ĐẠI HỌC THÁI NGUYÊN
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

—————o0o—————

**ĐÀM THỊ NGỌC TÂM**

# VỀ TÍNH CHẴN LẺ CỦA SỐ NHÂN TỬ BẤT KHẢ QUY MODULO $P$ CỦA ĐA THỨC HỆ SỐ NGUYÊN

**LUẬN VĂN THẠC SĨ TOÁN HỌC**

THÁI NGUYÊN, 5/2019

ĐẠI HỌC THÁI NGUYÊN
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

—————o0o—————

**ĐÀM THỊ NGỌC TÂM**

# VỀ TÍNH CHẴN LẺ CỦA SỐ NHÂN TỬ BẤT KHẢ QUY MODULO $P$ CỦA ĐA THỨC HỆ SỐ NGUYÊN

**Chuyên ngành: Phương pháp Toán sơ cấp**
**Mã số: 8 46 01 13**

**LUẬN VĂN THẠC SĨ TOÁN HỌC**

GIÁO VIÊN HƯỚNG DẪN
**TS. NGUYỄN DUY TÂN**

THÁI NGUYÊN, 5/2019

# Mục lục

# Mở đầu

Cho $f(x) \in \mathbb{Z}[x]$ là một đa thức chuẩn (monic) hệ số nguyên bậc $n$ và không có nghiệm phức kép. Gọi $D(f)$ là biệt thức của $f$. Cho $p$ là một số nguyên tố lẻ và gọi $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ là trường hữu hạn có $p$ phần tử. Gọi $\bar{f}(x) \in \mathbb{F}_p[x]$ là đa thức nhận được từ $f$ bằng cách thu gọn hệ số modulo $p$. Gọi $r$ là số nhân tử bất khả quy của $\bar{f}$. Khi đó một định lý của Stickelberger khẳng định rằng $r$ và $n$ có cùng tính chẵn lẻ, tức là $r \equiv n \pmod 2$, khi và chỉ khi $D(f)$ là bình phương modulo $p$.

Mục tiêu của luận văn là tìm hiểu về chứng minh của Định lý Stickelberger này cũng như ứng dụng của nó trong chứng minh luật thuận nghịch bậc hai.

Ngoài phần Mở đầu, Kết luận và Tài liệu tham khảo, bố cục của luận văn được chia làm ba chương.

**Chương 1. Một số kiến thức chuẩn bị**

Chương này trình bày một số kiến thức về kết thức của hai đa thức, biệt thức của đa thức và đồng cấu Frobenius.

**Chương 2. Định lý Stickelberger**

Chương này trình bày về Định lý Stickelberger, một số ví dụ minh họa, và một tương tự của định lý này cho đa thức thực.

**Chương 3. Định lý Stickelberger và luật thuận nghịch bậc hai**

Chương này trình bày về ký hiệu Legendre, luật thuận nghịch bậc hai và một chứng minh của luật này sử dụng Định lý Stickelberger.

Luận văn này được thực hiện và hoàn thành vào tháng 5 năm 2019 tại trường Đại học Khoa học- Đại học Thái Nguyên. Qua đây, tác giả xin bày tỏ lòng biết ơn sâu sắc tới TS Nguyễn Duy Tân, người đã tận tình hướng dẫn trong suốt quá trình làm việc để hoàn thành luận văn này. Tác giả xin gửi lời cảm ơn chân thành đến Khoa Toán-Tin, Trường Đại học Khoa học - Đại học Thái Nguyên, đã tạo mọi điều kiện để giúp tác giả học tập và hoàn thành luận văn cũng như chương trình thạc sĩ. Tác giả cũng xin gửi lời cảm ơn tới tập thể lớp cao học K11D, khóa 05/2017 - 05/2019 đã động viên giúp đỡ tác giả trong quá trình học tập và hoàn thành luận văn

này. Đồng thời tác giả xin gửi lời cảm ơn tới Ban giám hiệu và các đồng nghiệp tại trường THCS Hưng Đạo, Đông Triều, Quảng Ninh đã tạo điều kiện cho tác giả trong suốt quá trình học tập và hoàn thành luận văn.

Xin chân thành cảm ơn.

Thái Nguyên, tháng 5 năm 2019

Xác nhận của người hướng dẫn

**TS. Nguyễn Duy Tân**

Người viết luận văn

**Đàm Thị Ngọc Tâm**

# Chương 1. Một số kiến thức chuẩn bị

Chương này trình bày một số kiến thức về kết thức của hai đa thức, biệt thức của đa thức và đồng cấu Frobenius. Tài liệu tham khảo sử dụng cho chương này là tài liệu [2, Section 6.6] và [3, Chapter 15].

