critérios de irredutibilidade

Buscamos por critérios para decidir quando um polinômio em $\mathbb{Q}[x]$ é irredutível. Nosso ponto de partida é:

Teorema 1.1 (Lema de Gauss)**.** *Um polinômio em $\mathbb{Z}[x]$ de grau ≥ 1 é irredutível em $\mathbb{Z}[x]$ se e somente se é primitivo e é irredutível em $\mathbb{Q}[x]$.*

Para aplicações é mais útil a versão seguinte, que você deve mostrar como um exercício.

Corolário 1.2. *Seja $f \in \mathbb{Z}[x]$ de grau ≥ 1. Se não é possível decompor f como um produto de polinômios ambos de grau ≥ 1 em $\mathbb{Z}[x]$, então f é irredutível em $\mathbb{Q}[x]$.*

Existem maneiras indiretas para produzir polinômios irredutíveis sobre os inteiros. Estudaremos aqui duas delas: redução módulo um primo p e o critério de Eisenstein.

redução módulo p

Seja p um primo fixado. Dado um polinômio $f = a_r x^r + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, seja $\overline{f} := \overline{a}_r x^r + \cdots + \overline{a}_1 x + \overline{a}_0 \in \mathbb{Z}_p[x]$ o polinômio cujos coeficientes são dados pelas classes residuais dos coeficientes de f. Temos então uma função $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ dada por $\varphi(f) = \overline{f}$ que satisfaz as seguintes propriedades:

- $\varphi(1) = \overline{1}$
- $\varphi(f+g) = \overline{f+g} = \overline{f} + \overline{g} = \varphi(f+g)$
- $\varphi(f \cdot g) = \overline{f \cdot g} = \overline{f} \cdot \overline{g} = \varphi(f \cdot g)$

(verifique como exercício). Em outras palavras, φ é um homomorfismo de anéis.

Suponha que $f = gh$ em $\mathbb{Z}[x]$. Então $\overline{f} = \overline{g}\overline{h}$ em $\mathbb{Z}_p[x]$, o que sugere o seguinte critério:

"*Se $\overline{f}$ é irredutível em $\mathbb{Z}_p[x]$, então f é irredutível em $\mathbb{Z}[x]$.*"

Isso seria útil, pois é mais simples testar se polinômios são irredutíveis módulo p: $\mathbb{Z}_p$ é um corpo, e é finito. Parece uma boa idéia. Glup.

Exemplo 1.3. Seja $f = 3x^2 + x$. Então $f = x(3x+1)$ é redutível em $\mathbb{Z}[x]$; porém, para $p = 3$, temos $\overline{f} = x \cdot \overline{1}$, que é irredutível em $\mathbb{Z}_3[x]$.

No exemplo, o problema é que um dos fatores se tornou *invertível* em $\mathbb{Z}_p[x]$. A boa notícia é que esse método funciona desde que a redução módulo p não diminua o grau do polinômio.

Proposição 1.4. *Seja $f \in \mathbb{Z}[x]$ um polinômio de grau $n \geq 1$. Seja p um número primo tal que $\overline{f}$ também tenha grau n em $\mathbb{Z}_p[x]$. Se $\overline{f}$ é irredutível em $\mathbb{Z}_p[x]$, então f não se escreve como produto de polinômios de grau ≥ 1 em $\mathbb{Z}[x]$. Em particular, f é irredutível em $\mathbb{Q}[x]$.*

Demonstração. Assuma, por contradição, que $f = gh$ com $g, h \in \mathbb{Z}[x]$ ambos não constantes. Escreva

$$f = a_n x^n + \cdots + a_0, \qquad g = b_r x^r + \cdots + b_0, \qquad h = c_s x^s + \cdots + c_0$$

com $a_n \neq 0$, $b_r \neq 0$, $c_s \neq 0$, $r \geq 1$, $s \geq 1$ e $r + s = n$. Por hipótese, $\overline{a}_n \neq \overline{0}$ em $\mathbb{Z}_p$; como $\overline{a}_n = \overline{b}_r \cdot \overline{c}_s$ e $\mathbb{Z}_p$ é um domínio, temos que $\overline{b}_r \neq \overline{0}$ e $\overline{c}_s \neq \overline{0}$ e logo tanto $\overline{g}$ como $\overline{h}$ tem grau ≥ 1. Como $\overline{f} = \overline{g} \cdot \overline{h}$, temos uma contradição com a hipótese da irredutibilidade de $\overline{f}$. □

