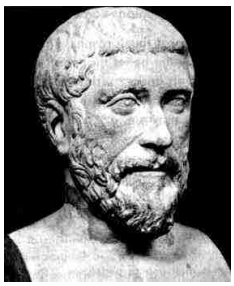
Somas de Quadrados

Angelo Papa Neto - IFCE

papaneto@gmail.com

Sumário

1 Introdução



Pitágoras (585 a.C. - 501a.C.)

O Teorema de Pitágoras afirma que os lados de um triângulo retângulo guardam entre si uma relação notável, a saber, se sobre o lado maior contruirmos um quadrado, ele terá área igual à soma das áreas dos quadrados construídos sobre os dois outros lados do triângulo. Mais do que isso, vale a recíproca, isto é, um triângulo onde vale essa propriedade é, necessariamente, retângulo.

Devemos notar dois fatos importantes sobre o Teorema de Pitágoras. Primeiramente, esse era um resultado conhecido, e utilizado, primeiro na Babilônia, depois no Egito, bem antes do florecimento da escola pitagórica,

na Grécia. Esse conhecimento prévio do resultado era, no entanto, empírico. Mais precisamente, egípcios e mesopotâmios conheciam exemplos de triângulos retângulos com lados inteiros e usavam esses triângulos como "esquadro" para levantar paredes. Talvez o mais utilizado desses triângulos tenha sido aquele que tem lados 3, 4 e 5 ($3^2 + 4^2 = 5^2$). O trio de números inteiros $(3, 4, 5)$ é chamado *trio pitagórico*.

Os egípcios usavam uma corda com 12 nós, como na figura abaixo, que quando esticada da forma correta fornecia um ângulo reto.

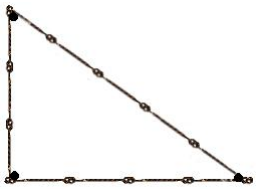


Figura 1: Corda com nós.

Esse fato, mesmo isolado do resultado geral de Pitágoras, é notável, pois **nos permite fazer uma observação geométrica sobre um triângulo a partir de uma propriedade aritmética dos seus lados**. Ele pode ser colocado no ponto inicial de um fluxo de idéias que culminaria com a Geometria Analítica e o Cálculo. Vale observar que o chinês Tschou-Gun também conhecia o triângulo retângulo de lados $3, 4, 5$, cerca de 1100 a.C..

Há indícios[1] de que uma fórmula para se determinar trios pitagóricos já era conhecida na Mesopotâmia, há mais de 3500 anos. Uma fórmula que gera trios pitagóricos (a, b, c) é

$$a = m^2 - n^2, \;\; b = 2mn, \;\; c = m^2 + n^2,$$

com m e n inteiros e $n < m$. É fácil verificar que $a^2 + b^2 = c^2$. Note que a hipotenusa c de um triângulo com lados inteiros é, neste caso, uma soma de dois quadrados de números inteiros $(c = m^2 + n^2)$.

Avançando aproximadamente 2000 anos no tempo, da época de Pitágoras até o século XVII, nos deparamos com outro fato importante sobre o Teorema de Pitágoras: a introdução de coordenadas no plano, ou no espaço, feita por Fermat e Descartes, coloca o Teorema de Pitágoras como ferramenta essencial para o cálculo de distâncias. Assim, a distância entre dois pontos A e B, cujas coordenadas são (x_A, y_A) e (x_B, y_B) é

$$d(A, B) = \sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}.$$

Em geral, se A e B são pontos em um espaço de n dimensões, cujas coordenadas são $(a_1, \ldots, a_n)$ e $(b_1, \ldots, b_n)$, então a distância entre esses pontos é dada por

$$d(A, B) = \sqrt{(a_1 - b_1)^2 + \cdots + (a_n - b_n)^2}.$$

[1] O tablete de argila *Plimpton* 322, originário da Mesopotâmia e atualmente guardado na Universidade Columbia, nos Estados Unidos, data de aproximadamente 1800 a.C. e contém uma grande quantidade de trios pitagóricos formados por inteiros surpreendentemente grandes.

Graças a Riemann, sabemos que esse modo de medir distâncias é apenas um dentre muitos. De fato, podemos interpretar a soma de quadrados $(a_1 - b_1)^2 + \cdots + (a_n - b_n)^2$ como a imagem $b(A - B, A - B)$ de uma função[2] $b : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, dada por

$$b(X, Y) = x_1 y_1 + \cdots + x_n y_n, \;\; X = (x_1, \ldots, x_n), \;\; Y = (y_1, \ldots, y_n),$$

onde $A - B = (a_1 - b_1, \ldots, a_n - b_n)$.

Assim, se $X = A - B$, então $d(A, B) = \sqrt{q(X)}$, onde $q(X) = b(X, X)$. Note que $q(X) = x_1^2 + \cdots + x_n^2$ é um polinômio de grau 2 com n indeterminadas, onde cada termo tem grau 2. Um polinômio desse tipo é chamado *forma quadrática*. Como estamos interessados em medir distâncias, o número $\sqrt{q(X)}$ deve ser real, logo devemos ter $q(X) \geq 0$ para qualquer possível escolha de $X = (x_1, \ldots, x_n)$. É claro que a forma dada $q(X) = x_1^2 + \cdots + x_n^2$ cumpre essa condição. Cabem aqui duas perguntas:

(1) Existem polinômios $p(x_1, \ldots, x_n)$ tais que $p(a_1, \ldots, a_n) \geq 0$ para todo $(a_1, \ldots, a_n) \in \mathbb{R} \times \cdots \times \mathbb{R}$?

(2) Se existe um polinômio como em (1), ele é necessariamente uma soma de quadrados de outros polinômios?

David Hilbert (1862 - 1943)

David Hilbert respondeu às duas perguntas, a primeira de modo positivo e a segunda de modo negativo. Um dos objetivos desse curso é responder essas perguntas, não necessariamente da mesma forma que Hilbert. Diante da resposta à segunda pergunta, Hilbert levantou outro questionamento similar, mas um pouco menos exigente:

(3) Dado um polinômio que satisfaz (1), é possível escrevê-lo como soma de quadrados de funções racionais?

Uma função racional é dada por uma fração onde numerador e denominador são polinômios. Por exemplo:

$$\frac{x+1}{x-1}, \;\; \frac{1}{x} \;\; \text{e} \;\; \frac{1 + x + x^2}{2 + 3x + x^3 - x^4}$$

são funções racionais. A pergunta (3) foi colocada por Hilbert na sua famosa conferência de 1900, onde ele expôs 23 problemas que desafiariam e nortearam o desenvolvimento da Matemática no século XX. Era o décimo sétimo problema dos 23, por isso é conhecido como o 17º problema de Hilbert. Sua solução foi encontrada por Emil Artin em 1927. As idéias de Artin serão expostas mais adiante.

Emil Artin (1898 - 1962)

[2]Uma função desse tipo satisfaz três propriedades básicas: é *linear* em relação a cada uma das suas variáveis, e por isso é chamada *função bilinear*; é *simétrica*, isto é, $b(X, Y) = b(Y, X)$ e é *positiva definida*, isto é, $b(X, X) \geq 0$, com $b(X, X) = 0$ se, e somente se, $X = (0, \ldots, 0)$.

Longe de representar o final da história, a solução de Artin para o 17º problema de Hilbert abriu caminho para que se desenvolvessem duas áreas da Matemática: a Álgebra Real e a Teoria dos Modelos.

No Capítulo 3 exibiremos a teoria dos corpos ordenados e uma solução do 17º problema de Hilbert. Antes, no Capítulo 2, veremos uma série de resultados sobre a representação de números inteiros como somas de quadrados de outros números inteiros.

2 Representação de números inteiros como somas de quadrados

Os inteiros $1, 4, 9, 16, 25, 36, \ldots$ são quadrados de outros inteiros. Observando aqueles que não são quadrados, vemos que alguns podem ser escritos como somas de dois quadrados: $2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, enquanto outros não: $7, 11, 15, 21$. Essa observação não nos leva, a princípio, a conclusões mais precisas. Se aumentarmos o número de possíveis quadrados a serem somados, veremos que alguns dos números que não são somas de dois quadrados, são somas de três quadrados: $11 = 1^1 + 1^2 + 3^2$, $21 = 1^2 + 2^2 + 4^2$, enquanto outros números positivos ainda resistem a serem expressos como somas de quadrados: 7 e 15, por exemplo. Mas, se permitirmos quatro quadrados, veremos que $7 = 1^2 + 1^2 + 1^2 + 2^2$ e $15 = 1^2 + 1^2 + 2^2 + 3^2$.

Dos exemplos que examinamos, os números 7 e 15 foram, digamos, os mais "resistentes" a serem expressos como somas de quadrados. A que se deve essa resistência? Será que existem inteiros positivos que não podem ser escritos como somas de quatro quadrados? Tentaremos responder a essas perguntas a seguir.

2.1 Congruências

Dado um número inteiro n, os possíveis restos de sua divisão por 8 são $0, 1, 2, 3, 4, 5, 6, 7$. Se $n = 8q + r$, onde $q \in \mathbb{Z}$ é o quociente e $r \in \mathbb{Z}$, $0 \leq r < 8$ é o resto da divisão, temos que $8 \mid n - r$. Usando a notação de Gauss, escrevemos

$$n \equiv r \ (\text{mod } 8)$$

e dizemos que n é **congruente** a r, módulo 8. Em geral, se $m \in \mathbb{Z}$, $m > 1$, dizemos que dois inteiros a e b são *congruentes módulo* m se $m \mid a - b$. Nesse caso, indicamos

$$a \equiv b \ (\text{mod } m).$$

C.F. Gauss (1777 - 1855)

A relação de congruência entre inteiros possui as seguintes propriedades:

1. Reflexividade: $a \equiv a \ (\text{mod } m)$, para todo $a \in \mathbb{Z}$.

2. Simetria: $a \equiv b \pmod{m}$ implica $b \equiv a \pmod{m}$, quaiquer que sejam $a, b \in \mathbb{Z}$.

3. Transitividade: $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$ implicam que $a \equiv c \pmod{m}$, quaiquer que sejam $a, b, c \in \mathbb{Z}$.

4. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$ e $ac \equiv bd \pmod{m}$, $a, b, c, d \in \mathbb{Z}$.

5. Se $a \equiv b \pmod{m}$ e $n \in \mathbb{Z}$, $n > 0$, então $a^n \equiv b^n \pmod{m}$.

6. Se $ab \equiv ac \pmod{m}$ e $d = (a, m)$ é o máximo divisor comum entre a e m, então

$$b \equiv c \left(\mod \frac{m}{d} \right).$$

   Em particular, se $(a, m) = 1$, então podemos "cancelar" a na congruência $ab \equiv ac \pmod{m}$, obtendo $b \equiv c \pmod{m}$.

7. Se $(a, m) = 1$, então existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{m}$. dizemos que a e b são **inversos** módulo m.

As demonstrações desses resultados seguem diretamente da definição e são vistas em um curso de Teoria dos Números. Convidamos o leitor a tentar demonstrá-las. O importante, nesse ponto, é perceber que a relação de congruência comporta-se como uma igualdade (na verdade, é uma relação de equivalência, pois é reflexiva, simétrica e transitiva).

No que se segue, iremos usar o seguinte resultado não trivial:

Teorema 2.1 (Wilson) *Se p é um número primo, então $(p-1)! \equiv -1 \pmod{p}$.*

A recíproca desse resultado também é verdadeira, embora não precisemos disso aqui.

2.2 Inteiros que são somas de dois quadrados

A igualdade

$$(a^2 + b^2) \cdot (c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{1}$$

é conhecida como **identidade de Brahmagupta-Fibonacci**. Foi apresentada por Leonardo Fibonacci em 1225, no trabalho *Liber Quadratorum*, mas já era conhecida pelo matemático hindu Brahmagupta no século VII. Com ela, podemos determinar quais inteiros são somas de dois quadrados, resolvendo o mesmo problema para números primos. Isso ocorre pois temos a nossa disposição, em $\mathbb{Z}$, o resultado muito forte enunciado a seguir.

Fibonacci (1170 - 1250)

Teorema 2.2 (Teorema Fundamental da Aritmética) *Se n é um número inteiro diferente de $-1, 0$ e 1, então o valor absoluto de n pode ser escrito como produto de primos de modo único, a menos da ordem em que aparecem os fatores, que não são necessariamente distintos.*

A demonstração desse teorema é dada em um curso elementar de Teoria dos Números. Embora não pareça, a parte sublinhada é a mais importante.

De posse do Teorema 2.2 e da igualdade (1), podemos concluir que, se $n = p_1 p_2 \cdots p_t$, com p_i primo para cada i, então n será soma de dois quadrados se os primos que aparecem um número ímpar se vezes no produto $p_1 \cdots p_t$ são, cada um, soma de dois quadrados.

Por exemplo, $3185 = 7 \cdot 7 \cdot 13 \cdot 5 = 7^2 \cdot (2^2 + 3^2) \cdot (1^2 + 2^2)$ pode ser escrito como soma de dois quadrados, pela igualdade (1).

Assim, a questão deve ser respondida para números primos. Estando o problema resolvido para o primo $2 = 1^2 + 1^2$, podemos considerar $p > 2$. Notemos que, como p é ímpar, o resto de sua divisão por 4 é igual a 1 ou 3, pois os outros dois restos fornecem os números pares $4k$ (resto 0) e $4k + 2$ (resto 2). Dessa forma, um primo ímpar p é de um dos dois tipos: $p = 4k + 1$ ou $p = 4k + 3$. Em termos de congruências, $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$.

Teorema 2.3 *Um número primo ímpar p pode ser escrito como soma de dois quadrados se, e somente se, $p \equiv 1 \pmod 4$.*

Demonstração: suponha, primeiro, que $p = a^2 + b^2$, onde $a, b \in \mathbb{Z}$. Como p é ímpar, a e b não podem ser simultaneamente pares nem simultaneamente ímpares. Logo um deles é par e o outro é ímpar, digamos, a par e b ímpar. O quadrado de um número par é divisível por 4, logo $a^2 \equiv 0 \pmod 4$. O quadrado de um número ímpar só pode deixar resto 1 quando dividido por 4, logo $b^2 \equiv 1 \pmod 4$. Assim, $p \equiv a^2 + b^2 \equiv 0 + 1 \equiv 1 \pmod 4$.

Reciprocamente, suponha que p é primo e $p \equiv 1 \pmod 4$, isto é, que $p = 4k + 1$, com $k \in \mathbb{Z}$. Então existe $\ell \in \mathbb{Z}$ tal que

$$p \mid \ell^2 + 1.$$

De fato, podemos escrever

$$(p-1)! = (p-1)(p-2)\cdots(\overbrace{p-2k}^{2k+1})(2k)(2k-1)\cdots 2 \cdot 1.$$

Reduzindo módulo p, obtemos

$$(p-1)! \equiv (-1)(-2)\cdots(-2k)(2k)(2k-1)\cdots 2 \cdot 1 \equiv (-1)^{2k}[(2k)!]^2 \ (\bmod p).$$

Fazendo $\ell = (2k)!$ e usando o Teorema 2.1 de Wilson, obtemos:

$$-1 \equiv \ell^2 \ (\bmod p),$$

isto é, $p \mid \ell^2 + 1$.

Considere, agora, o conjunto

$$C = \{\ell x - y \mid 0 \leq x < \sqrt{p}, 0 \leq y < \sqrt{p}\}.$$

Existem $\lfloor\sqrt{p}\rfloor + 1$ escolhas para cada x e cada y. Como $(\lfloor\sqrt{p}\rfloor + 1)^2 > (\sqrt{p})^2 = p$, existem dois pares ordenados distintos (x_1, y_1) e (x_2, y_2) tais que[3]

$$\ell x_1 - y_1 \equiv \ell x_2 - y_2 \ (\mod p).$$

Se $x = x_1 - x_2$ e $y = y_1 - y_2$, então $\ell x \equiv y \pmod{p}$ e x e y não são ambos nulos.

