỷ khi và chỉ khi $\Delta = p^2 - 4q$ là bình phương của một số hữu tỷ.

$$\text{Nếu } a \neq 0 \text{ thì } m = n \text{ và } \begin{cases} a = -b \\ 2n - a^2 = p \\ n^2 = q \end{cases}$$

Vì a và n là những số hữu tỷ nên q và $2\sqrt{q} - p$ phải là bình phương của những số hữu tỷ.

Từ các kết quả trên suy ra rằng đa thức $x^4 + px^2 + q$ là bất khả quy trong $\mathbb{Q}[x]$ khi và chỉ khi q , $p^2 - 4q$ và $2\sqrt{q} - p$ không phải là bình phương của những số hữu tỷ.

Bài tập 8. Cho $a_1, a_2, \dots, a_n$ là các số nguyên phân biệt. Chứng minh rằng đa thức $f(x) = (x - a_1)^2 (x - a_2)^2 \dots (x - a_n)^2 + 1$ là bất khả quy trong $\mathbb{Q}[x]$.

Giải: Giả sử ngược lại rằng $f(x)$ là khả quy, tức là $f(x)$ có sự phân tích thực sự:

$$f(x) = g(x)h(x) \text{ với } g, h \in \mathbb{Z}[x], 0 < \deg g, \deg h < 2n.$$

Vì $f(x)$ không có nghiệm thực nên $g(x), h(x)$ cũng không có nghiệm thực, do đó chúng không đổi dấu.

$$\text{Giả sử } g(x) > 0, h(x) > 0 \quad (\forall x).$$

$$\text{Vì } f(a_i) = 1 \text{ nên } g(a_i) = h(a_i) = 1 \quad (i = 1, 2, \dots, n).$$

Suy ra $\deg g = \deg h = n$ (vì nếu có đa thức nào có bậc bé hơn n thì đa thức đó đồng nhất bằng 1, vô lý).

Vậy $g(x), h(x)$ có dạng:

$$\begin{aligned} g(x) &= 1 + a(x - a_1)(x - a_2) \dots (x - a_n), \\ f(x) &= 1 + b(x - a_1)(x - a_2) \dots (x - a_n) \end{aligned} \quad \text{trong đó } a, b \in \mathbb{Z}.$$

So sánh hệ số cao nhất và hệ số tự do của hai vế của đẳng thức $f(x) = g(x)h(x)$ ta được $ab = 1$ và $1 + (-1)^n a_1 \dots a_n (a + b) + a_1^2 \dots a_n^2 = 1 + a_1^2 \dots a_n^2$.

$$\text{Suy ra } ab = 1 \text{ và } a + b = 0.$$

Rõ ràng là không tồn tại những số nguyên như vậy.

Do đó $f(x)$ là đa thức bất khả quy trong $\mathbb{Q}[x]$.

Bài tập 9. Tìm nghiệm hữu tỷ của các đa thức:

$$a, 2x^3 + 3x^2 + 6x - 4;$$

$$b, x^5 + 2x^4 + 6x^3 + 3x^2 - 12x - 48.$$

Giải

$$a, \text{ Đặt } f(x) = 2x^3 + 3x^2 + 6x - 4$$

$$+ \text{ Các ước của } a_0 = 4 \text{ là } p \in \{\pm 1; \pm 2; \pm 4\}.$$

$$+ \text{ Các ước của } a_n = 2 \text{ là } q \in \{\pm 1; \pm 2\}.$$

$$\text{Lập phân số } \frac{p}{q} \in \left\{ \pm \frac{1}{2}; \pm 1; \pm 2; \pm 4 \right\}.$$

$$+ \text{ Tính } f(1), f(-1)$$

	2	3	6	-4
$x=1$	2	3	9	$-5 \neq 0$
$x=-1$	2	1	5	$-9 \neq 0$

$\Rightarrow \pm 1$ không phải là nghiệm hữu tỷ của $f(x)$.

Kiểm tra $\frac{p}{q} = \frac{1}{2}$ thỏa mãn $\begin{cases} p-q \mid f(1) \\ p+q \mid f(-1) \end{cases}$

+ Dùng Hoocne:

	2	3	6	-4
$x = \frac{1}{2}$	2	4	8	0

Suy ra $f(x) = (2x-1)(x^2+2x+4)$

+ Xét $g(x) = x^2 + 2x + 4$ không có nghiệm hữu tỷ.

Vậy $x = \frac{1}{2}$ là nghiệm hữu tỷ của $f(x)$.

b, Đặt $f(x) = x^5 + 2x^4 + 6x^3 + 3x^2 - 12x - 48$

+ Các ước của $a_0 = 48$ là $p \in \{\pm 1; \pm 2; \pm 3; \pm 4; \pm 6; \pm 8; \pm 12; \pm 16; \pm 24; \pm 48\}$.

+ Các ước của $a_n = 1$ là $q \in \{\pm 1\}$.

Lập phân số $\frac{p}{q} \in \{\pm 1; \pm 2; \pm 3; \pm 4; \pm 6; \pm 8; \pm 12; \pm 16; \pm 24; \pm 48\}$.

+ Tính $f(1), f(-1)$

	1	2	6	3	-12	-48
$x=1$	1	3	9	12	0	$-48 \neq 0$
$x=-1$	1	1	5	-2	-10	$-38 \neq 0$

$\Rightarrow \pm 1$ không phải là nghiệm hữu tỷ của $f(x)$.

Kiểm tra $\frac{p}{q}$ không có số nào thỏa mãn $\begin{cases} p-q \mid f(1) \\ p+q \mid f(-1) \end{cases}$

Vậy $f(x)$ không có nghiệm hữu tỷ.

Bài tập 10. Chứng minh rằng đa thức $x^3 + 3x^2y^2 + 2x^2y + xy^4 + 7y + y^2$ là bất khả quy trong $\mathbb{Q}[x, y]$.

Giải: Ta có y là phần tử nguyên tố trong $\mathbb{Q}[y]$ vì $\mathbb{Q}[y]/(y) \cong \mathbb{Q}$.

