ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN HÀ LINH

ĐA THỨC BẤT KHẢ QUY

LUẬN VĂN THẠC SỸ TOÁN HỌC

Thái Nguyên – 2012

Mục lục

LỜI CẢM ƠN

Tôi xin gửi lời biết ơn chân thành nhất đến PGS.TS Lê Thị Thanh Nhàn. Cô đã dành rất nhiều thời gian và tâm huyết trong việc hướng dẫn tôi. Cho đến hôm nay, luận văn thạc sĩ của tôi đã được hoàn thành cũng chính là nhờ sự nhắc nhở, đôn đốc, sự giúp đỡ nhiệt tình của Cô.

Tôi xin trân trọng cảm ơn Ban Giám hiệu, Khoa Toán - Tin và Phòng Đào tạo - Khoa học và Quan hệ quốc tế của trường Đại học Khoa học - Đại học Thái Nguyên. Tôi xin trân trọng cảm ơn các Thầy Cô đã tận tình truyền đạt những kiến thức quý báu cũng như tạo mọi điều kiện thuận lợi nhất để tôi hoàn thành luận văn này.

Tôi xin chân thành bày tỏ lòng biết ơn đến gia đình, bạn bè, những người đã không ngừng động viên, hỗ trợ và tạo mọi điều kiện tốt nhất cho tôi trong suốt thời gian học tập và thực hiện luận văn.

LỜI NÓI ĐẦU

Trong lý thuyết đa thức, đa thức bất khả quy đóng một vai trò quan trọng giống như vai trò của số nguyên tố trong tập các số nguyên. Nếu Định lý cơ bản của Số học cho phép coi các số nguyên tố như là những viên gạch xây nên tập các số nguyên, thì các đa thức bất khả quy chính là những viên gạch xây nên tập tất cả đa thức. Bởi vì mỗi đa thức bậc dương dạng chuẩn (tức là hệ số cao nhất bằng 1) với hệ số trên một trường đều viết được thành tích của hữu hạn đa thức bất khả quy dạng chuẩn và sự phân tích đó là duy nhất nếu không kể đến thứ tự các nhân tử.

Bài toán xét tính bất khả quy của các đa thức trên trường phức $\mathbb{C}$ và trên trường thực $\mathbb{R}$ đã được giải quyết từ đầu thế kỉ 19, khi người ta chứng minh được Định lý cơ bản của Đại số. Cụ thể, các đa thức bất khả quy trên $\mathbb{C}$ là và chỉ là các đa thức bậc nhất; các đa thức bất khả quy trên $\mathbb{R}$ là và chỉ là các đa thức bậc nhất hoặc bậc hai với biệt thức âm. Tuy nhiên bài toán xét tính bất khả quy của đa thức trên trường hữu tỷ $\mathbb{Q}$ hoặc trên trường thặng dư $\mathbb{Z}_p$ (với p là số nguyên tố) vẫn đang thử thách các nhà toán học trên thế giới.

Mục đích của luận văn là trình bày một số kết quả về đa thức bất khả quy trên một trường, đặc biệt là trên trường $\mathbb{Q}$ và trường $\mathbb{Z}_p$. Nội dung của luận văn được viết dựa theo cuốn sách ``Lý thuyết Galois" của J. Rotman [Rot], cuốn sách ``Đa thức và tính bất khả quy" của A. Schinzel [Sc], bài báo ``Tính bất khả quy của đa thức" đăng trên Tạp chí Đại số của I. Seres [S] và bài báo ``Tiêu chuẩn bất khả quy của đa thức" đăng trên tạp chí nổi tiếng Ann. Math của H. L. Dorwart - O. Ore [DO].

Luận văn gồm 3 chương. Chương 1 trình bày một số kiến thức cơ sở về đa thức bất khả quy và sử dụng đa thức bất khả quy để chứng minh Định

lý Kronecker về sự tồn tại của trường phân rã của đa thức (Định lý 1.3.2) và Định lý của Galois về sự tồn tại một trường có hữu hạn phần tử (Định lý 1.3.5). Chương 2 trình bày một số phương pháp xét tính bất khả quy của đa thức trên trường $\mathbb{Q}$ như phương pháp tìm nghiệm hữu tỷ, phương pháp dùng Bổ đề Gauss, tiêu chuẩn Eisenstein và phương pháp rút gọn theo môđun một số nguyên tố. Bằng cách sử dụng Định lý Kronecker về sự tồn tại trường phân rã và Định lý Lagrange về cấp của nhóm hữu hạn (Định lý 3.1.7), tính bất khả quy của một số đa thức trên trường $\mathbb{Z}_p$ (với p là một số nguyên tố) được trình bày trong Chương 3.

Chương 1

Đa thức bất khả quy

Trước khi trình bày khái niệm và một số kết quả về đa thức bất khả quy, chúng ta trình bày kiến thức cơ sở về đa thức.

1.1 Khái niệm đa thức

1.1.1 Định nghĩa. Một tập F cùng với hai phép toán, kí hiệu là phép cộng và phép nhân, được gọi là *trường* nếu các tính chất sau thỏa mãn

(i) Kết hợp: $a + (b + c) = (a + b) + c$ và $(ab)c = a(bc)$ với mọi $a, b, c \in F$.

(ii) Giao hoán: $a + b = b + a$ và $ab = ba$ với mọi $a, b \in F$.

(iii) Luật phân phối: $a(b + c) = ab + ac$ với mọi $a, b, c \in F$.

(iv) Tồn tại *phần tử đơn vị* $1 \in F$ sao cho $a1 = 1a = a$ với mọi $a \in F$.

(v) Tồn tại phần tử $0 \in F$ sao cho $a + 0 = 0 + a = a$ với mọi $a \in F$.

(vi) Mỗi $a \in F$, tồn tại phần tử đối $-a \in F$ sao cho $a + (-a) = 0$.

(vii) Mỗi $0 \neq a \in F$, tồn tại *phần tử nghịch đảo* $a^{-1} \in F$ sao cho $aa^{-1} = 1$.

1.1.2 Định nghĩa. Cho F là một trường và $a_0, a_1, \ldots, a_m \in F$. Một biểu thức có dạng $f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$ được gọi là một *đa thức* một biến x. Tập các đa thức với hệ số trên F được kí hiệu là $F[x]$. Nếu

$a_m \neq 0$ thì ta nói *bậc* của $f(x)$ là m và kí hiệu là $\deg f(x) = m$. Hệ số a_m được gọi là *hệ số cao nhất* của f. Nếu $a_m = 1$ thì $f(x)$ được gọi là *đa thức dạng chuẩn* (monic polynomial). Hai đa thức là *bằng nhau* nếu nó có cùng bậc và các hệ số tương ứng là bằng nhau. Với hai đa thức $f(x) = \sum a_i x^i$ và $g(x) = \sum b_i x^i$, ta định nghĩa *tổng* $f(x) + g(x) = \sum (a_i + b_i)x^i$ và *tích* $f(x)g(x) = \sum c_k x^k$, trong đó $c_k = \sum_{i+j=k} a_i b_j$.

Từ định nghĩa trên ta có ngay các tính chất sau đây.

1.1.3 Bổ đề. *Cho $f(x), g(x), h(x) \in F[x]$. Khi đó*

(i) $\deg(f(x) + g(x)) \leqslant \max\{\deg f(x), \deg g(x)\}$.

(ii) Nếu $f(x) \neq 0$ và $g(x) \neq 0$ thì $f(x)g(x) \neq 0$ và

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

(iii) Nếu $f(x) \neq 0$ và $f(x)g(x) = f(x)h(x)$ thì $g(x) = h(x)$.

1.1.4 Định nghĩa. Cho $f(x), g(x) \in F[x]$. Nếu $f(x) = q(x)g(x)$ với $q(x) \in F[x]$ thì ta nói rằng $g(x)$ là *ước* của $f(x)$ hay $f(x)$ là *bội* của $g(x)$ và ta viết $g(x)|f(x)$. Tập các bội của $g(x)$ được kí hiệu là (g).

Ta có ngay các tính chất đơn giản sau đây.

1.1.5 Bổ đề. *Các phát biểu sau là đúng.*

(i) Với $c \in F$ và k là số tự nhiên ta có $(x - c)|(x^k - c^k)$.

(ii) Nếu $f(x) \in F[x]$ và $c \in F$ thì tồn tại $q(x) \in F[x]$ sao cho

$$f(x) = q(x)(x - c) + f(c).$$

1.1.6 Định nghĩa. Cho $f(x) = a_m x^m + \ldots + a_0 \in F[x]$. Giả sử K là một trường chứa F. Một phần tử $c \in K$ được gọi là nghiệm của $f(x)$ nếu $f(c) = a_m c^m + \ldots + a_0 = 0$. Trong trường hợp này ta cũng nói c là nghiệm của phương trình $f(x) = 0$.

1.1.7 Bổ đề. *Cho $f(x) \in F[x]$ và $c \in F$. Khi đó*

(i) c là nghiệm của $f(x)$ nếu và chỉ nếu $f(x)$ là bội của $x - c$.

(ii) Số nghiệm của $f(x)$ không vượt quá $\deg f(x)$.

1.1.8 Mệnh đề. (Thuật toán chia với dư). *Cho $f(x), g(x) \in F[x]$ với $g(x) \neq 0$. Khi đó tồn tại duy nhất cặp đa thức $q(x), r(x) \in F[x]$ sao cho*

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

trong đó $r(x) = 0$ hoặc $\deg r(x) < \deg g(x)$.

1.1.9 Định nghĩa. Một tập con $I \neq \emptyset$ của $F[x]$ được gọi là một *iđêan* của $F[x]$ nếu nó thỏa mãn các điều kiện sau

(i) Nếu $f(x), g(x) \in I$ thì $f(x) + g(x) \in I$;

(ii) Nếu $f(x) \in I$ và $q(x) \in F[x]$ thì $q(x)f(x) \in I$.

Chú ý rằng tập con $I \neq \emptyset$ của $F[x]$ là iđêan nếu và chỉ nếu $f - g \in I$ và $fh \in I$ với mọi $f(x), g(x) \in I$ và $h(x) \in F[x]$.

1.1.10 Mệnh đề. *Nếu $I \neq \{0\}$ là một iđêan trong $F[x]$ và $d(x) \neq 0$ là đa thức có bậc bé nhất trong I thì*

$$I = (d) = \{d(x)q(x) \mid q(x) \in F[x]\}.$$

Chứng minh. Cho đa thức $f(x) \in I$. Viết $f(x) = d(x)q(x) + r(x)$ trong đó $r(x) = 0$ hoặc $\deg r(x) < \deg d(x)$. Vì $f(x), d(x) \in I$ nên ta có $r(x) = f(x) - d(x)q(x) \in I$. Do đó $r(x) = 0$ theo cách chọn $d(x)$. Suy ra $f(x) = d(x)q(x)$. Ngược lại, vì $d(x) \in I$ nên $d(x)q(x) \in I$ với mọi $q(x) \in F[x]$. □

1.1.11 Định nghĩa. Một đa thức dạng chuẩn $d(x) \in F[x]$ được gọi là *ước chung lớn nhất* của $f(x), g(x) \in F[x]$ nếu $d(x)|f(x)$, $d(x)|g(x)$ và nếu $h(x)|f(x)$ và $h(x)|g(x)$ thì $h(x)|d(x)$. Ta kí hiệu ước chung lớn nhất của

$f(x)$ và $g(x)$ là $\gcd(f(x), g(x))$. Nếu $\gcd(f(x), g(x)) = 1$ thì ta nói $f(x)$ và $g(x)$ là *nguyên tố cùng nhau.*

Từ Mệnh đề 1.1.10 ta có kết quả sau.

1.1.12 Mệnh đề. *Nếu $f(x), g(x)$ là hai đa thức không đồng thời bằng 0 thì $\gcd(f(x), g(x))$ luôn tồn tại và là tổ hợp tuyến tính của $f(x)$ và $g(x)$, tức là tồn tại $a(x), b(x) \in F[x]$ sao cho*

$$\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

1.1.13 Hệ quả. *Cho $p(x), f(x), g(x) \in F[x]$. Nếu $\gcd(p(x), f(x)) = 1$ và $p(x)|f(x)g(x)$ thì $p(x)|g(x)$.*

Chứng minh. Theo giả thiết, $1 = p(x)a(x) + f(x)b(x)$. Suy ra

$$g(x) = p(x)a(x)g(x) + f(x)b(x)g(x).$$

Do $p(x)$ là ước của đa thức ở vế phải nên $p(x)|g(x)$. □

Với $0 \neq g(x) \in F[x]$, kí hiệu $g^*(x) = g(x)/a_n$ trong đó a_n là hệ số cao nhất của $g(x)$. Chú ý rằng $g^*(x)$ là đa thức dạng chuẩn. Để tìm ước chung lớn nhất ta có thuật toán sau:

1.1.14 Mệnh đề. (Thuật toán Euclid tìm ước chung lớn nhất). *Cho hai đa thức $f(x), g(x) \in F[x]$ với $g(x) \neq 0$. Nếu $g(x)|f(x)$ thì*

$$\gcd(f(x), g(x)) = g^*(x).$$

Nếu ngược lại, chia liên tiếp ta được

$$\begin{aligned}
f(x) &= q(x)g(x) + r(x),\ r(x) \neq 0, \deg r(x) < \deg g(x).\\
g(x) &= q_1(x)r(x) + r_1(x),\ r_1(x) \neq 0, \deg r_1(x) < \deg r(x).\\
&\cdots\cdots\cdots\\
r_{n-2}(x) &= q_n(x)r_{n-1}(x) + r_n(x),\ r_n(x) \neq 0, \deg r_n(x) < \deg r_{n-1}(x).\\
r_{n-1}(x) &= q_{n+1}(x)r_n(x).
\end{aligned}$$

Khi đó $\gcd(f(x), g(x)) = r_n^*(x)$.