Assim, obtemos $\ell^2 x^2 \equiv y^2 \pmod{p}$ e como $\ell^2 \equiv -1 \pmod{p}$, temos $-x^2 \equiv y^2 \pmod{p}$, isto é, $p \mid x^2 + y^2$. Finalmente, como $0 < x^2 + y^2 < 2(\sqrt{p})^2 = 2p$ e o único múltiplo de p nesse intervalo é p, obtemos $p = x^2 + y^2$. □

Lema 2.4 *Suponha que n é divisível por um primo q da forma $4k + 3$.*

(1) *Se $n = a^2 + b^2$ e $q \mid n$ então $q \mid a$ e $q \mid b$.*

(2) *Se n é soma de dois quadrados, então q aparece um número par de vezes na fatoração de n.*

Demonstração: (1) se $q \nmid a$, então $(a, q) = 1$ e existe $c \in \mathbb{Z}$ tal que $ac \equiv 1 \pmod{q}$. Por outro lado, $q \mid n$ implica que $n \equiv 0 \pmod{q}$, ou seja, $a^2 + b^2 \equiv 0 \pmod{q}$. Multiplicando por c^2, obtemos $(ac)^2 + (bc)^2 \equiv 0 \pmod{q}$, isto é, $1 + (bc)^2 \equiv 0 \pmod{q}$. Logo, $q \mid \ell^2 + 1$, com $\ell = bc$. Pelo que vimos na demonstração do Teorema 2.3, $q \mid \ell^2 + 1$ implica que q é soma de dois quadrados, o que por sua vez implica que q é da forma $4k+1$, contradição. Portanto $q \mid a$. Por simetria, o mesmo argumento serve para mostrar que $q \mid b$.
(2) Se $q = 4k + 3$ é primo e $q \mid n$, $n = a^2 + b^2$, então, por (1), $q \mid a$ e $q \mid b$. Logo, $q^2 \mid n$ e $n = q^2 n_1$, onde $n_1 = (\frac{a}{q})^2 + (\frac{b}{q})^2$. Se $q \mid n_1$, repetindo o argumento obtemos $q^2 \mid n_1$. Assim, n é divisível por q^{2g}, onde g é um inteiro positivo. □

Pierre de Fermat (1601 - 1665)

O Teorema 2.5 a seguir nos diz exatamente quais são os inteiros positivos que podem ser escritos como somas de dois quadrados. O problema de representar um inteiro como soma de dois quadrados aparece diversas vezes na *Arithmetica* de Diofanto ($\sim$ 250 d.C.). Esse era o livro "de cabeceira" do jurista e matemático amador Pierre de Fermat (1601-1665). Em uma carta a Marin Mersenne (1588-1648), datada de 25 de dezembro de 1640, Fermat enunciou o resultado abaixo, mas não o demonstrou, embora tenha indicado depois inclusive o método que havia usado na demonstração[4].

[3]Isso é consequência do princípio de Dirichlet. Veja a página 11.

[4]O método da *descida infinita*, uma criação do próprio Fermat.

Tudo indica que Fermat realmente conhecia uma demonstração correta do resultado, mas a primeira demonstração deve-se a Leonhard Euler (1707-1783), comunicada em uma carta a Christian Goldbach (1690-1764), datada de 6 de maio de 1747. É interessante notar que a demonstração dada por Euler em 1747 usa o método sugerido por Fermat, cem anos antes.

Euler (1707 - 1783)

Teorema 2.5 (Fermat-Euler) *Seja n um inteiro positivo. Então n é uma soma de dois quadrados se e somente se todo divisor primo de n da forma $4k+3$ aparece um número par de vezes na fatoração de n como produto de primos.*

Demonstração: a parte mais difícil já foi feita no Teorema 2.3. Como já discutimos no início da seção, se n é um inteiro maior do que 1 e

$$n = 2^a p_1^{b_1} \cdots p_t^{b_t} \tag{2}$$

é a fatoração de n como produto de primos, onde $p_1, \ldots, p_t$ são primos ímpares, $a \geq 0$ e $b_i \geq 0$, para cada i, então os primos $p_1, \ldots, p_t$ e os inteiros não negativos $a, b_1, \ldots, b_t$ são determinados de modo único.

Cada expoente $a, b_1, \ldots, b_t$ indica o número de vezes que o primo aparece na decomposição (2). Quando um desses inteiros for igual a zero, o primo não aparece na fatoração. Por exemplo, n é ímpar se, e somente se, $a = 0$.

Pelo Teorema 2.3, os primos do tipo $4k+1$ são somas de dois quadrados, enquanto os primos da forma $4k+3$ não são somas de quadrados. Podemos supor, sem perda de generalidade, que os r primeiros primos ($1 \leq r \leq t$) $p_1, \ldots, p_r$ são do tipo $4k+1$, enquanto os demais primos $p_{r+1}, \ldots, p_t$ são da forma $4k+3$. Podemos, então, escrever $p_i = x_i^2 + y_i^2$, para $i = 1, \ldots, r$ e, aplicando a igualdade (1) um número finito de vezes, vemos que, para cada i, $1 \leq i \leq r$, $p_i^{b_i} = X_i^2 + Y_i^2$, com $X_i, Y_i \in \mathbb{Z}$.

Se para cada $i \in \{r+1, \ldots, t\}$, b_i for par, os fatores primos do tipo $4k+3$ aparecem como quadrados, ou seja,

$$n = 2^a p_1^{b_1} \cdots p_t^{b_t} = \overbrace{(1^2+1^2)^a (X_1^2+Y_1^2)\cdots(X_r^2+Y_r^2)}^{A^2+B^2} \cdot \overbrace{(p_{r+1}^{b_{r+1}/2})^2 \cdots (p_t^{b_t/2})^2}^{=C^2} = (AC)^2 + (BC)^2.$$

onde usamos, novamente, por repetidas vezes a igualdade (1). Assim, n é uma soma de dois quadrados.

Reciprocamente, se n é soma de dois quadrados, então o Lema 2.4, parte (2), garante que qualquer fator primo da forma $4k+3$ aparece um número par de vezes na decomposição de n como produto de fatores primos. □

2.3 Inteiros que não são somas de três quadrados

No início da seção 2.1, vimos que, se $n \in \mathbb{Z}$, então $n \equiv r (\text{mod } 8)$, onde $r \in \{0, 1, 2, 3, 4, 5, 6, 7\}$. Usando as propriedades de congruência listadas nessa mesma seção, vemos que $n^2 \equiv s \,(\text{mod } 8)$, onde $s \in \{0, 1, 4\}$. Com isso, obtemos o seguinte resultado.

Teorema 2.6 *Qualquer inteiro que deixa resto* 7 *quando dividido por* 8 *não pode ser escrito como soma de três quadrados.*

Demonstração: primeiramente, se n deixa resto 7 quando dividido por 8, então n pode ser escrito como $n = 8k + 7$, com $k \in \mathbb{Z}$. Sendo a soma de um número par com um número ímpar, $8k + 7$ é, necessariamente, ímpar.

Suponha, agora, que $n = x_1^2 + x_2^2 + x_3^2$, como $x_1, x_2, x_3 \in \mathbb{Z}$. Então

$$7 \equiv n \equiv x_1^2 + x_2^2 + x_3^2 \ (\text{ mod } 8),$$

isto é, $7 \equiv s_1 + s_2 + s_3 \,(\text{mod } 8)$, com $s_1, s_2, s_3 \in \{0, 1, 4\}$. Essa última congruência indica que $s_1+s_2+s_3$ deve ser ímpar (por quê?). Logo, o número de parcelas ímpares nessa soma deve ser 1 ou 3. Como as únicas opções para as parcelas são $\{0, 1, 4\}$, temos que $s_1+s_2+s_3 = 1+1+1 = 3$, $s_1 + s_2 + s_3 = 1 + 0 + 4 = 5$, $s_1 + s_2 + s_3 = 0 + 1 + 0 = 1$ ou $s_1 + s_2 + s_3 = 1 + 4 + 4 = 9 \equiv 1($ mod 8). Como nenhum desses resultados é igual a 7, n não pode ser escrito como soma de três quadrados. □

Corolário 2.7 *Um inteiro da forma* $4^m(8k + 7)$ *não pode ser escrito como soma de três quadrados.*

Demonstração: suponha o contrário, isto é, que $n = 4^m(8k + 7)$ pode ser escrito como soma de três quadrados, digamos $n = x_1^2 + x_2^2 + x_3^2$. Se $m = 0$, então $n = 8k + 7$ e, pelo Teorema 2.6, não pode ser escrito como soma de três quadrados. Se $m > 1$, então $4 \mid n$, ou seja, $n \equiv 0 \,($ mod 4). Assim $x_1^2 + x_2^2 + x_3^2 \equiv 0 \,(\text{mod } 4)$. Se x_1, x_2 e x_3 fossem ímpares, então $x_1^2 + x_2^2 + x_3^2$ seria ímpar e não poderia ser divisível por 4. Se apenas um deles fosse ímpar, também teríamos $x_1^2 + x_2^2 + x_3^2$ ímpar, o que não é possível. Finalmente, se dois deles fossem ímpares e o terceiro fosse par, então $x_1^2 + x_2^2 + x_3^2$ seria congruente a 2 módulo 4, o que não ocorre no nosso caso. Portanto, os três inteiros x_1, x_2 e x_3 são pares e temos

$$\frac{n}{4} = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2.$$

Podemos, então, repetir o mesmo argumento para $\frac{n}{4} = 4^{m-1}(8k + 7)$. Fazendo isso um número finito de vezes, chegaríamos a conclusão de que $8k + 7$ é soma de três quadrados, o que, pelo Teorema 2.6 não é verdade. □

Cabe aqui a observação de que os números do tipo descrito no Corolário 2.7 são os únicos (inteiros positivos) que não podem ser escritos como somas de três quadrados. De fato, vale o seguinte resultado:

Teorema 2.8 (Gauss - Legendre) *Um inteiro positivo pode ser expresso como soma de três quadrados se, e somente se, não for da forma* $4^m(8k+7)$.

A demonstração desse teorema requer o uso da teoria dos resíduos quadráticos e não a faremos aqui. O leitor interessado poderá encontrá-la, por exemplo, em [8], Teorema 187, p. 194. Ao invés da demonstração do Teorema, abriremos espaço aqui para uma pequena futilidade, mas que tem algo de interessante.

Figura 2: **Louis Legendre (1755 - 1797)**

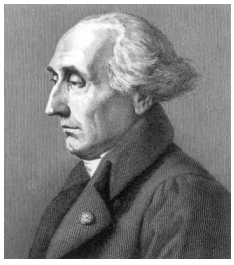
Figura 3: **Adrien-Marie Legendre (1752 - 1833)**

A Figura 2 é reconhecida há mais de cem anos como sendo do matemático A.-M. Legendre, mas é, na verdade, um retrato de um homônimo, o político francês Louis Legendre. Assim, a única imagem disponível de Adrien-Marie Legendre é uma caricatura, mostrada na Figura 3. Essa é uma descoberta recente (veja [5]).

2.4 O Teorema dos Quatro Quadrados

Como acabamos de demonstrar na seção 2.3, existe uma infinidade de inteiros que não podem ser escritos como somas de três quadrados. Nesse ponto cabe o seguinte questionamento: existem inteiros que não podem ser escritos como somas de quatro quadrados? Como veremos, a resposta a essa pergunta é negativa.

O Teorema de Lagrange, também conhecido como Teorema dos Quatro Quadrados, afirma que todo inteiro não negativo é soma de, no máximo, 4 quadrados. O primeiro a enunciar, sem demonstração, esse fato foi Claude Bachet (1587-1638), em 1621. O resultado também foi enunciado por Fermat em 1636, mas , como de costume, ele não revelou sua demonstração (embora dissesse que tinha uma). Joseph



Lagrange (1736 - 1813)

Louis Lagrange (1736-1813) publicou uma demonstração em 1798, no artigo intitulado *Essai sur la theorie des nombres*, mas suas idéias remontam a 1770. Euler também estudou o problema, e deu contribuições significativas em uma série de artigos publicados entre 1747 e 1751. Ele só obteve uma demonstração em 1772. Em 1801, Gauss apresentou sua demonstração do teorema, na seção 293 do seu famosíssimo livro *Disquistiones Arithmeticae*.

Um fato de fundamental importância para os argumentos de Lagrange e Euler é a chamada *identidade de Euler*, comunicada em uma carta a Goldbach em 1748:

Lema 2.9 (Euler, 1748) *Se m e n são somas de quatro quadrados, então o produto mn também é uma soma de quatro quadrados.*

Demonstração: de fato, se $m = a^2 + b^2 + c^2 + d^2$ e $n = A^2 + B^2 + C^2 + D^2$, então

$$mn = r^2 + s^2 + t^2 + u^2,$$

onde

$r = aA+bB+cC+dD$, $s = aB-bA+cD-dC$, $t = aC-bD-cA+dB$ e $u = aD+bC-cB-dA$.

Isso demonstra o resultado. □

De modo análogo ao que fizemos para a soma de dois quadrados na seção 2.2, podemos usar o Lema 2.9 repetidas vezes, juntamente com o Teorema 2.2, para reduzir o problema ao caso em que n é primo. De fato, se todo primo for uma soma de quatro quadrados, como todo número inteiro maior do que 1 é primo ou é produto de primos, o Lema 2.9 nos garante que todo inteiro será soma de quatro quadrados.

Para demonstrarmos o Lema 2.10 a seguir, usaremos o seguinte princípio[5], devido ao matemático alemão[6] Johann Peter Gustav Lejeune Dirichlet: *se um conjunto com n elementos é reunião de m subconjuntos distintos, com $n > m$, então pelo menos um destes subconjuntos contém mais de um elemento.*

Dirichlet (1805 - 1859)

Lema 2.10 *Seja $p > 2$ um inteiro primo. Então a equação*

$$X^2 + Y^2 + 1 \equiv 0 \ (\mod p)$$

admite uma solução $x_0, y_0 \in \mathbb{Z}$, com $0 \leq x_0 \leq \frac{p-1}{2}$ e $0 \leq y_0 \leq \frac{p-1}{2}$.

[5] O princípio de Dirichlet também é conhecido como *princípio das gavetas* ou *princípio da casa dos pombos*.

[6] A cidade de Düren, onde Dirichlet nasceu, hoje Alemanha, era parte do império Napoleônico em 1805. A família de Dirichlet era da cidade de Richelet, na Bélgica. Isso explica a origem do seu nome, uma corruptela de "Le jeune de Richelet", ou seja, o jovem de Richelet.

Demonstração: Consideremos os seguintes conjuntos de números inteiros

$$S_1 = \{1 + k^2 \mid k = 0, 1, \ldots, \frac{p-1}{2}\} \quad \text{e} \quad S_2 = \{-l^2 \mid l = 0, 1, \ldots, \frac{p-1}{2}\}.$$

Se $1 + k_1^2 \equiv 1 + k_2^2 (\text{mod } p)$ então $p | k_1^2 - k_2^2 = (k_1 - k_2)(k_1 + k_2)$. Sendo p primo, temos $p|(k_1 - k_2)$ ou $p|(k_1 + k_2)$. Como $0 \leq k_1, k_2 \leq \frac{p-1}{2}$, temos $0 \leq k_1 + k_2 \leq p - 1$, logo $k_1 + k_2 \equiv 0 \,(\text{mod } p)$ implica $k_2 = -k_1$ e $1 + k_1^2 = 1 + k_2^2$. Por outro lado, temos $-\frac{p-1}{2} \leq k_1 - k_2 \leq \frac{p-1}{2}$, logo $k_1 - k_2 \equiv 0 \,(\text{mod } p)$ implica $k_1 = k_2$ e $1 + k_1^2 = 1 + k_2^2$. Resumindo, temos:

$$\text{se } 1 + k_1^2 \neq 1 + k_2^2, \text{ com } 1 + k_1^2, 1 + k_2^2 \in S_1, \text{ então } 1 + k_1^2 \not\equiv 1 + k_2^2 \,(\text{mod } p).$$

Analogamente, se $l_1, l_2 \in S_2$ e $l_1 \neq l_2$, então $l_1 \not\equiv l_2 \,(\text{mod } p)$.

Sobre os conjuntos S_1 e S_2, observamos que

- $S_1 \cap S_2 = \emptyset$, pois S_1 possui somente elementos positivos enquanto S_2 possui somente elementos negativos.
- $|S_1 \cup S_2| = |S_1| + |S_2| = \frac{p-1}{2} + 1 + \frac{p-1}{2} + 1 = p + 1 > p$.

pelo princípio de Dirichlet, existem $1 + x_0^2 \in S_1$ e $-y_0^2 \in S_2$ tais que

$$1 + x_0^2 \equiv -y_0^2 \,(\text{mod } p),$$

com $0 \leq x_0 \leq \frac{p-1}{2}$ e $0 \leq y_0 \leq \frac{p-1}{2}$. □

Teorema 2.11 (Lagrange, 1770 - Euler, 1772) *Todo inteiro positivo é soma de quatro quadrados.*

Demonstração: pelo que discutimos acima, o uso do Lema 2.9 nos permite reduzir a verificação a números primos. Para $p = 2$ o resultado é claro, pois $p = 1^2 + 1^2 + 0^2 + 0^2$. Podemos supor, então, que $p > 2$. Pelo Lema 2.10, $p \mid a^2 + b^2 + c^2 + d^2$, onde $a = x_0$, $b = y_0$, $c = 1$ e $d = 0$, como no Lema. De outro modo,

$$mp = a^2 + b^2 + c^2 + d^2,$$

onde $m \in \mathbb{Z}$. Claro que $m \geq 0$, pois $p > 1$ e mp é soma de quadrados, logo positivo. Se $m = 0$, teríamos $0 = a^2 + b^2 + c^2 + d^2 = x_0^2 + y_0^2 + 1 + 0 \geq 1 > 0$, absurdo. Logo, $m \geq 1$.