Xét đa thức $x^3 + 3x^2y^2 + 2x^2y + xy^4 + 7y + y^2$ xem như là đa thức ẩn x lấy hệ tử trong $\mathbb{Q}[y]$.

$$f(x) = x^3 + (3y^2 + y)x^2 + y^4x + 7y + y^2$$

Sử dụng tiêu chuẩn Eisenstein với $p = y$ là số nguyên tố ta có:

$$\begin{cases} y \mid (3y^2 + y, y^4, 7y + y^2) \\ y \nmid 1 = a_3 \\ y^2 \nmid 7y + y^2 = a_0 \end{cases}$$

Vậy đa thức $f(x)$ bất khả quy trong $\mathbb{Q}[y][x] = \mathbb{Q}[y, x] \cong \mathbb{Q}[x, y]$.

Bài tập 11. Dùng tiêu chuẩn Eisenstein chứng minh rằng các đa thức sau là bất khả quy trong $\mathbb{Q}[x]$:

$a, 3x^8 - 4x^6 + 8x^5 - 10x + 6;$

$b, x^4 - x^3 + 2x + 1;$

$c, x^4 - 13x^3 + 45x^2 - 61x + 25;$

$d, x^4 + x^3 + x^2 + x + 1.$

Giải:

$a, f(x) = 3x^8 - 4x^6 + 8x^5 - 10x + 6$

Sử dụng tiêu chuẩn Eisenstein với $p = 2$ là số nguyên tố ta có:

$$\begin{cases} 2 \mid (-4, 8, 0, 0, 0, -10, 6) \\ 2 \nmid 3 = a_8 \\ 4 \nmid 6 = a_0 \end{cases}$$

Vậy $f(x) = 3x^8 - 4x^6 + 8x^5 - 10x + 6$ bất khả quy trong $\mathbb{Q}[x]$.

$b, f(x) = x^4 - x^3 + 2x + 1$

Đặt $t = x - 1$ khi đó:

$$\begin{aligned} f(x) &= (t+1)^4 - (t+1)^3 + 2(t+1) + 1 \\ &= t^4 + 4t^3 + 6t^2 + 4t + 1 - t^3 - 3t^2 - 3t - 1 + 2t + 2 + 1 \\ &= t^4 + 3t^3 + 3t^2 + 3t + 3 = g(t) \end{aligned}$$

Sử dụng tiêu chuẩn Eisenstein với $p = 3$ là số nguyên tố ta có:

$$\begin{cases} 3 \mid (3, 3, 3, 3) \\ 3 \nmid 1 = a_4 \\ 9 \nmid 3 = a_0 \end{cases}$$

Suy ra $g(t)$ bất khả quy trong $\mathbb{Q}[x]$.

Vậy $f(x) = x^4 - x^3 + 2x + 1$ bất khả quy trong $\mathbb{Q}[x]$.

$$c, f(x) = x^4 - 13x^3 + 45x^2 - 61x + 25$$

Đặt $t = x - 1$ khi đó:

$$\begin{aligned} f(x) &= (t+1)^4 - 13(t+1)^3 + 45(t+1)^2 - 61(t+1) + 25 \\ &= t^4 + 4t^3 + 6t^2 + 4t + 1 - 13t^3 - 39t^2 - 39t - 13 + 45t^2 + 90t + 45 - 61t - 61 + 25 \\ &= t^4 - 9t^3 + 12t^2 - 6t - 3 = g(t) \end{aligned}$$

Sử dụng tiêu chuẩn Eisenstein với $p = 3$ là số nguyên tố ta có:

$$\begin{cases} 3 \mid (-9, 12, -6, -3) \\ 3 \nmid 1 = a_4 \\ 9 \nmid -3 = a_0 \end{cases}$$

Suy ra $g(t)$ bất khả quy trong $\mathbb{Q}[x]$.

Vậy $f(x) = x^4 - 13x^3 + 45x^2 - 61x + 25$ bất khả quy trong $\mathbb{Q}[x]$.

$$d, f(x) = x^4 + x^3 + x^2 + x + 1$$

Đặt $t = x - 1$ khi đó:

$$\begin{aligned} f(x) &= (t+1)^4 + (t+1)^3 + (t+1)^2 + (t+1) + 1 \\ &= t^4 + 4t^3 + 6t^2 + 4t + 1 + t^3 + 3t^2 + 3t + 1 + t^2 + 2t + 1 + t + 1 + 1 \\ &= t^4 + 5t^3 + 10t^2 + 10t + 5 = g(t) \end{aligned}$$

Sử dụng tiêu chuẩn Eisenstein với $p = 5$ là số nguyên tố ta có:

$$\begin{cases} 5 \mid (5, 10, 10, 5) \\ 5 \nmid 1 = a_4 \\ 25 \nmid 5 = a_0 \end{cases}$$

Suy ra $g(t)$ bất khả quy trong $\mathbb{Q}[x]$.

Vậy $f(x) = x^4 + x^3 + x^2 + x + 1$ bất khả quy trong $\mathbb{Q}[x]$.

2.3 Phân tích đa thức trên trường hữu hạn

2.3.1 Một số tính chất của trường hữu hạn

Định nghĩa 1. Trường hữu hạn là trường có hữu hạn phần tử.

Định lý 14. Nếu F là trường hữu hạn thì đặc số của F là một số nguyên tố.

Chứng minh: Ta có đặc số của trường hoặc là 0 hoặc là một số nguyên.

Giả sử F là trường hữu hạn có đặc số 0 thì F chứa trường con nguyên tố đẳng cấu với $\mathbb{Q}$.

Nhưng $\mathbb{Q}$ là trường vô hạn nên trường con nguyên tố của F là vô hạn nên trường con nguyên tố của F là vô hạn (mâu thuẫn).

Vậy đặc số của trường hữu hạn là một số nguyên tố.

Định nghĩa 2. (Trường phân rã của một đa thức)

i) Cho K là trường và $f(x)$ là đa thức bậc $n \geq 1$ trên K . Khi đó, trường E chứa trường K như trường con, được gọi là **trường phân rã** của đa thức $f(x)$ trên K nếu $f(x)$ có đúng n nghiệm (kể cả nghiệm bội) trong E và E là trường tối thiểu chứa K và các nghiệm của $f(x)$.

ii) Cho đa thức $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in K[x]$ ta gọi đa thức sau đây là đạo hàm của $f(x)$: $f'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1}$.