Chứng minh. Từ đẳng thức cuối ta có $r_n(x)|r_{n-1}(x)$. Thay vào đẳng thức thứ hai từ dưới lên ta có $r_n(x)|r_{n-2}(x)$. Cứ tiếp tục lập luận với các đẳng thức từ dưới lên trên ta suy ra $r_n(x)|g(x)$ và $r_n(x)|f(x)$. Do đó $r_n^*(x)|f(x)$ và $r_n^*(x)|g(x)$. Giả sử $h(x)|f(x)$ và $h(x)|g(x)$. Từ đẳng thức đầu tiên ta có $h(x)|r(x)$. Từ đẳng thức thứ hai ta có $h(x)|r_1(x)$. Cứ tiếp tục lập luận trên với các đẳng thức từ trên xuống dưới ta có $h(x)|r_n(x)$. Do đó $h(x)|r_n^*(x)$. □

1.2 Đa thức bất khả quy

1.2.1 Định nghĩa. Một đa thức $f(x) \in F[x]$ được gọi là *bất khả quy* nếu $\deg f(x) > 0$ và $f(x)$ không phân tích được thành tích của hai đa thức có bậc bé hơn. Nếu $\deg f(x) > 0$ và $f(x)$ là tích của hai đa thức có bậc bé hơn thì ta nói $f(x)$ là *khả quy*.

Sau đây là một số ví dụ về đa thức bất khả quy.

1.2.2 Bổ đề. *Các phát biểu sau là đúng.*

(i) Đa thức bậc nhất luôn bất khả quy.

(ii) Nếu $f(x)$ *bậc lớn hơn* 1 *và có nghiệm trong* F *thì* $f(x)$ *khả quy.*

(iii) Đa thức bậc 2 *và bậc* 3 *là bất khả quy nếu và chỉ nếu nó không có nghiệm trong* F.

(iv) Đa thức $f(x)$ *có bậc dương là bất khả quy nếu và chỉ nếu* $f(x+a)$ *là bất khả quy với mọi* $a \in F$.

Chứng minh. (i) Rõ ràng đa thức bậc nhất không thể là tích của hai đa thức bậc thấp hơn.

(ii) Nếu $\deg f(x) > 1$ và $f(x)$ có nghiệm $x = a \in F$ thì $f = (x-a)g$ trong đó $\deg g = \deg f - 1 \geq 1$. Vì thế f khả quy.

(iii) Cho $f(x)$ có bậc 2 hoặc 3. Nếu f khả quy thì nó phân tích được thành tích của hai đa thức bậc thấp hơn, một trong hai đa thức đó phải có bậc 1, do đó $f(x)$ có nghiệm trong F. Nếu $f(x)$ có nghiệm trong F thì theo (ii), $f(x)$ là khả quy.

(iv) Cho đa thức $f(x) \in F[x]$ có bậc dương và $a \in F$. Với mỗi $h \in F$, đặt $h_1(x) = h(x-a)$. Chú ý rằng $\deg h_1(x) = \deg h(x)$ với mọi $h \in F$. Vì thế $f(x+a) = k(x)g(x)$ là phân tích của $f(x+a)$ thành hai đa thức có bậc thấp hơn khi và chỉ khi $f(x) = k_1(x)g_1(x)$ là phân tích của $f(x)$ thành tích của hai đa thức có bậc thấp hơn. Vì vậy $f(x)$ khả quy khi và chỉ khi $f(x+a)$ khả quy. □

Tiếp theo, chúng ta định nghĩa khái niệm đa thức bất khả quy của một phần tử chứa F trong một trường. Trước hết ta cần kết quả sau.

1.2.3 Định nghĩa. Cho K là một trường chứa F và $a \in K$. Ta nói a là *phần tử đại số trên* F nếu tồn tại một đa thức $0 \neq f(x) \in F[x]$ nhận a làm nghiệm. Nếu a không đại số trên F thì ta nói a là *siêu việt* trên F.

1.2.4 Mệnh đề. *Cho K là một trường chứa F và $a \in K$ là phần tử đại số trên F. Khi đó tồn tại duy nhất một đa thức $p(x) \in F[x]$ bất khả quy dạng chuẩn nhận a làm nghiệm, và mọi đa thức $g(x) \in F[x]$ nhận a làm nghiệm đều là bội của $p(x)$.*

Chứng minh. Vì a là nghiệm của một đa thức khác 0 với hệ số trong F nên tồn tại đa thức khác 0 với hệ số trong F có bậc bé nhất nhận a làm nghiệm. Gọi $p(x) \in F[x]$ là dạng chuẩn của đa thức này. Khi đó a là nghiệm của $p(x)$. Ta chứng minh $p(x)$ bất khả quy. Giả sử $p(x)$ không bất khả quy. Khi đó $p(x)$ phân tích được thành tích của hai đa thức trong $F[x]$ với bậc bé hơn, và do đó một trong hai đa thức này phải nhận a làm nghiệm, điều này là mâu thuẫn với cách chọn $p(x)$. Giả sử $g(x) \in F[x]$

nhận a làm nghiệm. Nếu $p(x)$ không là ước của $g(x)$ thì vì $p(x)$ bất khả quy nên $\gcd(g(x), p(x)) = 1$, do đó $1 = p(x)q(x) + g(x)h(x)$ với $q(x), h(x) \in F[x]$. Thay $x = a$ vào cả hai vế ta được $1 = 0$, điều này là vô lí. Vậy $g(x)$ chia hết cho $p(x)$. Giả sử $q(x) \in F[x]$ cũng là đa thức bất khả quy dạng chuẩn nhận a làm nghiệm. Theo chứng minh trên, $q(x)$ là bội của $p(x)$. Viết $q(x) = p(x)k(x)$. Vì $q(x)$ bất khả quy nên $k(x) = b \in F$. Do đó $q(x) = bp(x)$. Đồng nhất hệ số cao nhất của hai vế với chú ý rằng $q(x)$ và $p(x)$ đều có dạng chuẩn, ta suy ra $b = 1$. Vì thế $p(x) = q(x)$. □

1.2.5 Định nghĩa. Đa thức $p(x) \in F[x]$ bất khả quy dạng chuẩn xác định như trong mệnh đề trên được gọi là *đa thức bất khả quy* của a.

1.2.6 Ví dụ. Đa thức $x^3 - 2 \in \mathbb{Q}[x]$ là đa thức bất khả quy của $\sqrt[3]{2} \in \mathbb{R}$; đa thức $x^2 + 1 \in \mathbb{R}[x]$ là đa thức bất khả quy của $i \in \mathbb{C}$.

Đa thức bất khả quy có tính chất tương tự như tính chất của số nguyên tố. Trước hết, chúng ta đã biết, Bổ đề Euclid phát biểu rằng số tự nhiên $p > 1$ là số nguyên tố nếu và chỉ nếu $p|ab$ kéo theo $p|a$ hoặc $p|b$ với mọi số tự nhiên a, b. Mệnh đề sau đây là điều tương tự cho đa thức bất khả quy.

1.2.7 Mệnh đề. *Nếu $p(x) \in F[x]$ bất khả quy và $p(x)|a(x)b(x)$ thì $p(x)|a(x)$ hoặc $p(x)|b(x)$ với mọi $a(x), b(x) \in F[x]$. Đặc biệt, một đa thức bất khả quy là ước của một tích hữu hạn đa thức thì nó phải là ước của ít nhất một trong các đa thức đó.*

Chứng minh. Cho $p(x)|a(x)b(x)$. Giả sử $p(x)$ không là ước của $a(x)$ và cũng không là ước của $b(x)$. Khi đó $\gcd(p(x), a(x)) = 1$. Do đó tồn tại $s(x), r(x) \in F[x]$ sao cho $1 = s(x)p(x) + r(x)a(x)$. Tương tự, tồn tại $e(x), f(x) \in F[x]$ sao cho $1 = e(x)p(x) + f(x)b(x)$. Nhân vế với vế của

hai đẳng thức này ta có

$$1 = p(x)g(x) + r(x)f(x)a(x)b(x)$$

với $g(x) \in F[x]$. Đa thức bên vế phải của đẳng thức trên là bội của $p(x)$, trong khi đó đa thức bên vế trái là 1 không chia hết cho $p(x)$. Điều này là vô lí. □

Tiếp theo, Định lý cơ bản của Số học nói rằng mỗi số tự nhiên lớn hơn 1 đều phân tích được thành tích các thừa số nguyên tố và sự phân tích này là duy nhất nếu không kể đến thứ tự các thừa số. Kết quả sau đây là một sự tương tự của định lý này đối với đa thức.

1.2.8 Định lý. *Mỗi đa thức dạng chuẩn bậc dương có thể phân tích được thành tích các đa thức bất khả quy dạng chuẩn và sự phân tích này là duy nhất nếu không kể đến thứ tự các nhân tử.*

Chứng minh. Trước hết, chúng ta chứng minh sự tồn tại phân tích bằng quy nạp theo bậc của đa thức. Giả sử $f(x) \in F[x]$ là đa thức dạng chuẩn bậc $d > 0$. Nếu $d = 1$ thì $f(x)$ là bất khả quy nên sự phân tích bất khả quy của $f(x)$ là $f(x) = f(x)$, kết quả đúng cho trường hợp $d = 1$. Cho $d > 1$ và giả sử kết quả đã đúng cho các đa thức bậc nhỏ hơn d. Nếu $f(x)$ bất khả quy thì $f(x)$ có sự phân tích bất khả quy là $f(x) = f(x)$. Vì thế ta giả thiết $f(x)$ không bất khả quy. Khi đó $f(x) = g(x)h(x)$ với $\deg g(x), \deg h(x) < \deg f(x)$. Đặt $g^*(x) = g(x)/a_k$ với a_k là hệ số cao nhất của $g(x)$. Khi đó ta có $f(x) = g^*(x)(a_k h(x))$. Đồng nhất hệ số cao nhất ở hai vế ta được $1 = a_k b_t$, trong đó b_t là hệ số cao nhất của $h(x)$. Đặt $h^*(x) = a_k h(x)$. Khi đó $f(x) = g^*(x)h^*(x)$ với $g^*(x), h^*(x)$ là các đa thức dạng chuẩn có bậc nhỏ hơn d. Theo giả thiết quy nạp, $g^*(x)$ và $h^*(x)$ phân tích được thành tích các đa thức bất khả quy dạng chuẩn. Vì

thế $f(x)$ phân tích được thành tích của hữu hạn đa thức bất khả quy dạng chuẩn.

Bây giờ ta chứng minh tính duy nhất của phân tích. Giả sử $f(x)$ có hai sự phân tích thành nhân tử bất khả quy dạng chuẩn

$$f(x) = p_1(x)p_2(x)\dots p_n(x) = q_1(x)q_2(x)\dots q_m(x).$$

Ta chứng minh bằng quy nạp theo n rằng $n = m$ và sau một phép hoán vị ta có $p_i(x) = q_i(x)$ với mọi $i = 1, \dots, n$. Cho $n = 1$. Khi đó ta có $p_1(x) = q_1(x)q_2(x)\dots q_m(x)$. Suy ra $p_1(x)|q_1(x)q_2(x)\dots q_m(x)$. Do $p_1(x)$ là bất khả quy nên $p_1(x)$ là ước của một nhân tử $q_i(x)$ nào đó, không mất tính tổng quát ta có thể giả thiết $p_1(x)|q_1(x)$. Biểu diễn $q_1(x) = p_1(x)t_1(x)$. Vì $q_1(x)$ bất khả quy nên $t_1(x) = a \in F$. Đồng nhất hệ số cao nhất của hai vế của đẳng thức $q_1(x) = ap_1(x)$ với chú ý rằng $p_1(x)$ và $q_1(x)$ là dạng chuẩn, ta có $1 = 1.a$. Suy ra $a = 1$ và do đó $p_1(x) = q_1(x)$. Nếu $m > 1$ thì $1 = q_2(x)\dots q_m(x)$, điều này là vô lí. Vậy, kết quả đúng cho $n = 1$. Cho $n > 1$. Vì $p_1(x)|q_1(x)q_2(x)\dots q_m(x)$ và $p_1(x)$ là bất khả quy nên không mất tính tổng quát ta có thể giả thiết $p_1(x)|q_1(x)$. Lại do $q_1(x)$ là bất khả quy và $p_1(x), q_1(x)$ đều có dạng chuẩn nên tương tự như lập luận trên ta có $p_1(x) = q_1(x)$. Giản ước cả hai vế cho $p_1(x)$ ta được

$$p_2(x)p_3(x)\dots p_n(x) = q_2(x)q_3(x)\dots q_m(x).$$

Theo giả thiết quy nạp ta có $n - 1 = m - 1$ và bằng việc đánh số lại các nhân tử $q_i(x)$ ta suy ra $p_i(x) = q_i(x)$ với mọi $i = 2, \dots, n$. □

1.3 Trường phân rã của đa thức

Trong tiết này, dựa vào tính chất bất khả quy, chúng ta chỉ ra rằng với mỗi đa thức $f(x) \in F[x]$, tồn tại một trường K tối thiểu chứa trường F và

chứa tất cả các nghiệm của $f(x)$. Trường K có tính chất trên được gọi là *trường phân rã* của đa thức $f(x)$ trên F.

1.3.1 Định nghĩa. Cho F và F' là hai trường.

(i) Một tập con T của F được gọi là *trường con* của F nếu $x^{-1} \in T$ với mọi $0 \neq x \in T$ và $x+y, xy, -1 \in T$ với mọi $x, y \in T$. Chú ý rằng tập con T của F là trường con của F nếu phép cộng và nhân đóng kín trong T và T là một trường với hai phép toán này.

(ii) Một ánh xạ $\varphi : F \to F'$ được gọi là một *đồng cấu* nếu $\varphi(1) = 1$, $\varphi(x+y) = \varphi(x) + \varphi(y)$ và $\varphi(xy) = \varphi(x)\varphi(y)$ với mọi $x, y \in F$.

(iii) Một đồng cấu $\varphi : F \to F'$ được gọi là *đơn cấu* nếu φ là đơn ánh. Trong trường hợp này $\varphi(F)$ là một trường con của F'. Vì thế ta nói F *nhúng* được vào F' và ta cũng có thể coi F' là một *trường chứa* F.

(iv) Một đồng cấu $\varphi : F \to F'$ được gọi là *toàn cấu* nếu φ là toàn ánh.