Por outro lado, do Lema 2.10, sabemos que $0 \leq x_0 \leq \frac{p-1}{2} < \frac{p}{2}$ e $0 \leq y_0 \leq \frac{p-1}{2} < \frac{p}{2}$. Assim,

$$mp = x_0^2 + y_0^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2.$$

Isso implica que $m < p$. Portanto, $1 \leq m < p$.

Escolha m como sendo o **menor inteiro** satisfazendo as condições acima. A seguir, mostraremos que $m = 1$. Comecemos mostrando que m é ímpar. Se m fosse par, então

$a^2+b^2+c^2+d^2 = mp \equiv 0 (\text{mod } 2)$ e, uma vez que $(a+b+c+d)^2 \equiv a^2+b^2+c^2+d^2 (\text{mod } 2)$, teríamos $a+b+c+d \equiv 0 \pmod 2$. Assim, sem perda de generalidade, poderíamos supor que $a+b \equiv 0 \pmod 2$ e $c+d \equiv 0 \pmod 2$, ou seja, $a+b$ e $c+d$ seriam pares e, portanto, $a-b$ e $c-d$ também seriam, logo, teríamos

$$\frac{m}{2}p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2,$$

onde os quatro termos entre parênteses são inteiros. Mas isso contradiz a minimalidade de m. Portanto, m é ímpar.

Vamos mostrar agora que $m = 1$. Supondo o contrário, teríamos $m \geq 3$, pois m é ímpar. Sejam $a_0, b_0, c_0, d_0 \in \mathbb{Z}$ escolhidos de modo que

$$a_0 \equiv a \ (\text{mod } m), b_0 \equiv b \ (\text{mod } m), c_0 \equiv c \ (\text{mod } m), d_0 \equiv d \ (\text{mod } m) \quad \text{e} \tag{3}$$

$$-\frac{m}{2} < a_0, b_0, c_0, d_0 < \frac{m}{2}.$$

É possível fazer essa escolha porque $\{-\frac{m-1}{2}, \ldots, \frac{m-1}{2}\}$ é um *sistema completo de restos*[7], módulo m.

Assim, temos

$$a_0^2+b_0^2+c_0^2+d_0^2 \equiv a^2+b^2+c^2+d^2 \equiv mp \equiv 0 \ (\text{mod } m),$$

isto é,

$$a_0^2+b_0^2+c_0^2+d_0^2 = mn, \tag{4}$$

onde $n \in \mathbb{Z}$ e $n > 0$. Caso contrário, teríamos $a_0 = b_0 = c_0 = d_0 = 0$ e, daí, $a \equiv 0 \pmod m$, $b \equiv 0 \pmod m$, $c \equiv 0 \pmod m$ e $d \equiv 0 \pmod m$. Logo $m^2 \mid a^2+b^2+c^2+d^2$, ou seja, $m^2 \mid mp$ e $m \mid p$, o que contradiz o fato de p ser primo, pois $1 < m < p$. Por outro lado, por (4),

$$mn = a_0^2+b_0^2+c_0^2+d_0^2 < 4 \cdot \frac{m^2}{4} = m^2,$$

o que implica que $mn < m^2$ e $n < m$.

Uma vez que $mn = a_0^2+b_0^2+c_0^2+d_0^2$ e $mp = a^2+b^2+c^2+d^2$, o produto $m^2np = (mn)(mp)$ é, pelo Lema 2.9, também uma soma de quatro quadrados. Mais precisamente, o Lema 2.9 nos diz que

$$m^2np = (a^2+b^2+c^2+d^2) \cdot (a_0^2+b_0^2+c_0^2+d_0^2) = r^2+s^2+t^2+u^2,$$

onde

$$r = aa_0+bb_0+cc_0+dd_0, s = ab_0-ba_0+cd_0-dc_0, t = ac_0-bd_0-ca_0+db_0 \text{ e } u = ad_0+bc_0-cb_0-da_0.$$

As congruências em (3) nos dizem que r, s, t e u são todos divisíveis por m. Por exemplo,

$$s = ab_0 - ba_0 + cd_0 - dc_0 \equiv ab - ba + cd - dc \equiv 0 \ (\text{mod } m).$$

[7]Um sistema completo de restos, módulo m é um conjunto $R = \{r_1, \ldots, r_m\}$ cujos elementos são incongruentes módulo m e, para cada inteiro n, existe $r \in R$ tal que $n \equiv r \pmod m$.

Assim, dividindo $m^2np = r^2 + s^2 + t^2 + u^2$ por m^2, obtemos

$$np = \left(\frac{r}{m}\right)^2 + \left(\frac{s}{m}\right)^2 + \left(\frac{t}{m}\right)^2 + \left(\frac{u}{m}\right)^2,$$

com $0 < n < m$. Mas isso contradiz a minimalidade de m. A contradição veio de supormos $m > 1$. Logo $m = 1$ e

$$p = mp = a^2 + b^2 + c^2 + d^2,$$

o que completa a demonstração. □

2.5 A demonstração de Hurwitz do Teorema dos Quatro Quadrados

O objetivo desta seção é dar uma demonstração alternativa do Teorema 2.11 que estudamos na seção anterior. Advertimos que os métodos usados aqui são de Álgebra Abstrata. Nesse sentido, a presente seção contrasta com o restante do texto pelo seu caráter não elementar. Incluímos essa demonstração pela beleza dos argumentos e por ser uma boa ilustração do uso da Álgebra Abstrata em Teoria dos Números. Informamos, ainda, que essa seção é inteiramente baseada em parte do trabalho [9], no qual o leitor interessado pode encontrar mais detalhes sobre os quatérnios de Hamilton, a principal ferramenta aqui utilizada.

Adolf Hurwitz (1859 - 1919)

Exibiremos uma demonstração (veja [14]), devida a Adolf Hurwitz[8], que faz uso de uma subálgebra da álgebra $\mathbb{H}$ dos quatérnios. Para isso, precisamos de algumas definições preliminares.

Queremos generalizar a álgebra de quatérnios, considerando os coeficientes de um quatérnio pertencendo a um anel que não seja necessariamente um corpo.

Seja A um anel comutativo com unidade. Denotamos por $\mathbb{H}(A)$ o A-módulo livre $A^4 = \{(a_1, a_2, a_3, a_4) \mid a_1, a_2, a_3, a_4 \in A\}$ com base $\mathbf{1} = (1, 0, 0, 0)$, $\mathbf{i} = (0, 1, 0, 0)$, $\mathbf{j} = (0, 0, 1, 0)$ e $\mathbf{k} = (0, 0, 0, 1)$ e produto definido por

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -\mathbf{1}$$

e estendido por (bi-)linearidade a todo par de "vetores" $u, v \in A^4$. Munido desse produto, $\mathbb{H}(A)$ torna-se um anel não comutativo (pois, por exemplo, $\mathbf{ij} = -\mathbf{ji}$).

Observação: se $A = \mathbb{R}$, o corpo dos números reais, então $\mathbb{H}(A) = \mathbb{H}$, a álgebra de quatérnios usual. Veremos adiante um exemplo em que A é um corpo mas $\mathbb{H}(A)$ não é um anel de divisão.

A álgebra de quatérnios sobre $\mathbb{Z}$, $\mathbb{H}(\mathbb{Z})$, é chamada *anel dos inteiros de Lipschitz*. Vamos considerar um anel H, chamado *anel dos inteiros de Hurwitz*, dado por

$$\mathsf{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{Z} \quad \text{ou} \quad a, b, c, d \in \frac{1}{2} + \mathbb{Z}\}, \tag{5}$$

[8]O trabalho de Hurwitz sobre o Teorema de Lagrange, cuja demonstração é essecialmente a que está nas páginas seguintes, foi produzido em 1896.

onde $\frac{1}{2}+\mathbb{Z} = \{\frac{1}{2}+n \mid n \in \mathbb{Z}\} = \{\frac{2n+1}{2} \mid n \in \mathbb{Z}\}$ é o conjunto das frações cujo numerador é ímpar e o denominador é 2.

Lema 2.12 *Mantendo as notações estabelecidas acima, temos:*

1. $\mathbb{H}(\mathbb{Z}) \subset \mathsf{H} \subset \mathbb{H}(\mathbb{Q})$, *onde "$\subset$" indica subanel.*
2. *Para todo* $z \in \mathsf{H}$, $z+\overline{z} \in \mathbb{Z}$ *e* $N(z) = z\overline{z} \in \mathbb{Z}$.
3. *Um elemento* $z \in \mathsf{H}$ *é invertível se, e somente se,* $N(z) = 1$.
4. *Todo ideal à esquerda (respectivamente à direita)* I *de* H *é* **principal**, *isto é,* $I = \mathsf{H}z$ *(respectivamente* $I = z\mathsf{H}$*).*

Demonstração: A única afirmação não imediata do item 1 é que H é fechado para o produto. Para demonstrarmos este fato,consideremos $z, z' \in \mathsf{H}$, digamos $z = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ e $z' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$. Se $a, a', b, b', c, c', d, d' \in \mathbb{Z}$, então $zz' \in \mathbb{H}(\mathbb{Z}) \subset \mathsf{H}$. Consideremos o elemento $u = \frac{1}{2}(1+\mathbf{i}+\mathbf{j}+\mathbf{k}) \in \mathsf{H}$. Todo elemento $z \in \mathsf{H}$ pode ser escrito como $z = u+z_0$, onde $z_0 \in \mathbb{H}(\mathbb{Z})$. Observemos que

- $u \cdot \mathbf{1} = \mathbf{1} \cdot u = u \in \mathsf{H}$;
- $u \cdot \mathbf{i} = \frac{1}{2}(-1+\mathbf{i}+\mathbf{j}-\mathbf{k}) \in \mathsf{H}$ e $\mathbf{i} \cdot u = \frac{1}{2}(-1+\mathbf{i}-\mathbf{j}+\mathbf{k}) \in \mathsf{H}$;
- $u \cdot \mathbf{j} = \frac{1}{2}(-1-\mathbf{i}+\mathbf{j}+\mathbf{k}) \in \mathsf{H}$ e $\mathbf{j} \cdot u = \frac{1}{2}(-1+\mathbf{i}+\mathbf{j}-\mathbf{k}) \in \mathsf{H}$;
- $u \cdot \mathbf{k} = \frac{1}{2}(-1+\mathbf{i}-\mathbf{j}+\mathbf{k}) \in \mathsf{H}$ e $\mathbf{k} \cdot u = \frac{1}{2}(-1-\mathbf{i}+\mathbf{j}+\mathbf{k}) \in \mathsf{H}$.

Logo, se $z_0 \in \mathbb{H}(\mathbb{Z})$, então $uz_0 \in \mathsf{H}$ e $z_0u \in \mathsf{H}$. Além disso, somando as igualdades acima, obtemos $u^2 = \frac{1}{2}(-2+2\mathbf{i}+2\mathbf{j}+2\mathbf{k}) \in \mathsf{H}$. Agora, se $z = u+z_0$ e $z' = u+z_0'$ são elementos de $\mathsf{H} \setminus \mathbb{H}(\mathbb{Z})$, então

$$zz' = (u+z_0)(u+z_0') = u^2 + uz_0' + z_0u + z_0z_0' \in \mathsf{H}$$

e do mesmo modo, $z'z \in \mathsf{H}$.

Daqui por diante, estabeleceremos a seguinte notação

$$\mathsf{H} = \mathsf{H}_1 \cup \mathsf{H}_{1/2} \tag{6}$$

onde $\mathsf{H}_1 = \{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \mid a,b,c,d \in \mathbb{Z}\} = \mathbb{H}(\mathbb{Z})$ e $\mathsf{H}_{1/2} = \{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \mid a,b,c,d \in \frac{1}{2}+\mathbb{Z}\}$. É claro que a reunião em (6) é disjunta.

Para demonstrarmos o item 2, consideremos $z \in \mathsf{H} = \mathsf{H}_1 \cup \mathsf{H}_{\mathbf{1}/2}$. Se $z \in \mathsf{H}_1$ então é imediato que $z+\overline{z} \in \mathbb{Z}$ e $N(z) = z\overline{z} \in \mathbb{Z}$. Caso $z \in \mathsf{H}_{1/2}$, temos

$$z = (\frac{1}{2}+a) + (\frac{1}{2}+b)\mathbf{i} + (\frac{1}{2}+c)\mathbf{j} + (\frac{1}{2}+d)\mathbf{k}, \quad \text{com} \quad a,b,c,d \in \mathbb{Z}.$$

Logo, $z + \overline{z} = 1 + 2a \in \mathbb{Z}$ e

$$z\overline{z} = (\frac{1}{2} + a)^2 + (\frac{1}{2} + b)^2 + (\frac{1}{2} + c)^2 + (\frac{1}{2} + d)^2 =$$

$$= 1 + a + b + c + d + a^2 + b^2 + c^2 + d^2 \in \mathbb{Z}.$$

Se $z \in \mathsf{H}$ é invertível, então existe $w \in \mathsf{H}$ tal que $zw = 1$. Dessa última igualdade segue que $N(zw) = N(1) = 1$, onde N é a função **norma** que associa a cada elemento $q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ de H o número $N(q) = a^2 + b^2 + c^2 + d^2$. Como **a norma é multiplicativa**[9], isto é, $N(q \cdot q') = N(q) \cdot N(q')$, temos que $N(z)N(w) = 1$. Como $N(z), N(w) \in \mathbb{Z}$ e $N(z), N(w) > 0$, temos $N(z) = N(w) = 1$. Reciprocamente, se $z \in \mathsf{H}$ tem norma igual a 1, então $z\overline{z} = \overline{z}z = N(z) = 1$ implica que $\overline{z} = z^{-1} \in \mathsf{H}$, isto é, z é invertível em H. Demonstramos, assim, o item 3 do Lema.

Finalmente, para demonstrarmos o item 4 observemos inicialmente que um número racional está sempre entre dois números inteiros consecutivos. Assim, se $z = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}(\mathbb{Q})$, existem $a', b', c', d' \in \mathbb{Z}$ tais que

$$|a - a'| \leq \frac{1}{2}, |b - b'| \leq \frac{1}{2}, |c - c'| \leq \frac{1}{2}, |d - d'| \leq \frac{1}{2}.$$

Como veremos mais adiante, é necessário que encontremos desigualdades *estritas* nas expressões acima. Este é o ponto em que os inteiros de Hurwitz são mais úteis em relação aos inteiros de Lipschitz. De fato, considerando $a', b', c', d' \in \frac{1}{2} + \mathbb{Z}$ obtemos

$$|a - a'| < \frac{1}{2}, |b - b'| < \frac{1}{2}, |c - c'| < \frac{1}{2}, |d - d'| < \frac{1}{2}.$$

Portanto, se $x = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k} \in \mathsf{H}$, temos

$$N(x - z) = (a - a')^2 + (b - b')^2 + (c - c')^2 + (d - d')^2 < \frac{4}{4} = 1.$$

Seja I um ideal à esquerda de H. O conjunto $N(I) = \{N(y) \mid y \in I \setminus \{0\}\} \subset \mathbb{N}$ tem um menor elemento[10] $N(u)$, com $u \in I$, $u \neq 0$. O inverso de u em $\mathbb{H}(\mathbb{Q})$ é $u^{-1} = \frac{\overline{u}}{N(u)}$. Dado $y \in I$, seja $yu^{-1} \in \mathbb{H}(\mathbb{Q})$.

Pela discussão acima, existe $x \in \mathsf{H}$ tal que $N(yu^{-1} - x) < 1$. Logo

$$N(y - xu) = N\left(\left(yu^{-1} - x\right)u\right) = N(yu^{-1} - x)N(u) < N(u).$$

Uma vez que $y - xu \in I$, pela minimalidade de $N(u)$ temos, necessariamente, que $y - xu = 0$, isto é, $y = xu$. Como tomamos $y \in I$ arbitrário, temos $I \subset \mathsf{H}u$. Sendo a inclusão inversa imediata, temos a igualdade $I = \mathsf{H}u$.