Định lý 15. Cho F_q là trường hữu hạn thì với mọi $a \in F_q$ ta đều có $a^q = a$.

Chứng minh: Với $a = 0$ thì ta có $a^q = a$.

Với $a \neq 0$ thì số phần tử của nhóm nhân F_q^* là $q-1$.

Suy ra $|F_q^*| = q-1$.

Khi đó với mọi $a \in F_q^*$ ta đều có $a^{q-1} = 1$ hay $a^q = a$.

Vậy $a^q = a$ với mọi $a \in F_q$.

Định lý 16. Cho trường hữu hạn F_q và K là trường con của F_q thì đa thức $x^q - x$ trong $K[x]$ có sự phân tích trong $F_q[x]$ là $x^q - x = \prod_{a \in F_q} (x - a)$ và F_q là trường phân rã của đa thức $x^q - x$ trên K .

Chứng minh: Theo định lý 15 ta có $a^q - a$ với mọi $a \in F_q$ hay a là nghiệm của đa thức $x^q - x$.

Ta viết q phần tử của F_q là $a_1, a_2, \dots, a_q$.

Khi đó mỗi đa thức $x - a_i \in F_q[x]$, $i = 1, 2, \dots, q$ đều là ước của đa thức $x^q - x$, hơn nữa các đa thức $x - a_i \in F_q[x]$, $i = 1, 2, \dots, q$ nguyên tố cùng nhau nên tích $(x - a_1)(x - a_2) \dots (x - a_q)$ cũng là ước của $x^q - x$.

Do đa thức $(x - a_1)(x - a_2) \dots (x - a_q)$ có bậc là q nên ta có

$$x^q - x = (x - a_1)(x - a_2) \dots (x - a_q).$$

Vậy F_q là trường phân rã của đa thức $x^q - x$ trên K .

Định lý 17. Nhóm nhân của trường hữu hạn là nhóm cyclic.

Chứng minh: Giả sử F là một trường hữu hạn gồm q phần tử.

Đặt $h = |F^*| = q - 1$. Nếu $h = 1$ hoặc h là số nguyên tố thì rõ ràng F^* là nhóm cyclic.

Do đó, ta có thể giả sử h là số nguyên dương lớn hơn 1 và không là số nguyên tố.

Giả sử $h = p_1^{\alpha_1} \dots p_m^{\alpha_m}$, với $m \geq 2$, p_i nguyên tố khác nhau đôi một, $\alpha_i \in \mathbb{N}$, $\forall i \in \overline{1, m}$.

Khi đó, $\frac{h}{p_i} < h$ và đa thức $x^{\frac{h}{p_i}} - 1$ có không quá $\frac{h}{p_i}$ nghiệm trong F^* , suy ra

tồn tại $a_i \in F^*$ sao cho $a_i^{\frac{h}{p_i}} \neq 1$.

Đặt $b_i = a_i^{\frac{h}{p_i^{\alpha_i}}}$. Ta sẽ chứng minh $|b_i| = p_i^{\alpha_i}$.

Ta có $b_i^{p_i^{\alpha_i}} = a_i^h = 1$ và $b_i \neq 1$ vì nếu $b_i = 1$ thì $1 = b_i^{p_i^{\alpha_i-1}} = \left(a_i^{\frac{h}{p_i^{\alpha_i}}}\right)^{p_i^{\alpha_i-1}} = a_i^{\frac{h}{p_i}}$ (mâu thuẫn).

Do đó $|b_i| \mid p_i^{\alpha_i}$ và $|b_i| \neq 1$, suy ra $|b_i| = p_i^{\beta_i}, 1 \leq \beta_i \leq \alpha_i$.

Mặt khác, $b_i^{p_i^{\alpha_i-1}} = a_i^{\frac{h}{p_i}} \neq 1$. Vì vậy $|b_i| = p_i^{\alpha_i}$.

Đặt $b = b_1 b_2 \dots b_m$. Khi đó, do p_i , với $i \in \overline{1, m}$ là các số nguyên tố khác nhau đôi một và F giao hoán nên $|b| = |b_1 b_2 \dots b_m| = p_1^{\alpha_1} \dots p_m^{\alpha_m} = h = |F^*|$.

Vậy $F^* = \langle b \rangle$.

Hệ quả 2. *Mỗi nhóm con hữu hạn của nhóm nhân của một trường là một nhóm xyclic.*

Chứng minh: Giả sử F là một trường và G là một nhóm con hữu hạn cấp n của nhóm nhân F^* .

Xét trường hợp $\text{char } F = p \neq 0$. Gọi F_p là trường con nguyên tố của trường F .

Vì $|G| = n$ nên mọi phần tử của G đều là nghiệm của đa thức $x^n - 1$.

Do đó, mọi phần tử của G đều đại số trên F_p , suy ra $F_p(G)$ là mở rộng hữu hạn, đại số trên F_p , do đó $F_p(G)$ là một trường hữu hạn.

Theo định lý 17, $(F_p(G))^*$ là một nhóm xyclic.

Vì vậy, G là một nhóm con xyclic của nhóm $(F_p(G))^*$.

Xét trường hợp $\text{char } F = 0$. Vì tất cả n phần tử của G đều là nghiệm của đa thức $x^n - 1$ và đa thức $x^n - 1$ bậc n có không quá n nghiệm nên G là tập nghiệm của đa thức $x^n - 1$. Lập luận tương tự như chứng minh định lý 16 (ở đó, h được thay bởi n), ta có G là một nhóm xyclic.

Định nghĩa 3. *Mỗi phần tử sinh của nhóm xyclic F_q^* được gọi là một phần tử nguyên thủy của F_q .*

2.3.2. Đa thức bất khả quy trên trường hữu hạn

Bổ đề 2. Cho $f(x) \in F_q[x]$ là đa thức bất khả quy bậc m trên F_q và n là một số nguyên dương. Khi đó, $f(x)$ chia hết $x^{q^n} - x$ nếu và chỉ nếu m chia hết n .