(v) Một đồng cấu $\varphi : F \to F'$ được gọi là *đẳng cấu* nếu φ là song ánh. Trong trường hợp này ta nói F và F' là *đẳng cấu* với nhau và ta có thể đồng nhất hai trường F và F' với nhau.

1.3.2 Định lý. (Kronecker). *Cho $f(x) \in F[x]$ là một đa thức có bậc dương. Khi đó tồn tại một trường tối thiểu chứa F và chứa tất cả các nghiệm của $f(x)$. Đặc biệt, mỗi đa thức trên một trường đều có trường phân rã.*

Chứng minh. Kí hiệu $f^*(x)$ là đa thức dạng chuẩn của $f(x)$. Vì các nghiệm của $f(x)$ cũng là các nghiệm của $f^*(x)$ nên ta có thể giả thiết $f(x)$ có dạng chuẩn. Ta chứng minh định lý bằng quy nạp theo $\deg f(x) = n$. Giả sử $n = 1$. Khi đó $f(x) = x - a$ với $a \in F$. Do a là nghiệm duy nhất của $f(x)$ nên ta chỉ việc chọn $K = F$. Giả thiết rằng $n > 1$ và định lý đã đúng cho trường hợp đa thức bậc nhỏ hơn n. Trước hết ta chứng minh cho trường hợp $f(x)$ bất khả quy. Đặt

$$I = (f) = \{g(x)f(x) \mid g(x) \in F[x]\}.$$

Dễ kiểm tra được I là một iđêan của $F[x]$. Với mỗi $g(x) \in F[x]$ ta đặt

$$g(x) + I = \{g(x) + h(x) \mid h(x) \in I\}.$$

Ta có thể chỉ ra rằng $g(x)+I = h(x)+I$ nếu và chỉ nếu $g(x)-h(x) \in I$. Đặt $K = \{g(x) + I \mid g(x) \in F[x]\}$. Trước hết ta kiểm tra quy tắc cộng

$$(g(x) + I) + (h(x) + I) = (g(x) + h(x)) + I$$

là một phép toán trên K. Thật vậy, nếu $g + I = g_1 + I$ và $h + I = h_1 + I$ thì $g - g_1 \in I$ và $h - h_1 \in I$. Do đó $g - g_1$ và $h - h_1$ là bội của f. Suy ra $(g + h) - (g_1 + h_1) = (g - g_1) + (h - h_1)$ là bội của f. Vì thế $(g + h) - (g_1 + h_1) \in I$ hay $(g + h) + I = (g_1 + h_1) + I$. Suy ra quy tắc cộng ở trên là một phép toán trên K. Hoàn toàn tương tự, ta có thể chỉ ra rằng quy tắc nhân

$$(g + I)(h + I) = gh + I$$

là một phép toán trên K. Dễ thấy phép cộng và phép nhân trên K có tính chất kết hợp, giao hoán; Phép nhân phân phối với phép cộng; Phần tử không của K là $0+I$; Phần tử đơn vị của K là $1+I$; Phần tử đối xứng của $g + I \in K$ là $-g + I \in K$. Ta chứng minh mọi phần tử khác $0 + I \in K$ đều có nghịch đảo. Lấy $g + I \in K$ với $g + I \neq 0 + I$. Khi đó $g \notin I$. Do đó g không là bội của f. Vì f bất khả quy nên $\gcd(f, g) = 1$. Vì thế ta có biểu diễn $1 = f(x)p(x) + g(x)q(x)$ với $p(x), q(x) \in F[x]$. Chú ý rằng $fp \in I$. Do đó $fp + I = 0 + I$. Suy ra

$$1 + I = (fp + gq) + I = (fp + I) + (gq + I) = gq + I = (g + I)(q + I).$$

Do đó $g + I$ khả nghịch trong K. Vậy K làm thành một trường với phép cộng và nhân ở trên. Xét ánh xạ $\varphi : F \to K$ cho bởi $\varphi(a) = a + I$. Rõ ràng φ là một đồng cấu. Nếu $\varphi(a) = \varphi(b)$ với $a, b \in F$ thì $a + I = b + I$. Vì thế $a - b \in I$. Suy ra $a - b$ là bội của $f(x)$. Nếu $a - b \neq 0$ thì $a - b$

là đa thức có bậc 0 nên nó không thể là bội của đa thức $f(x)$ bậc dương, điều này là vô lí. Do đó $a - b = 0$. Suy ra $a = b$. Vì vậy φ là đơn cấu, do đó ta có thể xem K là một trường chứa F. Đặt $\alpha = x + I \in K$. Giả sử $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Đồng nhất phần tử $a \in F$ với phần tử $a + I \in K$, khi đó trong trường K ta có

$$\begin{aligned} f(\alpha) &= (x+I)^n + (a_{n-1}+I)(x+I)^{n-1} + \ldots + (a_0+I) \\ &= (x^n + I) + (a_{n-1}x^{n-1} + I) + \ldots + (a_0 + I) \\ &= (x^n + a_{n-1}x^{n-1} + \ldots + a_0) + I \\ &= f(x) + I = 0 + I. \end{aligned}$$

Vì vậy α là một nghiệm của đa thức $f(x)$ trong trường K. Do đó tồn tại $f_1(x) \in K[x]$ sao cho $f(x) = (x - \alpha)f_1(x)$, trong đó $\deg f_1(x) = n - 1$. Theo giả thiết quy nạp, tồn tại một trường K_1 chứa K và chứa tất cả các nghiệm của $f_1(x)$. Do đó K_1 chứa F và chứa tất cả các nghiệm của $f(x)$. Gọi K^* là giao của tất cả các trường con của K_1 chứa F và chứa tất cả các nghiệm của $f(x)$. Khi đó K^* là trường tối thiểu chứa F và chứa các nghiệm của $f(x)$.

Tiếp theo, ta chứng minh cho trường hợp $f(x)$ khả quy. Trong trường hợp này, tồn tại hai đa thức dạng chuẩn bậc dương $g(x), h(x) \in F[x]$ sao cho $f(x) = g(x)h(x)$ và $\deg g, \deg h < n = \deg f$. Theo giả thiết quy nạp, tồn tại một trường K chứa F và chứa tất cả các nghiệm của $g(x)$. Ta coi $h(x)$ là đa thức với hệ số trong K. Theo giả thiết quy nạp, tồn tại một trường chứa K_1 và chứa tất cả các nghiệm của $h(x)$. Vì thế K_1 là trường chứa F và chứa các nghiệm của $f(x)$. Lấy giao của tất cả các trường con của K_1 chứa F và chứa các nghiệm của $f(x)$, ta được trường tối thiểu chứa F và các nghiệm của $f(x)$. □

1.3.3 Ví dụ. Kí hiệu $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$ là giao của các trường con của $\mathbb{C}$ chứa

$\mathbb{Q}$ và chứa các phần tử $i\sqrt{3}, \sqrt[3]{2}$. Khi đó trường phân rã của $f(x) = x^3 - 2$ trên $\mathbb{Q}$ là $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$. Thật vậy, dễ thấy 3 nghiệm của $x^3 - 2$ là

$$x_1 = \sqrt[3]{2}, x_2 = \sqrt[3]{2}(-\frac{1}{2} + \frac{i\sqrt{3}}{2}), x_3 = \sqrt[3]{2}(-\frac{1}{2} - \frac{i\sqrt{3}}{2}).$$

Do đó $x_1, x_2, x_3 \in \mathbb{Q}(i\sqrt{3}, \sqrt[3]{2})$. Ngược lại, trường bé nhất chứa $\mathbb{Q}$ và các nghiệm x_1, x_2, x_3 phải chứa $i\sqrt{3}$ và $\sqrt[3]{2}$.

Sử dụng Định lý 1.3.2 về sự tồn tại trường phân rã của đa thức, chúng ta có thể chỉ ra số phần tử của một trường hữu hạn và sự tồn tại một trường có hữu hạn phần tử. Chú ý đơn giản sau đây là rất có ích. Nếu T là một trường con của trường F thì F có cấu trúc là không gian véc tơ trên T với phép cộng là phép cộng của F và tích vô hướng là phép nhân các phần tử của T với các phần tử của F.

1.3.4 Mệnh đề. *Nếu F là một trường hữu hạn thì số phần tử của F là lũy thừa của một số nguyên tố.*

Chứng minh. Với mỗi số tự nhiên n, kí hiệu $n1 = 1 + \ldots + 1$ là tổng của n phần tử 1 và $(-n)1$ là tổng của n phần tử -1. Quy ước $01 = 0$. Ta khẳng định rằng tồn tại một số nguyên dương k sao cho $k1 = 0$. Giả sử ngược lại, khi đó tương ứng $\varphi : \mathbb{Q} \to F$ cho bởi $\varphi(n/m) = (n1)(m1)^{-1}$ là đơn cấu trường. Do $\mathbb{Q}$ có vô hạn phần tử nên F có vô hạn phần tử, điều này là vô lí. Vậy, tồn tại số nguyên dương k để $k1 = 0$. Gọi p là số nguyên dương bé nhất có tính chất $p1 = 0$. Ta chứng minh p là số nguyên tố. Thật vậy, vì $p1 = 1 \neq 0$ nên $p > 1$. Nếu p không nguyên tố thì $p = nm$ trong đó $1 < n, m < p$. Suy ra $0 = p1 = (n1)(m1)$. Do $n, m < p$ nên $n1 \neq 0$ và $m1 \neq 0$. Do đó $n1$ và $m1$ khả nghịch. Gọi $a, b \in F$ lần lượt là nghịch đảo của $n1$ và $m1$. Khi đó

$$0 = 0(ab) = (n1)a(m1)b = 1.1 = 1,$$

điều này là vô lí. Vậy p là số nguyên tố. Tiếp theo ta khẳng định $m1 = 0$ nếu và chỉ nếu $m \in p\mathbb{Z}$. Thật vậy, nếu $m \in p\mathbb{Z}$ thì rõ ràng $m1 = 0$. Nếu $m1 = 0$ thì ta viết $m = ps + r$ với $s, r \in \mathbb{Z}$ và $0 \leqslant r < p$, và do đó $0 = m1 = ps1 + r1 = r1$. Do $r < p$ nên $r = 0$ theo cách chọn p, khẳng định được chứng minh. Đặt

$$T = \{(n1)(m1)^{-1} \mid n \in \mathbb{Z}, m \notin p\mathbb{Z}\} \subseteq F.$$

Dễ kiểm tra được T là trường con của F. Ta chứng minh T có đúng p phần tử. Thật vậy, với mỗi $m \notin p\mathbb{Z}$, do p nguyên tố nên $\gcd(m, p) = 1$. Suy ra $1 = ms + pt$ với $s, t \in \mathbb{Z}$. Suy ra

$$1 = 1.1 = (m1)(s1) + pt1 = (m1)(s1).$$

Do đó $(m1)^{-1} = s1$ với $s \in \mathbb{Z}$. Suy ra $T = \{n1 \mid n \in \mathbb{Z}\}$. Với mỗi $n \in \mathbb{Z}$, viết $n = pt + r$ với $0 \leqslant r < p$ ta được $n1 = pt1 + r1 = r1$. Do đó $T = \{n1 \mid 0 \leqslant n < p\}$. Nếu $0 \leqslant n, n' < p$ và $n1 = n'1$ thì $(n - n')1 = 0$ và do đó $n - n'$ là bội của p, do đó $n = n'$. Suy ra T là trường con của F có đúng p phần tử. Chú ý rằng F là không gian véc tơ trên T. Gọi q là số phần tử của F và $d = \dim_T F$ là chiều của $T-$không gian véc tơ F. Gọi $\{e_1, \ldots, e_d\}$ là một cơ sở của F. Khi đó mỗi phần tử $x \in F$ được biểu diễn một cách duy nhất dưới dạng $x = a_1e_1 + \ldots + a_ne_n$, trong đó $a_i \in T$ với mọi $i = 1, \ldots, n$. Vì thế, số phần tử của F là $q = p^d$. □

1.3.5 Định lý. *(Galois). Với mỗi số nguyên tố p và mỗi số nguyên dương d, tồn tại một trường có đúng p^d phần tử.*

Chứng minh. Đặt $q = p^d$. Do p nguyên tố nên $\mathbb{Z}_p$ là một trường. Theo Định lý Kronecker, tồn tại một trường K chứa $\mathbb{Z}_p$ và chứa các nghiệm của đa thức $x^q - x$. Đặt $E = \{\alpha \in K \mid g(\alpha) = 0\}$, tức là E là tập tất cả các nghiệm của $g(x)$ trong K. Kí hiệu $g'(x) = qx^{q-1} - 1$ là đạo hàm

của $g(x)$. Vì $1 \in \mathbb{Z}_p$ nên ta có $p1 = 0$. Do đó $q1 = p^d 1 = 0$. Suy ra $g'(x) = (q1)x^{q-1} - 1 = -1$. Do đó ước chung lớn nhất của $g(x)$ và $g'(x)$ bằng 1. Suy ra $g(x)$ không có nghiệm bội trong K. Điều này cũng có nghĩa là E có đúng q phần tử. Như vậy, định lý được chứng minh nếu ta chỉ ra E là một trường. Nếu p lẻ thì q lẻ và do đó $g(-1) = -1 + 1 = 0$ và vì thế $-1 \in E$. Nếu p chẵn thì vì p nguyên tố nên $p = 2$. Suy ra

$$g(-1) = (-1)^q + 1 = 1 + 1 = 2.1 = p.1 = 0.$$

Do đó $-1 \in E$. Vậy trong mọi trường hợp ta đều có $-1 \in E$. Cho $a, b \in E$. Khi đó $g(a) = g(b) = 0$. Suy ra $a^q = a$ và $b^q = b$. Suy ra $(ab)^q = ab$. Do đó $g(ab) = 0$ và vì thế $ab \in E$. Chú ý rằng

$$(a+b)^q = a^q + C_q^1 a^{q-1}b + \ldots + C_q^{q-1}ab^{q-1} + b^q = a + b,$$

trong đó C_q^k là số tổ hợp chập k của q phần tử. Vì $q = p^d$ và p nguyên tố nên bằng quy nạp ta dễ dàng kiểm tra được C_q^k là bội của p với mọi $k = 1, \ldots, q-1$. Do đó ta có $C_q^k a^{q-k}b^k = (C_q^k 1)a^{q-k}b^k = 0$ với mọi $k = 1, \ldots, q-1$. Vì thế $(a+b)^q = a^q + b^q$. Theo trên ta đã có $a^q = a$ và $b^q = b$. Do đó $(a+b)^q - (a+b) = 0$, và vì thế $a + b \in E$. Cho $0 \neq a \in E$ Khi đó $a^q = a$. Do $a \neq 0$ nên nhân cả hai vế với a^{-1} ta được $a^{q-1} = 1$. Suy ra a^{q-2} là nghịch đảo của a trong E. Vậy E là một trường. □

Từ định lý trên ta suy ra các tính chất sau.

