1 O menor divide!

O protótipo dos argumentos de "menor divide" é ilustrado pelo seguinte

Exercício 1.1 Determine todos os subconjuntos $I \subset \mathbb{Z}$ que satisfazem as duas propriedades a seguir:
(i) I é fechado por soma: $a, b \in I \Rightarrow a + b \in I$;
(ii) Se $a \in I$ e $m \in \mathbb{Z}$ então $ma \in I$.
Um conjunto I satisfazendo (i) e (ii) acima é chamado de **ideal**.

A solução é a seguinte. Primeiro note que $I = \{0\}$ é uma resposta possível. Agora suponha que $I \neq \{0\}$, então existe um número positivo em I já que se $a \in I$ então $-a \in I$ por (ii). Seja $d \in I$ o **menor** número positivo em I. Denote por

$$(d) \stackrel{\text{df}}{=} \{md \mid m \in \mathbb{Z}\} \qquad \text{(conjunto dos múltiplos de } d\text{)}$$

Vamos mostrar que $I = (d)$. De fato, por (ii) temos que $(d) \subset I$; por outro lado, se $a \in I$, dividindo a por d podemos escrever $a = dq + r$ com $q, r \in \mathbb{Z}$ e $0 \leq r < d$. Como $r = a + (-q) \cdot d \in I$ por (i) e (ii) e $r < d$ temos, pela definição de d, que r só pode ser 0, e que portanto a é um múltiplo de d, isto é, $I \subset (d)$.

Resumindo: um ideal I de $\mathbb{Z}$ é da forma (d) para algum $d \in \mathbb{Z}$. Ideais da forma (d), "gerados" por um único elemento d, são chamados **ideais principais**.

Eis aqui uma aplicação: **o teorema de Bézout**. Sejam a e b dois inteiros, e considere o subconjunto de $\mathbb{Z}$ dado por

$$(a, b) \stackrel{\text{df}}{=} \{ax + by \mid x, y \in \mathbb{Z}\}$$

É claro que (a, b) é um ideal, e pelo exercício, existe um inteiro d tal que $(d) = (a, b)$. Mas afinal, quem é esse d? Primeiramente, como $a, b \in (d)$ temos que $d \mid a$ e $d \mid b$. Por outro lado, se $d' \mid a$ e $d' \mid b$ temos que $d' | ax + by$ para qualquer elemento $ax + by \in (a, b)$; em particular, $d' \mid d$. Portanto d só pode ser o mdc de a e b, e como $d \in (a, b)$, temos que $d = ax + by$ para algum $x, y \in \mathbb{Z}$.

Os exercícios seguintes são análogos ao anterior:

Exercício 1.2 Seja $\mathbb{Q}[x]$ o conjunto dos polinômios em x com coeficientes em $\mathbb{Q}$. Seja I um ideal de $\mathbb{Q}[x]$, isto é, $I \subset \mathbb{Q}[x]$ é um subconjunto satisfazendo
(i) I é fechado por soma: $a(x), b(x) \in I \Rightarrow a(x) + b(x) \in I$;
(ii) Se $a(x) \in I$ e $r(x) \in \mathbb{Q}[x]$ então $r(x) \cdot a(x) \in I$.
Mostre que existe $d(x) \in \mathbb{Q}[x]$ tal que

$$I = \big(d(x)\big) \stackrel{\text{df}}{=} \{m(x) \cdot d(x) \mid m(x) \in \mathbb{Q}[x]\} \qquad \text{(conjunto dos múltiplos de } d(x)\text{)}$$

Em outras palavras, todo ideal de $\mathbb{Q}[x]$ é principal. Mostre que entretanto existe um ideal J de $\mathbb{Z}[x]$ que não é principal.