## 1.1 Kết thức của hai đa thức

Giả sử $f, g$ là hai đa thức biến $x$ với các hệ số trong một trường $F$. Giả sử $K$ là một trường đóng đại số chứa $F$. Gọi $\alpha_1, \ldots, \alpha_n$ là tất cả các nghiệm (kể cả bội) của $f$ trong $K$, tức là

$$f(x) = a(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n), \text{ với } a \in K \text{ nào đó.}$$

Tương tự, gọi $\beta_1, \ldots, \beta_m$ là tất cả các nghiệm (kể cả bội) của $g$ trong $K$, tức là

$$g(x) = b(x-\beta_1)(x-\beta_2)...(x-\beta_m), \text{ với } b \in K \text{ nào đó.}$$

Ta định nghĩa *kết thức* của $f$ và $g$, $R(f,g)$ là

$$R(f,g) = a^m b^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) \quad (n = \deg f, m = \deg g).$$

Ta liệt kê dưới đây một số tính chất của kết thức.

**Tính chất 1.1.1.** $R(g,f) = (-1)^{mn} R(f,g)$.

*Chứng minh.* Ta có

$$R(g,f) = a^m b^n \prod_{j=1}^{m}\prod_{i=1}^{n}(\beta_j - \alpha_i) = a^m b^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) = (-1)^{mn} R(f,g).$$

Ta có điều phải chứng minh □

**Tính chất 1.1.2.** *$R(f,g) = 0$ nếu $f$ và $g$ có một nhân tử chung bậc dương.*

*Chứng minh.* Nếu $f$ và $g$ có một nhân tử chung là $h(x) \in F[x]$. Khi đó gọi $\alpha \in K$ một nghiệm của $h$ trong $K$. Như vậy tồn tại $i$, $j$ sao cho $\alpha_i = \alpha$ và $\beta_j = \alpha$. Ta suy ra trong tích định nghĩa $R(f,g)$ có nhân tử $\alpha_i - \beta_j = 0$ và do vậy $R(f,g) = 0$. □

**Tính chất 1.1.3.** $R(f,g) = a^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b^n \prod_{j=1}^{m} f(\beta_j)$.

*Chứng minh.* Vì $g(x) = b\prod_{j=1}^{n}(x - \beta_i)$, nên ta có $g(\alpha_i) = b\prod_{j=1}^{n}(\alpha_i - \beta_j)$, với mọi $i = 1, \ldots, n$. Do vậy

$$a^m \prod_{i=1}^{n} g(\alpha_i) = a^m b^n \prod_{i=1}^{n}\prod_{j=1}^{n}(\alpha_i - \beta_j) = R(f,g).$$

Tương tự (hoặc sử dụng Tính chất 1.1.1) ta suy ra

$$R(f,g) = (-1)^{mn} b^n \prod_{j=1}^{m} f(\beta_j).$$

□

**Tính chất 1.1.4.** *Nếu $g(x) = fq + r$, thì $R(f,g) = a^{m-\deg r} R(f,r)$.*

*Chứng minh.* Từ Tính chất 1.1.3, ta có

$$R(f,g) = a^{\deg g} \prod_{i}^{n} g(\alpha_i) = a^{\deg g} \prod_{i=1}^{n} [f(\alpha_i)q(\alpha_i) + r(\alpha_i)].$$

Vì $\alpha_i$ là nghiệm của của $f$, nên $f(\alpha_i) = 0$ và do vậy $f(\alpha_i)q(\alpha_i) + r(\alpha_i) = r(\alpha)$. Do đó ta có

$$R(f, g) = a^{\deg g} \prod_{i=1}^{n} r(\alpha_i).$$

Mặt khác, cũng theo Tính chất 1.1.3 $R(f, r) = a^{\deg r} \prod_{i=1}^{n} r(\alpha_i)$. Do vậy

$$R(f, g) = a^{\deg g} \prod_{i=1}^{n} r(\alpha_i) = a^{\deg g - \deg r} R(f, r).$$

□

**Tính chất 1.1.5.** *$R(f, b) = b^{\deg f}$ nếu $b$ là vô hướng.*

*Chứng minh.* Đặt $g(x) = b$. Theo Tính chất 1.1.3

$$R(f, g) = a^0 \prod_{i=1}^{n} g(\alpha_i) = b^n.$$

□

Các Tính chất 1.1.1,1.1.4, 1.1.5 cho phép ta tính toán kết thức của bất kì hai đa thức nào bằng thuật toán chia của Euclid. Các tính chất này cũng cho phép ta chứng minh được rằng kết thức $R(f, g)$ là một phần tử của trường $F$ mặc dù nó được định nghĩa dựa theo các phần tử trong trường lớn hơn $K$.

**Tính chất 1.1.6.** *Ta có $R(f, g)$ nằm trong $F$.*

*Chứng minh.* Ta chứng minh bằng quy nạp theo $\deg f$. Nếu $g = b$ là hằng số thuộc $F$. Thì theo Tính chất 1.1.1 và 1.1.5, $R(f, g) = R(b, f) = R(f, b) = b^n$ thuộc $F$.