1.3.6 Ví dụ. Tồn tại trường có 81 phần tử. Không tồn tại trường có 100 phần tử.

Chương 2

Một số phương pháp xét tính bất khả quy trên $\mathbb{Q}$

Định lý cơ bản của Đại số phát biểu rằng mỗi đa thức bậc dương với hệ số phức luôn có ít nhất một nghiệm phức. Chú ý rằng nếu $f(x) \in \mathbb{C}[x]$ có nghiệm $x = \alpha \in \mathbb{C}$ thì $f(x) = (x - \alpha)g(x)$ với $g(x) \in \mathbb{C}[x]$. Vì thế nếu $\deg f(x) \geq 2$ thì $f(x)$ có thể phân tích được thành tích của hai đa thức có bậc thấp hơn. Do đó *các đa thức bất khả quy trên* $\mathbb{C}$ *là và chỉ là các đa thức bậc nhất*. Giả sử $f(x) \in \mathbb{R}[x]$. Chú ý rằng nếu số phức $\alpha = a + bi$ là nghiệm của $f(x)$ với $\alpha \notin \mathbb{R}$ thì số phức liên hợp $\overline{\alpha} = a - bi$ cũng là nghiệm của $f(x)$. Vì thế $f(x)$ chia hết cho $(x-a-bi)(x-a+bi)$. Rõ ràng $(x-a-bi)(x-a+bi) = x^2-2ax+a^2+b^2 \in \mathbb{R}[x]$ và $x^2-2ax+a^2+b^2$ không có nghiệm thực. Do đó *các đa thức bất khả quy trên* $\mathbb{R}$ *là và chỉ là các đa thức bậc nhất hoặc đa thức bậc hai không có nghiệm thực*.

Mặc dù bài toán xét tính bất khả quy của các đa thức trên $\mathbb{C}$ và trên $\mathbb{R}$ đã được giải quyết từ khi người ta chứng minh được Định lý cơ bản của Đại số (chứng minh hoàn chỉnh đầu tiên cho Định lý cơ bản của Đại số được đưa ra bởi Gauss năm 1816), nhưng bài toán xét tính bất khả quy của các đa thức trên $\mathbb{Q}$ cho đến nay vẫn là bài toán mở. Mục tiêu của chương này nhằm trình bày một số tiêu chuẩn để một đa thức là bất khả quy trên $\mathbb{Q}$.

Giả sử $f(x) \in \mathbb{Q}[x]$. Chú ý rằng $f(x)$ là bất khả quy trên $\mathbb{Q}$ khi và chỉ khi $af(x)$ là bất khả quy với mọi $0 \neq a \in \mathbb{Z}$. Vì thế, bằng việc nhân với mẫu số chung của các hệ số của $f(x)$, ta được một đa thức với hệ số nguyên mà tính bất khả quy trên $\mathbb{Q}$ của nó tương đương với tính bất khả quy của $f(x)$. Do đó ta chỉ cần xét tính bất khả quy trên $\mathbb{Q}$ cho các đa thức với hệ số nguyên. Từ nay đến hết chương này, luôn giả thiết $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, trong đó $a_n \neq 0$ và $n > 0$.

2.1 Nghiệm hữu tỷ và tính bất khả quy trên $\mathbb{Q}$

Như đã trình bày trong chương trước, điều kiện đủ để một đa thức bậc lớn hơn 1 khả quy trên $\mathbb{Q}$ là nó có nghiệm trong $\mathbb{Q}$. Vì vậy, để xét tính khả quy của đa thức, trong nhiều trường hợp ta có thể dùng phương pháp tìm nghiệm hữu tỷ. Trước hết chúng ta đưa ra cách tìm nghiệm hữu tỷ cho các đa thức với hệ số nguyên.

2.1.1 Mệnh đề. *Nếu $\frac{r}{s}$ là phân số tối giản và là nghiệm hữu tỷ của $f(x)$ thì r là ước của a_0 và s là ước của a_n.*

Chứng minh. Giả sử $\frac{r}{s} \in \mathbb{Q}$ trong đó r, s là các số nguyên, $s > 0$ và $(r, s) = 1$. Nếu $\frac{r}{s}$ là nghiệm của đa thức $f(x)$ thì $f(\frac{r}{s}) = 0$. Ta có

$$0 = f(\frac{r}{s}) = a_n(\frac{r}{s})^n + a_{n-1}(\frac{r}{s})^{n-1} + \ldots + a_1\frac{r}{s} + a_0.$$

Suy ra $0 = a_n r^n + a_{n-1}r^{n-1}s + \ldots + a_1 r s^{n-1} + a_0 s^n$. Vì thế ta có

$$a_n r^n = -(a_{n-1}r^{n-1}s + \ldots + a_1 r s^{n-1} + a_0 s^n).$$

Vế phải của đa thức này là bội của s. Vì $(r, s) = 1$ nên s là ước của a_n
Tương tự ta có $a_0 s^n = -(a_n r^n + a_{n-1}r^{n-1}s + \ldots + a_1 r s^{n-1})$. Vế phải của đa thức này là bội của r. Vì $(r, s) = 1$ nên r là ước của a_0. □

2.1.2 Hệ quả. *Nghiệm hữu tỷ (nếu có) của* $f(x) = x^n + \ldots + a_1x + a_0$ *là nghiệm nguyên và số nguyên này là ước của số hạng tự do.*

2.1.3 Mệnh đề. *Nếu phân số tối giản* $\frac{r}{s}$ *là nghiệm của* $f(x)$ *thì* $r - ms$ *là ước của* $f(m)$ *với* m *là số nguyên bất kì. Đặc biệt,* $(r + s)$ *là ước của* $f(-1)$ *và* $(r - s)$ *là ước của* $f(1)$.

Chứng minh. Phân tích $f(x)$ theo các luỹ thừa của $x - m$ ta được

$$f(x) = a_n(x - m)^n + b_{n-1}(x - m)^{n-1} + \ldots + b_1(x - m) + b_0.$$

Các hệ số $b_0, b_1, \ldots, b_{n-1} \in \mathbb{Z}$ vì $m \in \mathbb{Z}$. Ta có $f(m) = b_0$ và cho $x = \frac{r}{s}$ ta được $f(\frac{r}{s}) = 0$. Chú ý rằng

$$0 = f(\frac{r}{s}) = a_n(\frac{r}{s} - m)^n + b_{n-1}(\frac{r}{s} - m)^{n-1} + \ldots + b_1(\frac{r}{s} - m) + f(m).$$

Từ đó ta có

$$0 = a_n(r - ms)^n + b_{n-1}(r - ms)^{n-1}s + \ldots + b_1(r - ms)s^{n-1} + f(m)s^n.$$

Suy ra

$$f(m)s^n = -\{a_n(r - ms)^n + b_{n-1}(r - ms)^{n-1}s + \ldots + b_1(r - ms)s^{n-1}\}.$$

Vế phải của đa thức là bội của $r - ms$. Do đó $f(m)s^n$ là bội của $r - ms$ hay $r - ms$ là ước của $f(m)$.
Trường hợp đặc biệt, với $m = 1$ thì $r - s$ là ước $f(1)$, $m = -1$ thì $r + s$ là ước $f(-1)$. □

Sau đây là một số ví dụ minh họa về việc xét tính khả quy của đa thức bằng phương pháp tìm nghiệm hữu tỷ.

2.1.4 Ví dụ. Xét tính bất khả quy trên $\mathbb{Q}$ của các đa thức sau.

(i) $10x^3 + 3x^2 - 106x + 21$;

(ii) $9x^3 + 6x^2 - 8x + 7$;

(iii) $x^3 - x^2 + x - 6$;

(iv) $6x^4 + 19x^3 - 7x^2 - 26x + 12$.

Giải. (i) Giả sử đa thức $f(x) = 10x^3 + 3x^2 - 106x + 21$ có nghiệm hữu tỷ $\frac{r}{s}$, với $\frac{r}{s}$ là phân số tối giản. Theo Mệnh đề 2.1.1, $r|21$ và $s|10$. Từ đó suy ra $r = \pm 1, \pm 3, \pm 7, \pm 21$ và $s = \pm 1, \pm 2, \pm 5, \pm 10$. Ta tính được $f(1) = -72$, $f(-1) = 120$. Vậy các số hữu tỷ thoả mãn Mệnh đề 2.1.3 là $\pm\frac{1}{2}, \pm\frac{1}{5}, \pm 3, \frac{3}{2}, \pm\frac{3}{5}, \pm 7, -\frac{7}{2}, \pm\frac{7}{5}$. Thử lại ta thấy chỉ có $\frac{1}{5}, 3, -\frac{7}{2}$ là nghiệm của $f(x)$. Vậy $f(x)$ có nghiệm hữu tỷ, do đó nó khả quy trên $\mathbb{Q}$.

(ii) Để xét tính bất khả quy của đa thức $f(x) = 9x^3+6x^2-8x+7$ ta nhân hai vế của $f(x)$ với 3 ta được $f(3x) = 27x^3+18x^2-24x+21$. Đặt $y = 3x$ ta được $f(y) = y^3+2y^2-8y+21$. Giả sử $f(y)$ có nghiệm hữu tỷ. Vì $a_n = 1$ nên theo Hệ quả 2.1.2, nghiệm hữu tỷ của $f(y)$ phải là nghiệm nguyên và $r|21$. Suy ra $r = \pm 1, \pm 3, \pm 7, \pm 21$. Ta thấy $f(1) = 16, f(-1) = 30$. Vậy chỉ có các số $-3, -7$ thoả mãn Mệnh đề 2.1.3 nhưng thử lại ta thấy $f(-3) \neq 0, f(-7) \neq 0$. Vậy đa thức $f(y)$ không có nghiệm hữu tỷ. Suy ra $f(x)$ bất khả quy trên $\mathbb{Q}$.

(iii) Giả sử đa thức $f(x) = x^3-x^2+x-6$ có nghiệm hữu tỷ và nghiệm đó phải là nghiệm nguyên vì $a_n = 1$. Các ước của 6 là $r = \pm 1, \pm 2, \pm 3, \pm 6$. Ta thấy $f(1) = -5$ và $f(-1) = -9$ nên chỉ có $r = 2$ thoả mãn Mệnh đề 2.1.3. Thử lại ta thấy rằng $f(2) = 0$. Vậy đa thức $f(x)$ có nghiệm hửu tỷ, do đó nó khả quy.

(iv) Giả sử đa thức $f(x) = 6x^4+19x^3-7x^2-26x+12$ có nghiệm hữu tỷ $\frac{r}{s}$, với $\frac{r}{s}$ là phân số tối giản. Theo Mệnh đề 2.1.1 thì $r|12$ và $s|6$. Suy ra $r = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$ và $s = \pm 1, \pm 2, \pm 3, \pm 6$. Ta tính được $f(1) = 4$ và $f(-1) = 18$. Do đó các số hữu tỷ thoả mãn Mệnh đề 2.1.3 là $\frac{1}{2}, -\frac{1}{3}, 2, -3$. Thử lại ta thấy $f(\frac{1}{2}) = 0$ và $f(-3) = 0$. Vậy $f(x)$ có

nghiệm hữu tỷ, do đó nó khả quy trên $\mathbb{Q}$.

2.1.5 Chú ý. Đối với đa thức bậc ≥ 4, ta không thể suy ra tính bất khả quy trên $\mathbb{Q}$ từ việc kiểm tra đa thức không có nghiệm hữu tỷ. Thật vậy, đa thức $(x^2+1)(x^2+1)$ không có nghiệm hữu tỷ, nhưng nó không bất khả quy.

2.2 Phương pháp dùng Bổ đề Gauss

Trong tiết này, chúng ta trình bày một tiêu chuẩn bất khả quy trên $\mathbb{Q}$ thông qua tiêu chuẩn không phân tích được trên $\mathbb{Z}[x]$.

2.2.1 Định lý. (Bổ đề Gauss). *Cho $p(x) \in \mathbb{Z}[x]$. Nếu $p(x) = g(x)f(x)$ là sự phân tích $p(x)$ thành tích của hai đa thức $g(x), f(x)$ với hệ số trong $\mathbb{Q}$ thì $p(x)$ cũng phân tích được thành tích của hai đa thức $g_*(x), f_*(x)$ với hệ số trong $\mathbb{Z}$ với $\deg g(x) = \deg g_*(x), \deg f(x) = \deg f_*(x)$. Đặc biệt, 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.*

Để chứng minh định lý trên, chúng ta cần nhắc lại khái niệm đa thức nguyên bản và một tính chất của đa thức nguyên bản.

2.2.2 Định nghĩa. Đa thức $f(x) \in \mathbb{Z}[x]$ được gọi là *nguyên bản* nếu ước chung lớn nhất của các hệ số của $f(x)$ là 1.