O resultado para ideais a direita tem exatamente a mesma demonstração. □

[9]Para uma demonstração desse fato, veja [9], Proposição 2.5. ou [14], Lema 2 b), p. 98. Esse fato tem relação direta com o Lema 2.9 da página 11.

[10]Princípio da boa ordem.

Observação: se $a, b, c, d \in \mathbb{Z}$, então $a^2+b^2+c^2+d^2$ é norma de algum quatérnio em $\mathbb{H}(\mathbb{Z})$. De fato, $a^2+b^2+c^2+d^2 = N(z)$, onde $z = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$. Agora, dadas as somas de quadrados $a_1^2+b_1^2+c_1^2+d_1^2$ e $a_2^2+b_2^2+c_2^2+d_2^2$, com $a_i, b_i, c_i, d_i \in \mathbb{Z}$, para $i = 1, 2$, temos

$$(a_1^2+b_1^2+c_1^2+d_1^2)\cdot(a_2^2+b_2^2+c_2^2+d_2^2) = N(z_1)N(z_2) = N(z_1z_2)$$

onde $z_1 = a_1+b_1\mathbf{i}+c_1\mathbf{j}+d_1\mathbf{k}$ e $z_2 = a_2+b_2\mathbf{i}+c_2\mathbf{j}+d_2\mathbf{k}$. Usando as propriedades operatórias dos quatérnios, que são as propriedades usuais das expressões algébricas, sujeitas às seguintes leis para a base $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \quad \text{e} \quad \mathbf{i}\cdot\mathbf{j}\cdot\mathbf{k} = -1$$

temos

$$z_1z_2 = (a_1a_2-b_1b_2-c_1c_2-d_1d_2)+(a_1b_2+a_2b_1+c_1d_2-d_1c_2)\mathbf{i}$$

$$+(a_1c_2+c_1a_2+d_1b_2-b_1d_2)\mathbf{j}+(a_1d_2+a_2d_1+b_1c_2-b_2c_1)\mathbf{k}.$$

Assim,

$$N(z_1z_2) = (a_1a_2-b_1b_2-c_1c_2-d_1d_2)^2+(a_1b_2+a_2b_1+c_1d_2-d_1c_2)^2+$$

$$+(a_1c_2+c_1a_2+d_1b_2-b_1d_2)^2+(a_1d_2+a_2d_1+b_1c_2-b_2c_1)^2.$$

Isso nos fornece uma nova demonstração do Lema 2.9: o produto de duas somas de quadrados de números inteiros é uma soma de quadrados de números inteiros. Uma vez que todo número inteiro positivo pode ser escrito como produto de inteiros primos, e $2 = 1^2+1^2+0^2+0^2$, o Teorema 2.11 segue diretamente do resultado abaixo.

Lema 2.13 *Todo número primo ímpar positivo pode ser escrito como soma de quatro quadrados de números inteiros.*

Antes de iniciar a demonstração do Lema 2.13, veremos dois lemas auxiliares.

Lema 2.14 *Se $n \in \mathbb{Z}$, então o ideal $n\mathbb{H}(\mathbb{Z})$ é bilateral, isto é, $n\mathbb{H}(\mathbb{Z}) = \mathbb{H}(\mathbb{Z})n$, e*

$$\mathbb{H}(\mathbb{Z})/n\mathbb{H}(\mathbb{Z}) \simeq \mathbb{H}(\mathbb{Z}/n\mathbb{Z})$$

Demonstração: Consideremos o homomorfismo de anéis $\varphi : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{Z}/n\mathbb{Z})$ dado por $z \mapsto \overline{z}$, onde para $z = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$, definimos $\overline{z} = \overline{a}+\overline{b}\mathbf{i}+\overline{c}\mathbf{j}+\overline{d}\mathbf{k}$, a barra indicando a projeção módulo n de $\mathbb{Z}$ em $\mathbb{Z}/n\mathbb{Z}$.

Cada quatérnio $\overline{z} = \overline{a}+\overline{b}\mathbf{i}+\overline{c}\mathbf{j}+\overline{d}\mathbf{k} \in \mathbb{H}(\mathbb{Z}/n\mathbb{Z})$ é imagem de um quatérnio $z = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \in \mathbb{H}(\mathbb{Z})$, logo o homomorfismo φ é sobrejetor. Sendo $n \in \mathbb{Z}$ um escalar, temos $nz = zn$, para todo $z \in \mathbb{H}(\mathbb{Z})$, logo o ideal $n\mathbb{H}(\mathbb{Z})$ é bilateral. Além disso, temos

$$\ker(\varphi) = \{z \in \mathbb{H}(\mathbb{Z}) \mid \overline{z} = \overline{0}\} = \{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \mid a, b, c, d \in n\mathbb{Z}\} = n\mathbb{H}(\mathbb{Z}).$$

Pelo teorema dos isomorfismos de anéis, segue o resultado. □

Observação: o Lema 2.10, demonstrado na seção anterior, implica que existem elementos não nulos em $\mathbb{H}(\mathbb{Z}/p\mathbb{Z})$ que têm norma igual a zero. De fato, se $z = 1 + \overline{x}_0\mathbf{i} + \overline{y}_0\mathbf{j} \in \mathbb{H}(\mathbb{Z}/p\mathbb{Z})$, onde $x_0, y_0 \in \mathbb{Z}$ são os elementos cuja existência é garantida no Lema acima, então $z \neq 0$ e $N(z) = \overline{1} + \overline{x}_0^2 + \overline{y}_0^2 = \overline{0} \in \mathbb{Z}/p\mathbb{Z}$. Em particular, $\mathbb{H}(\mathbb{Z}/p\mathbb{Z})$ não é um anel de divisão, embora $\mathbb{Z}/p\mathbb{Z}$ seja um corpo.

De posse dos resultados acima, estamos em condições de demonstrar o Lema 2.13 e, conseqüentemente, o Teorema 2.11.

Demonstração do Lema 2.13: dado um número primo $p > 2$, temos $pz = zp$ para todo $z \in \mathsf{H}$, pois $z \in \mathbb{Z}$ é um escalar. Logo $\mathsf{H}p = p\mathsf{H}$, isto é, $p\mathsf{H}p^{-1} \subset \mathsf{H}$ e faz sentido considerarmos o quociente $\mathsf{H}/p\mathsf{H}$. Pelo Lema 2.12, item 1, $\mathbb{H}(\mathbb{Z}) \subset \mathsf{H}$, logo podemos considerar o homomorfismo $\psi : \mathbb{H}(\mathbb{Z}) \to \mathsf{H}/p\mathsf{H}$ dada por $z \mapsto z + p\mathsf{H}$.

Afirmamos que ψ é sobrejetivo. De fato, dado $z + p\mathsf{H} \in \mathsf{H}/p\mathsf{H}$, se $z \in \mathsf{H}_1 = \mathbb{H}(\mathbb{Z})$, temos $\psi(z) = z + p\mathsf{H}$. Se $z \in \mathsf{H}_{1/2}$, então $z = \frac{a}{2} + \frac{b}{2}\mathbf{i} + \frac{c}{2}\mathbf{j} + \frac{d}{2}\mathbf{k}$, com $a, b, c, d \in \mathbb{Z}$ ímpares. Assim,

$$z = \frac{a-p}{2} + \frac{b-p}{2}\mathbf{i} + \frac{c-p}{2}\mathbf{j} + \frac{d-p}{2}\mathbf{k} + p \cdot \frac{1}{2}(1 + \mathbf{i} + \mathbf{j} + \mathbf{k}).$$

Como p também é ímpar, $\frac{a-p}{2}, \frac{b-p}{2}, \frac{c-p}{2}, \frac{d-p}{2} \in \mathbb{Z}$. Logo, $z - z' \in p\mathsf{H}$, onde

$$z' = \frac{a-p}{2} + \frac{b-p}{2}\mathbf{i} + \frac{c-p}{2}\mathbf{j} + \frac{d-p}{2}\mathbf{k} \in \mathbb{H}(\mathbb{Z}).$$

Conseqüentemente, $\psi(z') = z$ e ψ é sobrejetiva.

O núcleo de ψ é dado por

$$\ker(\psi) = \{z \in \mathbb{H}(\mathbb{Z}) \mid \psi(z) = 0\} = \{z \in \mathbb{H}(\mathbb{Z}) \mid z \in p\mathsf{H}\}.$$

Agora, $z \in p\mathsf{H}$ se e somente se

$$z = \frac{p}{2}(a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}), \tag{7}$$

onde a', b', c', d' são todos pares (e $z \in \mathsf{H}_1$) ou todos ímpares (e $z \in \mathsf{H}_{1/2}$). Denotando $z = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, a igualdade (7) implica que $2a = pa'$, $2b = pb'$, $2c = pc'$ e $2d = pd'$. Como p é um primo ímpar, temos $p|a$, $p|b$, $p|c$ e $p|d$. Logo, $z = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in p\mathbb{H}(\mathbb{Z})$. Segue que $\ker(\psi) \subset p\mathbb{H}(\mathbb{Z})$ e vale mesmo a igualdade, pois a outra inclusão é imediata.

Pelo teorema dos isomorfismos de anéis, temos $\mathbb{H}(\mathbb{Z})/p\mathbb{H}(\mathbb{Z}) \simeq \mathsf{H}/p\mathsf{H}$. Desse isomorfismo e do Lema 2.14 segue que

$$\mathsf{H}/p\mathsf{H} \simeq \mathbb{H}(\mathbb{Z}/p\mathbb{Z}). \tag{8}$$

Pelo Lema 2.10, existe $\omega \in \mathbb{H}(\mathbb{Z}/p\mathbb{Z})$ tal que $\omega \neq 0$ e $N(\omega) = 0$ (veja a observação na página 18, logo após a demonstração do Lema 2.10). O elemento ω não é invertível, logo gera um ideal

não trivial à direita em $\mathbb{H}(\mathbb{Z}/p\mathbb{Z})$ que corresponde, via o isomorfismo (8) a um ideal à direita $w\mathsf{H}$ de H tal que

$$p\mathsf{H} \subsetneq w\mathsf{H} \subsetneq \mathsf{H}.$$

Portanto, existe $w' \in \mathsf{H}$ tal que $N(w') \neq 1$ e $p = ww'$. Aplicando a norma a esta última igualdade, obtemos

$$p^2 = N(w)N(w').$$

Agora, $N(w)$ e $N(w')$ são números inteiros diferentes de 1 e cujo produto é p^2. Isso implica que $N(w) = N(w') = p$. Se $w = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathsf{H}_1$ então $p = N(w) = a^2 + b^2 + c^2 + d^2$, com $a, b, c, d \in \mathbb{Z}$, como queríamos.

Para finalizarmos, vamos tratar o caso em que $w \in \mathsf{H}_{1/2}$, isto é, $w = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, com $a, b, c, d \in \frac{1}{2} + \mathbb{Z}$.

Como $w \in \mathsf{H}_{1/2}$ temos $2w \in \mathbb{H}(\mathbb{Z})$. Seja ξ a imagem de $2w$ pela projeção

$$\mathbb{H}(\mathbb{Z}) \xrightarrow{\pi} \mathbb{H}(\mathbb{Z})/4\mathbb{H}(\mathbb{Z}) \simeq \mathbb{H}(\mathbb{Z}/4\mathbb{Z}),$$

onde o isomorfismo é garantido pelo Lema 2.14. Uma vez que $N(2w) = 4N(w) \in 4\mathbb{Z}$, temos $\xi\overline{\xi} = N(\xi) = 0$ em $\mathbb{Z}/4\mathbb{Z}$.

Estamos considerando $w \in \mathsf{H}_{1/2}$. Logo, $2a, 2b, 2c, 2d$ são ímpares e

$$2a, 2b, 2c, 2d \equiv \pm 1 \ (\mod 4).$$

Podemos então considerar o conjugado $\overline{\xi} = \pi(z')$, com $z' = \pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}$.

Seja $u = \frac{1}{2}z' \in \mathsf{H}$. Temos $N(u) = 1$ e $\pi((2w)(2u)) = \xi\overline{\xi} = 0 \in \mathbb{Z}/4\mathbb{Z}$, logo $4wu = 4a_0 + 4b_0\mathbf{i} + 4c_0\mathbf{j} + 4d_0\mathbf{k}$, com $a_0, b_0, c_0, d_0 \in \mathbb{Z}$. Portanto $wu \in \mathbb{H}(\mathbb{Z})$ e, como $p = N(w) = N(w)\overbrace{N(u)}^{=1} = N(wu)$, temos, finalmente, $p = a_0^2 + b_0^2 + c_0^2 + d_0^2$, com $a_0, b_0, c_0, d_0 \in \mathbb{Z}$, como queríamos. □

2.6 Problemas quantitativos

Nas seções anteriores vimos que um número inteiro positivo sempre pode ser escrito como soma de, no máximo, quatro quadrados. Vimos também critérios para decidir quando é suficiente um número menor de quadrados para expressar um número dado.

No entanto, não abordamos a questão quantitativa: **de quantos modos um determinado número pode ser escrito como soma de quadrados**? Iremos expor alguns resultados nesse sentido a seguir.

De início, precisamos distinguir o que são maneiras distintas de representar um número como soma de quadrados. Por exemplo,

$$5 = 1^2 + 2^2 = (-1)^2 + 2^2 = 1^2 + (-2)^2 = (-1)^2 + (-2)^2 =$$

$$= 2^2 + 1^2 = 2^2 + (-1)^2 = (-2)^2 + 1^2 = (-2)^2 + (-1)^2.$$

Logo, 5 pode ser decomposto como soma de dois quadrados de 8 maneiras distintas. Note que estamos considerando como distintas expressões que só diferem pela ordem em que as parcelas aparecem.

Teorema 2.15 *O número de maneiras de escrever $n \in \mathbb{Z}$, $n > 0$, como soma de dois quadrados é*

$$U(n) = 4 \cdot \sum_{\substack{u|n \\ u \ \text{ímpar}}} (-1)^{\frac{u-1}{2}}.$$

A função $\sigma : \mathbb{N} \to \mathbb{N}$, dada por $\sigma(n) = \sum_{d|n} d$, fornece a soma dos divisores **positivos** de n. Por exemplo, $\sigma(6) = 1 + 2 + 3 + 6 = 12$ e $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$. Números inteiros positivos n tais que $\sigma(n) = 2n$ são chamados *números perfeitos*.

Teorema 2.16 *Seja $Q(n)$ o número de modos de escrever $n \in \mathbb{Z}$, $n > 0$, como soma de quatro quadrados. Temos:*

1. *Se n é ímpar, então $Q(n) = 8 \cdot \sigma(n)$.*
2. *Se n é par e $n = 2^\ell u$, com u ímpar, então $Q(n) = 24 \cdot \sigma(u)$.*

Não demonstraremos esses resultados e estamos incluíndo os mesmos aqui simplesmente como informação adicional. O leitor interessado pode encontrar as demonstrações em [8], p.166, Teorema 163 e p.180, Teorema 172.

3 Representação de polinômios como somas de quadrados

Apesar de não termos mencionado, a discussão do capítulo anterior só tem sentido para inteiros positivos, ou seja, já sabemos de imediato que nenhum inteiro negativo pode ser soma de quadrados. Isso se dá pelo simples fato de que somas de quadrados de números reais são sempre não negativas.

No presente capítulo, estudaremos o problema análogo para polinômios, isto é, buscaremos condições que sejam necessárias e suficientes para que um dado polinômio possa ser escrito como soma de quadrados de outros polinômios. Veremos que essa tarefa nem sempre é realizável. No entanto, se não for possível escrever um determinado polinômio como soma de quadrados de outros polinômios, veremos que, ainda assim, é possível escrevê-lo como soma de quadrados de "funções racionais", que são funções do tipo $\frac{p(x_1,\ldots,x_n)}{q(x_1,\ldots,x_n)}$, onde $p(x_1, \ldots, x_n)$ e $q(x_1, \ldots, x_n)$ são polinômios.

Se $f(x_1, \ldots, x_n)$ é um polinômio em n indeterminadas, com coeficientes reais, e

$$f(x_1, \ldots, x_n) = p_1(x_1, \ldots, x_n)^2 + \cdots + p_r(x_1, \ldots, x_n)^2,$$

onde $p_1, \ldots, p_r$ são polinômios em n indeterminadas com coeficientes reais, então

$$f(a_1, \ldots, a_n) \geq 0 \tag{9}$$

para toda n-upla $(a_1, \ldots, a_n) \in \mathbb{R}^n$. Chamamos essa condição de **semi-positividade** e dizemos que um polinômio f satisfazendo (9) é **semi-positivo** (o prefixo "semi" se deve ao fato de f poder ser igual a zero para alguns pontos de $\mathbb{R}^n$).