Para aplicar este critério, devemos encontrar um primo para o qual seja fácil decidir a irredutibilidade. Na prática isso é raro, mas não impossível.

Exemplo 1.5.

(1) Seja $f = x^2 - 1892 \in \mathbb{Z}[x]$. Para $p = 2$, temos $\overline{f} = x^2$ que é redutível em $\mathbb{Z}_2[x]$ e logo o critério da Proposição 1.4 não nos fornece nenhuma informação; por outro lado, para $p = 3$, temos $\overline{f} = x^2 - \overline{2}$ que é irredutível em $\mathbb{Z}_3[x]$ pois este é um polinômio de grau 2 que não possui raízes em $\mathbb{Z}_3$, como você pode facilmente verificar. Assim, f não se escreve como produto de polinômios não constantes em $\mathbb{Z}[x]$ e, sendo f primitivo, concluímos que f é irredutível em $\mathbb{Z}[x]$.

(2) Considere $f = 8x^3 + 50x^2 + 512x + 1529$. A Proposição 1.4 não se aplica diretamente para $p = 2$. Para $p = 3$, temos $\overline{f} = \overline{2}x^3 + \overline{2}x^2 + \overline{2}x + \overline{2}$ que possui uma raiz em $\mathbb{Z}_3$. Logo $\overline{f}$ é redutível em $\mathbb{Z}_3[x]$ e nada podemos concluir a partir da Proposição 1.4.

Para $p = 5$, temos $\overline{f} = \overline{3}x^3 + \overline{2}x - \overline{1}$. Este é um polinômio de grau 3 que não possui raízes em $\mathbb{Z}_5$ (verifique!) e logo é irredutível em $\mathbb{Z}_5[x]$. Sendo primitivo, segue da Proposição 1.4 que f é irredutível em $\mathbb{Z}[x]$ (e logo em $\mathbb{Q}[x]$, pelo Lema de Gauss).

(3) Há casos extremos em que o critério *nunca* funciona! Exemplos não são lá fáceis de se encontrar. Eis um deles: tome $f = x^4 - 10x^2 + 1$. Então:
   (a) f é irredutível em $\mathbb{Z}[x]$.
   (b) $\overline{f}$ é *redutível* em $\mathbb{Z}_p[x]$ para todo primo p.

Para provar o item (a), observe que f não possui raízes em $\mathbb{Q}$ e em seguida mostre que não é possível fatorar f como produto de dois polinômios de grau 2. Já o item (b) requer outras idéias...

O CRITÉRIO DE EISENSTEIN

Teorema 1.6 (Eisenstein)**.** *Seja* $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *um polinômio de grau* $n \geq 1$. *Se* p *é um número primo tal que*

- $p \nmid a_n$;
- $p \mid a_i$ *para* $i = 0, 1, \ldots, n-1$;
- $p^2 \nmid a_0$.

Então f *não se escreve como produto de polinômios de grau* ≥ 1 *em* $\mathbb{Z}[x]$. *Em particular,* f *é irredutível em* $\mathbb{Q}[x]$.