2.2.3 Bổ đề. *Tích của hai đa thức nguyên bản là đa thức nguyên bản.*

Chứng minh. Giả sử $f(x) = g(x)h(x)$, trong đó

$$g(x) = b_n x^n + \ldots + b_1 x + b_0$$
$$h(x) = c_k x^k + \ldots + c_1 x + c_0.$$

là các đa thức nguyên bản. Viết $f(x) = a_m x^m + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. Nếu $f(x)$ không nguyên bản thì tồn tại một số nguyên tố p sao cho nó là ước của mọi hệ số của f. Vì $h(x), g(x)$ là nguyên bản nên tồn tại chỉ số bé nhất s sao cho b_s không là bội của p và tồn tại chỉ số t bé nhất sao cho c_t không là bội của p. Chú ý rằng

$$a_{s+t} = b_{s+t}c_0 + b_{s+t-1}c_1 + \ldots + b_s c_t + b_{s-1}c_{t+1} + \ldots + b_0 c_{t+s}.$$

Theo cách chọn s và t ta có b_i, c_j là bội của p với mọi $i > s$ và $j > t$. Vì a_{s+t} là bội của p nên ta suy ra $b_s c_t$ là bội của p, điều này là vô lí với cách chọn b_s và c_t. □

Bây giờ ta có thể chứng minh Định lý 2.2.1.

Chứng minh Định lý 2.2.1. Giả sử $p(x) \in \mathbb{Z}[x]$ và $p(x) = f(x)g(x)$ với $f, g \in \mathbb{Q}[x]$. Ta có thể viết $f = af_1$ và $g = bg_1$ trong đó $a, b \in \mathbb{Q}$ và $f_1, g_1 \in \mathbb{Z}[x]$ là các đa thức nguyên bản. Theo Bổ đề 2.2.3, $f_1 g_1 \in \mathbb{Z}[x]$ là đa thức nguyên bản. Rõ ràng $p = abf_1 g_1 \in \mathbb{Z}[x]$. Ta chứng minh $ab \in \mathbb{Z}$. Thật vậy, giả sử $ab \notin \mathbb{Z}$. Khi đó $ab = \dfrac{r}{s}$ với $r, s \in \mathbb{Z}$, $s > 1$ và $\gcd(r, s) = 1$. Viết $f_1 g_1 = a_n x^n + \ldots + a_1 x + a_0$. Vì $f_1 g_1$ là nguyên bản nên $\gcd(a_n, a_{n-1}, \ldots, a_1, a_0) = 1$. Vì $p(x) \in \mathbb{Z}[x]$ nên

$$\frac{ra_n}{s}, \ldots, \frac{ra_1}{s}, \frac{ra_0}{s} \in \mathbb{Z}.$$

Suy ra s là ước chung của $a_n, \ldots, a_1, a_0$, điều này là vô lí. Vậy, $ab \in \mathbb{Z}$. Do đó $p = (abf_1)g_1$. Đặt $f_* = abf_1$ và $g_* = g_1$. Khi đó $p = f_* g_*$ là sự phân tích của p thành tích của hai đa thức với hệ số nguyên f_* và g_* với $\deg f = \deg f_*$ và $\deg g = \deg g_*$. □

Dưới đây là một số ví dụ minh họa việc xét tính bất khả quy trên $\mathbb{Q}$ của các đa thức bằng việc sử dụng Bổ đề Gauss.

2.2.4 Ví dụ. Xét tính bất khả quy của đa thức $f(x) = x^4 + 3x^3 + x^2 + 3$ trên $\mathbb{Q}$.

Giải. Ta chứng minh đa thức này bất khả quy trên $\mathbb{Q}$. Giả sử ngược lại, khi đó theo Định lý 2.2.1, $f(x)$ có sự phân tích thành tích $g(x)h(x)$ trong đó $g(x) \in \mathbb{Z}[x]$ có bậc 1 hoặc bậc 2, $h(x) \in \mathbb{Z}[x]$ có bậc 3 hoặc bậc 2. Vì hệ số cao nhất của $f(x)$ là 1 nên ta có thể giả thiết hệ số cao nhất của $g(x)$ và $h(x)$ cũng là 1. Nếu $g(x)$ bậc 1 thì theo Hệ quả 2.1.2 $f(x)$ có nghiệm nguyên là 3 hoặc -3. Tuy nhiên, thay vào ta có $f(3) \neq 0$ và $f(-3) \neq 0$. Do đó $g(x)$ có bậc 2 và vì thế $h(x)$ có bậc 2. Viết $g(x) = x^2 + ax + b$ và $h(x) = x^2 + cx + d$ với $a, b, c, d \in \mathbb{Z}$. Đồng nhất hệ số ở hai vế của đẳng thức $f = gh$ ta được

$$bd = 3, bc + ad = 0, ac + d + b = 1, c + a = 3.$$

Vì $bd = 3$ và vai trò của b, d là như nhau nên không mất tính tổng quát ta có thể giả thiết $b = 1$, $d = 3$ hoặc $b = -1$, $d = -3$. Nếu $b = 1, d = 3$ thì $c + 3a = 0, ac = -3, a + c = 3$. Suy ra $a = -\dfrac{3}{2} \notin \mathbb{Z}$, vô lí. Nếu $b = -1$ và $d = -3$ thì $-c - 3a = 0, ac = 5, c + a = 3$. Suy ra $a = -\dfrac{3}{2} \notin \mathbb{Z}$, vô lí. Như vậy, $f(x)$ không phân tích được thành tích của hai đa thức bậc nhỏ hơn 4 với hệ số nguyên. Suy ra $f(x)$ bất khả quy trên $\mathbb{Q}$.

2.2.5 Ví dụ. Xét tính bất khả quy của đa thức $f(x) = x^5 + x^3 + x^2 + 5$ trên $\mathbb{Q}$.

Giải. Ta sẽ chứng minh $f(x)$ là bất khả quy trên $\mathbb{Q}$. Thật vậy, giả sử $f(x)$ khả quy trên $\mathbb{Q}$. Khi đó, theo Định lý 2.2.1 ta có $f(x) = g(x)h(x)$ trong đó $g(x) \in \mathbb{Z}[x]$ có bậc 1 hoặc bậc 2, $h(x) \in \mathbb{Z}[x]$ có bậc 4 hoặc bậc 3. Theo Hệ quả 2.1.2, các nghiệm hữu tỷ của $f(x)$ chỉ có thể là ± 5. Tuy nhiên $f(5) \neq 0$ và $f(-5) \neq 0$. Do đó $g(x)$ không thể có bậc 1. Vậy $g(x)$ có bậc

2 và $h(x)$ có bậc 3. Viết $g(x) = x^2 + ax + b$ và $h(x) = x^3 + cx^2 + dx + e$ với $a, b, c, d, e \in \mathbb{Z}$. Đồng nhất hệ số ở hai vế của đẳng thức $f = gh$ ta được

$$a + c = 0, b + d + ac = 1, bc + ad + e = 1, ae + bd = 0, be = 5.$$

Vì $be = 5$ nên các khả năng sau xảy ra:
Trường hợp 1: $b = 1, e = 5$. Khi đó

$$a + c = 0, d + ac = 0, c + ad = -4, 5a + d = 0.$$

Suy ra hoặc $a = -5, c = 5, d = \frac{9}{5} \notin \mathbb{Z}$, vô lý; hoặc $a = 0, c = 0$ thay vào $c + ad = -4$, vô lí.
Trường hợp 2: Nếu $b = -1, e = -5$. Khi đó

$$a + c = 0, d + ac = 2, -c + ad = 6, -5a - d = 0.$$

Suy ra $a = \frac{-5 \pm \sqrt{17}}{2} \notin \mathbb{Z}$, vô lí.
Trường hợp 3: Nếu $b = 5, e = 1$. Khi đó

$$a + c = 0, d + ac = -4, 5c + ad = 0, a + 5d = 0.$$

Suy ra $d = \frac{1 \pm \sqrt{401}}{50} \notin \mathbb{Z}$, vô lí.
Trường hợp 4: Nếu $b = -5, e = -1$. Khi đó

$$a + c = 0, d + ac = 6, -5c + ad = 2, a + 5d = 0.$$

Suy ra $d = \frac{-25 \pm \sqrt{585}}{10} \notin \mathbb{Z}$, vô lí.
Vậy không có các số nguyên a, c, d nào thoả mãn các trường hợp trên. Vì vậy $f(x)$ không phân tích được thành tích của hai đa thức bậc nhỏ hơn 5 với hệ số nguyên. Do đó nó bất khả quy trên $\mathbb{Q}$.

2.3 Phương pháp dùng tiêu chuẩn Eisenstein

2.3.1 Định lý. *[Tiêu chuẩn Eisenstein]. Giả sử*

$$f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

là đa thức với hệ số nguyên sao cho có một số nguyên tố p thoả mãn các tính chất

(i) p không là ước của hệ số cao nhất a_n.

(ii) p là ước của các hệ số còn lại.

(iii) p^2 không là ước của hệ số tự do a_0.

Khi đó f là bất khả quy trên $\mathbb{Q}$.

Chứng minh. Giả sử f không bất khả quy trên $\mathbb{Q}$. Theo Định lý 2.2.1 ta có thể biểu diễn

$$f = gh = (b_0 + b_1 x + \ldots + b_m x^m)(c_0 + c_1 x + \ldots + c_k x^k),$$

trong đó $g, h \in \mathbb{Z}[x]$ với $\deg g = m < n$ và $\deg h = k < n$. Do p là ước của $a_0 = b_0 c_0$ nên p là ước của b_0 hoặc c_0. Lại do p^2 không là ước của a_0 nên trong hai số b_0 và c_0, có một và chỉ một số chia hết cho p. Giả thiết c_0 chia hết cho p. Khi đó b_0 không chia hết cho p. Vì $a_n = b_m c_k$ và a_n không chia hết cho p nên b_m và c_k đều không chia hết cho p. Gọi r là chỉ số bé nhất sao cho c_r không là bội của p. Chú ý rằng số r như vậy luôn tồn tại vì c_k không là bội của p. Trước hết ta xét trường hợp $r < n$. Khi đó p là ước của a_r. Vì $b_0 c_r = a_r - (b_1 c_{r-1} + b_2 c_{r-2} + \ldots + b_r c_0)$ với chú ý rằng các số $c_0, \ldots, c_{r-1}$ đều là bội của p nên $b_0 c_r$ là bội của p. Điều này là vô lí vì cả hai số b_0 và c_r đều không là bội của p. Xét trường hợp $r = n$. Khi đó $n = r \leqslant k \leqslant n$. Suy ra $k = n$, vô lí. Vậy f là bất khả quy trên $\mathbb{Q}$. □

Chúng ta cũng dùng tiêu chuẩn Eisenstein để kiểm tra tính chất bất khả quy của các đa thức sau đây gọi là đa thức chia đường tròn: Cho p là số

nguyên tố. *Đa thức chia đường tròn thứ* p là

$$\Phi_p(x) = x^{p-1} + \ldots + x + 1.$$

2.3.2 Hệ quả. *Với mỗi số nguyên tố* p*, đa thức chia đường tròn thứ* p *là bất khả quy trên* $\mathbb{Q}$*.*

Chứng minh. Chú ý rằng đa thức chia đường tròn $\Phi_p(x)$ là bất khả quy khi và chỉ khi $\Phi_p(x+1)$ là bất khả quy. Ta có

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x}.$$

Suy ra

$$\Phi_p(x+1) = x^{p-1} + C_p^1 x^{p-2} + \ldots + C_p^k x^{p-k-1} + \ldots + C_p^{p-2} x + p,$$

trong đó C_p^k là số tổ hợp chập k của p phần tử. Do p nguyên tố nên C_p^k là bội của p với mọi $k = 1, \ldots, p-2$. Vì thế $\Phi_p(x+1)$ là bất khả quy theo tiêu chuẩn Eisenstein. □

Hệ quả đơn giản sau đây chỉ ra rằng với mỗi số tự nhiên n luôn tồn tại các đa thức bất khả quy trên $\mathbb{Q}$ bậc n.

2.3.3 Hệ quả. *Cho* $a = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ *là sự phân tích tiêu chuẩn của số tự nhiên* a *thành tích các thừa số nguyên tố. Nếu* $n_j = 1$ *với một số* j *nào đó,* $1 \leqslant j \leqslant k$*, thì* $x^n - a$ *là bất khả quy với mọi* n*.*

Chứng minh. Theo giả thiết, a là bội của số nguyên tố p_j nhưng không là bội của p_j^2. Vì thế theo tiêu chuẩn Eisenstein ta có kết quả. □

2.3.4 Ví dụ. Theo tiêu chuẩn Eisenstein với $p = 2$ ta suy ra đa thức $x^5 - 4x + 2$ là bất khả quy trên $\mathbb{Q}$. Chú ý rằng tính chất bất khả quy của đa thức này không dễ kiểm tra bằng Bổ đề Gauss trong Định lý 2.2.1. Ngược lại, tính bất khả quy của đa thức trong Ví dụ 2.2.5 đã được kiểm tra bằng

việc dùng Bổ đề Gauss, nhưng không dễ kiểm tra tính bất khả quy của đa thức này bằng tiêu chuẩn Eisenstein.

2.3.5 Ví dụ. Xét tính bất khả quy trên $\mathbb{Q}$ của các đa thức sau.

(i) $x^{10} + 50$;

(ii) $5x^{11} - 9x^4 + 12x^3 + 36x + 6$;

(iii) $x^4 - 8x^3 + 10x^2 - 12x + 3$.

Giải. (i) Dễ thấy với $p = 2$ đa thức $x^{10} + 50$ bất khả quy trên $\mathbb{Q}$ (theo tiêu chuẩn Eisenstein).

(ii) Đa thức $5x^{11} - 9x^4 + 12x^3 + 36x + 6$ bất khả quy trên $\mathbb{Q}$ theo tiêu chuẩn Eisenstein với $p = 3$.

(iii) Đặt $x = y + 3$ ta có

$$f(x) = x^4 - 8x^3 + 10x^2 - 12x + 3 = y^4 + 4y^3 - 8y^2 - 60y - 78 = f(y).$$

Đa thức $f(y)$ bất khả quy trên $\mathbb{Q}$ theo tiêu chuẩn Eisenstein với $p = 2$. Do đó suy ra đa thức $f(x) = x^4 - 8x^3 + 10x^2 - 12x + 3$ bất khả quy trên $\mathbb{Q}$.

