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

**DƯƠNG THỊ LAN HƯƠNG**

# VỀ MỘT SỐ THUẬT TOÁN PHÂN TÍCH ĐA THỨC MỘT BIẾN THÀNH NHÂN TỬ

**LUẬN VĂN THẠC SĨ TOÁN HỌC**

**THÁI NGUYÊN - 2016**

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

**DƯƠNG THỊ LAN HƯƠNG**

# VỀ MỘT SỐ THUẬT TOÁN PHÂN TÍCH ĐA THỨC MỘT BIẾN THÀNH NHÂN TỬ

## LUẬN VĂN THẠC SĨ TOÁN HỌC

**Chuyên ngành: Phương pháp Toán sơ cấp**
**Mã số: 60 46 01 13**

NGƯỜI HƯỚNG DẪN KHOA HỌC:
**TS. Đoàn Trung Cường**

**THÁI NGUYÊN - 2016**

# Mục lục

# Danh sách ký hiệu

| | |
|---|---|
| $\mathbb{Z}$ | vành các số nguyên |
| $\mathbb{Q}$ | trường các số hữu tỷ |
| $\mathbb{F}_p$ | trường có $p$ phần tử |
| $K[X]$ | vành đa thức với hệ số trên trường K |
| $P(X)$ | đa thức một biến $X$ |
| $\deg P(X)$ | bậc của đa thức $P(X)$ |
| mod $p$ | modulo $p$ |
| $a \nmid b$ | $a$ không là ước của $b$ |
| $\gcd(P(X), Q(X))$ | ước chung lớn nhất của hai đa thức $P(X)$ và $Q(X)$ |

# Mở đầu

Đa thức là một khái niệm cơ sở của toán học. Một mặt đa thức là đối tượng nghiên cứu của đại số, một mặt chúng xuất hiện trong tất cả các lĩnh vực của toán học cũng như nhiều lĩnh vực khoa học khác. Các bài toán về đa thức xuất hiện cả trong toán phổ thông cũng như toán cao cấp. Trong toán phổ thông, những bài toán về đa thức thường là những bài toán khó, hay xuất hiện trong các kỳ thi học sinh giỏi, kể cả các kỳ thi Học sinh giỏi Quốc gia và Olympic Toán Quốc tế.

Khi xét đa thức, một vấn đề được người ta quan tâm là tính bất khả quy và rộng hơn là phân tích của đa thức đó thành tích các đa thức bất khả quy. Tính chất này cũng tương tự như của các số nguyên là tính chất nguyên tố và phân tích thành tích các số nguyên tố. Các câu hỏi về tính bất khả quy và phân tích bất khả quy của đa thức nói chung là khó trả lời hơn nhiều. Do vậy, việc hệ thống lại một số tiêu chuẩn về đa thức bất khả quy và nghiên cứu một số thuật toán phân tích đa thức một biến (với hệ số nguyên) thành nhân tử là cần thiết. Với lý do như vậy, chúng tôi chọn đề tài *"Về một số thuật toán phân tích đa thức một biến thành nhân tử"*.

Khác với các số nguyên, một thuật toán để phân tích một đa thức nguyên thành tích các đa thức nguyên bất khả quy là không hiển nhiên. Nếu xét đa thức với hệ số trên một trường hữu hạn thì việc phân tích sẽ khả thi hơn, vì chỉ có hữu hạn đa thức có bậc nhỏ hơn bậc của một đa thức cho trước. Với các đa thức hệ số nguyên, những thuật toán phân tích đa thức thành nhân tử mà hiệu quả (về mặt tính toán) đều đưa đa thức về xét trên trường hữu hạn, sau đó nâng phân tích tìm được lên lại vành các số nguyên.

Trong luận văn này, chúng tôi trình bày một số thuật toán phân tích một đa thức thành tích các nhân tử bất khả quy, trong đó xét các trường hợp đa thức nguyên,

đa thức có hệ số trên một trường hữu hạn $\mathbb{F}_p$. Nội dung chính của luận văn là trình bày chi tiết những kết quả chọn lọc trong một số tài liệu về tiêu chuẩn đa thức bất khả quy thông qua thu gọn mod $p$ (reduction mod $p$) và các thuật toán phân tích đa thức một biến thành nhân tử bất khả quy như thuật toán Kronecker, thuật toán Yun, thuật toán Zassenhaus.

