Aritmética em Álgebras de Quaterniões

Rafael Inácio
FCUP

Bolsa Novos Talentos

2025

Quaterniões de Hamilton (1843)

- William Rowan Hamilton introduziu

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}.$$

- Com a propriedade:

$$i^2 = j^2 = k^2 = ijk = -1.$$

- Primeiro exemplo de uma **algebra de divisão não comutativa**.

Quaterniões de Hamilton (1843)

Para um $u \in \mathbb{H}$ temos as seguintes notações

$$u = a + bi + cj + dk$$
$$\overline{u} = a - bi - cj - dk,$$
$$N(u) = u\overline{u} = a^2 + b^2 + c^2 + d^2.$$

Escrevemos $u = \Re(u) + V(u)$ onde $\Re(u) = a,\ V(u) = bi + cj + dk$ (quaternião puro).

Quaterniões de Hamilton (1843)

Para um $u \in \mathbb{H}$ temos as seguintes notações

$$u = a + bi + cj + dk$$
$$\overline{u} = a - bi - cj - dk,$$
$$N(u) = u\overline{u} = a^2 + b^2 + c^2 + d^2.$$

Escrevemos $u = \Re(u) + V(u)$ onde $\Re(u) = a,\ V(u) = bi + cj + dk$ (quaternião puro).

Quaterniões Racionais:
$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Q}\} = \mathbb{Q}[i, j, k]$

Anel de Inteiros

$$
\begin{tikzcd}
\mathbb{Z}[i] \arrow[r] & \mathbb{Q}[i] \\
\mathbb{Z} \arrow[u] \arrow[r] & \mathbb{Q} \arrow[u]
\end{tikzcd}
$$

Anel de Inteiros

$$
\begin{tikzcd}
\mathbb{Z}[i] \arrow[r] & \mathbb{Q}[i] \\
\mathbb{Z} \arrow[r] \arrow[u] & \mathbb{Q} \arrow[u]
\end{tikzcd}
$$

Qual será o análogo a $\mathbb{Z}[i]$ em $\mathbb{H}(\mathbb{Q})$?

$$
\begin{tikzcd}
\textbf{?} \arrow[r] & \mathbb{H}(\mathbb{Q}) \\
\mathbb{Z} \arrow[r] \arrow[u] & \mathbb{Q} \arrow[u]
\end{tikzcd}
$$

Subconjuntos de quaterniões

- **Inteiros de Lipschitz:**

  $$\mathcal{L} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\} = \mathbb{Z}[i, j, k]$$

Subconjuntos de quaterniões

- **Inteiros de Lipschitz:**

  $\mathcal{L} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\} = \mathbb{Z}[i, j, k]$

- **Inteiros de Hurwitz:**

  $\mathcal{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z} \text{ ou } a, b, c, d \in \frac{1}{2} + \mathbb{Z}\}$
  $= \mathbb{Z}[i, j, k, \frac{1+i+j+k}{2}]$

4 quadrados de Lagrange

Theorem (Teorema de Lagrange)

Todos os inteiros não negativos n podem ser escritos como soma de 4 quadrados de inteiros.

$$n = a^2 + b^2 + c^2 + d^2$$

Primos em Hurwitz

Um primo de Hurwitz é um elemento de $\mathcal{H}$ com norma um primo racional. Dizemos que um $\pi \in \mathcal{H}$ é um primo acima de p se $N(\pi) = p$.

Primos em Hurwitz

Um primo de Hurwitz é um elemento de $\mathcal{H}$ com norma um primo racional. Dizemos que um $\pi \in \mathcal{H}$ é um primo acima de p se $N(\pi) = p$.

Existem $p + 1$ primos, a menos de associados esquerdos, acima de $p > 2$. Para $p = 2$ apenas existe um primo, $1 + i$.

"Fatorização única"

[Lipschitz, 1886; Hurwitz, 1919]

Seja $\alpha \in \mathcal{H}$ primitivo e $m = N(\alpha)$. Para cada fatorização

$$m = p_1 p_2 \cdots p_{k-1} p_k$$

em primos racionais, existe uma "fatorização única"

$$\alpha = \pi_1 \pi_2 \cdots \pi_{k-1} \pi_k$$

em primos de Hurwitz, tais que $N(\pi_i) = p_i$.