2.4 Rút gọn theo môđun một số nguyên tố

Cho p là một số nguyên tố. Kí hiệu $\mathbb{Z}_p = \{\overline{a} | a \in \mathbb{Z}\}$, trong đó $\overline{a} = \overline{b} \in \mathbb{Z}_p$ khi và chỉ khi $a - b$ chia hết cho p. Ta có thể kiểm tra được $\mathbb{Z}_p$ là một trường với phép cộng $\overline{a} + \overline{b} = \overline{a + b}$ và phép nhân $\overline{a}\overline{b} = \overline{ab}$. Phần tử không là $\overline{0}$, phần tử đơn vị là $\overline{1}$. Trường $\mathbb{Z}_p$ có p phần tử.

Trong tiết này, chúng ta trình bày một phương pháp xét tính bất khả quy trên $\mathbb{Q}$ của đa thức bằng cách dựa vào Bổ đề Gauss và xét nó trên trường $\mathbb{Z}_p$ với p là một số nguyên tố phù hợp. Giả sử

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

Với mỗi số nguyên tố p, kí hiệu $\overline{a}_i \in \mathbb{Z}_p$ là số nguyên a_i môđun p (hay lớp thặng dư của a_i theo môđun p). Kí hiệu

$$\overline{f}(x) := \overline{a}_n x^n + \ldots + \overline{a}_1 x + \overline{a}_0 \in \mathbb{Z}_p[x].$$

2.4.1 Định lý. *Cho $f(x) \in \mathbb{Z}[x]$. Nếu tồn tại một số nguyên tố p sao cho $\deg f(x) = \deg \overline{f}(x)$ và $\overline{f}(x)$ bất khả quy trên $\mathbb{Z}_p$ thì $f(x)$ bất khả quy trên $\mathbb{Q}$.*

Chứng minh. Giả sử $\overline{f}(x)$ bất khả quy trong $\mathbb{Z}_p[x]$ và $\deg f(x) = \deg \overline{f}(x)$. Khi đó $\deg \overline{f}(x) > 0$. Suy ra $\deg f(x) > 0$. Ta cần chứng minh $f(x)$ bất khả quy trên $\mathbb{Q}$. Giả sử $f(x)$ không bất khả quy trên $\mathbb{Q}$. Theo Bổ đề Gauss, $f(x)$ có sự phân tích $f(x) = g(x)h(x)$ trong đó $g(x), h(x) \in \mathbb{Z}[x]$, $\deg f(x) > \deg g(x)$ và $\deg f(x) > \deg h(x)$. Chú ý rằng với mọi số nguyên a, b ta có $\overline{ab} = \overline{a}\ \overline{b}$ và $\overline{a+b} = \overline{a} + \overline{b}$. Vì thế ta có thể kiểm tra được $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$. Do đó $\deg \overline{f}(x) = \deg \overline{g}(x) + \deg \overline{h}(x)$. Vì $\deg f(x) = \deg \overline{f}(x)$, $\deg g(x) \geq \deg \overline{g}(x)$ và $\deg h(x) \geq \deg \overline{h}(x)$ nên ta suy ra $\deg g(x) = \deg \overline{g}(x)$ và $\deg h(x) = \deg \overline{h}(x)$. Vì thế $\overline{f}(x)$ phân tích được thành tích của hai đa thức $\overline{g}(x), \overline{h}(x)$ có bậc thấp hơn, mâu thuẫn với tính bất khả quy trên $\mathbb{Z}_p$ của $\overline{f}(x)$. □

2.4.2 Chú ý. Giả thiết $\deg f(x) = \deg \overline{f}(x)$ trong Định lý 2.4.1 là cần thiết. Chẳng hạn, xét đa thức $f(x) = 5(x-1)^9 + (x-1) \in \mathbb{Z}[x]$. Đa thức này không bất khả quy trên $\mathbb{Q}$ vì nó có ước thực sự là $x - 1$. Ta có $\overline{f}(x) = x - 1 \in \mathbb{Z}_5[x]$. Vì $\overline{f}(x)$ có bậc 1 nên rõ ràng nó là bất khả quy trên $\mathbb{Z}_5$.

2.4.3 Ví dụ. Xét tính bất khả quy trên $\mathbb{Q}$ của các đa thức sau.

(i) $5x^2 + 10x + 4$;

(ii) $3x^3 + 7x^2 + 10x - 5$;

(iii) $11x^4 - 5x^3 + 21x^2 - 9x + 6$.

Giải. (i) Đa thức $f(x) = 5x^2 + 10x + 4 \in \mathbb{Z}[x]$. Chọn $p = 3$, ta có $\overline{f}(x) = 2x^2 + x + 1 \in \mathbb{Z}_3[x]$. Đa thức $\overline{f}(x)$ không có nghiệm trong $\mathbb{Z}_3$ nên là bất khả quy. Vì $\deg f(x) = 2 = \deg \overline{f}(x)$ nên theo Định lý 2.4.1 đa thức $f(x)$ bất khả quy trên $\mathbb{Q}$.

(ii) Rút gọn trong $\mathbb{Z}_2[x]$, đa thức $f(x) = 3x^3 + 7x^2 + 10x - 5 \in \mathbb{Z}[x]$ trở thành $\overline{f}(x) = x^3 + x^2 - 1 \in \mathbb{Z}_2[x]$. Đa thức $\overline{f}(x)$ bất khả quy trên $\mathbb{Z}_2$ vì nó không có nghiệm trong $\mathbb{Z}_2$. Vì $\deg f(x) = 3 = \deg \overline{f}(x)$ nên theo Định lý 2.4.1 đa thức $f(x)$ bất khả quy trên $\mathbb{Q}$.

(iii) Rút gọn trên $\mathbb{Z}_5$, đa thức $f(x) = 11x^4 - 5x^3 + 21x^2 - 9x + 6 \in \mathbb{Z}[x]$ trở thành $\overline{f}(x) = x^4 + x^2 + x + 1 \in \mathbb{Z}_5[x]$. Dễ thấy $\overline{f}(x)$ không có nghiệm trên $\mathbb{Z}_5$ nên nó không có nhân tử bậc một. Giả sử nếu $\overline{f}(x)$ khả quy trong $\mathbb{Z}_5[x]$ thì $\overline{f}(x) = (x^2 + ax + b)(x^2 + cx + d)$ với $a, b, c, d \in \mathbb{Z}_5$. Đồng nhất hệ số ở hai vế của đẳng thức này ta được

$$a + c = 0, b + ac + d = 1, ad + bc = 1, bd = 1.$$

Vì $bd = 1$ và vai trò của b, d là như nhau nên không mất tính tổng quát ta có thể giả thiết $(b, d) = (1, 1)$ hoặc $(b, d) = (2, 3)$ hoặc $(b, d) = (4, 4)$. Nếu $(b, d) = (1, 1)$ thì $a + c = 0, ac = -1, a + c = 1$, vô lí. Nếu $(b, d) = (2, 3)$ thì $a + c = 0, ac = -4, 3a + 2c = 1$. Suy ra $a = 1, c = -1$ nhưng thay vào phương trình $ac = -4$ ta được $-1 = -4$, vô lí. Nếu $(b, d) = (4, 4)$ thì $a + c = 0, ac = -7, a + c = \dfrac{1}{4}$, vô lí. Vậy $\overline{f}(x)$ bất khả quy trên $\mathbb{Z}_5$. Vì $\deg f(x) = 4 = \deg \overline{f}(x)$ nên theo Định lý 2.4.1 đa thức $f(x)$ bất khả quy trên $\mathbb{Q}$.

2.4.4 Chú ý. Peter Cameron đã sử dụng Bổ đề Gauss và dùng phương pháp rút gọn theo môđun một số nguyên tố để đưa ra một chứng minh khác cho tiêu chuẩn Eisenstein như sau: Giả sử $f = gh$, trong đó g, h là các đa thức với hệ số nguyên và $\deg g = m < n$, $\deg h = k < n$. Gọi $a_t, t = 0, 1, \ldots, n$; $b_i, i = 0, 1, \ldots, m$ và $c_j, j = 0, 1, \ldots, k$ tương ứng là

các hệ số của f, g và h. Vì các hệ số $a_0, \ldots, a_{n-1}$ của f đều chia hết cho p nên ta có $\overline{f}(x) = \overline{a}_n x^n$. Chú ý rằng $n = m + k$ và $a_n = b_m c_k$. Do a_n không là bội của p theo giả thiết nên b_m và c_k đều không là bội của p. Vì thế

$$\overline{g}(x) = \overline{b}_m x^m + \text{ đa thức bậc thấp hơn} \in \mathbb{Z}_p[x],$$
$$\overline{h}(x) = \overline{c}_k x^k + \text{ đa thức bậc thấp hơn} \in \mathbb{Z}_p[x].$$

Ta có thể kiểm tra được $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$. Do đó $\overline{a}_n x^n = \overline{g}(x)\overline{h}(x)$. Chú ý rằng $\overline{a}_n x^n$ chỉ có duy nhất một ước bất khả quy là x. Vì thế $\overline{g}(x)$ và $\overline{h}(x)$ cũng chỉ có đúng một ước bất khả quy là x. Do đó $\overline{g}(x) = \overline{b}_m x^m$ và $\overline{h}(x) = \overline{c}_k x^k$. Do đó $\overline{b}_i = 0$ và $\overline{c}_j = 0$ với mọi $i < m$ và $j < k$. Đặc biệt, c_0 và b_0 đều chia hết cho p. Do đó a_0 chia hết cho p^2, vô lí.

Chương 3

Tính bất khả quy trên trường $\mathbb{Z}_p$

Mục đích của chương này là xét tính bất khả quy của các đa thức trên trường $\mathbb{Z}_p$ với p là một số nguyên tố. Để chứng minh các kết quả trong chương này, ngoài việc sử dụng Định lý Kronecker về sự tồn tại trường phân rã của một đa thức, chúng ta cần chuẩn bị thêm một số kết quả về lý thuyết nhóm, đặc biệt là nhóm nhân $\mathbb{Z}_p^*$.

3.1 Kiến thức chuẩn bị về nhóm nhân $\mathbb{Z}_p^*$

3.1.1 Định nghĩa. *Nhóm* là một tập G cùng với một phép toán (kí hiệu theo lối nhân) thoả mãn các điều kiện

(i) Phép toán có tính kết hợp: $a(bc) = (ab)c$ với mọi $a, b, c \in G$.

(ii) G có đơn vị: $\exists e \in G$ sao cho $ex = xe = x$ với mọi $x \in G$.

(iii) Mọi phần tử của G đều khả nghịch: Với mỗi $x \in G$, tồn tại $x^{-1} \in G$ sao cho $xx^{-1} = x^{-1}x = e$.

Một nhóm G được gọi là *nhóm giao hoán* (hay *nhóm Abel*) nếu phép toán là giao hoán, tức là $ab = ba$ với mọi $a, b \in G$. Nếu G có hữu hạn phần tử thì số phần tử của G được gọi là *cấp của* G. Nếu G có vô hạn phần tử thì ta nói G *có cấp vô hạn*.

3.1.2 Ví dụ. Cho $m > 1$ là một số nguyên. Với $a, b \in \mathbb{Z}$, ta định nghĩa

$\overline{a} = \overline{b}$ nếu và chỉ nếu $a - b$ chia hết cho m. Kí hiệu $\mathbb{Z}_m = \{\overline{a} \mid a \in \mathbb{Z}\}$ là tập các số nguyên môđun m (hay tập các lớp thặng dư theo môđun m). Kí hiệu $\mathbb{Z}_m^* = \{\overline{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$ là tập các số nguyên môđun m nguyên tố cùng nhau với m. Khi đó $\mathbb{Z}_m^*$ với phép nhân $\overline{a}\ \overline{b} = \overline{ab}$ là một nhóm giao hoán cấp $\varphi(m)$, trong đó φ là hàm Euler, tức là $\varphi(1) = 1$ và khi $m > 1$ thì $\varphi(m)$ là số các số tự nhiên nhỏ hơn m và nguyên tố cùng nhau với m. Phần tử đơn vị của $\mathbb{Z}_m^*$ là $\overline{1}$. Rõ ràng nếu m là số nguyên tố thì cấp của $\mathbb{Z}_m^*$ là $m - 1$.

3.1.3 Định nghĩa. Tập con H của một nhóm G được gọi là *nhóm con* của G nếu $e \in H$, $a^{-1} \in H$ và $ab \in H$ với mọi $a, b \in H$.

Cho G là một nhóm với phép toán kí hiệu theo lối nhân. Cho $a \in G$. Đặt $(a) = \{a^n \mid n \in \mathbb{Z}\}$. Khi đó (a) là nhóm con của G. Ta gọi (a) là *nhóm con xyclic sinh bởi* a. Cấp của nhóm con (a) được gọi là *cấp của phần tử* a.

3.1.4 Bổ đề. *Cho G là một nhóm với đơn vị e. Với mỗi $a \in G$, các phát biểu sau là tương đương*

(i) a có cấp n.

(ii) n là số nguyên dương bé nhất sao cho $a^n = e$.

(iii) $a^n = e$ và nếu $a^k = e$ thì k là bội của n với mọi $k \in \mathbb{Z}$.

Chứng minh. (i)⇒(ii). Trước hết ta khẳng định tồn tại một số nguyên dương k sao cho $a^k = e$. Giả sử ngược lại, với mọi cặp số tự nhiên $k < k'$ ta có $a^{k'-k} \neq e$. Suy ra $a^k \neq a^{k'}$. Điều này chứng tỏ (a) có cấp vô hạn, vô lí với giả thiết (i). Do đó, tồn tại những số nguyên dương k sao cho $a^k = e$. Gọi r là số nguyên dương bé nhất có tính chất $a^r = e$. Ta thấy rằng các phần tử $e, a, a^2, \ldots, a^{r-1}$ là đôi một khác nhau. Thật vậy, nếu $a^i = a^j$ với $0 \leqslant i \leqslant j < r$ thì $a^{j-i} = e$ và $0 \leqslant j - i < r$, do đó theo cách

chọn của r ta có $i = j$. Bây giờ ta chứng minh $G = \{e, a, a^2, \ldots, a^{r-1}\}$. Rõ ràng $G \supseteq \{e, a, a^2, \ldots, a^{r-1}\}$. Cho $b \in G$. Khi đó $b = a^k$ với $k \in \mathbb{Z}$. Viết $k = rq + s$ trong đó $q, s \in \mathbb{Z}$ và $0 \leqslant s \leqslant r - 1$. Ta có

$$b = a^k = a^{rq+s} = (a^r)^q a^s = a^s \in \{e, a, a^2, \ldots, a^{r-1}\}.$$

Vì thế $G = \{e, a, a^2, \ldots, a^{r-1}\}$ là nhóm cấp r. Suy ra $r = n$ và (ii) được chứng minh.