Nội dung của luận văn được trình bày trong ba chương:

*Chương 1. Kiến thức chuẩn bị*. Trong chương này chúng tôi trình bày các kiến thức cơ sở chuẩn bị cho các chương sau như định lý phân tích đa thức thành nhân tử, bổ đề Gauss, thuật toán chia đa thức và thuật toán tìm ước chung lớn nhất của hai đa thức.

*Chương 2. Thu gọn mod p và đa thức bất khả quy*. Chúng tôi trình bày việc xét tính chất bất khả quy của một đa thức nguyên thông qua thu gọn mod $p$ với $p$ là một số nguyên tố. Kết quả chính được trình bày là tiêu chuẩn bất khả quy Eisenstein và các mở rộng của nó. Các tiêu chuẩn này được trình bày rất ngắn gọn thông qua thu gọn mod $p$.

*Chương 3. Một số thuật toán phân tích đa thức thành nhân tử*. Trong chương này chúng tôi trình bày thuật toán Kronecker để phân tích một đa thức nguyên thành nhân tử. Đây là thuật toán đầu tiên để phân tích đa thức nguyên, tuy nhiên chỉ có ý nghĩa lý thuyết do về mặt tính toán thì rất không hiệu quả.

Tiếp theo chúng tôi trình bày thuật toán Yun để phân tích một đa thức thành các ước không chứa bình phương. Thuật toán tiếp theo chúng tôi trình bày là phân tích các đa thức với hệ số trên trường hữu hạn thành nhân tử. Ý tưởng của các thuật toán này được sử dụng trong thuật toán Zassenhaus, trình bày trong phần cuối cùng của Chương 3, để phân tích một đa thức nguyên thành tích các đa thức nguyên bất khả quy. Ý tưởng của thuật toán này là chuyển việc xét đa thức nguyên về xét trên trường $\mathbb{F}_p$, sau đó sử dụng thuật toán trước để phân tích đa thức thành tích các đa thức bất khả quy trên $\mathbb{F}_p$. Cuối cùng, sử dụng một dạng của Bổ đề Hensel để nâng phân tích này lên trên $\mathbb{Z}$.

Luận văn này được thực hiện tại Trường Đại học Khoa học - Đại học Thái

Nguyên và hoàn thành với sự hướng dẫn của TS. Đoàn Trung Cường (Viện Toán học - Viện Hàn lâm Khoa học và Công nghệ Việt Nam). Tác giả xin được bày tỏ lòng biết ơn chân thành và sâu sắc tới người hướng dẫn khoa học của mình, người đã đặt vấn đề nghiên cứu, dành nhiều thời gian hướng dẫn và tận tình giải đáp những thắc mắc của tác giả trong suốt quá trình làm luận văn.

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

Tác giả muốn gửi những lời cảm ơn tốt đẹp nhất tới tập thể Lớp B, cao học Toán khóa 8 (2014-2016) đã động viên và giúp đỡ tác giả rất nhiều trong suốt quá trình học tập.

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

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

*Thái Nguyên, ngày 20 tháng 5 năm 2016*

Tác giả

**Dương Thị Lan Hương**

# Chương 1

# Kiến thức chuẩn bị

Mục đích của chương này là nhắc lại một số kiến thức chuẩn bị cần thiết cho việc trình bày các kết quả trong các chương sau. Nội dung của chương là chúng tôi nhắc lại một số định lí về đa thức bất khả quy và phân tích bất khả quy, thuật toán chia đa thức, thuật toán tìm ước chung lớn nhất của hai đa thức. Hầu hết các kết quả trong chương này được trình bày dựa theo tài liệu [2].

## 1.1 Phân tích bất khả quy của đa thức

Trong tiết này, chúng ta nhắc lại một số kết quả về đa thức bất khả quy và sự tồn tại phân tích bất khả quy.