Exercício 1.3 Seja $\omega \in \mathbb{C}$ tal que $\omega^2 + \omega + 1 = 0$ (isto é, ω é uma raiz cúbica primitiva da unidade). Sejam

$$\mathbb{Z}[i] \stackrel{\text{df}}{=} \{a + bi \mid a, b \in \mathbb{Z}\} \qquad \text{(inteiros de Gauß)}$$
$$\mathbb{Z}[\omega] \stackrel{\text{df}}{=} \{a + b\omega \mid a, b \in \mathbb{Z}\} \qquad \text{(inteiros de Eisenstein)}$$

(a) Mostre que para todo $\alpha, \beta \in \mathbb{Z}[i]$ com $\beta \neq 0$ existem $q, r \in \mathbb{Z}[i]$ tais que

$$\alpha = \beta q + r, \qquad 0 \leq N(r) < N(\beta)$$

onde $N(\beta) \stackrel{\text{df}}{=} \beta \cdot \bar{\beta} = |\beta|^2$.

(b) Mostre o resultado do item anterior para $\alpha, \beta \in \mathbb{Z}[\omega]$, mas agora com $N(a + b\omega) \stackrel{\text{df}}{=} (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2$, $a, b \in \mathbb{Z}$.

(c) Mostre que ideais em $\mathbb{Z}[i]$ e $\mathbb{Z}[\omega]$ são todos principais.

Como no caso dos inteiros, temos

Teorema 1.1 (Bézout) *Sejam $a_1(x), a_2(x), \ldots, a_n(x) \in \mathbb{Q}[x]$, e seja $d(x)$ o mdc destes polinômios, i.e., $d(x)$ é o polinômio mônico (= coeficiente líder 1) de maior grau que simultaneamente divide todos os $a_i(x)$. Então existem $b_1(x), \ldots, b_n(x) \in \mathbb{Q}[x]$ tais que*

$$a_1(x) \cdot b_1(x) + \cdots + a_n(x) \cdot b_n(x) = d(x)$$

Um resultado análogo vale para inteiros de Gauß e Eisenstein, e deixamos para você enunciá-lo.

2 Polinômio minimal

Aqui damos a aplicação mais importante do exercício 1.2. Precisamos de uma definição:

Definição 2.1 Seja $\alpha \in \mathbb{C}$ um **número algébrico**, isto é raiz de algum polinômio não nulo com coeficientes *racionais*. O polinômio mônico não nulo de menor grau do qual α é raiz é chamado de **polinômio minimal**.

Observação 2.2 A despeito de boatos espalhados pelo Shine, o polinômio minimal não é um polinômio pequeno e malvado.

Por exemplo, se $\alpha = (1+\sqrt{5})/2$ então o polinômio minimal de α é $x^2 - x - 1 = 0$, pois α, sendo irracional, não é raiz de nenhum polinômio de grau 1 em $\mathbb{Q}[x]$.

Teorema 2.3 *Seja $\alpha \in \mathbb{C}$ um número algébrico e $d(x)$ o seu polinômio minimal. Se α é raiz de um polinômio $p(x) \in \mathbb{Q}[x]$, então $d(x) \mid p(x)$.*

Prova A demonstração é quase tautológica (mas não patalógica!). O subconjunto de $\mathbb{Q}[x]$

$$I \stackrel{\text{df}}{=} \{p(x) \in \mathbb{Q}[x] \mid p(\alpha) = 0\} \qquad \text{(conjunto dos polinômios que se anulam em } \alpha)$$

é um ideal de $\mathbb{Q}[x]$. Portanto ele é principal, gerado pelo polinômio mônico não nulo de menor grau $d(x)$ em I, que por definição é o polinômio minimal de α! □

Exercício 2.1 Seja $f(x) \in \mathbb{Q}[x]$. Mostre que se $\cos(2\pi/5)$ é raiz de $f(x)$ então $\cos(4\pi/5)$ também é uma raiz de $f(x)$.