Chứng minh:

($\Rightarrow$) Giả sử $f(x)$ chia hết $x^{q^n} - x$. Gọi α là một nghiệm của $f(x)$.

Khi đó, $\alpha^{q^n} - \alpha = 0$ suy ra $\alpha \in F_{q^n}$. Do đó, $F_q(\alpha) \subseteq F_{q^n}$.

Mặt khác vì $[F_q(\alpha) : F_q] = m$ nên $F_q(\alpha) = F_{q^m} \subseteq F_{q^n}$ ta suy ra $m \mid n$.

($\Leftarrow$) Ngược lại, giả sử $m \mid n$. Gọi α là một nghiệm của $f(x)$ nằm trong trường phân rã của $f(x)$ nên F_q .

Khi đó, $[F_q(\alpha) : F_q] = m$ suy ra $F_q(\alpha) = F_{q^m}$.

Vì $m \mid n$ nên $F_{q^m} \subseteq F_{q^n}$.

Do đó $\alpha \in F_{q^n}$ suy ra $\alpha^{q^n} - \alpha = 0$.

Vì vậy α là một nghiệm của đa thức $x^{q^n} - x$, kéo theo $f(x) \mid x^{q^n} - x$.

Định lý 18. Giả sử $f(x) \in F_q[x]$ là đa thức có bậc n thì $f(x)$ là đa thức bất khả quy trên F_q nếu và chỉ nếu:

$$f(x) \nmid (x^{q^i} - x) \text{ và } \gcd(f(x), x^{q^i} - x) = 1 \text{ với } i = 1, 2, 3, \dots, [n/2]$$

Chứng minh:

($\Rightarrow$) Nếu $f(x)$ bất khả quy trên F_q thì theo bổ đề 2, ta có $f(x) \nmid (x^{q^n} - x)$ và $\gcd(f(x), x^{q^i} - x) = 1$, với $i = 1, 2, \dots, [n/2]$.

($\Leftarrow$) Nếu $f(x)$ khả quy trên F_q thì $f(x)$ có nhân tử $g(x)$ bất khả quy trên F_q .

Giả sử $\deg g(x) = m$ và $m \leq [n/2]$.

Theo bổ đề 2, ta có $g(x) \mid (x^{q^m} - x)$, do đó $\gcd(f(x), x^{q^m} - x) \neq 1$ (mâu thuẫn).

Vậy $f(x)$ bất khả quy trên F_q .

Định lý 19. Cho $f(x) \in F_q[x]$ là đa thức bậc $n > 1$. Khi đó, các điều kiện sau tương đương:

i) $f(x)$ bất khả quy trên F_q .

ii) $(cx+d)^{\deg f(x)} f\left(\frac{ax+b}{cx+d}\right)$ bất khả quy, trong đó $a, b, c, d \in F_q$ sao cho

$$ad - bc \neq 0.$$

Chứng minh: Trước hết ta có nhận xét:

(+) Cho $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ là đa thức bậc n trên F_q . Khi đó:

$$(cx+d)^{\deg f(x)} f\left(\frac{ax+b}{cx+d}\right) = (cx+d)^n f\left(\frac{ax+b}{cx+d}\right) = \sum_{i=0}^n a_i (ax+b)^i (cx+d)^{n-i}$$

cũng là một đa thức trên F_q .

(+) Nếu $f(x)$ bất khả quy và $ad - bc \neq 0$ thì $(cx+d)^{\deg f(x)} f\left(\frac{ax+b}{cx+d}\right)$ là đa

thức có bậc n .

Bây giờ ta sẽ chứng minh (i) $\Leftrightarrow$ (ii):

($\Leftarrow$) Giả sử $(cx+d)^{\deg f(x)} f\left(\frac{ax+b}{cx+d}\right)$ bất khả quy trên F_q .

Nếu $f(x)$ khả quy thì $f(x)$ được phân tích thành ít nhất hai nhân tử bất khả quy.

Giả sử $f(x)$ là tích của m nhân tử bất khả quy trên F_q , với $2 \leq m \leq n$. Do đó,

$f(x) = f_1(x) f_2(x) \dots f_m(x)$, trong đó $f_1(x), f_2(x), \dots, f_m(x)$ là các đa thức bất khả quy trên F_q và $\deg f_1(x) = k_1 \geq 1, \deg f_2(x) = k_2 \geq 1, \dots, \deg f_m(x) = k_m \geq 1$ sao cho $k_1 + k_2 + \dots + k_m = n$. Ta có:

$$\begin{aligned} (cx+d)^{\deg f(x)} f\left(\frac{ax+b}{cx+d}\right) &= (cx+d)^n f_1\left(\frac{ax+b}{cx+d}\right) f_2\left(\frac{ax+b}{cx+d}\right) \dots f_m\left(\frac{ax+b}{cx+d}\right) \\ &= \left[(cx+d)^{k_1} f_1\left(\frac{ax+b}{cx+d}\right) \right] \left[(cx+d)^{k_2} f_2\left(\frac{ax+b}{cx+d}\right) \right] \dots \left[(cx+d)^{k_m} f_m\left(\frac{ax+b}{cx+d}\right) \right] \end{aligned}$$

Theo nhận xét trên, ta có:

$$(cx+d)^{k_1} f_1\left(\frac{ax+b}{cx+d}\right), (cx+d)^{k_2} f_2\left(\frac{ax+b}{cx+d}\right), \dots, (cx+d)^{k_m} f_m\left(\frac{ax+b}{cx+d}\right) \in F_q[x]$$

và lần lượt có bậc là $k_1, k_2, \dots, k_m$.

Ta suy ra $(cx+d)^{\deg f(x)} f\left(\frac{ax+b}{cx+d}\right)$ khả quy (mâu thuẫn).

Vậy $f(x)$ bất khả quy trên F_q .

($\Rightarrow$) Giả sử $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ bất khả quy trên F_q .

