Critérios de irredutibilidade

Começamos com o seguinte resultado, visto em sala.

Proposição 1.1. *Seja* $f \in \mathbb{Z}[x]$ *um polinômio de grau* ≥ 1*. Se* f *é irredutível em* $\mathbb{Z}[x]$*, então* f *é irredutível em* $\mathbb{Q}[x]$*.*

E se você pensar um pouco, perceberá que vale uma espécie de recíproca:

Proposição 1.2. *Seja* $f \in \mathbb{Z}[x]$ *um polinômio de grau* ≥ 1*. Suponha que* f *é irredutível em* $\mathbb{Q}[x]$*. Se existem* $g, h \in \mathbb{Z}[x]$ *tais que* $f = gh$*, então* $g \in \mathbb{Z}$ *ou* $h \in \mathbb{Z}$*.*

Ou seja, pode ser que um polinômio irredutível em $\mathbb{Q}[x]$ seja redutível em $\mathbb{Z}[x]$, mas se isto ocorrer então um dos fatores necessariamente é constante.

Um polinômio $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ é dito *primitivo* se $\text{mdc}(a_n, \ldots, a_0) = 1$. Como consequência, temos

Corolário 1.3. *Se* $f \in \mathbb{Z}[x]$ *é primitivo de grau* ≥ 1*, então*

f *é irredutível em* $\mathbb{Z}[x]$ *se e somente se* f *é irredutível em* $\mathbb{Q}[x]$*.*

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

Assim, se podemos escrever $f = gh$ em $\mathbb{Z}[x]$, vale então que $\overline{f} = \overline{g}\overline{h}$ em $\mathbb{Z}_p[x]$, o que sugere o seguinte critério:

"*Se* $\overline{f}$ *é irredutível em* $\mathbb{Z}[x]$*, 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 tem somente um número finito de elementos. Parece uma boa idéia, mas infelizmente... não funciona.

Exemplo 1.4. 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 podemos contornar isso em um contexto relativamente abrangente.

Proposição 1.5. *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. Suponhamos, por contradição, que $f = gh$ com $g, h \in \mathbb{Z}[x]$ ambos não constantes. Escrevemos

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

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 consequentemente que $\overline{b}_r \neq \overline{0}$ e $\overline{c}_s \neq \overline{0}$, ou seja, $\operatorname{grau} \overline{g} = r$ e $\operatorname{grau} \overline{h} = s$. Mas decorre daí que $\overline{f} = \overline{g} \cdot \overline{h}$ é uma fatoração como produto de polinômios ambos não invertíveis, o que contradiz nossa hipótese de que $\overline{f}$ é irredutível em $\mathbb{Z}_p[x]$. Isso termina a prova. □

Na prática, para aplicar este critério, devemos ter a felicidade de encontrar um primo p para o qual seja fácil decidir a irredutibilidade, o que é raro. De qualquer forma, alguns exemplos.

Exemplo 1.6.

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 1.5 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 $f = 8x^3 + 50x^2 + 512x + 31$. Não podemos aplicar diretamente o critério da Proposição 1.5 para $p = 2$. 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 1.5 que f é irredutível em $\mathbb{Z}[x]$ (e também em $\mathbb{Q}[x]$).

3. Há casos extremos em que o critério *nunca* funciona! Exemplos não são fáceis de se encontrar, mas existem: tome $f = x^4 - 10x^2 + 1$. Pode-se mostrar que:

   - f é irredutível em $\mathbb{Z}[x]$.
   - $\overline{f}$ é *redutível* em $\mathbb{Z}_p[x]$ para todo primo p.

Um critério bem popular é o:

Teorema 1.7 (Eisenstein)**.** *Seja* $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *um polinômio de grau* $n \geq 1$*. Suponha que exista um número primo* p *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. Suponhamos, por contradição, que $f = gh$ com $g, h \in \mathbb{Z}[x]$ ambos não constantes. Escrevemos

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

com $r \geq 1$, $s \geq 1$ e $r + s = n$. 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 supor

$$p \mid b_0 \quad \text{e} \quad p \nmid c_0. \tag{*}$$

Agora:

- p divide $a_1 = b_0 c_1 + b_1 c_0$ e logo de (*) segue-se que $p \mid b_1$.
- p divide $a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$ e como $p \mid b_1$, segue de (*) que $p \mid b_2$.
- Assim prosseguindo, demonstramos que $p \mid b_i$ para cada $i = 0, 1, \ldots, r$. Como $a_n = b_r c_s$, obtemos $p \mid a_n$, contradição.

□

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

Exemplo 1.8.

1. Tome $f = x^4 + 5x^3 + 10x^2 + 15x + 20$. Pelo Teorema 1.7 (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. O polinômio $x^3 + 3x + 9$ é irredutível em $\mathbb{Z}[x]$ (considere módulo 2) mas o critério de Eisenstein não se aplica aqui.

Eis uma aplicação importante do critério de Eisenstein.

Proposição 1.9. *Seja* p *um número primo. Então o polinômio*

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

é irredutível em $\mathbb{Q}[x]$.

Demonstração. É um truque: faça a substituição $x = y + 1$. Observe que

$$f(x) \text{ é irredutível em } \mathbb{Z}[x] \iff f(y) \text{ é irredutível em } \mathbb{Z}[y]$$

(basta substituir $y = x-1$ em qualquer fatoração de $f(y)$); e como $f(x) = (x^p-1)/(x-1)$, segue-se da fórmula do binômio de Newton que

$$f(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{1}y^{p-2} + \binom{p}{2}y^{p-3} + \cdots + \binom{p}{p-2}y + \binom{p}{p-1}.$$

Agora uma grata surpresa: como p é um número primo, temos que p divide $\binom{p}{i}$ para cada $i = 1, \ldots, p-1$ (este é um bom exercício!) e logo pelo critério de Eisenstein segue-se que $f(y)$ é irredutível em $\mathbb{Z}[y]$, terminando a prova. □

Exemplo 1.10. 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 $\mathbb{Q}[x]$; porém, em sala vimos que em $\mathbb{R}[x]$ temos a fatoração

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

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