O exercício anterior ilustra um princípio geral: se uma relação racional vale para um número algébrico α, então a mesma relação vale para qualquer outra raiz do polinômio minimal de α. Esta é uma generalização do fato bem conhecido de que se $a + b\sqrt{c}$, com $a, b, c \in \mathbb{Q}$ e $c \neq 0$, é raiz de um polinômio com coeficientes racionais então $a - b\sqrt{c}$ também é raiz (ou do fato de que se α é uma raiz de um polinômio com coeficientes reais então o conjugado $\bar{\alpha}$ também é raiz).

Definição 2.4 Um polinômio $p(x) \in \mathbb{Q}[x]$ é **irredutível** se ele não pode ser escrito como produto de dois polinômios não constantes em $\mathbb{Q}[x]$. Segue que um polinômio irredutível é o polinômio minimal de qualquer de suas raízes.

Exercício 2.2 Seja $p(x)$ um polinômio irredutível em $\mathbb{Q}[x]$ de grau maior do que 1. Prove que se $p(x)$ admite duas raízes r e s cujo produto é 1 então o grau de $p(x)$ é par.

Exercício 2.3 Sejam $p(x), q(x) \in \mathbb{Q}[x]$ polinômios mônicos irredutíveis e sejam a e b tais que $p(a) = q(b) = 0$ e $a + b \in \mathbb{Q}$. Prove que o polinômio $p(x)^2 - q(x)^2$ possui uma raiz racional.

Exercício 2.4 Seja $p(x)$ um polinômio irredutível em $\mathbb{Q}[x]$ de grau ímpar. Sejam $q(x), r(x) \in \mathbb{Q}[x]$ tais que $p(x)$ divide $q(x)^2 + q(x) \cdot r(x) + r(x)^2$. Prove que na verdade $p(x)^2$ divide $q(x)^2 + q(x) \cdot r(x) + r(x)^2$.

Exercício 2.5 Seja $f(x)$ um polinômio de coeficientes racionais e α tal que $\alpha^3 - 21\alpha = (f(\alpha))^3 - 21 f(\alpha) = 7$; por exemplo, podemos tomar $f(x) = (x^2 - 2x - 14)/3$ (verifique!). Prove que, para todo $n \geq 1$,

$$\left(f^{(n)}(\alpha)\right)^3 - 21 \cdot f^{(n)}(\alpha) = 7,$$

onde $f^{(n)}(\alpha) = \underbrace{f(f(\ldots f}_{n \text{ vezes}}(\alpha)))$.

Exercício 2.6 Seja $p(x) \in \mathbb{Z}[x]$ um polinômio mônico irredutível tal que $|p(0)|$ não é um quadrado perfeito. Mostre que $p(x^2)$ também é irredutível em $\mathbb{Z}[x]$.

Embora fora do paradigma "menor divide", já que estamos tratando do assunto, vamos só relembrar dois resultados importantes sobre irredutibilidade de polinômios:

Teorema 2.5 (Lema de Gauß) *Um polinômio mônico $p(x) \in \mathbb{Z}[x]$ é irredutível em $\mathbb{Z}[x]$ se e somente se ele é irredutível sobre $\mathbb{Q}[x]$.*

Teorema 2.6 *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio mônico e suponha que exista um primo p para o qual $f(x)$ é irredutível em $\mathbb{Z}/p\mathbb{Z}[x]$, i.e., não existem dois polinômios mônicos $g(x), h(x) \in \mathbb{Z}[x]$ tais que $f(x) \equiv g(x)h(x) \pmod{p}$. Então $f(x)$ é irredutível em $\mathbb{Z}[x]$.*

Exercício 2.7 Prove que $f(x) = x^n + 5x^{n-1} + 3$ é irredutível em $\mathbb{Z}[x]$ para todo $n > 1$.

Exercício 2.8 Seja p um primo. Prove que $x^{p-1} + x^{p-2} + \cdots + 1 = 0$ é irredutível em $\mathbb{Q}[x]$.