Demonstração. Suponha $f = gh$ com $g, h \in \mathbb{Z}[x]$, digamos

$$f = a_n x^n + \cdots + a_0, \qquad g = b_r x^r + \cdots + b_0, \qquad h = c_s x^s + \cdots + c_0$$

com b_r, c_s ambos não nulos. Como o primo p divide $a_0 = b_0 \cdot c_0$, temos que p divide b_0 ou p divide c_0 mas não ambos, pois supomos $p^2 \nmid a_0$. Trocando g e h caso necessário, podemos assumir

$$(*) \qquad p \mid b_0 \quad \text{e} \quad p \nmid c_0.$$

Agora:

- p divide $a_1 = b_0c_1 + b_1c_0$ e logo de (*) segue-se que $p \mid b_1$.
- p divide $a_2 = b_0c_2 + b_1c_1 + b_2c_0$ e como $p \mid b_1$, segue de (*) que $p \mid b_2$.
- Assim prosseguindo, concluímos que $p \mid b_i$ para cada $i = 0, 1, \ldots, n-1$.

Por hipótese p não divide $a_n = b_r c_s$ e em particular $p \nmid b_r$; logo a única possibilidade que nos resta é $r = n$. Como $n = r + s$, vem que $s = 0$, ou seja, h é constante, como queríamos mostrar. □

O critério de Eisenstein é uma máquina para produzir polinômios irredutíveis.

Exemplo 1.7.

(1) Tome $f = x^4 + 5x^3 + 10x^2 + 15x + 20$. Pelo Teorema 1.6 (aplicado com o primo $p = 5$), f não é produto de polinômios não constantes em $\mathbb{Z}[x]$. Mais uma vez, como f é primitivo, f é irredutível em $\mathbb{Z}[x]$.

(2) Seja $f = 6x^9 + 14x^2 + 28x + 14$. Não podemos aplicar o critério para $p = 2$; mas para $p = 7$ concluímos que f é irredutível em $\mathbb{Q}[x]$. Note que f é redutível em $\mathbb{Z}[x]$ (2 é um fator).

(3) No critério de Eisenstein, os papéis do termo líder e do termo constante podem ser trocados. De maneira mais geral, fica para você como exercício: *um polinômio* $a_n x^n + \cdots + a_1 x + a_0$ *é irredutível se e somente se* $a_0 x^n + \cdots + a_{n-1} x + a_n$ *é irredutível.*

(4) O polinômio $x^3 + 3x + 9$ é irredutível em $\mathbb{Z}[x]$ (tome a sua redução módulo 2) mas o critério de Eisenstein não se aplica aqui.

Apresentamos agora uma aplicação do critério de Eisenstein. Apesar de muito particular, é um resultado importante no estudo dos polinômios ciclotômicos e raízes da unidade.

Proposição 1.8. *Seja p um número primo. Então o polinômio*

$$f = x^{p-1} + x^{p-2} + \cdots + x + 1$$

é irredutível em $\mathbb{Q}[x]$.

Demonstração. Para começar, defina $g(x) = f(x + 1)$ e repare que f é irredutível se e somente se g é irredutível: basta observar que a partir de qualquer fatoração $f = f_1 f_2$ obtemos uma fatoração $g = f_1(x + 1)f_2(x + 1)$ e vice-versa, uma vez que $f(x) = g(x - 1)$.

Agora, como $f(x) = (x^p - 1)/(x - 1)$, segue-se da fórmula do binômio de Newton que

$$g(x) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}$$

e aqui nos espera uma surpresa: como p é um número primo, vale que p divide $\binom{p}{i}$ para cada $i = 1, \ldots, p-1$ (este é um bom exercício!). Segue do critério de Eisenstein que g é irredutível em $\mathbb{Z}[x]$, o que termina a demonstração. □

Vimos em uma das listas de exercícios que se n é composto, então $f = x^{n-1} + \cdots + x + 1$ é redutível em $\mathbb{Q}[x]$.

Exemplo 1.9. A irredutibilidade de um polinômio depende do ambiente onde ele é considerado. Acabamos de ver que $f = x^4 + x^3 + x^2 + x + 1$ é irredutível em $\mathbb{Q}[x]$; vimos em sala que f se fatora em $\mathbb{R}[x]$:

$$f = (x^2 - 2ax + 1)(x^2 - 2(a^2 - b^2)x + 1)$$

onde $a = \cos(2\pi/5)$ e $b = \operatorname{sen}(2\pi/5)$.