Giả sử khẳng định đã đúng với mọi mọi đa thức $f$ và $g$ với $f$ có bậc nhỏ hơn hoặc bằng $n - 1$. Xét $f$ và $g$ là hai đa thức tùy ý với $\deg f = n \geq 1$. Khi đó theo thuật toán chia đa thức, tồn tại hai đa thức $q$ và $r$ trong $F[x]$ sao cho

$$g = fq + r,$$

với $r = 0$ hoặc $\deg r < \deg f = n$. Theo Tính chất 1.1.4, Tính chất 1.1.1 và theo giả thiết quy nạp ta có $R(f, g) = R(f, r) = \pm R(r, f)$ thuộc $F$. Ta có điều phải chứng minh. □

**Tính chất 1.1.7.** *Ta có*

1. *Nếu* $f = f_1 f_2$ *thì* $R(f,g) = R(f_1,g)R(f_2,g)$.

2. *Nếu* $g = g_1 g_2$ *thì* $R(f,g) = R(f,g_1)R(f,g_2)$.

*Chứng minh.* Suy ra từ Tính chất 1.1.3. □

## 1.2 Biệt thức của đa thức

Cho $f = f(x) \in F[x]$ là đa thức với hệ số trong trường $F$ và $K$ là một trường đóng đại số chứa $F$.

*Biệt thức* của $f$ được định nghĩa là

$$D(f) = (-1)^{n(n-1)/2} R(f, f'),$$

ở đây $f'$ là đạo hàm của $f$ và $n = \deg f$.

Theo Tính chất 1.1.2, ta có $D(f) \neq 0$ nếu và chỉ nếu $f$ và $f'$ không có thừa số chung.

Chúng ta có thể tính toán $D(f)$ bằng cách sử dụng thuật toán Euclid trên $f$ và $f'$. Dưới đây là một số ví dụ.

**Ví dụ 1.2.1.** Xét $f(x) = x - a$. Khi đó $f'(x) = 1$, vì vậy

$$D(f) = (-1)^{(1.0)/2} R(f,1) = R(f,1) = 1^{\deg f} = 1.$$

**Ví dụ 1.2.2.** Xét $f(x) = x^2 + ax + b$. Khi đó $f'(x) = 2x + a$ và $D(f) = -R(f,f')$. Ta có

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

Đặt $r = b - \dfrac{a^2}{4}$. Ta có

$$\begin{aligned} D(f) &= -R(f,f') \\ &= -R(f',f) \quad \text{(theo Tính chất 1.1.1)} \\ &= 2^{\deg f - \deg r}(-1)R(f',r) \quad \text{( theo Tính chất 1.1.4)} \\ &= -2^{2-0}R(f',r) \\ &= -4r = a^2 - 4b. \end{aligned}$$

**Ví dụ 1.2.3.** Cho $f(x) = x^3 + qx + r$. Thì $f'(x) = 3x^2 + q$ và thực hiện thuật toán Euclid, ta có

$$x^3 + qx + r = (3x^2 + q)\left(\frac{x}{3}\right) + \left(\frac{2q}{3}x + r\right),$$
$$3x^2 + q = \left(\frac{2q}{3}x + r\right)\left(\frac{9x}{2q} - \frac{27r}{4q^2}\right) + \left(q + \frac{27r^2}{4q^2}\right).$$

Do đó

$$\begin{aligned} D(f) &= (-1)^{3\cdot 2/2} R(f, f') = -R(f, f') \\ &= -R(f', f) \quad \text{(theo Tính chất 1.1.1)} \\ &= -3^{\deg f - 1} R(f', \frac{2qx}{3} + r) \quad \text{(theo Tính chất 1.1.4)} \\ &= -9R(\frac{2qx}{3} + r, f') \quad \text{(theo Tính chất 1.1.1)} \\ &= -9\left(\frac{2q}{3}\right)^2 R(\frac{2qx}{3} + r, q + \frac{27r^2}{4q^2}) \\ &= -4q^2(q + \frac{27r^2}{4q^2}) = -4q^3 - 27r^2. \end{aligned}$$

**Ví dụ 1.2.4.** Xét $f(x) = x^n - 1 \in F[x]$. Ta đi tính biệt thức của $f(x)$. Gọi $\alpha_1, \ldots, \alpha_n$ là $n$ nghiệm trong $K$ (một trường đóng đại số chứa $F$) của đa thức $f(x) = x^n - 1$. Ta có $f'(x) = nx^{n-1}$. Do vậy

$$\begin{aligned} D(f) &= (-1)^{n(n-1)/2} R(f, f') = (-1)^{n(n-1)/2} \prod_{k=1}^{n} f'(\alpha_k) \\ &= (-1)^{n(n-1)/2} n^n \left(\prod_{k=1}^{n} \alpha_k\right)^{n-1} \\ &= (-1)^{n(n-1)/2} n^n (-1)^{n(n-1)} \\ &= (-1)^{n(n-1)/2} n^n. \end{aligned}$$

Vì theo định lý Viéte $\alpha_1 \cdots \alpha_n = (-1)^n$.

Đa thức $f(x) \in F[x]$ được gọi là một đa thức chuẩn (monic) nếu hệ số ứng với số mũ cao nhất của nó bằng 1.

**Mệnh đề 1.2.5.** *Cho $f$ là một đa thức monic và $\alpha_1, \ldots, \alpha_n$ là các nghiệm*