AULA 5

Critérios de irredutibilidade Em $\mathbb{Z}[x]$

META:

Determinar critérios de irredutibilidade em $\mathbb{Z}[x]$ para mostrar irredutibilidade em $\mathbb{Q}[x]$.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Aplicar os critérios de irredutibilidade para determinar se um dado polinômio com coeficientes inteiros é irredutível em $\mathbb{Q}[x]$.

PRÉ-REQUISITOS

A definição de isomorfismo de anéis e a noção de polinômio irredutível.

Critérios de irredutibilidade
Em $\mathbb{Z}[x]$

5.1 Introdução

Considere $f(x) = x^4 - 5x^2 + 1 \in \mathbb{Q}[x]$. Vamos testar a redutibilidade de $f(x)$ em $\mathbb{Q}[x]$? Pela aula anterior, é suficiente testarmos a redutibilidade de $f(x)$ em $\mathbb{Z}[x]$. As possíveis combinações dos graus para fatorações de $f(x)$ são da forma 1.1.1.1, 1.1.2, 1.3 e 2.2. As três primeiras implicam (pelo teorema do fator) na existência de pelo menos uma raiz racional. Pelo teste da raiz racional, as únicas possíveis raízes de $f(x)$ em $\mathbb{Q}[x]$ são $1, -1$. Mas, $f(1) = f(-1) = -3 \neq 0$. Logo, $f(x)$ não possui raízes em $\mathbb{Q}$ e, portanto, não possui fatores de grau 1. Deste modo, a única maneira de fatoração para $f(x)$ seria na forma

$$f(x) = (a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0), \quad a_0, a_1, b_0, b_1 \in \mathbb{Z}$$

No entanto, $f(x)$ é mônico e isto acarreta $a_2 = b_2 = 1$ (você consegue enxergar isto?). Assim temos:

$$f(x) = (x^2 + a_1x + a_0)(x^2 + b_1x + b_0).$$

Efetuando este produto obtemos:

$$x^4+(a_1+b_1)x^3+(a_0+a_1b_1+b_0)x^2+(a_1b_0+a_0b_1)x+a_0b_0 = x^4-5x^2+1$$

Da igualdade de polinômios, obtemos o seguinte sistema em $\mathbb{Z}$:

$$a_1 + b_1 = 0 \quad a_0 + a_1b_1 + b_0 = -5 \quad a_1b_0 + a_0b_1 = 0 \quad a_0b_0 = 1$$

Mas, $a_0b_0 = 1$ em $\mathbb{Z}$ acarreta $a_0 = b_0 = 1$ ou $a_0 = b_0 = -1$ e $a_1 + b_1 = 0$ acarreta $a_1 = -b_1$. Então, da equação

$$a_0 + a_1b_1 + b_0 = -5$$

podemos concluir que

$$a_1^2 - 1 - 1 = 5 \quad \text{ou} \quad a_1^2 + 1 + 1 = 5$$

donde $a_1^2 = 7$ ou $a_1^2 = 3$. Como não existem inteiros cujo quadrados são 3 ou 7 segue a impossibilidade de fatorar $f(x)$ em $\mathbb{Z}[x]$. Assim, $f(x)$ é irredutível em $\mathbb{Z}[x]$, logo também em $\mathbb{Q}[x]$.

Observe, prezado aluno, que a tarefa de caracterizar irredutibilidade pela definição é impraticável. Por exemplo, você saberia discutir a irredutibilidade do polinômio $x^{17}+6x^{13}-15x^4+3x^2-9x+12$ em $\mathbb{Q}[x]$? Imagine quantas combinações possíveis existem para se fatorar tal polinômio. Felizmente, existem critérios muito eficazes para nos auxiliar nesta tarefa. É o que nos ensina os critérios de irredutibilidade a seguir.