O ímpeto inicial para nosso estudo é dado pela seguinte colocação:

> *Se um polinômio (com coeficientes reais) é soma de quadrados, então ele é semi-positivo. Vale a recíproca? Em outras palavras, todo polinômio semi-positivo, com coeficientes reais, é necessariamente soma de quadrados de polinômios (de funções racionais)?*

Essa questão foi parcialmente respondida por Hilbert e totalmente esclarecida por Artin em 1927, como já explicamos na Introdução. Iremos expor suas idéias no que se segue.

3.1 Corpos ordenados

A seguir, trabalharemos com certas **estruturas algébricas**, que são constituídas de três partes:

- Um conjunto não vazio K.
- Uma **soma** em K, isto é, uma função $K \times K \to K$ que associa a cada par (a, b) de elementos de K um terceiro elemento, chamado **soma de** a **e** b e denotado por $a + b$.
- Um **produto** em K, ou seja, uma função $K \times K \to K$ que associa a cada par (a, b) de elementos de K um terceiro elemento, chamado **produto de** a **e** b e denotado por $a \cdot b$.

Usamos a notação $(K, +, \cdot)$ para enfatizar que não estamos lidando apenas com um conjunto, mas com um conjunto onde é possível somar e multiplicar elementos. A soma e o produto de elementos de K são chamados **operações**. Por vezes, escreveremos apenas "K" e não faremos menção às operações. Faremos isso quando já for claro que operações estivermos usando.

Essas operações devem satisfazer algumas condições para que a estrutura $(K, +, \cdot)$ ganhe um nome especial. Em particular, queremos que nossas estruturas tenham propriedades similares às dos "conjuntos numéricos" com os quais trabalhamos usualmente: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$. A seguir, listamos as propriedades compartilhadas por esses conjuntos numéricos.

1. A soma é associativa, isto é, dados $a, b, c \in K$, $a + (b + c) = (a + b) + c$.

2. Existe um elemento $e \in K$ tal que $a + e = e + a = a$, para todo $a \in K$. É possível demonstrar que esse elemento é único (tente!). Ele é chamado **elemento neutro da operação soma**, e é denotado pelo símbolo 0.

3. Dado $a \in K$, existe $b \in K$ tal que $a + b = b + a = 0$. É possível mostrar que, dado a, o elemento b satisfazendo a condição anterior, é único (tente fazer isso!). Ele é chamado inverso aditivo de a e é denotado por $-a$.

4. A soma é comutativa: dados $a, b \in K$, $a + b = b + a$.

5. O produto é associativo, ou seja, dados $a, b, c \in K$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

6. Existe um elemento $u \in K$ tal que $u \cdot a = a \cdot u = a$, para todo $a \in K$. Podemos mostrar que esse elemento é único. Ele é chamado **elemento neutro da operação produto** e é denotado pelo símbolo 1.

7. O produto é comutativo: $a \cdot b = b \cdot a$.

8. Vale a distributividade do produto em relação à soma: dados $a, b, c \in K$,

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

   Essa propriedade garante que as duas operações são compatíveis.

Devemos notar que, em $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, o produto tem a seguinte propriedade adicional:

9. Dado $a \in K$, $a \neq 0$, existe $b \in K$ tal que $a \cdot b = b \cdot a = 1$. Para cada a, o elemento b é único, é chamado **inverso** de a e é denotado por a^{-1}.

Se $(K, +, \cdot)$ tem as propriedades 1 - 8, dizemos que $(K, +, \cdot)$ é um *anel comutativo com unidade*. Se, além disso, $(K, +, \cdot)$ tiver a propriedade 9, dizemos que $(K, +, \cdot)$ é um *corpo*.

Exemplos:

a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são anéis comutativos com unidade e, dentre esses, apenas $\mathbb{Z}$ não é corpo.

b) Seja A um anel comutativo com unidade e $A[x]$ o conjunto dos polinômios com coeficientes em A na indeterminada x. Com as operações usuais de soma e produto de polinômios, $A[x]$ é um anel comutativo com unidade.

c) Podemos considerar $B = A[x]$ como anel de coeficientes e formar um novo anel de polinômios $B[y]$ na indeterminada y, onde os coeficientes são polinômios em x. Pela construção feita no exmplo anterior, $B[y]$ também é um anel comutativo com unidade. Indicamos de modo simplificado $B[y] = A[x, y]$.

d) Procedendo indutivamente, podemos supor construído o anel $B = A[x_1, \ldots, x_{n-1}]$. Colocando $A[x_1, \ldots, x_n] = B[x_n]$, temos que $A[x_1, \ldots, x_n]$ é um anel comutativo com unidade em n indeterminadas ($n \geq 1$).

e) Dado um corpo K, seja $A = K[x_1, \ldots, x_n]$ o anel dos polinômios em n indeterminadas, com coeficientes em K. Podemos construir o *corpo de frações* de A, dado por

$$K(x_1, \ldots, x_n) = \left\{ \frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)} \quad | \quad p, q \in K[x_1, \ldots, x_n] \right\}.$$

1. Fixado um inteiro primo p, considere o conjunto $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ e escreva, para $a, b \in \mathbb{Z}_p$,

$$a + b = r, \text{ onde } r \text{ é o resto da divisão de } a + b \text{ por } p.$$

$$a \cdot b = s, \text{ onde } s \text{ é o resto da divisão de } a \cdot b \text{ por } p.$$

Com essas duas operações, $(\mathbb{Z}_p, +, \cdot)$ é um corpo **finito** com p elementos.

Vamos, agora, definir uma relação de ordem em um conjunto não vazio K, ou seja, uma maneira de comparar quaisquer dois elementos de K, dizendo qual dos dois é maior. Uma relação $\leq$ em K é dita **relação de ordem** se

O-1 $a \leq a$, para todo $a \in K$ (reflexividade).

O-2 Dados $a, b \in K$, se $a \leq b$ e $b \leq a$, então $a = b$ (simetria).

O-3 Dados $a, b, c \in K$, se $a \leq b$ e $b \leq c$, então $a \leq c$ (transitividade).

Usamos as notações usuais

$$a \geq b \Leftrightarrow b \leq a,$$

$$b < a \Leftrightarrow b \leq a \text{ e } b \neq a,$$

$$a > b \Leftrightarrow b < a.$$

O conjunto K juntamente com a ordem $\leq$ é chamado **conjunto ordenado**. Usamos a notação $(K, \leq)$ para indicar o conjunto e uma ordem definida sobre ele. Também dizemos que o conjunto é **parcialmente ordenado**. Se, dados $a, b \in K$, tivermos $a \leq b$ ou $b \leq a$, dizemos que o conjunto K é **totalmente ordenado**. Dizemos também que a ordem $\leq$ é **total**.

Uma **cadeia** em um conjunto ordenado é uma sequência

$$a_1 \leq a_2 \leq a_3 \leq \cdots \leq a_n \leq \cdots$$

Um conjunto ordenado é chamado **indutivo** se toda cadeia possui uma cota superior, isto é, existe $b \in K$ tal que $a_i \leq b$ para todo a_i pertencente à cadeia. Um elemento $m \in K$ é dito **maximal** se $a \in K$ e $m \leq a$ implicar $m = a$. O teorema abaixo é um resultado clássico da Teoria dos Conjuntos que apenas enunciaremos aqui.

Max Zorn (1906 - 1993)

Teorema 3.1 (Lema de Zorn) *Todo conjunto parcialmente ordenado e indutivo possui um elemento maximal.*

Se K é *simultaneamente um corpo e um conjunto ordenado*, dizemos que que $(K, +, \cdot, \leq)$ é um **corpo ordenado** se valem as seguintes relações de compatibilidade entre a estrutura de corpo (soma e produto) e a estrutura de ordem (relação $\leq$) em K:

C-1 Se $a, b, c \in K$ e $b \leq c$, então $a + b \leq a + c$.

C-2 Se $a, b, c \in K$, $0 \leq a$ e $b \leq c$, então $ab \leq ac$.

C-3 Dados $a, b \in K$, temos $a \leq b$ ou $b \leq a$, isto é, a ordem $\leq$ é total.

Observação: dado $a \in K$, é uma consequência das propriedades de definição de corpo que $a^2 = a \cdot a = (-a) \cdot (-a) = (-a)^2$. Logo, $a^2 \geq 0$, para todo $a \in K$ (por quê?).

Exemplos:

1. $\mathbb{Q}$ e $\mathbb{R}$ são corpos ordenados, mas $\mathbb{C}$ não é um corpo ordenado. De fato, pela observação feita acima, i^2 deveria ser ≥ 0, mas sabemos que $i^2 = -1 < 0$.

2. Um corpo finito $\mathbb{Z}_p$ não pode ser ordenado. De fato, em $\mathbb{Z}_p$, $p = 0$, onde a igualdade é na verdade uma identificação *módulo p*. Dado $a \in \mathbb{Z}_p$, $a > 0$, teríamos $\overbrace{a + \cdots + a}^{p} > 0$, ou seja, $0 = 0 \cdot a = p \cdot a > 0$, absurdo.

3. Se K é um corpo ordenado, então $K(x)$ também é um corpo ordenado. Defina primeiro em $K[x]$ uma ordem *lexicográfica*[11] do seguinte modo: dados dois polinômios $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ e $q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$, colocamos

$$p(x) \leq q(x), \text{ se } \begin{cases} a_0 \leq b_0 \text{ ou} \\ a_0 = b_0 \text{ e } a_1 \leq b_1 \text{ ou} \\ a_0 = b_0, a_1 = b_1 \text{ e } a_2 \leq b_2 \text{ ou} \\ \vdots \\ a_0 = b_0, a_1 = b_1, \ldots, a_{n-1} = b_{n-1} \text{ e } a_n \leq b_n. \end{cases}$$

   Usamos, nas desigualdades acima, o mesmo símbolo para a ordem de K e de $K[x]$.

   Exercício: verifique que a ordem lexicográfica $\leq$ definida acima é, de fato uma ordem total, ou seja, quaisquer dois polinômios podem ser comparados via $\leq$.

[11] Esta é a ordem em que as palavras aparecem em um dicionário.

A ordem de $K(x)$ pode, então, ser definida colocando-se

$$\frac{p(x)}{q(x)} \geq 0$$

quando $p(x) \geq 0$ e $q(x) > 0$ ou quando $p(x) \leq 0$ e $q(x) < 0$. Também chamamos essa ordem em $K(x)$ de lexicográfica. Observe que, com a ordem lexicográfica, $K(x)$ passa a ter elementos "infinitamente pequenos". Por exemplo, $0 < x = 0 + 1 \cdot x < a$, para todo $a \in K$, $a > 0$. Assim, x é menor do que qualquer elemento positivo de K. Por outro lado, $a < \frac{1}{x}$, para todo $a \in K$ (verifique!).

No exemplo acima, $K(x)$ foi ordenado lexicograficamente, estabelecendo-se primeiramente uma ordem em $K[x]$, dada pela comparação de coeficientes. Nessa comparação foi atribuído a um termo do polinômio um peso tanto maior quanto menor for o seu grau. Assim como, no dicionário, o peso maior é atribuído a letra que está mais à esquerda:

ALGAZARRA
ÁLGEBRA
ALGEBRISTA
ALGEMA

Podemos ordenar os polinômios escolhendo uma ordem **anti-lexicográfica** que nada mais é do que fazer o mesmo que antes, atribuíndo, agora, um peso tanto maior quanto maior o grau do polinômio. No dicionário isso teria o efeito de ordenar as palavras comparando a ordem das letras e atribuindo um peso tanto maior quanto mais à direita estivesse a letra. Por exemplo, as quatro palavras acima seriam reordenadas como:

ALGEMA
ÁLGEBRA
ALGAZARRA
ALGEBRISTA

Uma função $f : A \to B$ entre dois anéis A e B é chamada **homomorfismo de anéis** se

- $f(a + a') = f(a) + f(a')$ e
- $f(aa') = f(a)f(a')$.

Associados a um homomorfismo estão o seu **núcleo** $\ker f = \{a \in A \mid f(a) = 0\}$ e sua **imagem** $\mathrm{Im} f = \{f(a) \mid a \in A\}$. Um homomorfismo é injetivo se, e somente se, $\ker f = \{0\}$ e é sobrejetivo se, e somente se, $\mathrm{Im} f = B$. Um homomorfismo é dito bijetivo se for injetivo e sobrejetivo.

Um homomorfismo $f : A \to B$ bijetivo é chamado **isomorfismo**. Quando existe um isomorfismo entre A e B, dizemos que A e B são **isomorfos** e indicamos $A \simeq B$. Isso significa que A e B são indistinguíveis como anéis, ou seja, um é a cópia do outro do ponto de vista das operações soma e produto.

Exemplo: $f : \mathbb{R} \to \mathbb{C}$, dado por $f(x) = x + 0 \cdot i$ é um homomorfismo tal que $\ker f = \{0\}$ e $\mathrm{Im} f$ é o eixo real $\{x + 0 \cdot i \mid x \in \mathbb{R}\}$. Dessa forma, $f : \mathbb{R} \to \mathrm{Im} f$ é um isomorfismo, ou seja, o eixo real $\mathrm{Im} f$ é uma cópia fiel de $\mathbb{R}$ contida em $\mathbb{C}$. Quando afirmamos que "$\mathbb{R} \subset \mathbb{C}$" queremos dizer que existe essa cópia.

O núcleo $\ker f$ de um homomorfismo de anéis $f : A \to B$ é um **ideal** de A. Com isso, queremos dizer que $I = \ker f$ possui as seguintes propriedades:

1. $x, y \in I$ implica $x + y \in I$.
2. $a \in A$ e $x \in I$ implica $ax \in I$.

Em um corpo K, os únicos ideais são os triviais: $\{0\}$ e K. De fato, se $I \neq \{0\}$ é um ideal de K, então existe $x \in I$, $x \neq 0$. Como K é um corpo, há um elemento $y \in K$ tal que $yx = 1$. Como $y \in K$ e $x \in I$, a propriedade 2 da definição de ideal nos diz que $1 = yx \in I$. Agora, dado $a \in K$, $a = a \cdot 1 \in I$, novamente pela condição 2. Isso significa que $K \subset I$. Como I também é subconjunto de K, vale $I = K$.

A seguir, usaremos alguns resultados de álgebra abstrata, que não serão demonstrados aqui. Esses resultados são vistos em um curso de *Estruturas Algébricas* e podem ser encontrados em qualquer livro sobre esse assunto, por exemplo [1], [4], [6] ou [7].

O primeiro fato que usaremos é que todo ideal I de $\mathbb{Z}$ é do tipo $I = (a) = \{ak \mid k \in \mathbb{Z}\}$, ou seja, todo ideal de $\mathbb{Z}$ é formado pelos múltiplos de um certo elemento, chamado *gerador* do ideal. Ideais desse tipo, gerados por um só elemento, são denominados *principais*.

O segundo fato diz respeito ao anel quociente $\mathbb{Z}/(a)$. Se $x, y \in \mathbb{Z}/(a)$, $x \neq 0$, $y \neq 0$ e $xy = 0$, dizemos que x e y são *divisores de zero* em $\mathbb{Z}/(a)$. Por exemplo, em $\mathbb{Z}/(6) \simeq \mathbb{Z}_6$, $2 \cdot 3 = 0$ e $2 \neq 0$, $3 \neq 0$, donde 2 e 3 são divisores de zero em $\mathbb{Z}/(6)$. As afirmações abaixo são equivalentes:

- $\mathbb{Z}/(a)$ não tem divisores de zero e $a \neq 0$.
- $\mathbb{Z}/(a)$ é um corpo.
- $a \in \mathbb{Z}$ é primo.

Vale salientar que esses fatos são de fácil verificação. Se não os demonstramos aqui é para não nos desviarmos excessivamente da nossa linha de raciocínio.

O terceiro fato, menos trivial do que os outros dois, é o que conhecemos como *Teorema do Isomorfismo*. Ele afirma que, se $f : A \to B$ é um homomorfismo de anéis, então

$$A/\ker f \simeq \mathrm{Im} f,$$

onde $A/\ker f$ é o anel quociente de A pelo ideal $\ker f$.