Do $ad - bc \neq 0$ nên $\gcd(ax+b, cx+d) = 1$.

Gọi γ là nghiệm của $(cx+d)^{\deg f(x)} f\left(\frac{ax+b}{cx+d}\right)$ nằm trong trường phân rã của

$$(cx+d)^{\deg f(x)} f\left(\frac{ax+b}{cx+d}\right) \text{ trên } F_q.$$

Khi đó $a\gamma + b \neq 0$ và $c\gamma + d \neq 0$.

$$\text{Đặt } \lambda = \frac{a\gamma + b}{c\gamma + d} \quad (1)$$

Ta có: $(c\gamma + d)^{\deg f(x)} f\left(\frac{a\gamma + b}{c\gamma + d}\right) = (c\gamma + d)^{\deg f(x)} f(\lambda) = 0$ kéo theo $f(\lambda) = 0$.

Do đó λ là một nghiệm của $f(x)$ và $\lambda \in F_q(\lambda) = F_{q^n}$.

Do (1) nên γ là một nghiệm đa thức $(ax+b) - \lambda(cx+d)$, đa thức này có bậc 1.

Do đó $\gamma \in F_q(\lambda)$. Rõ ràng $\lambda \in F_q(\gamma)$.

Ta được $F_q(\lambda) = F_q(\gamma)$. Mặt khác, $[F_q(\lambda) : F_q] = [F_{q^n} : F_q] = n$.

Vì vậy $[F_q(\gamma) : F_q] = [F_q(\lambda) : F_q] = n$.

Theo nhận xét trên $(cx+d)^{\deg f(x)} f\left(\frac{ax+b}{cx+d}\right)$ có bậc n .

Vậy $(cx+d)^{\deg f(x)} f\left(\frac{ax+b}{cx+d}\right)$ bất khả quy trên F_q .

Định lý 20. Cho $f(x) \in F_q[x]$ là đa thức bậc $n > 1$. Nếu $f(x)$ bất khả quy trên F_q thì:

i) Tổng các hệ tử của $f(x)$ khác 0.

ii) $\gcd(f(x), f'(x)) = 1$.

Chứng minh:

i) Giả sử tổng các hệ tử của $f(x)$ bằng 0 suy ra 1 là nghiệm của $f(x)$ (mâu thuẫn).

Vậy tổng các hệ tử của $f(x)$ khác 0.

ii) Giả sử $\gcd(f(x), f'(x)) = d(x) \neq 1$.

Ta có $f(x) = d(x)h(x)$, vì $\deg f'(x) < \deg f(x)$ nên $\deg h(x) \geq 1$ kéo theo $f(x)$ khả quy.

Vậy $f(x)$ bất khả quy trên F_q .

Khi $q = 2$ ta có định lý sau:

Định lý 21. Cho $f(x) \in F_2[x]$. Nếu $f(x)$ bất khả quy trên F_2 thì

i) Số các số hạng của $f(x)$ có hệ số bằng 1 là số lẻ.

ii) Có số hạng x^m của $f(x)$ với hệ số bằng 1 sao cho $2 \nmid m$.

Chứng minh:

i) Vì F_2 là trường đặc trưng 2 nên các hệ số của các số hạng khác 0 của đa thức $f(x)$ trên F_2 đều bằng 1.

Do đó số các số hạng của $f(x)$ có hệ số bằng 1 phải là số lẻ (nếu là số chẵn thì $f(1) = 0$).

ii) Nếu $f(x) = x$ thì hiển nhiên định lý đúng. Giả sử $f(x)$ không có dạng x .

Khi đó, ta có thể viết $f(x) = (x^{m_1} + x^{m_2} + \dots + x^{m_n})$, trong đó $m_i \geq 1, i \in \overline{1, n}$.

Giả sử $2 \mid m_i, \forall i \in \overline{1, n}$, suy ra $m_i = 2k_i$, với $k_i \in \mathbb{Z}, \forall i \in \overline{1, n}$. Khi đó:

$$\begin{aligned}
 f(x) &= (x^{2k_1} + x^{2k_2} + \dots + x^{2k_n}) + 1 \\
 &= (x^{k_1} + x^{k_2} + \dots + x^{k_n})^2 + 1 \\
 &= (x^{k_1} + x^{k_2} + \dots + x^{k_n} + 1)(x^{k_1} + x^{k_2} + \dots + x^{k_n} - 1)
 \end{aligned}$$

Do đó $f(x)$ khả quy (mâu thuẫn).

Vậy tồn tại $i \in \overline{1, n}$ sao cho $2 \nmid m_i$.

2.3.3. Phân tích đa thức trên trường hữu hạn

Bổ đề 3. Cho $g(x)$ là một đa thức trong $F_q[x]$ và s_1, s_2 là hai phần tử khác nhau của F_q . Khi đó, $\gcd(g(x) - s_1, g(x) - s_2) = 1$.

Chứng minh: Ta có $-(s_1 - s_2)^{-1}(g(x) - s_1) + (s_1 - s_2)^{-1}(g(x) - s_2) = 1$.

Do đó $\gcd(g(x) - s_1, g(x) - s_2) = 1$.

Bổ đề 4. Cho $f(x)$ là một đa thức có hệ tử của bậc cao nhất là 1 trong $F_q[x]$ và $g(x)$ là một đa thức trong $F_q[x]$. Khi đó, $g(x)$ thỏa mãn

$g(x)^q \equiv g(x) \pmod{f(x)}$ nếu và chỉ nếu $f(x) \mid \prod_{s \in F_q} (g(x) - s)$ nếu và chỉ nếu

$$f(x) \mid \prod_{s \in F_q} \gcd(f(x), g(x) - s).$$

Chứng minh: Ta có $X^q - X = \prod_{s \in F_q} (X - s)$, với $X \in F_q[x] / f(x)$.