5.2 Critério de Eisenstein

Seja $f(x) = a_0 + a_1x + \dots a_nx^n \in \mathbb{Z}[x]$ não constante. Suponha que existe um primo $p \in \mathbb{Z}$ tal que $p|a_0, \dots, p|a_{n-1}$, $p \nmid a_n$ e $p^2 \nmid a_0$. Vamos mostrar, nestas condições, que $f(x)$ é irredutível em $\mathbb{Q}[x]$. Seguiremos o raciocínio por redução ao absurdo. Suponhamos $f(x)$ redutível em $\mathbb{Q}[x]$ e um primo p nas condições acima. Pela aula anterior, $f(x)$ admitiria uma fatoração em $\mathbb{Z}[x]$, digamos

$$f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s)$$

com $b_i, c_j \in \mathbb{Z}$, $1 \leq r < n$ e $1 \leq s < n$. Temos a seguinte sequência de implicações:

1. $p|a_0$, $a_0 = b_0c_0$ e p primo $\Rightarrow p|b_0$ ou $p|c_0$. Podemos supor $p|b_0$.

2. $p \nmid a_n$, $a_n = b_rc_s \Rightarrow p \nmid b_r$ e $p \nmid c_s$.

3. $p^2 \nmid a_0$, $a_0 = c_0b_0$ e $p|b_0 \Rightarrow p \nmid c_0$.

4. $p|b_0$ e $p \nmid b_r \Rightarrow$ existe um menor inteiro k, $1 \leq k \leq r$, tal que $p \nmid p_k$.

O inteiro k, determinado no item 4, tem a seguinte propriedade:

$$p|b_i, \quad 0 \leq i < k, \quad \text{e} \quad p \nmid b_k$$

com $1 \leq k \leq r < n$. Desde que

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0$$

temos

$$b_kc_0 = a_k - b_0c_k - b_1c_{k-1} + \cdots - b_{k-1}c_1 \tag{5.5}$$

Mas, $p|a_k$ $(k < n)$ e $p|b_i$, para $i < k$. Então p divide cada parcela do membro direito da equação 5.5 e, portanto, $p|b_kc_0$. Isto implica $p|b_k$ e $p|c_0$, um absurdo. Este resultado é conhecido como critério de Eisenstein. Segue o enunciado em forma de teorema.

Teorema 5.1. *(Critério de Eisenstein) Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ não constante. Se existe um primo $p \in \mathbb{Z}$ tal que $p|a_0,\ldots,p|a_{n-1}$, $p \nmid a_n$ e $p^2 \nmid a_0$, então, $f(x)$ é irredutível em $\mathbb{Q}[x]$.*
□

Exemplo 5.1. O polinômio $x^{17} + 6x^{13} - 15x^4 + 3x^2 - 9x + 12$ dado na introdução é irredutível em $\mathbb{Q}[x]$ pelo critério de Eisenstein para $p = 3$. Os polinômios da forma $x^n - p$ são irredutíveis pelo critério de Eisenstein para p primo.

5.3 Critério $\mathbb{Z}_p[x]$

Embora o critério de Eisenstein seja bastante eficiente, existem muitos polinômios para os quais o critério não se aplica. Por exemplo, $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$. Neste caso, precisamos desenvolver um novo método. Para todo inteiro n está definido o homomorfismo de anéis de polinômios

$$\varphi_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$$

em que para cada polinômio $f(x) = a_0 + a_1x + \cdots a_rx^r$ associa o polinômio $\varphi_n(f(x)) = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_rx^r$ onde $\overline{a}_i$ denota a classe de equivalência de a_i no anel quociente $\mathbb{Z}_n$. Usaremos este homomorfismo para p primo. Assim, o anel quociente $\mathbb{Z}_p$ é um corpo e podemos então aplicar toda a teoria desenvolvida até aqui para anéis polinomiais sobre corpos.