Considere um corpo K e o homomorfismo $f : \mathbb{Z} \to K$ dado por $f(0) = 0$, $f(n) = \overbrace{1 + \cdot + 1}^{n}$, se $n > 0$, e $f(n) = \overbrace{-1 - \cdots - 1}^{-n}$, se $n < 0$. Pelo Teorema do Isomorfismo, temos que $\mathbb{Z}/\ker f \simeq \mathrm{Im} f \subset K$. Sendo subconjunto de um corpo, $\mathrm{Im} f$ não possui divisores de zero, logo $\mathbb{Z}/\ker f$ também não possui divisores de zero, pois é isomorfo a $\mathrm{Im} f$. Como $\ker f = (a)$, temos duas situações: se $a \neq 0$, pelas observações feitas acima, a é um número primo e $\mathbb{Z}_a$ possui uma cópia contida em K. Se $a = 0$, então $\ker f = \{0\}$ e f é injetivo. Logo, $\mathbb{Z}$ possui uma cópia condida em K. Como K é corpo, podemos afirmar que $\mathbb{Q}$ possui uma cópia contida em K.

A **característica** de um corpo K é o inteiro a do parágrafo anterior. Denotamos $a = \mathrm{car}\, K$. Pelo que vimos acima, a característica de um corpo só pode ser 0 ou um número primo p. Se um corpo K tem característica 0, então existe uma cópia de $\mathbb{Q}$ contida em K. Se, por outro lado, K tem característica igual a p, um primo, então existe uma cópia de $\mathbb{Z}_p$ contida em K. sobre corpos ordenados, podemos afirmar o seguinte.

Teorema 3.2 *Um corpo ordenado tem característica* 0.

Demonstração: se a carcterística do corpo K não é zero, tem que ser igual a um primo p. Logo, $\mathbb{Z}_p$ possui uma cópia contida em K. Se pudéssemos ordenar K sua ordem induziria uma ordem em $\mathbb{Z}_p$, o que já vimos ser impossível. □

Sejam $K \subset L$ corpos, com as mesmas operações. Dizemos que K é **subcorpo** de L, ou que L é uma **extensão** de K. Indicamos isso com a notação $L \mid K$. Podemos ver L como um espaço vetorial sobre K. A dimensão $\dim_K L$ de L como espaço vetorial sobre K é chamada **grau** da extensão $L \mid K$ e denotada por $[L : K]$. Se $[L : K] = n \in \mathbb{N}$, dizemos que que $L \mid K$ é uma extensão **finita**. Se $[L : K] = 2$, dizemos que $L \mid K$ é uma extensão **quadrática**.

3.2 Cones positivos e pré-ordens

Seja K um corpo ordenado. Já vimos, no final da seção anterior, que em geral K pode ser ordenado de várias maneiras. Para cada ordem $\leq$ de K, consideremos o conjunto

$$P = \{x \in K \mid 0 \leq x\}$$

dos elementos de K que são não negativos. Chamamos P de **cone positivo** associado à ordem $\leq$. Podemos recuperar a ordem $\leq$ a partir de P, colocando, para $a, b \in K$,

$$a \leq b \Leftrightarrow b - a \in P.$$

Assim, o estudo das ordens de K pode ser feito estudando-se os cones positivos de K. Por essa razão alguns autores chamam P também de *ordem* em K.

A seguir, iremos traduzir as propriedades da ordem $\leq$ em termos do seu cone positivo P.

1. $0 \in P$ (reflexividade).

2. $P \cap -P = \{0\}$, onde $-P = \{-x \mid x \in P\}$ (simetria).

3. $P + P \subset P$ (transitividade e C-1).

4. $P \cdot P \subset P$ (C-2).

5. $P \cup -P = K$ (C-3).

Podemos, então desenvolver nosso estudo independentemente da relação $\leq$, começando com um subconjunto não vazio $P \subset K$ que satisfaz as condições acima e chamando-o de **ordem**, ou mesmo **cone positivo**. Um corpo com um subconjunto distinguido P satisfazendo as condições acima, é dito **ordenado**. Adotaremos esse ponto de vista aqui.

A observação feita na página 24 nos diz que $a^2 \geq 0$, para todo $a \in K$. Se denotarmos por

$$K^2 = \{a^2 \mid a \in K\},$$

temos, então, que $K^2 \subset P$. Mais geralmente, usamos a notação $\sum K^2$ para o conjunto formado pelas somas finitas de quadrados de elementos de K, ou seja,

$$\sum K^2 = \left\{ \sum_{i=1}^{n} a_i^2 \mid n \in \mathbb{N}, a_i \in K \right\}.$$

Como P é "fechado para a soma", temos que $K^2 \subset P$ implica

$$\sum K^2 \subset P.$$

J.-P. Serre (1926 -)

Um corpo é dito **formalmente real** se $-1 \notin \sum K^2$, ou seja, -1 não pode ser escrito como soma de um número finito de quadrados de elementos de K. Uma das nossos objetivos a seguir é demonstrar que um corpo é formalmente real se, e somente se, é ordenado.

Uma das implicações é clara. De fato, suponhamos que K seja um corpo ordenado. Se $-1 \in \sum K^2$ teríamos $-1 \in P$, logo $-P = P$ e $P = P \cap -P = \{0\}$. Daí $K = P \cup -P = \{0\}$, o que não ocorre, pois K é um corpo não trivial[12], isto é, tal que $1 \neq 0$. Dessa forma, temos $-1 \notin \sum K^2$ e K é formalmente real.

Para mostrar a recíproca, isto é, que todo corpo formalmente real admite uma ordem, usaremos a noção de *pré-ordem*, introduzida pelo matemático francês Jean-Pierre Serre em 1949.

Uma **pré-ordem** em K é um subconjunto <u>próprio</u> $T \subset K$ tal que

[12] O corpo $K = \{0\}$ é chamado corpo trivial. Como ele só tem um elemento, é forçoso que $1 = 0$, isto é, os elementos neutros da soma e do produto coincidem. Esse corpo tem pouco ou nenhum interesse do ponto de vista prático.

1. $T + T \subset T$ e $TT \subset T$.

2. $K^2 \subset T$.

Lema 3.3 *Um corpo K de característica 0 é formalmente real se, e somente se, $\sum K^2$ é uma pré-ordem de K, que chamaremos* **pré-ordem fraca** *de K.*

Demonstração: é imediato que $\sum K^2$ satisfaz os itens 1 e 2 da definição de pré-ordem. Assim, a única possível obstrução para que $\sum K^2$ não seja uma pré-ordem é que $\sum K^2$ não seja subconjunto próprio de K, isto é, $\sum K^2 = K$. Claro que, se K é formalmente real, então $-1 \notin \sum K^2$ e, portanto, $\sum K^2 \neq K$.

Reciprocamente, suponha que $-1 \in \sum K^2$. Como todo $x \in K$ pode ser escrito na forma

$$x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2$$

(é possível divir por 2 em K pois sua característica é zero) temos que

$$x = \left(\frac{x+1}{2}\right)^2 + (-1) \cdot \left(\frac{x-1}{2}\right)^2 \in K^2 + (-1) \cdot K^2 \subset \sum K^2.$$

Portanto, se $-1 \in \sum K^2$, então $\sum K^2 = K$. Tomando essa implicação na forma contrapositiva, obtemos o seguinte: *se $\sum K^2$ é uma pré-ordem, então K é formalmente real.* □

Notemos, ainda, que se T é uma pré-ordem de K, então $\sum K^2 \subset T$, de modo que a pré-ordem fraca é a menor dentre todas as pré-ordens (em relação à inclusão). Como veremos mais adiante, há corpos ordenados para os quais a única pré-ordem possível é a fraca. Outra observação importante: se $t \in T$ e $t \neq 0$, então $t^{-1} = t \cdot (t^{-1})^2 \in T \cdot K^2 \subset T \cdot T \subset T$.

Toda ordem é um pré-ordem. Mostraremos, a seguir, que ordens são exatamente as pré-ordens maximais em relação á inclusão. Consideremos, de início, para uma pré-ordem T e $a \in K$, a notação

$$T[a] = T + a \cdot T = \{t_1 + at_2 \mid t_1, t_2 \in T\}.$$

Lema 3.4 *Seja $T \subset K$ uma pré-ordem e $a \in K$, $a \neq 0$. Então $T[a]$ é uma pré-ordem se, e somente se, $a \notin -T$.*

Demonstração: suponha que $a \notin -T$. Nesse caso, $-1 \notin T[a]$, do contrário, poderíamos escrever $-1 = t_1 + at_2$, com $t_1, t_2 \in T$ e $t_2 \neq 0$, daí $-t_2 a = 1 + t_1 \in T$, o que implicaria $a = -t_2^{-1}(1 + t_1) \in -T$, contradizendo a hipótese. Logo $T[a]$ é uma pré-ordem.

Reciprocamente, se $a \in -T$, então $(-a) \cdot a \in T[a]$ o que implica que $-1 \in T[a]$ e $T[a]$ não é uma pré-ordem. □

Corolário 3.5 *Uma pré-ordem $T \subset K$ é maximal (em relação à inclusão) se, e somente se, T é uma ordem.*

Demonstração: se T é uma ordem e $T \subset T'$, com T' pré-ordem, então $T' = T$ ou $T' = K$. De fato, se $T' \neq T$, então existe $t \neq 0$, $t \in T' \cap -T \subset T' \cap -T'$. Isso implica que $-1 = -t \cdot t^{-1} \in T'$ e daí $T' = K$.

Reciprocamente, seja $T' \subset K$ maximal e $a \in K$, $a \notin T$. Então $T[a]$ não é pré-ordem, logo, pelo Lema 3.4, $a \in -T$, ou seja, $T \cup -T = K$ e T é uma ordem. □

Corolário 3.6 *Toda pré-ordem $T \subset K$ está contida em pelo menos uma ordem de K.*

Demonstração: a família $\mathcal{F}$ formada por todas as pré-ordens de K que contêm T é um conjunto parcialmente ordenado pela inclusão. Uma cadeia de elementos de $\mathcal{F}$ tem sempre uma cota superior, logo $\mathcal{F}$ é indutivo e, pelo Lema de Zorn (Teorema 3.1 da página 24) existe um elemento maximal $P \in \mathcal{F}$. Pelo Corolário 3.5, P é uma ordem de K (contendo T). □

Teorema 3.7 (Artin-Schreier, 1925) *Um corpo é formalmente real se, e somente se, é ordenado.*

Demonstração: já mostramos que um corpo ordenado é formalmente real. Reciprocamente, se K é um corpo formalmente real, então $\sum K^2$ é uma pré-ordem e, pelo Corolário 3.6, existe uma ordem P em K, contendo $\sum K^2$. Logo, K é ordenado. □

No que se segue, usaremos a notação X_K para indicar o conjunto das ordens de um corpo formalmente real K e X/T para indicar o conjunto das ordens de K que contêm a pré-ordem T.

Teorema 3.8 (Artin) *Seja K um corpo formalmente real. Dada uma pré-ordem T de K,*

$$T = \bigcap_{P \in X/T} P.$$

Em particular,

$$\sum K^2 = \bigcap_{P \in X_K} P.$$

Demonstração: a inclusão $T \subset \bigcap_{P \in X/T} P$ é imediata. Vamos mostrar a inclusão inversa na forma contrapositiva. Se $a \notin T$, então, pelo Lema 3.4, $T[-a]$ é uma pré-ordem. Logo, existe euma ordem $P_0 \in X_K$ que contém $T[-a]$. Assim $P_0 \supset T[-a] \supset T$ implica $P_0 \in X/T$, enquanto $-a \in P_0$ implica que $a \notin P_0$. Logo, $a \notin \bigcap_{P \in X/T} P$. Mostramos, portanto, que $a \notin T$ implica $a \notin \bigcap_{P \in X/T} P$, o que é equivalente a mostrar a inclusão desejada. □

O Teorema 3.8 de Artin nos diz que $a \in K$ é positivo em relação a todas as ordens de K se e somente se é uma soma de quadrados de lementos de K. Essa é uma ferramenta essencial para a resolução do problema de Hilbert do qual trataremos na seção seguinte.

3.3 O 17º problema de Hilbert

No final do século XIX, David Hilbert, em conexão com seus trabalhos sobre os fundamentos da Geometria, obteve alguns resultados sobre positividade de polinômios que o levaram a estabelecer a seguinte conjectura.

Conjectura 3.9 *Seja $f \in \mathbb{R}[x_1, \ldots, x_n]$ um polinômio com n indeterminadas e coeficientes reais. Se $f(a_1, \ldots, a_n) \geq 0$, para todo $(a_1, \ldots, a_n) \in \mathbb{R}^n$, então f é uma soma de quadrados de polinômios em $\mathbb{R}[x_1, \ldots, x_n]$.*

Hilbert demonstrou que essa conjectura é verdadeira se $n = 1$:

Proposição 3.10 *Suponha que $f \in \mathbb{R}[x]$ e $f \neq 0$, isto é, não é identicamente nulo. Seja*

$$f(x) = a \prod_i (x - a_i)^{k_i} \cdot \prod_j ((x - b_j)^2 + c_j^2)^{\ell_j}$$

a fatoração de f como produto de irredutíveis[13] em $\mathbb{R}[x]$. Então as seguintes afirmações são equivalentes:

1. *$f(a) \geq 0$, para todo $a \in \mathbb{R}$.*
2. *$d > 0$ e k_i é par, para todo i.*
3. *$f = g^2 + h^2$, com $g, h \in \mathbb{R}[x]$.*

Demonstração:[10] a única implicação que não é imediata é $2 \Rightarrow 3$. Para demonstrá-la, basta usar a identidade de Brahmagupta-Fibonacci (veja a página 5). □

No entanto, a Conjectura 3.9 é **falsa** se $n \geq 2$. O próprio Hilbert demonstrou isso em 1888 (!), mas sem exibir um contra-exemplo. O primeiro exemplo que polinômio positivo que não é soma de quadrados de polinômios foi dado pelo matemático norte amenricano de origem judaico-russa Theodore Samuel Motzkin em 1967. O exemplo de Motzkin é o polinômio de duas indeterminadas

Motzkin (1908 - 1970)

$$M(x, y) = 1 - 3x^2y^2 + x^2y^4 + x^4y^2.$$

Sobre esse polinômio, temos o seguinte resultado:

Teorema 3.11 *Seja M o polinômio dado acima. Então:*

(1) *$M(a, b) \geq 0$, para todo $(a, b) \in \mathbb{R} \times \mathbb{R}$.*

[13] Válida pelo Teorema Fundamenteal da Álgebra.

(2) *M não é uma soma de quadrados em $\mathbb{R}[x,y]$.*

Demonstração:[10] (1) Use a desigualdade

$$\frac{a+b+c}{3} \geq \sqrt[3]{abc}, \text{ se } a,b,c \geq 0$$

com $a=1$, $b=x^2y^4$ e $c=x^4y^2$.

(2) Suponha que $M(x,y)=\sum_{i=1}^{r} f_i(x,y)^2$, com $f_i(x,y) \in \mathbb{R}[x,y]$. Como o grau de $M(x,y)$ é 6, cada f_i tem grau no máximo 3, logo é combinação linear, com coeficientes em $\mathbb{R}$, de

$$1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3.$$

Se x^3 aparecesse em algum f_i x^6 apareceria em M com coeficiente positivo. Logo nenhum dos f_i tem x^3 como termo. De modo análogo, y^3, x^2, y^2, x e y também não aparecem. Portanto,

$$f_i(x,y) = a_i + b_i xy + c_i x^2 y + d_i xy^2.$$

Comparando coeficientes, concluímos que a igualdade $M=\sum_i f_i^2$ implica que $-3=\sum_i b_i^2$, o que é absurdo, pois $b_i \in \mathbb{R}$ para cada i. □

Embora não seja soma de quadrados de polinômios, o polinômio de Motzkin admite a representação

$$M(x,y) = \left(\frac{x^2y(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{xy^2(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{xy(x^2+y^2-2)}{x^2+y^2}\right)^2 + \left(\frac{x^2-y^2}{x^2+y^2}\right)^2$$

como soma de quatro quadrados de funções racionais, ou seja, elementos de $\mathbb{R}(x,y)$.

Vamos tratar o problema de representar um polinômio positivo como soma de quadrados de polinômios no apêndice.