3 Ordem

Uma outra aplicação do princípio do "menor divide" é bem conhecida:

Definição 3.1 Sejam a e n inteiros primos entre si. A **ordem** de a módulo n é o menor inteiro positivo d tal que

$$a^d \equiv 1 \pmod{n}$$

Teorema 3.2 *Sejam a e n inteiros primos entre si e seja k tal que $a^k \equiv 1 \pmod{n}$. Então $d \mid k$. Em particular, $d \mid \phi(n)$.*

PROVA O conjunto dos inteiros k tais que $a^k \equiv 1 \pmod{n}$ forma um ideal. □

Exercício 3.1 Seja a e n dois inteiros positivos primos entre si. Mostre que $n \mid \phi(a^n - 1)$.

Exercício 3.2 Mostre que se n é um inteiro maior do que 1, então n não divide $2^n - 1$.

Exercício 3.3 Determine todos os inteiros $n \geq 1$ tais que $(2^n + 1)/n^2$ seja inteiro.

Exercício 3.4 Existe um inteiro positivo n com exatamente 2000 fatores primos distintos tal que $n \mid 2^n + 1$?

Exercício 3.5 Determine todos os pares (n, p) de inteiros estritamente positivos tais que
p é primo,
$n \leq 2p$, e
$(p-1)^n + 1$ é divisível por n^{p-1}.

4 Polinômio minimal, de novo!

Como última aplicação do princípio do "menor divide", vamos considerar o polinômio minimal de uma matriz A em $M_m(\mathbb{Q})$, o conjunto das matrizes quadradas $m \times m$ e entradas em $\mathbb{Q}$. Se $p(x) = a_n x^n + \cdots + a_1 x + a_0$ é um polinômio com coeficientes racionais, então definimos $p(A)$ como sendo a matriz em $M_m(\mathbb{Q})$ dada por

$$p(A) \stackrel{\text{df}}{=} a_n \cdot A^n + \cdots + a_1 \cdot A + a_0 \cdot I$$

onde I denota a matriz identidade $m \times m$.

Dizemos que A satisfaz $p(x)$ se $p(A) = 0$ é a matriz nula. Dada uma matriz A como acima sempre existe um polinômio não nulo $p(x) \in \mathbb{Q}[x]$ tal que $p(A) = 0$; escrevermos $p(x) = a_{n^2} x^{n^2} + \cdots + a_0$, onde a_i são variáveis, e olharmos para o sistema dado por $p(A) = 0$, que é homogêneo e composto por n^2 equações. Como temos $n^2 + 1$ variáveis a_i, é claro que há uma solução com $a_i \in \mathbb{Q}$ e pelo menos uma variável não nula.

Definição 4.1 Seja $A \in M_m(\mathbb{Q})$. O polinômio mônico $p(x) \in \mathbb{Q}[x]$ não nulo de menor grau que A satisfaz é chamado **polinômio minimal** de A.

Pelos comentários acima, temos que o grau do polinômio minimal de A é menor ou igual a n^2. Na verdade pode-se provar que ele não excede n (o teorema de Cayley-Hamilton diz que A satisfaz $p(x) \stackrel{\text{df}}{=} \det(xI - A)$, que é chamado **polinômio característico** de A). Mas em todo caso temos

Teorema 4.2 *Seja $A \in M_m(\mathbb{Q})$ e $p(x) \in \mathbb{Q}[x]$ o seu polinômio minimal. Se $f(x) \in \mathbb{Q}[x]$ é tal que $f(A) = 0$ então $p(x) \mid f(x)$.*

Exercício 4.1 Prove o teorema de Cayley-Hamilton para matrizes em $M_2(\mathbb{Q})$.

Exercício 4.2 Seja $p \geq 5$ um primo. Determine todas as matrizes $A \in M_2(\mathbb{Q})$ tais que $A^p = I$.

Exercício 4.3 Determine os possíveis valores para o determinante de uma matriz $A \in M_2(\mathbb{C})$ tal que $A^3 - A^2 - 3A + 2I = 0$.