Seja $f(x) = a_0 + a_1x + \cdots a_nx^n \in \mathbb{Z}[x]$ de grau n. Considere um primo p tal que $p \nmid a_n$. Então, $\varphi_p(f(x))$ é um polinômio em $\mathbb{Z}_p[x]$ de grau n visto que $\overline{a}_n \neq \overline{0}$ pois $p \nmid a_n$. Vamos mostrar que se $\varphi_p(f(x))$ é irredutível em $\mathbb{Z}_p[x]$ então $f(x)$ é irredutível em $\mathbb{Z}[x]$. Usaremos a contrapositiva. Se $f(x)$ é redutível em $\mathbb{Z}[x]$ então $f(x) = g(x)h(x)$ com $g(x), h(x)$ polinômios não constantes em $\mathbb{Z}[x]$ de graus menores do que n, digamos r e s, respectivamente. Se b_r e c_s são os coeficientes líderes de $g(x)$ e $h(x)$, respectivamente, então $a_n = b_rc_s$. Como $p \nmid a_n$, então, $p \nmid b_r$ e $p \nmid c_s$. Assim, $\overline{b}_r$ e $\overline{c_s}$ são não nulos em $\mathbb{Z}_p$. Então, deg $\varphi_p(g(x)) =$ deg $g(x)$ e deg $\varphi_p(h(x)) =$ deg $h(x)$. Como $\varphi_p(f(x)) = \varphi_p(g(x))\varphi_p(h(x))$ segue que $\varphi_p(f(x))$ é redutível em $\mathbb{Z}_p[x]$. Temos demonstrado o seguinte resultado:

Teorema 5.2. *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio não constante e seja p um primo que não divida o coeficiente líder de $f(x)$. Se $\varphi_p(f(x))$ é irredutível em $\mathbb{Z}_p[x]$ então $f(x)$ é irredutível em $\mathbb{Q}[x]$.*
□

Exemplo 5.2. Vamos mostrar que $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$ é irredutível em $\mathbb{Q}[x]$. Para $p = 2$ temos $\varphi_2(f(x)) = x^5 + x^2 + 1$.

$\varphi_p(f(x))$ não admite fatores lineares em $\mathbb{Z}_2[x]$, pois não possui raízes em $\mathbb{Z}_2$ (verifique isto). Os únicos polinômios de grau dois em $\mathbb{Z}_2[x]$ são x^2, x^2+x, x^2+1 e x^2+x+1 e nenhum destes divide $\varphi_p(f(x))$ (use o algoritmo da divisão para verificar isto!). Assim, $f(x)$ também não admite fatores quadráticos em $\mathbb{Z}_2[x]$. Finalmente, $\varphi_p(f(x))$ também não admite fatores de grau 3 e 4 pois se tivesse o outro fator seria de grau 2 ou 1, que é impossível. Logo, $\varphi_p(f(x))$ é irredutível em $\mathbb{Z}_2[x]$. Pelo teorema 5.2 $f(x)$ é irredutível em $\mathbb{Q}[x]$.

5.4 Critério $f(x+c)$

Seja $f(x) \in k[x]$ e $c \in k$. A aplicação $\Psi : k[x] \to k[x]$, $\Psi(f(x)) = f(x+c)$, define um isomorfismo. Assim, $f(x)$ é irredutível em $k[x]$ se e somente se $\Psi(f(x)) = f(x+c)$ é irredutível em $k[x]$. Em forma de teorema:

Teorema 5.3. *Seja $f(x) \in k[x]$, k corpo, e $c \in k$. Se $f(x+c)$ é irredutível em $k[x]$ se e somente se $f(x)$ é irredutível em $k[x]$.* $\square$

Tal critério aparentemente não traz nehuma luz à caracterização da irredutibilidade de um polinômio. Mas, ele aplicado em conjunto com outros critérios pode ser bastante útil. Por exemplo, considere $f(x) = x^4+4x+1 \in \mathbb{Q}[x]$. Temos $f(x+1) = (x+1)^4+4(x+1)+1 = x^4+4x^3+6x^2+8x+6$ irredutível pelo critério de Eisenstein para $p = 2$. Logo, x^4+4x+1 é irredutível em $\mathbb{Q}[x]$. Prezado aluno, você pode fazer o teste de irredutibilidade tentando fatorar tal polinômio como foi feito na introdução à esta aula e verificar qual dos dois métodos é o mais trabalhoso. Outro exemplo segue na seção a seguir.