Khi đó, ta thay X bởi $\overline{g(x)} = g(x) + (f(x)) \in F_q[x] / f(x)$ vào công thức $X^q - X = \prod_{s \in F_q} (X - s)$ ta được

$$[g(x) + f(x)]^q - [g(x) + f(x)] = \prod_{s \in F_q} [g(x) + f(x) - s].$$

$$\text{Vì } [g(x) + f(x)]^q = [g(x)]^q + [f(x)]^q \equiv [g(x)]^q \pmod{f(x)}$$

Và $g(x) + f(x) \equiv g(x) \pmod{f(x)}$ nên ta có:

$$g(x)^q - g(x) = \prod_{s \in F_q} (g(x) - s) \pmod{f(x)}.$$

Do đó $g(x)$ thỏa mãn điều kiện $g(x)^q \equiv g(x) \pmod{f(x)}$ nếu và chỉ nếu:

$$\prod_{s \in F_q} (g(x) - s) \equiv 0 \pmod{f(x)}, \text{ nghĩa là } f(x) \mid \prod_{s \in F_q} (g(x) - s).$$

Hơn nữa, $f(x) \mid \prod_{s \in F_q} (g(x) - s)$ nếu và chỉ nếu $f(x) \mid \prod_{s \in F_q} \gcd(f(x), g(x) - s)$.

Định lý 22. Cho $f(x)$ là đa thức có hệ tử bậc cao nhất là 1 của $F_q[x]$ và $g(x)$ là đa thức của $F_q[x]$ sao cho $g(x)^q \equiv g(x) \pmod{f(x)}$ thì $f(x) = \prod_{s \in F_q} \gcd(f(x), g(x) - s)$.

Chứng minh: Ta dễ thấy rằng $\gcd(f(x), g(x) - s) \mid f(x), \forall s \in F_q$.

Theo bổ đề 3 ta có $\gcd(g(x) - s_1, g(x) - s_2) = 1$, với $s_1, s_2 \in F_q$ và $s_1 \neq s_2$.

Vì $\gcd(\gcd(f(x), g(x) - s_1), \gcd(f(x), g(x) - s_2)) = 1$ nên

$$\prod_{s \in F_q} \gcd(f(x), g(x) - s) \mid f(x).$$

Mặt khác, theo bổ đề 3 và bổ đề 4 ta có:

$$f(x) \mid \prod_{s \in F_q} \gcd(f(x), g(x) - s).$$

Vậy $f(x) = \prod_{s \in F_q} \gcd(f(x), g(x) - s)$.

Định lý 23. Cho $f(x) \in F_q[x]$, trong đó q là lũy thừa của số nguyên tố p và $f'(x) = 0$ thì: $f(x) = h(x)^p$ với $h(x) \in F_q[x]$.

Chứng minh: Lấy $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ với $a_0, a_1, a_2, \dots, a_n \in F_q$ và $a_n \neq 0$.

Khi đó $f'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1}$.

Vì $f'(x) = 0$ nên $a_1 = 2a_2 = \dots = na_n = 0$ suy ra $a_i = 0, \forall i = \overline{1, n}$.

Tức là $p \mid a_i, \forall i = \overline{1, n}$. Khi đó ta có thể viết lại các hệ tử a_i đó như sau:

$$\begin{cases} a_1 = a_1p \\ \dots \\ a_n = a_np \end{cases} \text{ với } a_i \in F_q, \forall i = \overline{1, n}.$$

Vì thế ta có thể viết $f(x)$ dưới dạng sau: $f(x) = a_0 + a_1x^p + \dots + a_nx^{np}$.

Xét $\sigma: F_q \rightarrow F_q$
 $b \mapsto b^p$ là một đồng cấu.

Thật vậy:

$$\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$$

$$\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$$

Khi đó trong F_q có $a_i = b_i^p, \forall i = \overline{0, n}$. Suy ra:

$$\begin{aligned} f(x) &= b_0^p + b_1^p x^p + \dots + b_n^p x^{np} \\ &= b_0^p + (b_1 x)^p + \dots + (b_n x^n)^p \\ &= (b_0 + b_1 x + \dots + b_n x^n)^p \end{aligned}$$

Đặt $h(x) = b_0 + b_1 x + \dots + b_n x^n$.

Khi đó $h(x) \in F_q[x]$ và $f(x) = h(x)^p$.

Định lý 24. Cho $f(x)$ là lũy thừa của một đa thức bất khả quy trên F_q và giả sử rằng $f'(x) \neq 0$.

i, Nếu $\gcd(f(x), f'(x)) = 1$ thì $f(x)$ là đa thức bất khả quy.

ii, Nếu $\gcd(f(x), f'(x)) \neq 1$ thì $p(x) = \frac{f(x)}{\gcd(f(x), f'(x))}$ là đa thức bất khả quy.

Khi đó, $f(x) = p(x)^m$ với $m = \frac{\deg f(x)}{\deg p(x)}$.

Chứng minh: Lấy $f(x) = p(x)^m$ với $p(x)$ là một đa thức bất khả quy trong $F_q[x]$.

Khi đó $f'(x) = mp(x)^{m-1}$, vì $f'(x) \neq 0$, $\gcd(f(x), f'(x)) = p(x)^{m-1}$.

Nếu $\gcd(f(x), f'(x)) = 1$ thì $m = 1$.

Do đó $f(x) = p(x)$ là một đa thức bất khả quy.

Nếu $\gcd(f(x), f'(x)) \neq 1$ thì $p(x) = \frac{f'(x)}{\gcd(f(x), f'(x))}$ là một đa thức bất khả quy.

Định lý 25. Một đa thức trong $\mathbb{Z}_2[x]$ có một nhân tử $x+1$ nếu và chỉ nếu nó có một số chẵn các hệ số khác 0.

Chứng minh: Xét đa thức với các hệ tử thuộc trường hữu hạn $\mathbb{Z}_2[x]$

$$p(x) = a_0 + a_1x + \dots + a_nx^n,$$

Theo định lý nhân tử, $(x+1)$ là một nhân tử của $p(x)$ nếu và chỉ nếu $p(1) = 0$. (Nhớ rằng $x-1 = x+1$ trong $\mathbb{Z}_2[x]$). Bây giờ

$$p(1) = a_0 + a_1 + \dots + a_n$$

bằng 0 trong $\mathbb{Z}_2$ nếu và chỉ nếu $p(x)$ có một số chẵn các hệ số khác 0.