(ii)⇒(iii). Giả sử $a^k = e$. Viết $k = nq + r$ với $0 \leqslant r < n$. Vì $a^n = e$ nên $e = a^k = a^{nq}a^r = a^r$. Theo cách chọn n ta phải có $r = 0$, suy ra k chia hết cho n.

(iii)⇒(i). Gọi r là số nguyên dương bé nhất sao cho $a^r = e$. Theo (iii), r là bội của n. Do đó n là số nguyên dương bé nhất thỏa mãn $a^n = e$. Tương tự như chứng minh (i)⇒(ii) ta suy ra cấp của a là n. □

3.1.5 Ví dụ. Xét nhóm nhân $\mathbb{Z}_7^*$. Cấp của $\mathbb{Z}_7^*$ là $\varphi(7) = 6$. Nhóm con xyclic sinh bởi $\overline{2}$ là $(\overline{2}) = \{\overline{1}, \overline{2}, \overline{4}\}$. Do đó cấp của $\overline{2}$ trong nhóm nhân $\mathbb{Z}_7^*$ là 3. Chú ý rằng 3 là số nguyên dương bé nhất thỏa mãn $(\overline{2})^3 = \overline{1} \in \mathbb{Z}_7$. Vì thế theo bổ đề trên ta cũng suy ra cấp của $\overline{2}$ là 3.

3.1.6 Định nghĩa. Cho H là nhóm con của G với phép toán kí hiệu theo lối nhân. Với $a \in G$, kí hiệu $Ha = \{ha \mid h \in H\}$. Chú ý rằng $Ha = Hb$ nếu và chỉ nếu $ab^{-1} \in H$. Ta gọi Ha là *lớp ghép trái* của H trong G ứng với phần tử a. Khi H chỉ có hữu hạn lớp ghép trái thì số các lớp ghép trái của H được gọi là *chỉ số của H trong G*.

3.1.7 Định lý. *(**Lagrange**). Trong một nhóm hữu hạn, cấp và chỉ số của một nhóm con là ước của cấp của toàn nhóm.*

Chứng minh. Giả sử G là nhóm có cấp n và H là nhóm con của G có cấp m. Với mỗi $a \in G$ ta có $a = ea \in Ha$. Vì thế, mỗi phần tử của G

đều thuộc một lớp ghép trái của H. Giả sử $Ha \cap Hb \neq \emptyset$. Khi đó tồn tại $h, h' \in H$ sao cho $ha = h'b$. Suy ra $a = h^{-1}h'b$. Cho $xa \in Ha$, trong đó $x \in H$. Khi đó $xa = (xh^{-1}h')b \in Hb$. Suy ra $Ha \subseteq Hb$. Tương tự, $Hb \subseteq Ha$ và do đó $Ha = Hb$. Vậy hai lớp ghép trái bất kì của H nếu khác nhau thì phải rời nhau. Với mỗi $a \in G$, rõ ràng ánh xạ $f : H \to Ha$ xác định bởi $f(h) = ha$ là một song ánh. Vì thế mỗi lớp ghép trái của H đều có đúng m phần tử. Gọi chỉ số của H là s. Từ các lập luận trên ta suy ra $n = sm$. Vì thế s và m đều là ước của n. □

3.1.8 Ví dụ. Xét nhóm nhân $\mathbb{Z}_7^*$. Cấp của $\mathbb{Z}_7^*$ là 6. Cấp của nhóm con $(\overline{2}) = \{\overline{1}, \overline{2}, \overline{4}\}$ là 3. Theo chứng minh Định lý Lagrange, chỉ số của nhóm con $\{\overline{1}, \overline{2}, \overline{4}\}$ là $6 : 3 = 2$.

3.2 Tính bất khả quy trên trường $\mathbb{Z}_p$

Trong suốt tiết này, luôn giả thiết p là một số nguyên tố. Khi đó $\mathbb{Z}_p$ là một trường với phép cộng và phép nhân các số nguyên môđun p. Để thuận tiện, các phần tử của $\mathbb{Z}_p$ vẫn được kí hiệu như các số nguyên, trong đó ta hiểu hai phần tử $a, b \in \mathbb{Z}_p$ là bằng nhau nếu và chỉ nếu $a - b$ là bội của p.

Giả sử $f(x)$ là đa thức với hệ số nguyên. Coi $f(x)$ như đa thức trong $\mathbb{Z}_p[x]$. Trong trường hợp khi bậc của $f(x)$ không lớn và p là số nguyên tố nhỏ thì ta có thể kiểm tra tính bất khả quy của $f(x)$ trên $\mathbb{Z}_p$ trực tiếp từ định nghĩa đa thức bất khả quy. Sau đây là một ví dụ minh họa.

3.2.1 Ví dụ. Đa thức $x^4 + x + 1$ là bất khả quy trên $\mathbb{Z}_2$.

Chứng minh. Giả sử $f(x) = x^4 + x + 1$ không bất khả quy trên $\mathbb{Z}_2$. Vì $f(x)$ không có nghiệm trong $\mathbb{Z}_2$ nên nó không có nhân tử bậc nhất. Vì thế nó phân tích được thành tích của hai đa thức bậc hai: $f(x) = g(x)h(x)$ với $g(x), h(x) \in \mathbb{Z}_2[x]$ và $\deg g(x) = \deg h(x) = 2$. Các đa thức bậc hai

trong $\mathbb{Z}_2[x]$ là $x^2, x^2+x, x^2+1, x^2+x+1$. Dễ thấy đa thức bậc hai duy nhất trong $\mathbb{Z}_2[x]$ không có nghiệm trong $\mathbb{Z}_2$ là x^2+x+1. Vì $f(x)$ không có nghiệm trong $\mathbb{Z}_2$ nên $g(x)$ và $h(x)$ cũng không có nghiệm trong $\mathbb{Z}_2$. Do đó $g(x) = h(x) = x^2+x+1$. Rõ ràng x^4+x+1 không chia hết cho x^2+x+1, tức là $f(x)$ không chia hết cho $g(x)$, điều này là vô lí. Vậy, x^4+x+1 là bất khả quy trên $\mathbb{Z}_2$. □

Trong trường hợp tổng quát, khi p là số nguyên tố bất kì, việc kiểm tra tính bất khả quy trên trường $\mathbb{Z}_p$ nhìn chung không thực hiện được. Mục đích của tiết này là sử dụng Định lý Kronecker về trường phân rã (Định lý 1.3.2) và Định lý Lagrange trong lý thuyết nhóm (Định lý 3.1.7) để xét tính bất khả quy của đa thức trên $\mathbb{Z}_p$ trong một số trường hợp đặc biệt.

3.2.2 Mệnh đề. *Đa thức x^2+1 là bất khả quy trên $\mathbb{Z}_p$ với mọi số nguyên tố p thỏa mãn $p \equiv 3(\mathrm{mod}\ 4)$.*

Chứng minh. Cho p là số nguyên tố thỏa mãn $p \equiv 3(\mathrm{mod}\ 4)$. Giả sử x^2+1 không bất khả quy trên $\mathbb{Z}_p$. Khi đó x^2+1 phân tích được thành tích của hai đa thức bậc 1. Do đó x^2+1 có nghiệm $\alpha \in \mathbb{Z}_p$. Vì thế $\alpha^2 = -1$. Suy ra $\alpha^4 = 1$. Do $p \equiv 3(\mathrm{mod}\ 4)$ nên $p \neq 2$. Vì thế $1 \neq -1 \in \mathbb{Z}_p$. Suy ra $\alpha \neq \pm 1$ và $\alpha^2 \neq 1$. Ta khẳng định $\alpha^3 \neq 1$. Thật vậy, nếu $\alpha^3 = 1$ thì $\alpha^2\alpha = 1$. Do đó $-\alpha = 1$ hay $\alpha = -1$. Điều này là vô lí. Vậy $\alpha^n \neq 1$ với mọi $n = 1, 2, 3$ và $\alpha^4 = 1$. Chú ý rằng $\alpha \neq 0$ vì 0 không là nghiệm của x^2+1. Do đó $\alpha \in \mathbb{Z}_p^*$. Theo Bổ đề 3.1.4, cấp của phần tử α trong nhóm nhân $\mathbb{Z}_p^*$ là 4. Vì p là số nguyên tố nên cấp của nhóm nhân $\mathbb{Z}_p^*$ là $p-1$. Theo Định lý Lagrange, cấp của α là ước của cấp của nhóm nhân $\mathbb{Z}_p^*$. Do đó 4 là ước của $p-1$. Từ giả thiết ta ta có $p-1$ đồng dư với 2 theo môđun 4. Điều này là vô lí. Vậy x^2+1 là bất khả quy trên $\mathbb{Z}_p$. □

3.2.3 Mệnh đề. *Đa thức x^2+x+1 là bất khả quy trên $\mathbb{Z}_p$ với mọi số nguyên tố p thỏa mãn $p \equiv 2(\mathrm{mod}\ 3)$.*

Chứng minh. Cho p là số nguyên tố thỏa mãn $p \equiv 2(\mathrm{mod}\ 3)$. Giả sử $f(x) = x^2 + x + 1$ không bất khả quy trên $\mathbb{Z}_p$. Khi đó $f(x)$ là tích của hai đa thức bậc 1. Do đó $f(x)$ có nghiệm $\alpha \in \mathbb{Z}_p$. Chú ý rằng 0 không là nghiệm của $f(x)$. Vì thế $\alpha \neq 0$ và do đó $\alpha \in \mathbb{Z}_p^*$. Vì

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

và vì α là nghiệm của $f(x)$ nên α là nghiệm của $x^3 - 1$. Suy ra $\alpha^3 = 1$. Ta khẳng định 1 không là nghiệm của $f(x)$. Thật vậy, nếu 1 là nghiệm của $f(x)$ thì $1 + 1 + 1 = 0 \in \mathbb{Z}_p$ và do đó 3 là bội của p. Tuy nhiên, $p \equiv 2(\mathrm{mod}\ 3)$. Điều này là vô lí. Vậy 1 không là nghiệm của $f(x)$ và do đó $\alpha \neq 1$. Nếu $\alpha^2 = 1$ thì $1 = \alpha^3 = \alpha^2\alpha = \alpha$, điều này là vô lí. Như vậy, $\alpha^n \neq 1$ với $n = 1, 2$ và $\alpha^3 = 1$. Theo Bổ đề 3.1.4, cấp của α trong nhóm nhân $\mathbb{Z}_p^*$ là 3. Chú ý rằng $\mathbb{Z}_p^*$ có cấp là $p - 1$ đồng dư với 1 theo môđun 3. Theo Định lý Lagrange, 3 là ước của $p - 1$. Điều này vô lí. Do đó, $x^2 + x + 1$ là đa thức bất khả quy trên $\mathbb{Z}_p$. □

3.2.4 Mệnh đề. *Đa thức $f(x) = x^4 + x^3 + x^2 + x + 1$ là bất khả quy trên $\mathbb{Z}_p$ với mọi số nguyên tố p thỏa mãn $p \neq 5$ và $p \not\equiv \pm 1(\mathrm{mod}\ 5)$.*

Chứng minh. Cho p là số nguyên tố thỏa mãn $p \neq 5$ và $p \not\equiv \pm 1(\mathrm{mod}\ 5)$. Theo Định lý 1.3.2 (Kronecker), tồn tại một trường K chứa $\mathbb{Z}_p$ và chứa các nghiệm của $f(x)$. Gọi α là một nghiệm của $f(x)$. Rõ ràng 0 không là nghiệm của $f(x)$, vì thế $\alpha \neq 0$.

• Khẳng định 1: $\alpha^n \neq 1$ với mọi $n = 1, 2, 3, 4$ và $\alpha^5 = 1$. Thật vậy, rõ ràng $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) = (x-1)f(x)$. Do đó α là nghiệm của $x^5 - 1$. Suy ra $\alpha^5 = 1$. Nếu $\alpha = 1$ thì $5 = 0 \in \mathbb{Z}_p$ và do đó 5 là bội của p, điều này là mâu thuẫn với giả thiết $p \neq 5$. Suy ra $\alpha \neq 1$. Nếu $\alpha^2 = 1$ thì $1 = \alpha^5 = (\alpha^2)^2\alpha = \alpha$, điều này là vô lí. Nếu $\alpha^3 = 1$ thì $1 = \alpha^5 = \alpha^3\alpha^2 = \alpha^2$, vô lí. Nếu $\alpha^4 = 1$ thì $1 = \alpha^5 = \alpha^4\alpha = \alpha$, vô

lí. Như vậy, $\alpha^n \neq 1$ với mọi $n = 1, 2, 3, 4$ và $\alpha^5 = 1$. Khẳng định được chứng minh.

• Khẳng định 2: $f(x)$ không có nhân tử bậc nhất trong $\mathbb{Z}_p[x]$. Thật vậy, giả sử $f(x)$ có nhân tử bậc nhất. Khi đó $f(x)$ có nghiệm $\alpha \in \mathbb{Z}_p$. Vì $\alpha \neq 0$ nên $\alpha \in \mathbb{Z}_p^*$. Theo Khẳng định 1, $\alpha^n \neq 1$ với mọi $n = 1, 2, 3, 4$ và $\alpha^5 = 1$. Vì thế, theo Bổ đề 3.1.4, cấp của α trong nhóm nhân $\mathbb{Z}_p^*$ là 5. Theo Định lý Lagrange, 5 là ước của cấp của $\mathbb{Z}_p^*$. Từ giả thiết, $\mathbb{Z}_p^*$ có cấp $p-1$ không chia hết cho 5. Điều này là vô lí.