Diante da não validade da primeira conjectura, Hilbert reformulou-a e colocou-a como uma dos 23 problemas apresentados no congresso internacional de matemáticos em 1900 em Paris. Esse era o décimo sétimo problema:

Conjectura 3.12 (17º problema de Hilbert) *Seja $f \in \mathbb{R}[x_1,\ldots,x_n]$ um polinômio com n indeterminadas e coeficientes reais. Se $f(a_1,\ldots,a_n) \geq 0$, para todo $(a_1,\ldots,a_n) \in \mathbb{R}^n$, então $f \in \sum K^2$, onde $K=\mathbb{R}(x_1,\ldots,x_n)$.*

O último ingrediente do qual necessitamos para demonstrar a validade da Conjectura 3.12 acima, é um teorema de Lógica Matemática, conhecido como *princípio da transferência* de Tarski. Lembremos que uma extensão ordenada de $\mathbb{R}$ é um corpo ordenado K que contém $\mathbb{R}$ e tal que a ordem de $\mathbb{R}$ é dada pela restrição de qualquer ordem de K a $\mathbb{R}$. De outro modo, se $P \in X_K$, então $P \cap \mathbb{R} = \mathbb{R}^2$.

Teorema 3.13 (Princípio da Transferência - Tarski) *Suponha que $(K, \leq)$ é uma extensão ordenada de $(\mathbb{R}, \leq)$ e que existe $(x_1, \ldots, x_n) \in K^n$ satisfazendo algum conjunto finito de equações e inequações com coeficientes em $\mathbb{R}$. Então existe $(a_1, \ldots, a_n) \in \mathbb{R}^n$ satisfazendo as mesmas equações e inequações.*

Demonstração de 3.12: suponha que $f(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ não é soma de quadrados de funções racionais, isto é, $f \notin \sum K^2$, onde $K = \mathbb{R}(x_1, \ldots, x_n)$. Então, como

$$f \notin \bigcap_{P \in X_K} P,$$

existe uma ordem P_0 de K tal que $f \notin P_0$, ou seja, $f(x_1, \ldots, x_n) < 0$ em relação a essa ordem.

Temos que $K \supset \mathbb{R}$ é uma extensão ordenada de $\mathbb{R}$. Pelo princípio de Tarski, existe $(a_1, \ldots, a_n) \in \mathbb{R}^n$ tal que $f(a_1, \ldots, a_n) < 0$. □

Alfred Tarski (1902 - 1983)

4 Apêndice: o teorema de Hilbert sobre polinômios positivos

Resumo

Seguindo argumentos de Choi e Lam (cf. [3]) e usando exemplos explícitos de formas positivas que não são somas de quadrados, exibimos uma demonstração do Teorema de Hilbert, de 1888, que caracteriza os polinômios que são somas de quadrados de polinômios.

4.1 Introdução

Um polinômio $f(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ é dito **positivo semidefinido** (ou, simplesmente, **positivo**) se $f(a) \geq 0$, para todo $a = (a_1, \ldots, a_n) \in \mathbb{R}^n$. Se existem $h_1, \ldots, h_r \in \mathbb{R}[x_1, \ldots, x_n]$ tais que $f = h_1^2 + \cdots + h_r^2$, dizemos que f é uma **soma de quadrados**. Usamos as notações $p_{n,d}$ para o conjunto dos polinômios positivos com n indeterminadas e grau d, necessariamente par, e $\sigma_{n,d}$ para o conjunto dos polinômios de n indeterminadas e grau d (d par) que são somas de quadrados. Como somas de quadrados de números reais não podem ser negativas, temos $\sigma_{n,d} \subset p_{n,d}$.

Em 1888, David Hilbert demonstrou que $\sigma_{n,d} = p_{n,d}$ se, e somente se, $n = 1$ e d é par, ou $d = 2$ e $n \geq 1$, ou $(n, d) = (2, 4)$. Hilbert trabalhou com polinômios homogêneos, também chamados de **formas**, que são polinômios $F(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ de grau d tais que $F(\lambda x_1, \ldots, \lambda x_n) = \lambda^d p(x_1, \ldots, x_n)$. A vantagem de trabalhar com formas é que todos os termos (monômios) de uma forma têm o mesmo grau.

Toda forma F se anula na origem, isto é, $F(0, \ldots, 0) = 0$. Se uma forma $p \in \mathbb{R}[x_1, \ldots, x_n]$ se anula em um ponto $a = (a_1, \ldots, a_n) \in \mathbb{R}^n \setminus \{(0, \ldots, 0)\}$, então ela também se anula em quelquer ponto $(\lambda a_1, \ldots, \lambda a_n)$ da reta determinada pelo ponto a e pela origem. Assim, o ambiente geométrico natural onde devemos considerar formas é o espaço projetivo real de dimensão $n - 1$, $\mathbb{P}^{n-1}$, que é o conjunto das retas de $\mathbb{R}^n$ que passam pela origem:

$$(a_1 : \cdots : a_n) = \{(\lambda a_1, \ldots, \lambda a_n) \mid \lambda \in \mathbb{R}\}.$$

Dado um polinômio $f(x_1, \ldots, x_n)$ de grau d em n variáveis, o polinômio $f_h(x_1, \ldots, x_n, x_{n+1}) = x_{n+1}^d f(\frac{x_1}{x_{n+1}} \ldots, \frac{x_n}{x_{n+1}})$ é um polinômio homogêneo, chamado **homogenização** de f. É possível recuperar f a partir de f_h, pois $f_h(x_1, \ldots, x_n, 1) = f(x_1, \ldots, x_n)$.

Se $f(x_1, \ldots, x_n)$ é um polinômio positivo de grau d par, então

$$f_h(x_1, \ldots, x_{n+1}) = x_{n+1}^d f(\frac{x_1}{x_{n+1}} \ldots, \frac{x_n}{x_{n+1}})$$

também é positivo. Reciprocamente, se f_h é positivo, então f é positivo. Da mesma forma, f é soma de quadrados se, e somente se, f_h o é. Assim, as funções $f \mapsto f_h$ e $f_h \mapsto f$ definidas acima, estabelecem correspondências

$$p_{n,d} \leftrightarrow P_{n+1,d} \quad \text{e} \quad \sigma_{n,d} \leftrightarrow \Sigma_{n+1,d},$$

onde $P_{n+1,d}$ e $\Sigma_{n+1,d}$ são os conjuntos formados pelos polinômios homogêneos que são positivos e somas de quadrados, respectivamente.

Esses argumentos mostram que, para resolver totalmente o problema, é suficiente trabalharmos com formas. O resultado de Hilbert pode, então, ser enunciado da seguinte maneira:

Teorema 4.1 (Hilbert, 1888) *Seja $P_{n,d}$ o conjunto das formas positivas semidefinidas com n indeterminadas e grau d (necessariamente par) e seja $\Sigma_{n,d}$ o conjunto das formas que são somas de quadrados. Então $P_{n,d} = \Sigma_{n,d}$ se, e somente se,*

(1) $n = 2$ e d é um número natural par.

(2) $d = 2$ e n é um número natural.

(3) $(n, d) = (3, 4)$.

Os casos (1) e (2) podem ser considerados "casos triviais", pois decorrem de teoremas gerais e básicos, como veremos na próxima seção. O caso excepcional (3) será tratado na seção 3, seguindo a demonstração de Choi e Lam, [3].

4.2 Os casos "triviais"

Vamos mostrar que $P_{2,d} = \Sigma_{2,d}$, se d é par, e também que $P_{n,2} = \Sigma_{n,2}$. Esses casos podem ser vistos como "triviais" pois fazem uso apenas de dois resultados clássicos: o Teorema Fundamental da Álgebra e o Teorema sobre diagonalização de matrizes simétricas.

Vamos começar pelo caso em que $n = 2$. Seja $F \in P_{2,d}$, isto é, F é uma forma de grau d (par) em duas indeterminadas. Podemos escrever

$$F = F(x, y) = \sum_{i+j=d} x^i y^j = \sum_{i=0}^{d} x^i y^{d-i} = y^d \sum_{i=0}^{d} \left(\frac{x}{y}\right)^i.$$

Fazendo $t = x/y$, obtemos $\sum_{i=0}^{d} (x/y)^i = P(t)$, onde $P(t) = \sum_{i=0}^{d} t^i$. Como d é par e F é um polinômio positivo, P é também positivo, isto é, $P(t) \geq 0$, para todo $t \in \mathbb{R}$. Pelo Teorema Fudamental da Álgebra,

$$P(t) = (t - a_1)^{m_1} \cdots (t - a_r)^{m_r} \cdot q_1(t)^{\ell_1} \cdots q_s(t)^{\ell_s},$$

onde $a_1, \ldots, a_r$ são as raízes reais de $P(t)$ e $m_1, \ldots, m_r \in \mathbb{N}$ são suas multiplicidades, todas pares, pois P é positivo. Para cada $1 \leq j \leq s$, $q_j(t)$ é um polinômio quadrático, cujas raízes são números complexos conjugados. No caso em que $\ell_j < 0$, para manter a positividade de P é necessário supor que $q_j(t)$ é positivo para qualquer t real. Isso significa que $q_j(t) = a_j t^2 + b_j t + c_j$, com $a_j, b_j, c_j \in \mathbb{R}$, $a_j > 0$ e $\Delta_j = b_j^2 - 4a_j c_j < 0$. Dessa forma, se ℓ_j é ímpar, o polinômio

$$q_j(t) = a_j \left[\left(t + \frac{b_j}{2a_j} \right)^2 + \left(\frac{-\Delta_j}{4a_j^2} \right) \right]$$

é soma de dois quadrados.

Concluímos então que $P(t)$ é o produto de polinômios que são, ou quadrados ou somas de dois quadrados. A identidade $(a^2+b^2)\cdot(c^2+d^2) = (ac-bd)^2+(ad+bc)^2$ garante que o produto de uma soma de dois quadrados por outra soma de dois quadrados é ainda uma soma de dois quadrados. Assim, o polinômio $P(t)$ é soma de dois quadrados e

$$F(x,y) = y^d \cdot P(x/y) = (y^{d/2})^2 \cdot P(x/y)$$

é soma de dois quadrados. Isso mostra que $P_{2,d} \subset \Sigma_{2,d}$. Como a outra inclusão sempre é válida, tem-se a igualdade.

Seja, agora, $F \in P_{n,2}$, ou seja,

$$F(x_1,\ldots,x_n) = \sum_{\substack{1\le i\le n\\ 1\le j\le n}} a_{ij}x_ix_j$$

é uma **forma quadrática** de dimensão n. Para que os coeficientes de F sejam simétricos, podemos considerar

$$F(x_1,\ldots,x_n) = \sum_{\substack{1\le i\le n\\ 1\le j\le n}} b_{ij}x_ix_j,$$

onde

$$b_{ij} = \begin{cases} a_{ij} & se \quad i=j \\ a_{ij}/2 & se \quad i\neq j \end{cases}$$

Assim,

$$F(x_1,\ldots,x_n) = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

onde $B = (b_{ij})$ é uma matriz simétrica. Um resultado clássico da Álgebra Linear, afirma que toda matriz simétrica é diagonalizável, isto é, existe uma matriz não-singular $P = (p_{ij})$ (ou seja, $\det P \neq 0$) tal que $P^{-1}\cdot B\cdot P = D$, sendo

$$D = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix}$$

uma matriz diagonal. Assim, $B = P\cdot D\cdot P^{-1}$ e

$$F(x_1,\ldots,x_n) = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \cdot P \cdot \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix} \cdot P^{-1} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Agora,

$$\begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \cdot P = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \cdot \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix} = \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix},$$

onde $y_j = x_1p_{1j} + \cdots + x_np_{nj}$, para cada $1 \leq j \leq n$. A matriz P fornece, portanto, uma mudança de variáveis em F de modo que

$$F(y_1, \ldots, y_n) = \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \lambda_1 y_1^2 + \cdots + \lambda_n x_n^2.$$

Uma vez que $F(y_1, \ldots, y_n) \geq 0$, para qualquer $(y_1, \ldots, y_n) \in \mathbb{R}^n$, temos $\lambda_1 = F(1, 0, \ldots, 0) \geq 0, \ldots, \lambda_n = F(0, \ldots, 0, 1) \geq 0$. Assim,

$$F(y_1, \ldots, y_n) = (\sqrt{\lambda_1}y_1)^2 + \cdots (\sqrt{\lambda_n}y_n)^2$$

é uma soma de quadrados de polinômios. Isso mostra que $P_{n,2} = \Sigma_{n,2}$.

4.3 O Teorema de Krein-Milman para cones

Nesta seção apresentaremos um resultado clássico descoberto por H. Minkowski (1911) e generalizado por Krein e Milman (1940). A versão que iremos aplicar mais adiante vale para cones, que definiremos a seguir.

Um conjunto $S \subset \mathbb{R}^n$ é chamado **cone** se $x \in S$ implica $\lambda x \in S$ para cada $\lambda \geq 0$. Por exemplo, $A = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_i \geq 0\}$ é um cone. Se $v_1, \ldots, v_m$ são vetores linearmente independentes em $\mathbb{R}^n$, então $B = \{\alpha_1 v_1 + \cdots \alpha_m v_m \mid \alpha_i \in \mathbb{R}, \alpha_i \geq 0\}$ é um cone.

O conjunto $P_{n,d}$ também pode ser visto como um cone no espaço $\mathbb{R}^m$, onde $m = \binom{n+d-1}{n-1}$, via a identificação $s \in P_{n,d} \leftrightarrow (a_1, \ldots, a_m)$, onde os a_i são os coeficientes de s.

Seja K um cone em $\mathbb{R}^m$ e seja $u \in K$. O conjunto $[u] = \{\lambda u \mid \lambda \in \mathbb{R},\ \lambda > 0\} \subset K$ é chamado **raio** determinado por u. Cada raio é uma classe de equivalência da relação $u \sim v \Leftrightarrow v = \lambda u, \lambda \in \mathbb{R}, \lambda > 0$ definida sobre $\mathbb{R}^m$.

O espaço quociente $K/\sim$ é o conjunto dos raios $[u]$, com $u \in K$. Dizemos que K é **projetivamente compacto** quando $K/\sim$ é compacto.

O cone K é dito **convexo** se, dados $u, v \in K$, temos $(1-t)u + tv \in K$, para todo $t \in \mathbb{R}$, $0 \leq t \leq 1$. Um raio $[u] \in K/\sim$ é dito **extremo** se $[u] = (1-t)[v] + t[w]$, com $t \in \mathbb{R}$, $0 < t < 1$, implica $[u] = [v] = [w]$. Dada uma família $\{[u_i]\}_{i \in I}$ de raios, o **fecho convexo** dessa família é o conjunto

$$F = \left\{ \sum_{i \in J} \alpha_i [u_i] \mid 0 \leq \alpha_i \leq 1,\ \sum_{i \in J} \alpha_i = 1 \right\}$$

onde $J \subset I$ é finito, ou seja, F é o conjunto das combinações lineares convexas de elementos da família.

Teorema 4.2 (Krein-Milman, 1940) *Seja K um cone convexo e projetivamente compacto. Então K é o fecho convexo de seus raios extremos.*

Demonstração: veja [12], p.277.

4.4 O Teorema de Hilbert sobre quádricas ternárias

Uma forma quártica ternária é uma forma de grau 4 em três indeterminadas. O item (3) do Teorema 4.1 afirma que $P_{3,4} = \Sigma_{3,4}$, ou seja, toda forma quártica ternária positiva semidefinida é uma soma de quadrados (de formas quadráticas). Nesta seção, demonstraremos esse fato, seguindo [3] (veja também [2], p.111).

Dados dois polinômios $f, g \in \mathbb{R}[x_1, \ldots, x_n]$, escrevemos $f \geq g$ em $\mathbb{R}^n$ para indicar que $f - g$ é um polinômio positivo semidefinido em $\mathbb{R}^n$. Mais precisamente, $(f-g)(a) \geq 0$, para todo $a \in \mathbb{R}^n$.

Lema 4.3 *Se $s \in P_{3,4}$, então existe uma forma quadrática não-nula q tal que $s \geq q^2$ em $\mathbb{R}^3$.*

Demonstração: vamos usar a notação usual da geometria projetiva: se $(x, y, z) \neq (0, 0, 0)$, então

$$(x : y : z) = \{(\lambda x, \lambda y, \lambda z) \mid \lambda \in \mathbb{R}\}$$

é a reta que passa por (x, y, z) e pela origem $(0, 0, 0)$. O **plano projetivo real** é o conjunto de todas essas retas, ou seja,

$$\mathbb{P}_2(\mathbb{R}) = \{(x : y : z) \mid (x, y, z) \in \mathbb{R}^3,\ (x, y, z) \neq (0, 0, 0)\}.$$

Esse é o ambiente ideal para se considerar como domínio de funções polinomiais dadas por polinômios homogêneos (de três variáveis), uma vez que, se F é homogêneo de grau d e $F(x, y, z) = 0$ então $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z) = 0$. Logo, F se anula ao longo de toda a reta $(x : y : z)$.