Nhắc lại, một đa thức khác hằng với hệ số trên một trường là bất khả quy nếu nó không phân tích được thành tích của hai đa thức có bậc nhỏ hơn. Ví dụ, mọi đa thức bậc nhất $aX+b$, với $a \neq 0$, đều là bất khả quy.

Tính chất bất khả quy của một đa thức phụ thuộc vào trường hệ số được xét. Ví dụ, đa thức $P(X) = X^2 + 1$ là đa thức bất khả quy trong $\mathbb{R}[X]$ nhưng là đa thức khả quy trong $\mathbb{C}[X]$ vì $P(X) = (X-i)(X+i)$.

Để xét tính chất bất khả quy của một đa thức, ta hay dùng bổ đề đơn giản sau để biến đổi đa thức về dạng mà ta có thể áp dụng một số tiêu chuẩn bất khả quy đã biết.

**Bổ đề 1.1.1.** *Cho đa thức $P(X)$ với hệ số trên một trường $K$. Với mỗi $a \in K$, đa thức $P(X)$ là bất khả quy khi và chỉ khi đa thức $P(X+a)$ là bất khả quy.*

*Chứng minh.* Trước hết nhận xét rằng $\deg P(X) = \deg P(X+a)$. Ngoài ra, một phân tích $P(X) = H(X)K(X)$ tương đương với một phân tích $P(X+a) = H(X+a)K(X+a)$. Vì vậy $P(X)$ là khả quy khi và chỉ khi $P(X+a)$ là khả quy. □

Hai đa thức $P(X), Q(X)$ được gọi là liên hợp nếu $P(X) = \lambda Q(X)$ với một hằng số $\lambda \neq 0$ nào đó.

**Định lí 1.1.2** (Phân tích thành nhân tử)**.** *Giả sử K là một trường. Khi đó mọi đa thức $P(X) \in K[X]$ khác hằng đều có phân tích*

$$P(X) = P_1^{\alpha_1} \dots P_r^{\alpha_r}$$

*với $P_i \in K[X]$ là đa thức bất khả quy đôi một không liên hợp, $\alpha_1, \dots, \alpha_r > 0$. Hơn nữa phân tích này là duy nhất sai khác một thứ tự của các ước bất khả quy.*

Với đa thức nguyên, ta cũng định nghĩa một đa thức nguyên khác hằng là bất khả quy nếu nó không phân tích được thành tích hai đa thức có bậc nhỏ hơn. Với định nghĩa này thì đa thức nguyên bất khả quy không là một phần tử bất khả quy trong vành $\mathbb{Z}[X]$ như định nghĩa thông thường. Ví dụ, đa thức nguyên $2X+4 = 2(X+2)$ vẫn là đa thức bất khả quy theo định nghĩa trên. Trong toàn bộ luận văn này ta sẽ sử dụng định nghĩa đa thức nguyên bất khả quy này.

Một đa thức nguyên cũng là một đa thức hữu tỷ (có hệ số trên trường các số hữu tỷ $\mathbb{Q}$). Liên hệ giữa tính chất bất khả quy trên $\mathbb{Z}$ và trên $\mathbb{Q}$ được thể hiện trong định lý nổi tiếng sau, thường gọi là Bổ đề Gauss.

**Định lí 1.1.3** (Bổ đề Gauss)**.** *Cho một đa thức nguyên $P(X)$ khác hằng. Giả sử có phân tích $P(X) = G(X)F(X)$ với $G(X), F(X)$ là các đa thức có hệ số hữu tỷ. Khi đó tồn tại các đa thức nguyên $G_*(X)$, $F_*(X)$ sao cho $\deg G(X) = \deg G_*(X)$, $\deg F(X) = \deg F_*(X)$ và $P(X) = G_*(X)F_*(X)$. Nói riêng, nếu $P(X)$ là khả quy trên $\mathbb{Q}$ thì nó phân tích được thành tích của hai đa thức với hệ số nguyên có bậc thấp hơn.*