2.3.4 Bài tập vận dụng

Bài tập 1. Chứng minh rằng tổng của tất cả các phần tử của trường hữu hạn bằng 0 ngoại trừ trường F_2 .

Giải: Giả sử F_q là trường hữu hạn và $F_q \neq F_2$.

Khi đó mọi phần tử thuộc F_q đều là nghiệm của phương trình $x^q - x = 0$.

Vì $F_q \neq F_2$ nên theo Viet ta có $\sum_{a \in F_q} a = 0$.

Bài tập 2. Chứng minh rằng 3 và 5 là phần tử nguyên thủy của F_7 nhưng 2 không phải. Tìm $x, y \in \{1, 2, 3, 4, 5, 6\}$ sao cho $2 = 3^x = 5^x$ trong F_7 .

Giải:

* Chứng minh rằng 3 và 5 là phần tử nguyên thủy của F_7 nhưng 2 không phải:

Ta có $|F_7^*| = 6 = 2 \cdot 3$. Xét đa thức $x^2 - 1$, dễ thấy $a_1 = 2$ không là nghiệm của $x^2 - 1$.

Đặt $b_1 = 2^2$. Xét đa thức $x^3 - 1$, ta có $a_2 = 3$ không là nghiệm của đa thức $x^3 - 1$.

Đặt $b_2 = 3^3$ và đặt $b = b_1.b_2 = 2^2.3^3 = 3$, khi đó $|b| = 2.3 = 6 = |F_7^*|$. Suy ra $b = 3$ là phần tử sinh của F_7^* . Vậy $b = 3$ là phần tử nguyên thủy của F_7 .

Ta có số phần tử nguyên thủy của F_7 là $\varphi(6) = 2$. 3^k là phần tử nguyên thủy trong F_7 khi và chỉ khi $\gcd(k, 6) = 1$, suy ra $k = 5$ (lấy $k \neq 1$).

Mà $3^5 = 5$ nên 5 là phần tử nguyên thủy của F_7 . Do $2 \neq 3$ và $2 \neq 5$ nên 2 không là phần tử nguyên thủy của F_7 .

* Tìm $x, y \in \{1, 2, 3, 4, 5, 6\}$ sao cho $2 = 3^x = 5^y$ trong F_7 .

Ta có:

$$\begin{array}{ll} 3^1 = 3 & 5^1 = 5 \\ 3^2 = 2 & 5^2 = 4 \\ 3^3 = 6 & 5^3 = 6 \\ 3^4 = 4 & 5^4 = 2 \\ 3^5 = 5 & 5^5 = 3 \\ 3^6 = 1 & 5^6 = 1 \end{array} \quad \text{và}$$

Suy ra $2 = 3^2 = 5^4$.

Vậy ta tìm được $x = 2$ và $y = 4$.

Bài tập 3. Tìm tất cả các đa thức bất khả quy bậc hai trên trường $\mathbb{Z}_3$.

Giải: Đa thức $f(x) = ax^2 + bx + c \in \mathbb{Z}_3[x]$ là bất khả quy bậc hai nếu nó không có nghiệm trong $\mathbb{Z}_3$ và nếu $a \neq 0$.

$$\text{Khi đó } a.f(0).f(1).f(-1) = ac[(a+c)^2 - b^2] \neq 0.$$

Với $b = 0$ ta có $ac(a+c)^2 \neq 0$, suy ra $a = c = 1$, hoặc $a = c = -1$.

Tương ứng là các đa thức: $x^2 + 1$ và $-x^2 - 1$.

Với $b \neq 0$ thì $a = b = c = 1$ hoặc $a = -1, b = 1, c = 1$ hoặc $a = -1, b = -1, c = 1$.

Tương ứng là các đa thức: $x^2 + x + 1$; $-x^2 + x + 1$; $x^2 - x - 1$; $-x^2 - x + 1$.

Bài tập 4. Tìm tất cả các đa thức bất khả quy có bậc nhỏ hơn hoặc bằng 4 trên $\mathbb{Z}_2$.

Giải: Các đa thức bậc 1 là các đa thức bất khả quy; trong $\mathbb{Z}_2[x]$ những đa thức đó gồm có x và $x+1$.

Xét $p(x) = a_0 + \dots + a_n x^n \in \mathbb{Z}_2[x]$.

Nếu $p(x)$ có bậc n , thì $a_n \neq 0$, và 1 là một nghiệm nếu và chỉ nếu $p(x)$ có một số chẵn các số hạng khác 0.

Do đó sau đây là các đa thức bậc 2, 3 và 4 trong $\mathbb{Z}_2[x]$ không có nhân tử tuyến tính:

Bậc 2: $x^2 + x + 1$

Bậc 3: $x^3 + x + 1$
 $x^3 + x^2 + 1$

Bậc 4: $x^4 + x + 1$
 $x^4 + x^2 + 1$
 $x^4 + x^3 + 1$
 $x^4 + x^3 + x^2 + x + 1$.

Nếu một đa thức bậc 2 hoặc 3 là khả quy, nó phải có một nhân tử tuyến tính; do đó các đa thức bậc 2 và 3 ở trên là bất khả quy.

Nếu một đa thức bậc 4 là khả quy, thì nó có nhân tử tuyến tính hoặc nó là tích của 2 nhân tử bậc 2 bất khả quy.

Khi đó chỉ có đa thức bậc 2 bất khả quy trong $\mathbb{Z}_2[x]$, và bình phương của nó $(x^2 + x + 1) = x^4 + x^2 + 1$ là khả quy.

Vậy các đa thức bất khả quy bậc nhỏ hơn hoặc bằng 4 trên $\mathbb{Z}_2$ là:

Bậc 1: x
 $x + 1$

Bậc 2: $x^2 + x + 1$

Bậc 3: $x^3 + x + 1$
 $x^3 + x^2 + 1$

Bậc 4: $x^4 + x + 1$
 $x^4 + x^3 + 1$
 $x^4 + x^3 + x^2 + x + 1$.

Bài tập 5. Tìm tất cả các đa thức bất khả quy bậc 2 trên $\mathbb{Z}_2$.