Seja $Z(s) \subset \mathbb{P}_2(\mathbb{R})$ o conjunto

$$Z(s) = \{(x : y : z) \in \mathbb{P}_2(\mathbb{R}) \mid s(x, y, z) = 0\}.$$

Temos três casos:

Caso 1: $\boxed{Z(s) = \emptyset}$.

Neste caso, $s(x, y, z) \neq 0$, para todo $(x, y, z) \neq (0, 0, 0)$. Em particular, $s(x, y, z) > 0$, para todo $(x, y, z) \in S^2$ (esfera unitária). Como $(x, y, z) \in S^2 \Leftrightarrow x^2 + y^2 + z^2 = 1$, temos

$$\frac{s(x, y, z)}{(x^2 + y^2 + z^2)^2} = s(x, y, z) > 0 \Rightarrow \frac{s(x, y, z)}{(x^2 + y^2 + z^2)^2} \geq \varepsilon > 0 \Rightarrow s(x, y, z) \geq \varepsilon(x^2 + y^2 + z^2)^2,$$

para todo $(x, y, z) \in S^2$.

Dado $(x, y, z) \in \mathbb{R}^3$, $(x, y, z) \neq (0, 0, 0)$, existe $\lambda \in \mathbb{R}$ $(\lambda = (x^2 + y^2 + z^2)^{1/2})$ tal que $(\lambda x, \lambda y, \lambda z) \in S^2$. Logo,

$$s(\lambda x, \lambda y, \lambda z) \geq \varepsilon((\lambda x)^2 + (\lambda y)^2 + (\lambda z)^2)^2 \Rightarrow \lambda^4 s(x, y, z) \geq \varepsilon\lambda^4(x^2 + y^2 + z^2)^2 \Rightarrow$$

$$\Rightarrow s(x, y, z) \geq \varepsilon(x^2 + y^2 + z^2)^2,$$

para todo $(x, y, z) \in \mathbb{R}^3 \setminus \{(0, 0, 0)\}$. Basta, então, tomarmos $q(x, y, z) = \sqrt{\varepsilon}(x^2 + y^2 + z^2)$.

Caso 2: $Z(s)$ tem exatamente um elemento.

Mudando coordenadas, se necessário, podemos supor que $Z(s) = \{(1 : 0 : 0)\}$. Se $\mathrm{Gr}_x(s) = 4$, isto é, o grau de x em s é igual a 4,

$$s(x, y, z) = ax^4 + (\text{termos que dependem de } y \text{ e } z),$$

então $s(1 : 0 : 0) = a \neq 0$. Como $s(1 : 0 : 0) = 0$, s não pode ter um termo onde x apareça com grau 4, logo $\mathrm{Gr}_x(s) < 4$. devemos observar que $\mathrm{Gr}_x(s)$ é par, do contrário $s(x : 1 : 1)$ mudaria de sinal quando x percorresse $\mathbb{R}$. Assim, $\mathrm{Gr}_x(s) < 4$ implica que $\mathrm{Gr}_x(s) = 0$ ou $\mathrm{Gr}_x(s) = 2$. Se $\mathrm{Gr}_x(s) = 0$, então teria apenas duas indeterminadas e, por isso, $s \notin P_{3,4}$. Assim, $\mathrm{Gr}_x(s) = 2$ e podemos escrever

$$s(x, y, z) = x^2 f(y, z) + 2xg(y, z) + h(y, z). \tag{10}$$

Completando quadrados, obtemos

$$fs = (xf + g)^2 + (fh - g^2). \tag{11}$$

Como $s \geq 0$ em $\mathbb{R}^3$, o coeficiente $f(y, z)$ de x^2 na expressão quadrática (10) deve ser maior ou igual a zero em $\mathbb{R}^2$. O mesmo vale para o coeficiente linear $h(y, z)$ em (10), isto é, $h > 0$ em $\mathbb{R}^2$.

O discriminante da expressão (10) é $\Delta = 4g^2 - 4fh$. Como s não muda de sinal, $\Delta \leq 0$, isto é,

$$fh - g^2 \geq 0. \tag{12}$$

O polinômio $f(y, z)$ é uma forma quadrática, pois $x^2 f(y, z)$ tem grau 4. A forma quadrática

$$f(y, z) = ay^2 + 2byz + cz^2 = \begin{pmatrix} y & z \end{pmatrix} \cdot \begin{pmatrix} a & b \\ b & c \end{pmatrix} \cdot \begin{pmatrix} y \\ z \end{pmatrix}$$

é dita **degenerada** se $\det \begin{pmatrix} a & b \\ b & c \end{pmatrix} = 0$ e é dita **não-degenerada** se $\det \begin{pmatrix} a & b \\ b & c \end{pmatrix} \neq 0$. Se f é degenerada, então $cf = (by + cz)^2$, se $c \neq 0$, ou $af = (ay)^2$, se $c = 0$. Se f é não-degenerada, então $f(y, z) = 0$ se, e somente se, $(y, z) = (0, 0)$.

Se f não é degenerada, então $f > 0$ sobre $\mathbb{R}^2 \setminus \{(0, 0)\}$. Se $(fh - g^2)(b, c) = 0$ com $(b, c) \neq (0, 0)$, então, por (11),

$$f(b, c)s\left(-\frac{g(b, c)}{f(b, c)} : b : c\right) = \left(-\frac{g(b, c)}{f(b, c)} f(b, c) + g(b, c)\right)^2 + 0 = 0 \Rightarrow$$

$$\Rightarrow \left(-\frac{g(b, c)}{f(b, c)} : b : c\right) \in Z(s) = \{(1 : 0 : 0)\},$$

o que é uma contradição com $(b, c) \neq (0, 0)$.

Assim, existe $\varepsilon > 0$ tal que $\frac{fh-g^2}{f^3} \geq \varepsilon$ sobre S^1 (o círculo de raio 1 centrado em na origem de $\mathbb{R}^2$). Repetindo argumentos já usados anteriormente, concluímos que $fh - g^2 \geq \varepsilon f^3$ sobre $\mathbb{R}^2$. Então

$$fs = (xf + g)^2 + (fh - g^2) \geq fh - g^2 \geq \varepsilon f^3$$

sobre $\mathbb{R}^3$, portanto $s \geq \varepsilon f^2$ sobre $\mathbb{R}^3$. Basta tomarmos, então, $q = \sqrt{\varepsilon} f$.

No caso em que f é degenerada, temos que $f \geq 0$ implica $f = f_1^2$, onde $f_1 = f_1(y, z) = ay+bz$ é uma forma linear. Por (12) sabemos que $fh - g^2 \geq 0$, logo $f_1^2 h - g^2 \geq 0$. O conjunto dos zeros de f_1 é $Z(f_1) = \{(b : -a)\}$. Assim, de $(f_1^2 h - g^2)(b : -a) \geq 0$ e $f_1(b : -a) = 0$ vem que $-g(b : -a)^2 \geq 0$, ou seja, $g(b : -a) = 0$. Pelo Teorema do resto, f_1 divide g, isto é, $g = f_1 g_1$, para algum polinômio g_1.

Agora, (11) implica que $fs = (xf + g)^2 + (fh - g^2) \geq (xf + g)^2$, pois $fh - g^2 \geq 0$. Logo,

$$fs \geq (xf + g)^2 = (xf_1^2 + f_1 g_1)^2 = f_1^2 (xf_1 + g_1)^2 \Rightarrow fs \geq f(xf_1 + g_1)^2 \overset{f \geq 0}{\Rightarrow} s \geq (xf_1 + g_1)^2.$$

Caso 3: $\boxed{Z(s) \text{ tem pelo menos dois elementos}}$.

Podemos assumir, sem perda de genaralidade, que $(1 : 0 : 0)$ e $(0 : 1 : 0)$ pertencem a $Z(s)$. De modo análogo ao que fizemos no caso anterior, concluímos que $\mathrm{Gr}_x(s) = \mathrm{Gr}_y(s) = 2$. Temos, então,

$$s(x, y, z) = x^2 f(y, z) + 2xzg(y, z) + z^2 h(y, z)$$

e

$$fs = (xf + zg)^2 + z^2(fh - g^2), \tag{13}$$

onde f, g e h são formas quadráticas em y, z e f, h e $fh - g^2$ são todas não-negativas sobre $\mathbb{R}^2$.

Se f é uma forma degenerada, então podemos proceder como no caso anterior. Se h é degenerada, podemos fazer o mesmo, usando

$$hs = (zh + xg)^2 + x^2(fh - g^2).$$

Assim, podemos supor que f e h não são degeneradas. Neste caso, $f > 0$ e $h > 0$ sobre $\mathbb{R}^2 \setminus \{(0, 0)\}$. Finalmente, temos dois subcasos:

(a) A forma $fh - g^2$ possui um zero não-trivial (b, c). Considere $\alpha = -\frac{g(b,c)}{f(b,c)}$ e

$$s_1(x, y, z) = s(x + \alpha z, y, z) = x^2 f + 2xz(g + \alpha f) + z^2(h + 2\alpha g + \alpha^2 f).$$

Como $(fh - g^2)(b, c) = 0$, temos $(h + 2\alpha g + \alpha^2 f)(b, c) = \left(\frac{fh-g^2}{f}\right)(b, c) = 0$. Assim,

$$x^2 f = s_1(x, y, z) = x^2 f + 2xzG(y, z) + z^2 H(y, z),$$

com $G(y, z) = g(y, z) + \alpha f(y, z)$, $H(y, z) = h(y, z) + 2\alpha g(y, z) + \alpha^2 f(y, z)$ e $H(b, c) = 0$. Assim, este caso pode ser tratado como antes, pois H é degenerada.

(b) A forma $fh - g^2$ é positiva sobre $\mathbb{R}^2 \setminus \{(0,0)\}$. Neste caso, existe $\varepsilon > 0$ tal que

$$\frac{fh - g^2}{(y^2 + z^2)f} \geq \varepsilon$$

sobre S^1. Portanto

$$fh - g^2 \geq \varepsilon(y^2 + z^2)f$$

sobre $\mathbb{R}^2$. Logo, por (13),

$$fs = (xf + zg)^2 + z^2(fh - g^2) \geq z^2(fh - g^2) \geq \varepsilon z^2(y^2 + z^2)f \Rightarrow$$

$$\Rightarrow s \geq \varepsilon z^2(y^2 + z^2) \geq \varepsilon z^4$$

sobre $\mathbb{R}^3$, isto é, $s \geq q^2$ sobre $\mathbb{R}^3$, com $q = \sqrt{\varepsilon} z^2$. □

Vamos, agora, mostrar que $P_{3,4} = \Sigma_{3,4}$. Como $P_{3,4}$ é um cone convexo projetivamente compacto, o Teorema 4.2 garante que toda forma em $P_{3,4}$ pode ser escrita como combinação linear de um número finito de formas extremas pertencentes a $P_{3,4}$. Assim, é suficiente mostrarmos que toda forma extrema $s \in P_{3,4}$ pode ser escrita como soma de quadrados. Seja, pois, $s \in P_{3,4}$ uma forma extrema. Pelo Lema 4.3, existe uma forma q tal que $s \geq q^2$, ou seja, $s = q^2 + t$, onde $q \neq 0$ e $t = 0$ ou $t \in P_{3,4}$. Como s é extrema, temos $q^2 = as$, para algum $a \in \mathbb{R}$, $0 < a \leq 1$. Portanto $s \in \Sigma_{3,4}$.

4.5 Conclusão da demonstração

Nesta seção vamos concluir a demonstração do Teorema 4.1. Nas seções anteriores, já demonstramos que as três condições listadas no enunciado desse teorema são suficientes para que $P_{n,d} = \Sigma_{n,d}$. A seguir, demonstraremos que essas condições também são necessárias para que valha essa igualdade. Mais precisamente, exibiremos exemplos que mostram que, excetuando-se os três casos listados no eneunciado do Teorema 4.1, a inclusão $\Sigma_{n,d} \subset P_{n,d}$ é sempre estrita.

Inicialmente, vamos exibir formas $q \in P_{4,4} \setminus \Sigma_{4,4}$ e $s \in P_{3,6} \setminus \Sigma_{3,6}$. Seja

$$q(x, y, z, w) = w^4 + x^2y^2 + y^2z^2 + z^2x^2 - 4xyzw.$$

Sabemos que $\frac{a+b+c+d}{4} \geq \sqrt[4]{abcd}$. Fazendo $a = w^4$, $b = x^2y^2$, $c = y^2z^2$ e $d = z^2x^2$, obtemos $q(x, y, z, w) \geq 0$, ou seja, $q \in P_{4,4}$. Vamos mostrar que $q \notin \Sigma_{4,4}$. Suponhamos o contrário, isto é, $q = \sum_{i=1}^{k} q_i^2$. Nenhum q_i poderia conter x^2, y^2 ou z^2, pois q não contém x^4, y^4 ou z^4. Mais ainda, nenhum q_i poderia conter wx, wy ou wz, pois q não contém w^2x^2, w^2y^2 ou w^2z^2. Assim, cada q_i seria uma combinação linear dos monômios xy, yz, zx e w^2 e, portanto, não haveria o termo $xyzw$ na soma $\sum_{i=1}^{k} q_i^2$. Isso mostra que $q \notin \Sigma_{4,4}$.

Se $n \geq 4$ e $d > 4$ (d par), então $x^{d-4}q \in P_{n,d} \setminus \Sigma_{n,d}$.

Consideremos, agora, $s(x, y, z) = z^6 + x^4y^2 + x^2y^4 - 3x^2y^2z^2$. Como $x^2y^2z^2$ é a média geométrica de z^6, x^4y^2 e x^2y^4, temos que $s \geq 0$ sobre $\mathbb{R}^3$. Suponha que $s = \sum_{i=1}^{k} s_i^2$. De modo

similar ao que fizemos no caso anterior, vemos que nenhum s_i pode conter $x^3, y^3, x^2z, y^2z, xz^2$ ou yz^2. Assim, cada s_i é uma combinação linear dos monômios xy^2, x^2y, xyz e z^3. Se a_i é o coeficiente de xyz em s_i, então o coeficiente de $x^2y^2z^2$ em s é igual a $\sum_{i=1}^{k} a_i^2$, logo $-3 = \sum_{i=1}^{k} a_i^2$, com $a_1, \ldots, a_k \in \mathbb{R}$, absurdo. Isso mostra que $s \notin \Sigma_{3,6}$.

Se $n \geq 3$ e $d > 6$ (d par), então $x^{d-6}s \in P_{n,d} \setminus \Sigma_{n,d}$. Isso completa a demonstração do Teorema 4.1.

Referências

[1] P.B. Bhattacharya, S.K. Jain & S.R. Nagpaul, *Basic Abstract Algebra*, Cambridge, 1999.

[2] Bochnak, J., Coste, M., Roy, M.-F., *Real Algebraic Geometry*, Springer-Verlag, 1998.

[3] Choi, M.-D., Lam, T.-Y., *Extremal Positive Semidefinite Forms*, Math. Ann., 231, 1977, pp. 1-18.

[4] David S. Dummit & Richard M. Foote, *Abstrct Algebra*, Willey.

[5] Duren, P. *Changing Faces: The Mistaken Portrait of Legendre*, disponível em http://www.ams.org/notices/200911/rtx091101440p.pdf

[6] Garcia, A. & Lequain, Y., *Elementos de Álgebra* - quinta edição - Projeto Euclides, IMPA, Rio de Janeiro, 2008.

[7] Gonçalves, A., *Introdução à Álgebra* - Projeto Euclides, IMPA, 1995.

[8] Landau, E. *Teoria Elementar dos Números*, coleção clássicos da Matemática - Ed. Ciência Moderna, 2002.

[9] Lima, D.P. de O. *Introdução aos Quatérnios*, monografia de conclusão de curso - CEFET - CE, 2007.

[10] Marshall, M., *positive Polynomials and Sums of Squares*, Università de Pisa, Pisa, 2000.

[11] Powers, V. et al, *A new approach to Hilbert theorem on ternary quartics*, Comptes Rendus Mathématique, Vol.339, No. 9 (Nov. 2004), pp. 617-620.

[12] Rajwade, A.R., *Squares*, London Mathematical Society Lecture Notes, Vol.171, Cambridge University Press, 1993.

[13] Rudin, W., *Sums of Squares of Polynomials*, The American Mathematical Monthly, Vol.107, No. 9 (Nov. 2000), pp. 813-821, MAA.

[14] Samuel, P., *Théorie Algébrique des Nombres*, Hermann, Paris, 1967.