O Lema de Gauss

Nosso objetivo é comparar fatorações de polinômios em $\mathbb{Z}[x]$ e em $\mathbb{Q}[x]$. Para começar, note que há de se tomar um cuidado especial com as constantes. Por exemplo, $2 \cdot x$ é irredutível em $\mathbb{Q}[x]$ mas não é irredutível em $\mathbb{Z}[x]$, pois 2 e x são fatores irredutíveis. O ponto aqui é que toda constante não-nula em $\mathbb{Q}$ é invertível, uma vez que $\mathbb{Q}$ é um corpo. Como veremos a seguir, excetuando-se situações similares, os polinômios que são irredutíveis em $\mathbb{Z}[x]$ permanecem irredutíveis em $\mathbb{Q}[x]$.

O *conteúdo* de um polinômio $f \in \mathbb{Z}[x]$ é definido como o máximo divisor comum dos seus coeficientes. Ou seja, se $f = a_n x^n + \cdots + a_1 x + a_0$, então

$$c(f) = \text{mdc}(a_0, \ldots, a_n).$$

Por exemplo, se $f = 30x^5 + 18x^4 + 12x - 24$, então $c(f) = 6$.

Dizemos que f é *primitivo* se seu conteúdo é 1. Note que se d é o conteúdo de f, então podemos escrever $f = d \cdot \tilde{f}$, com $\tilde{f}$ primitivo. No exemplo acima: $f = 6 \cdot (5x^5 + 3x^4 + 2x - 4)$. É natural perguntar sobre o conteúdo do produto de dois polinômios. Começamos com um caso particular.

Proposição 1.1. *O produto de polinômios primitivos é um polinômio primitivo.*

Demonstração. Sejam $f = a_n x^n + \cdots + a_0$ e $g = b_m x^m + \cdots + b_0$ em $\mathbb{Z}[x]$ e seja $d = c(fg)$. Suponha que exista um primo p que divida d. Como f é primitivo, p não pode dividir todos os a_i's; tome k como o primeiro índice para o qual isso acontece, ou seja, p divide $a_0, \ldots, a_{k-1}$ mas $p \nmid a_k$. Agora, escrevemos $fg = \sum c_j x^j$, com

$$\begin{aligned}
c_0 &= a_0 b_0 \\
c_1 &= a_0 b_1 + a_1 b_0 \\
&\vdots \\
c_k &= a_0 b_k + \cdots + a_{k-1} b_0 + a_k b_0 \\
c_{k+1} &= a_0 b_{k+1} + \cdots + a_k b_1 + a_{k+1} b_0 \\
&\vdots \\
c_{n+m} &= a_n b_m.
\end{aligned}$$

Convido você a olhar para o coeficiente c_k com detalhe: temos que p divide $a_0, \ldots, a_{k-1}$ e o próprio c_k. Segue daí que p também divide a última parcela da soma, $a_k b_0$. Como $p \nmid a_k$ e p é primo, necessariamente $p \mid b_0$. O mesmo argumento, aplicado agora ao coeficiente c_{k+1}, nos diz que p divide b_1; assim prosseguindo, mostramos que p divide b_j para cada $j = 0, \ldots, m$. Temos uma contradição, já que assumimos que g também é primitivo.

Concluímos que não existe nenhum primo que divida d. Portanto fg é primitivo, como queríamos demonstrar. □

Eis um exercício: mostre que se $a \in \mathbb{Z}$ é uma constante, então $c(a \cdot f) = a \cdot c(f)$. Agora sim, o caso geral.

Corolário 1.2. *Para quaisquer* $f, g \in \mathbb{Z}[x]$*, vale* $c(fg) = c(f)c(g)$.

Demonstração. Sejam d, e os conteúdos de f e g e escreva $f = d \cdot \tilde{f}$ e $g = d \cdot \tilde{g}$, com $\tilde{f}$ e $\tilde{g}$ primitivos. Então

$$c(fg) = c(de \cdot \tilde{f}\tilde{g}) = de \cdot c(\tilde{f}\tilde{g}) = de$$

onde a última igualdade é consequência da Proposição 1.1. □

Teorema 1.3 (Lema de Gauss)**.** *Seja* $f \in \mathbb{Z}[x]$ *um polinômio de grau* ≥ 1*. Então* f *é irredutível em* $\mathbb{Z}[x]$ *se e somente se* f *é primitivo e irredutível em* $\mathbb{Q}[x]$*.*

Demonstração. Suponha f irredutível em $\mathbb{Z}[x]$. Como $\operatorname{grau} f \geq 1$, segue que f é primitivo. Sejam $g, h \in \mathbb{Q}[x]$ tais que $f = gh$. Queremos mostrar que g ou h é constante.

Escreva $g = \frac{a}{b}\tilde{g}$ com $a, b \in \mathbb{Z}$ e $\tilde{g} \in \mathbb{Z}[x]$ primitivo (tome um denominador comum para todos os coeficientes de g e depois tome o conteúdo do polinômio que aparece no numerador). Da mesma forma, escreva $h = \frac{c}{d}\tilde{h}$ com $c, d \in \mathbb{Z}$ e $\tilde{h} \in \mathbb{Z}[x]$ primitivo. Temos então uma igualdade de polinômios em $\mathbb{Z}[x]$:

$$bd \cdot f = ac \cdot \tilde{g}\tilde{h}$$

e tomando o conteúdo dos dois lados, obtemos pela Proposição 1.1 que $bd = ac$. Logo $f = \tilde{g}\tilde{h}$. Como f é irredutível em $\mathbb{Z}[x]$, vem que $\tilde{g}$ ou $\tilde{h}$ é invertível em $\mathbb{Z}[x]$ e em particular uma constante, como queríamos mostrar.

Reciprocamente, suponha $f = gh$ com $g, h \in \mathbb{Z}[x]$. Se f é irredutível em $\mathbb{Q}[x]$, então g ou h deve ser uma constante; e se, adicionalmente, f é primitivo, então essa constante deve ser invertível. Logo f é irredutível em $\mathbb{Z}[x]$. □

A Proposição 1.1 é às vezes ela mesma chamada de Lema de Gauss. Isso se justifica: ela é o ponto crucial da prova do Teorema 1.3.

Para terminar, o que fizemos aqui se generaliza para qualquer domínio de fatoração única, com essencialmente a mesma demonstração. O enunciado do resultado geral fica assim:

Teorema 1.4 (Lema de Gauss)**.** *Sejam* D *um domínio fatorial e* K *seu corpo de frações. Seja* $f \in D[x]$ *um polinômio de grau* ≥ 1*. Então* f *é irredutível em* $D[x]$ *se e somente se* f *é primitivo e irredutível em* $K[x]$*.*