5.5 O polinômio ciclotômico $\Phi_p(x)$, p primo

Em matemática, a palavra *ciclotomia* remonta ao problema histórico de dividir o círculo em um dado número de partes iguais ou, equivalentemente, de construir polígonos regulares com régua e compasso. É conhecido que um polígono regular de n lados é construtível (isto significa com régua e compasso) se e somente se $\phi(n)$ é uma potência de 2. Lembramos que $\phi(n)$ denota a função phi de Euler em $n \in \mathbb{Z}_{\geq 0}$ e corresponde à quantidade de inteiros positivos $< n$ relativamente primo com n. Na teoria de grupos, $\phi(n)$ é a ordem do grupo multiplicativo das unidades de $\mathbb{Z}_n$. Pode-se mostrar que $\phi(n)$ é uma potência de 2 se e somente se $n = 2^r p_1 \cdots p_k$ com $p_i = 2^{2^{q_i}} + 1$ primo para todo $i = 1, \ldots, r$. Os primos da forma $2^{2^{q_i}} + 1$ são chamados primos de Fermat (1601-1665). Fermat conjecturou que todos os números da forma $2^{2^q} + 1$ são primos. De fato, $2^{2^q} + 1$ é primo para $q < 5$, mas Euler (1707-1783) mostrou em 1732 que $2^{2^5} + 1 = 641 \times 6.700.417$. Na literatura corrente consta que até o momento não se conhece nenhum primo de Fermat para q acima de 4.

A relação da ciclotomia com nossa aula consiste no fato que dividir o círculo em n arcos iguais é equivalente à construção com régua e compasso da n-ésima raiz complexa da unidade. Um número complexo $\zeta = a + bi$ é dito construtível se o ponto do plano complexo (a, b) é construtível com régua e compasso. Sabe-se que um complexo ζ é construtível somente se o corpo $\mathbb{Q}[\zeta]$ possui como dimensão vetorial sobre $\mathbb{Q}$ uma potência de 2. A dimensão vetorial de $\mathbb{Q}[\zeta]$ sobre $\mathbb{Q}$ é chamada *grau* pelo fato de coincidir com o grau do polinômio mônico irredutível sobre $\mathbb{Q}$ tendo ζ como raiz. Denota-se por $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ o grau de $\mathbb{Q}[\zeta]$ sobre $\mathbb{Q}$. Se $\zeta = \exp^{\frac{2\pi i}{n}}$ é uma n-ésima raiz complexa da unidade então $[\mathbb{Q}[\zeta] : \mathbb{Q}] = \phi(n)$.

A prova deste resultado é não trivial e precisa antes de mais nada determinar o polinômio mínimo de ζ. Tal polinômio é chamado o n-ésimo polinômio ciclotômico e denotado por $\Phi_n(x)$.
Se $\zeta = \exp^{\frac{2\pi i}{n}}$ é uma n-ésima raiz da unidade então $\zeta^n = \exp^{2\pi i} = 1$ donde ζ é raiz do polinômio $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots x + 1)$. Se $\zeta \neq 1$ então ζ é raiz do polinômio $x^{n-1} + x^{n-2} + \cdots x + 1$. Quando $n = p$ é primo, $q(x) = x^{p-1} + x^{p-2} + \cdots x + 1$ é irredutível sobre $\mathbb{Q}$ e portanto é o p-ésimo polinômio ciclotômico $\Phi_p(x)$. De fato, $\dfrac{x^p - 1}{x - 1} = q(x)$. Assim,

$$
\begin{aligned}
q(x+1) &= \frac{(x+1)^p - 1}{x + 1 - 1} \\
&= \frac{x^p + \begin{pmatrix} p \\ p-1 \end{pmatrix} x^{p-1} + \cdots + \begin{pmatrix} p \\ 1 \end{pmatrix} x + 1 - 1}{x} \\
&= \frac{x^p + \begin{pmatrix} p \\ p-1 \end{pmatrix} x^{p-1} + \cdots + \begin{pmatrix} p \\ 1 \end{pmatrix} x}{x} \\
&= x^{p-1} + \begin{pmatrix} p \\ p-1 \end{pmatrix} x^{p-2} + \cdots + \begin{pmatrix} p \\ 1 \end{pmatrix}
\end{aligned}
$$

Como p divide $\begin{pmatrix} p \\ r \end{pmatrix}$ para todo r, $0 < r < p$, segue pelo critério de Eisenstein que $q(x) = x^{p-1} + x^{p-2} + \cdots x + 1$ é irredutível.