• Khẳng định 3: $f(x)$ không có nhân tử bậc hai trong $\mathbb{Z}_p[x]$. Thật vậy, giả sử $f(x)$ có nhân tử bậc hai. Khi đó $f(x) = q(x)r(x)$, trong đó $q(x), r(x) \in \mathbb{Z}_p[x]$ và $\deg q(x) = \deg r(x) = 2$. Chú ý rằng $q(x), r(x)$ là bất khả quy trên $\mathbb{Z}_p$ vì nếu ngược lại thì $q(x)$ hoặc $r(x)$ có nhân tử bậc nhất và do đó $f(x)$ có nhân tử bậc nhất, điều này mâu thuẫn với Khẳng định 2. Do α là nghiệm của $f(x)$ nên nó là nghiệm của $q(x)$ hoặc $r(x)$. Không mất tính tổng quát, ta giả thiết α là nghiệm của $q(x)$. Đặt $F = \mathbb{Z}_p$ và $T = \{a + b\alpha \mid a, b \in \mathbb{Z}_p\}$. Rõ ràng phép cộng đóng kín trong T. Cho $u = a + b\alpha, v = c + d\alpha \in T$. Viết $q(x) = a_0 + a_1x + a_2x^2$ với $a_0, a_1, a_2 \in \mathbb{Z}_p$. Do α là nghiệm của $q(x)$ nên $a_0 + a_1\alpha + a_2\alpha^2 = 0$. Lại do $q(x)$ có bậc hai nên $a_2 \neq 0$. Vì thế $\alpha^2 = -a_2^{-1}(a_0 + a_1\alpha)$. Do đó

$$\begin{aligned} uv &= ac + bd\alpha^2 + (ad + bc)\alpha \\ &= ac - bda_0a_2^{-1} + (ad + bc - bda_1a_2^{-1})\alpha \in T. \end{aligned}$$

Vì thế T đóng kín với phép cộng và phép nhân. Dễ kiểm tra được T là một trường con của trường K. Xét T như $F-$không gian véc tơ. Rõ ràng $\{1, \alpha\}$ là một hệ sinh của $F-$không gian véc tơ T. Giả sử $a.1 + b\alpha = 0$ với $a, b \in F$. Nếu $b = 0$ thì $a = 0$. Nếu $b \neq 0$ thì $\alpha = -ab^{-1} \in F = \mathbb{Z}_p$, vô lí với Khẳng định 2. Do đó $\{1, \alpha\}$ là một cơ sở của $F-$không gian véc tơ T, và vì thế chiều của không gian này là 2. Do F có p phần tử và

$\dim_F T = 2$ nên T có p^2 phần tử. Suy ra nhóm nhân $T^* = T \setminus \{0\}$ có cấp là $p^2 - 1 = (p-1)(p+1)$. Vì $\alpha \neq 0$ nên $\alpha \in T^*$. Theo Khẳng định 1 ta có $\alpha^n \neq 1$ với mọi $n = 1, 2, 3, 4$ và $\alpha^5 = 1$. Vì thế, theo Bổ đề 3.1.4, cấp của α trong nhóm nhân T^* là 5. Theo Định lý Lagrange, 5 là ước của $(p-1)(p+1)$. Vì $p \not\equiv \pm 1 (\mathrm{mod}\ 5)$ theo giả thiết nên 5 không là ước của $(p-1)(p+1)$, vô lí. Vậy $f(x)$ bất khả quy trên $\mathbb{Z}_p$. □

3.2.5 Mệnh đề. *Đa thức* $f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ *là bất khả quy trên* $\mathbb{Z}_p$ *với mọi số nguyên tố* $p \equiv 3 (\mathrm{mod}\ 7)$ *hoặc* $p \equiv 5 (\mathrm{mod}\ 7)$.

Chứng minh. Cho $p \equiv 3 (\mathrm{mod}\ 7)$ hoặc $p \equiv 5 (\mathrm{mod}\ 7)$ với p là số nguyên tố. Theo Định lý 1.3.2 (Kronecker), tồn tại một trường K chứa $\mathbb{Z}_p$ và chứa tất cả các nghiệm của $f(x)$. Gọi $\alpha \in K$ là một nghiệm của $f(x)$. Rõ ràng 0 không là nghiệm của $f(x)$, vì thế $\alpha \neq 0$.

• Khẳng định 1: $\alpha^n \neq 1$ với mọi $n = 1, 2, 3, 4, 5, 6$ và $\alpha^7 = 1$. Thật vậy, rõ ràng $x^7 - 1 = (x-1)f(x)$. Do đó α là nghiệm của $x^7 - 1$. Suy ra $\alpha^7 = 1$. Nếu $\alpha = 1$ thì $7 = 0 \in \mathbb{Z}_p$ và do đó 7 là bội của p, điều này là mâu thuẫn với giả thiết về p. Nếu $\alpha^2 = 1$ thì $1 = \alpha^7 = (\alpha^2)^3\alpha = \alpha$, điều này là vô lí. Nếu $\alpha^3 = 1$ thì $1 = \alpha^7 = (\alpha^3)^2\alpha = \alpha$, vô lí. Nếu $\alpha^4 = 1$ thì $1 = \alpha^7 = \alpha^4\alpha^3 = \alpha^3$, vô lí. Nếu $\alpha^5 = 1$ thì $1 = \alpha^7 = \alpha^5\alpha^2 = \alpha^2$, vô lí. Nếu $\alpha^6 = 1$ thì $1 = \alpha^7 = \alpha^6\alpha = \alpha$, vô lí. Như vậy, $\alpha^n \neq 1$ với mọi $n = 1, 2, 3, 4, 5, 6$ và $\alpha^7 = 1$.

• Khẳng định 2: $f(x)$ không có nhân tử bậc nhất trong $\mathbb{Z}_p[x]$. Thật vậy, nếu $f(x)$ có nhân tử bậc nhất thì $f(x)$ có nghiệm trong $\alpha \in \mathbb{Z}_p$. Theo Khẳng định 1, $\alpha^n \neq 1$ với mọi $n = 1, 2, 3, 4, 5, 6$ và $\alpha^7 = 1$. Vì $\alpha \neq 0$ nên $\alpha \in \mathbb{Z}_p^*$. Do đó cấp của α trong nhóm nhân $\mathbb{Z}_p^*$ là 7. Theo giả thiết, $\mathbb{Z}_p^*$ có cấp $p-1$, trong đó $p-1$ đồng dư với 2 theo môđun 7 hoặc đồng dư với 4 theo môđun 7. Theo Định lý Lagrange, 7 là ước của $p-1$, điều này là vô lí.

• Khẳng định 3: $f(x)$ không có nhân tử bậc hai trong $\mathbb{Z}_p[x]$. Thật vậy, giả sử $f(x)$ có nhân tử $q(x) \in \mathbb{Z}_p[x]$ bậc hai. Theo Khẳng định 2, $f(x)$ không có nhân tử bậc nhất. Vì thế $q(x)$ không có nhân tử bậc nhất. Suy ra $q(x)$ là bất khả quy trên $\mathbb{Z}_p$. Lấy $\alpha \in K$ là một nghiệm của $q(x)$. Tương tự như chứng minh Mệnh đề 3.2.4, ta suy ra tập $T = \{a + b\alpha \mid a, b \in \mathbb{Z}_p\}$ là một trường con của K, trường này có p^2 phần tử. Vì $\alpha \neq 0$ nên $\alpha \in T^*$. Theo Khẳng định 1, ta có $\alpha^n \neq 1$ với mọi $n = 1, 2, 3, 4, 5, 6$ và $\alpha^7 = 1$. Vì thế cấp của α trong nhóm nhân T^* là 7. Theo Định lý Lagrange, 7 là ước của cấp của nhóm nhân T^*. Chú ý rằng T^* có cấp $p^2 - 1$. Tuy nhiên $p^2 - 1$ không chia hết cho 7 vì nó đồng dư với 1 hoặc 3 theo môđun 7. Điều này là vô lí.

• Khẳng định 4: $f(x)$ không có nhân tử bậc ba trong $\mathbb{Z}_p[x]$. Thật vậy, giả sử $f(x)$ có nhân tử bậc ba $q(x) \in \mathbb{Z}_p[x]$. Theo các Khẳng định 2, 3, đa thức $q(x)$ bất khả quy trên $\mathbb{Z}_p$. Tương tự như chứng minh Khẳng định 3, ta có thể chứng minh được tập

$$T = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}_p\}$$

là một trường con của K, trường này có p^3 phần tử. Vì $\alpha \neq 0$ nên $\alpha \in T^*$. Theo Khẳng định 1, ta có $\alpha^n \neq 1$ với mọi $n = 1, 2, 3, 4, 5, 6$ và $\alpha^7 = 1$. Vì thế cấp của α trong nhóm nhân T^* là 7. Theo Định lý Lagrange, 7 là ước của cấp của nhóm nhân T^*. Nhóm nhân T^* có cấp $p^3 - 1$. Chú ý rằng $p^3 - 1$ không chia hết cho 7 vì nó đồng dư với 5 theo môđun 7, vô lí.

Vậy $f(x)$ không có nhân tử bậc một, bậc hai hay bậc ba, do đó nó bất khả quy trên $\mathbb{Z}_p$. □

3.2.6 Mệnh đề. *Đa thức $f(x) = x^{10} + x^9 + \ldots + x + 1$ là bất khả quy trên trường $\mathbb{Z}_p$ với mọi số nguyên tố p sao cho $p \equiv 2, 6, 7, 8 \pmod{11}$.*

Chứng minh. Cho p là số nguyên tố sao cho $p \equiv 2, 6, 7, 8 \pmod{11}$. Theo Định lý Kronecker, tồn tại một trường K chứa $\mathbb{Z}_p$ và chứa các nghiệm của

$f(x)$. Gọi $\alpha \in K$ là một nghiệm của $f(x)$. Tương tự như chứng minh Mệnh đề 3.2.5, ta có thể chỉ ra rằng $\alpha^n \neq 1$ với mọi $n = 1, 2, \ldots, 10$ và $\alpha^{11} = 1$. Rõ ràng 0 không là nghiệm của $f(x)$, do đó $\alpha \neq 0$.

Cho $d \in \{1, 2, 3, 4, 5\}$. Giả sử $f(x)$ có nhân tử $q(x)$ bất khả quy bậc d. Gọi $\alpha \in K$ là một nghiệm của $q(x)$. Đặt

$$T = \Big\{ \sum_{i=0}^{d-1} a_i \alpha^i \mid a_i \in \mathbb{Z}_p, \ \forall i \Big\}.$$

Do $\deg q(x) = q$ nên T là một trường. Xét T như một $\mathbb{Z}_p-$không gian véc tơ. Do $q(x)$ bất khả quy nên ta có thể chỉ ra rằng $\{1, \alpha, \ldots, \alpha^{d-1}\}$ là một cơ sở của T. Do đó $\dim_{\mathbb{Z}_p} T = d$ và vì thế T có p^d phần tử. Do $\alpha \neq 0$ nên $\alpha \in T^*$. Vì $\alpha^n \neq 1$ với mọi $n = 1, 2, \ldots, 10$ và $\alpha^{11} = 1$ nên α có cấp 11 trong nhóm nhân T^*. Theo Định lý Lagrange, 11 là ước của $p^d - 1$. Theo giả thiết, ta có

(i) $p - 1$ đồng dư với một trong các số $1, 5, 6, 7$ theo môđun 11.

(ii) $p^2 - 1$ đồng dư với một trong các số $3, 2, 4, 8$ theo môđun 11.

(ii) $p^3 - 1$ đồng dư với một trong các số $7, 6, 1, 5$ theo môđun 11.

(iii) $p^4 - 1$ đồng dư với một trong các số $4, 8, 2, 3$ theo môđun 11.

(iv) $p^5 - 1$ đồng dư với 9 theo môđun 11.

Như vậy, $p^d - 1$ không là bội của 11 với mọi $d \leqslant 5$. Suy ra $f(x)$ không có nhân tử bất khả quy bậc d với mọi $d \leqslant 5$. Vì thế $f(x)$ bất khả quy trên $\mathbb{Z}_p$. □

KẾT LUẬN

Trong luận văn này, chúng tôi đã trình bày các nội dung sau đây về đa thức bất khả quy trên một trường:

• Trình bày một số kiến thức cơ sở về đa thức bất khả quy.

• Sử dụng đa thức bất khả quy để chứng minh Định lý Kronecker về sự tồn tại trường phân rã của một đa thức (Định lý 1.3.2) và chứng minh Định lý của Galois về sự tồn tại một trường hữu hạn (Định lý 1.3.5).

• Đưa ra một số phương pháp xét tính bất khả quy của đa thức trên $\mathbb{Q}$ như phương pháp tìm nghiệm hữu tỷ, phương pháp dùng Bổ đề Gauss (Định lý 2.2.1), phương pháp dùng tiêu chuẩn Eisenstein (Định lý 2.3.1) và phương pháp rút gọn theo môđun một số nguyên tố (Định lý 2.4.1).

• Sử dụng Định lý Kronecker về trường phân rã (Định lý 1.3.2) và Định lý Lagrange về cấp của nhóm hữu hạn (Định lý 3.1.7) để xét tính bất khả quy của một vài đa thức trên trường $\mathbb{Z}_p$ với p là số nguyên tố.

Tài liệu tham khảo

[Bo] N. C. Bonciocat, *Upper bound for the number of factors for a class of polynomials with rational coefficients*, Acta Arithmetica, **(2) 113** (2004), 175-187.

[C] Nguyễn Tự Cường, *Đại số hiện đại, tập 1*, NXB ĐHQGHN, 2001.

[DO] H. L. Dorwart and O. Ore, *Criteria for the irreducibility of polynomials*, Ann. Math, **(2) 34** (1934), 81-94.

[G] P. Garrett, *Abstract Algebra*, Chapman - Hall/CRC, 2007.

[Rot] J. Rotman, *Galois Theory*, Springer (2001), Second Edition.

[Sc] A. Schinzel, *Polynomials with special regards to reducibility*, Cambridge University Press, 2000.

[S] I. Seres, *Irreducibility of polynomials*, Journal of Algebra, **2** (1965), 283-286.