Giải: Gọi $f(x) = ax^2 + bx + c$ là đa thức bất khả quy trên $\mathbb{Z}_2$.

Do $f(x)$ bất khả quy nên $f(x)$ không có nghiệm trong $\mathbb{Z}_2$.

Suy ra $a.f(0).f(1) \neq 0$ hay $ac(a+b+c) \neq 0$.

$$\text{Do đó: } \begin{cases} ac \neq 0 \\ a+b+c \neq 0 \end{cases} \Leftrightarrow \begin{cases} a \neq 0 \\ c \neq 0 \\ a+b+c \neq 0 \end{cases} \Leftrightarrow \begin{cases} a=1 \\ b=1 \\ c=1 \end{cases}$$

Vậy đa thức $x^2 + x + 1$ là đa thức bất khả quy duy nhất trên $\mathbb{Z}_2$.

Bài tập 6. Nếu p là một số nguyên tố, chứng minh rằng $(x-a) \mid (x^{p-1}-1)$ trong $\mathbb{Z}_p[x]$ với mọi số $a \neq 0$ trong $\mathbb{Z}_p$. Từ đó chứng minh rằng:

$$x^{p-1}-1 = (x-1)(x-2)\dots(x-p+1) \text{ trong } \mathbb{Z}_p[x].$$

Giải: Do p là một số nguyên tố nên $(\mathbb{Z}_p^*, \cdot)$ là một nhóm cấp $p-1$.

Do đó với mọi $\bar{a} \in \mathbb{Z}_p^*$ ta có: $\bar{a}^{p-1} = \bar{1}$, hay là: $\bar{a}^{p-1} - \bar{1} = \bar{0}$.

Vậy mọi $x = \bar{a} \in \mathbb{Z}_p^*$ là nghiệm của đa thức $x^{p-1}-1$.

Theo chứng minh trên thì đa thức $x^{p-1}-1$ có $p-1$ nghiệm là $\bar{1}, \bar{2}, \dots, \overline{p-1}$.

Do p là số nguyên tố nên $\mathbb{Z}_p$ là một trường.

Vì vậy đa thức $x^{p-1}-1$ bậc $p-1$ có đúng $p-1$ nghiệm như trên. Do đó:

$$x^{p-1}-1 = (x-1)(x-2)\dots(x-p+1).$$

Bài tập 7. Chứng minh rằng $(n-1)! \equiv -1 \pmod{n}$ nếu và chỉ nếu n là số nguyên tố.

Giải: Giả sử n là số nguyên tố. Khi đó, theo Bài tập 6 ta có:

$$x^{n-1}-1 \equiv (x-1)(x-2)\dots(x-n+1) \pmod{n} \quad (*)$$

Thay $x=0$ vào đẳng thức (*) ta được:

$$(n-1)! \equiv -1 \pmod{n}$$

Ngược lại, giả sử $(n-1)! \equiv -1 \pmod{n}$. Ta chứng minh n là số nguyên tố.

Thật vậy, nếu n là hợp số thì tồn tại hai số $a, b \in \{2, 3, \dots, n-1\}$ sao cho $a.b = n$, nghĩa là $ab \equiv 0 \pmod{n}$.

Do đó: $(n-1)! = 1.2\dots(n-1) \equiv 0 \pmod{n}$, trái với giả thiết.

Bài tập 8. Chứng minh đa thức $P(x) = x^5 + 4x^4 + 2x^3 + 5x - 7$ là bất khả quy trên $\mathbb{Z}_2[x]$.

Giải: Trong $\mathbb{Z}_2[x]$ ta được $\bar{P}(x) = x^5 + x^2 + 1$.

Giả sử $\bar{P}(x) = f(x).g(x)$, với $f, g \in \mathbb{Z}_2$.

Nếu $\deg f = 1$ hoặc $\deg g = 1$ dễ thấy là vô lý vì $\bar{P}$ không có nghiệm trong $\mathbb{Z}_2$.

Suy ra $\bar{P}(x) = (x^2 + ax + b)(x^3 + cx^2 + dx + e)$, với $a, b, c, d, e \in \mathbb{Z}_2$.

Đồng nhất hệ số hai vế ta được điều vô lý.

Vậy đa thức $P(x) = x^5 + 4x^4 + 2x^3 + 5x - 7$ là bất khả quy trên $\mathbb{Z}_2[x]$.

Phần 3. KẾT LUẬN

Khóa luận này đã nghiên cứu sự phân tích đa thức trên các trường số. Nội dung của khóa luận này gồm hai chương:

Chương 1: Kiến thức chuẩn bị. Trong chương này, trình bày một số định nghĩa, tính chất của miền nguyên, trường, vành đa thức và đa thức bất khả quy. Từ những kết quả đó, tìm hiểu về sự phân tích đa thức trong mỗi trường khác nhau ở chương 2.

Chương 2: Phân tích đa thức trên các trường số. Ở chương này làm rõ các tính chất của đa thức trên các trường số và đưa ra một số tiêu chuẩn để phân tích đa thức trên các trường số.

Phần 4. TÀI LIỆU THAM KHẢO

Tiếng Anh:

[1]. R. Lidl and H. Niederreiter, *Introduction to finite fields and their application*, Cambridge University Press, 1986.

[2]. Serge Lang, *Algebra*, Columbia University, New York, 1965

Tiếng Việt:

[1]. Lê Thanh Hà, *Đa thức và nhân tử hóa*, NXB Giáo dục, 2000.

[2]. Nguyễn Tiến Quang, *Đại số đại cương*, NXB Giáo dục, 2008.

[3]. Nguyễn Tiến Quang, *Hướng dẫn giải bài tập Đại số đại cương*, NXB Giáo dục, 2009.

[4]. <http://luanvan.co/luan-van/mot-so-tinh-chat-cua-truong-huu-han-3270/>

Phần 5. PHỤ LỤC

Tam Kỳ, ngày 02 tháng 5 năm 2019

Duyệt

Người thực hiện

Đơn vị (Khoa/ tổ bộ môn)

Nguyễn Phan Hoài Linh