5.6 Conclusão

Embora não exista um método geral para determinar irredutibilidade em $\mathbb{Q}[x]$, conseguimos, por meio dos critérios elaborados nesta aula, caracterizar a irredutibilidade de certos tipos de polinômios. O principal critério é o de Eisenstein. Eles são de extrema utilidade tanto na teoria dos corpos quanto na teoria de Galois.

RESUMO

Critério de Eisenstein

Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ não constante. Se existe um primo $p \in \mathbb{Z}$ tal que $p|a_0, \ldots, p|a_{n-1}$, $p \nmid a_n$ e $p^2 \nmid a_0$ então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Critério $\mathbb{Z}_p[x]$

Seja $f(x) \in \mathbb{Z}[x]$ um polinômio não constante e seja p um primo que não divida o coeficiente líder de $f(x)$. Se $\phi_p(f(x))$ é irredutível em $\mathbb{Z}_p[x]$ então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Critério $f(x+c)$

Seja $f(x) \in k[x]$, k corpo, e $c \in k$. Se $f(x+c)$ é irredutível em $k[x]$ então $f(x)$ é irredtível em $k[x]$.

O polinômio ciclotômico $\Phi_p(x)$, p primo

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

PRÓXIMA AULA

Na próxima aula iniciaremos a segunda fase do curso. Será uma aula de transição entre o estudo de polinômios e a teoria de corpos. Estudaremos os anéis quocientes obtidos por meio de ideais em $k[x]$. É muito importante que você ganhe maturidade na estrutura de tais anéis, pois será a teoria que dará suporte à toda teoria dos corpos vista neste curso.

ATIVIDADES

ATIV. 5.1. Mostre que os seguintes polinômios $f(x) \in \mathbb{Z}[x]$ são irredutíveis sobre $\mathbb{Q}[x]$.

a) $f(x) = x^4 + 2x^3 + 2x^2 + 2x + 2$.

b) $f(x) = x^7 - 31$.

c) $f(x) = x^6 + 15$.

d) $f(x) = x^3 + 6x^2 + 5x + 25$.

e) $f(x) = x^4 + 8x^3 + x^2 + 2x + 5$.

f) $f(x) = x^4 + 10x^3 + 20x^2 + 30x + 22$.

ATIV. 5.2. Determine quais dos seguintes polinômios são irredutíveis sobre $\mathbb{Q}$.

a) $x^3 - x + 1$ *b)* $x^3 + 2x + 10$

c) $x^3 - 2x^2 + x + 15$ *d)* $x^4 + 2$

e) $x^4 - 2$ *f)* $x^4 - x + 1$

ATIV. 5.3. Determine quais dos seguintes polinômios sobre os seguintes corpos K são irredutíveis:

a) $x^7 + 22x^3 + 11x^2 - 44x + 33$, $K = \mathbb{Q}$

b) $x^3 - 7x^2 + 3x + 3$, $K = \mathbb{Q}$

c) $x^4 - 5$, $K = \mathbb{Z}_{17}$

d) $x^3 - 5$, $K = \mathbb{Z}_{11}$

LEITURA COMPLEMENTAR

CLARK, Allan, Elements of abstract algebra. Dover, 1984

GONÇALVES, Adilson, Introdução à álgebra, IMPA, Projeto Euclides, 5.ed., Rio de Janeiro, 2008.

HUNGERFORD, Thomas W., Abstract algebra: an introduction, Saunders College Publishing, 1990.