Metacomutação

$\Pi_p =$ conjunto dos primos acima de p, a menos de associados esquerdos

Metacomutação

Π_p = conjunto dos primos acima de p, a menos de associados esquerdos

$\pi \in \Pi_p, \xi \in \mathcal{H}$, $N(\xi) = q \neq p$ (também primo) $\rightsquigarrow \pi\xi = \xi'\pi'$

Metacomutação

Π_p = conjunto dos primos acima de p, a menos de associados esquerdos

$\pi \in \Pi_p, \xi \in \mathcal{H}$, $N(\xi) = q \neq p$ (também primo) $\rightsquigarrow \pi\xi = \xi'\pi'$

Isto dá origem ao mapa da metacomutação:

$$\begin{array}{rccc} \mu_\xi: & \Pi_p & \to & \Pi_p \\ & \pi & \mapsto & \pi' \end{array}$$

Metacomutação

Π_p = conjunto dos primos acima de p, a menos de associados esquerdos

$\pi \in \Pi_p, \xi \in \mathcal{H}$, $N(\xi) = q \neq p$ (também primo) $\rightsquigarrow \pi\xi = \xi'\pi'$

Isto dá origem ao mapa da metacomutação:

$$\begin{array}{rccc} \mu_\xi : & \Pi_p & \to & \Pi_p \\ & \pi & \mapsto & \pi' \end{array}$$

- μ_ξ é uma permutação: o seu sinal é $\left(\frac{q}{p}\right)$. [H. Cohn, A. Kumar, 2015]

Metacomutação

Π_p = conjunto dos primos acima de p, a menos de associados esquerdos

$\pi \in \Pi_p, \xi \in \mathcal{H}$, $N(\xi) = q \neq p$ (também primo) $\rightsquigarrow \pi\xi = \xi'\pi'$

Isto dá origem ao mapa da metacomutação:

$$\begin{array}{cccc} \mu_\xi : & \Pi_p & \to & \Pi_p \\ & \pi & \mapsto & \pi' \end{array}$$

- μ_ξ é uma permutação: o seu sinal é $\left(\frac{q}{p}\right)$. [H. Cohn, A. Kumar, 2015]
- tem $1 + \left(\frac{\Re(\xi)-q}{p}\right)$ pontos fixos se $p \nmid V(\xi)$, caso contrário $\mu_\xi = id$.

Metacomutação

$\Pi_p =$ conjunto dos primos acima de p, a menos de associados esquerdos

$\pi \in \Pi_p, \xi \in \mathcal{H}$, $N(\xi) = q \neq p$ (também primo) $\rightsquigarrow \pi\xi = \xi'\pi'$

Isto dá origem ao mapa da metacomutação:

$$\begin{array}{rccc} \mu_\xi : & \Pi_p & \to & \Pi_p \\ & \pi & \mapsto & \pi' \end{array}$$

- μ_ξ é uma permutação: o seu sinal é $\left(\frac{q}{p}\right)$. [H. Cohn, A. Kumar, 2015]
- tem $1 + \left(\frac{\Re(\xi)-q}{p}\right)$ pontos fixos se $p \nmid V(\xi)$, caso contrário $\mu_\xi = id$.
- todos os ciclos não triviais têm o mesmo comprimento, $\ell_{\xi,p}$.

Metacomutação

Π_p = conjunto dos primos acima de p, a menos de associados esquerdos

$\pi \in \Pi_p, \xi \in \mathcal{H}$, $N(\xi) = q \neq p$ (também primo) $\rightsquigarrow \pi\xi = \xi'\pi'$

Isto dá origem ao mapa da metacomutação:

$$\begin{array}{rccc} \mu_\xi : & \Pi_p & \to & \Pi_p \\ & \pi & \mapsto & \pi' \end{array}$$

- μ_ξ é uma permutação: o seu sinal é $\left(\frac{q}{p}\right)$. [H. Cohn, A. Kumar, 2015]
- tem $1 + \left(\frac{\Re(\xi)-q}{p}\right)$ pontos fixos se $p \nmid V(\xi)$, caso contrário $\mu_\xi = id$.
- todos os ciclos não triviais têm o mesmo comprimento, $\ell_{\xi,p}$.
- para p ímpar, existem primos ξ tais que $\ell_{\xi,p} = p$. [António Leite]

Exemplo

Por exemplo o quaternião $\alpha = \pi\xi$, com $\pi = 1 - i + j$ e $\xi = 1 + 2i + j + k$, também pode ser escrito da forma

$$\alpha = \xi_1 \pi_1 = (1 - i + j - 2k)(1 + j + k)$$

Pode-se verificar que π e π_1 não são associados esquerdos, em particular, $\mu_\xi \neq id$.

1-3-5

Existem muitas formas de escrever um número como soma de 4 quadrados.

Aliás, para todo o $m \in \mathbb{N}_0$ existem inteiros x, y, z, t, n tais que:

$$\begin{cases} m &= x^2 + y^2 + z^2 + t^2 \\ n^2 &= x + 3y + 5z \end{cases}$$

Próximos passos

- Estudar problemas diofantinos análogos a este.

Próximos passos

- Estudar problemas diofantinos análogos a este.

- Estudar a aritmética dos "anéis de inteiros" noutras álgebras de quaterniões.

Referências

- A. Machiavelo, Nikolaos Tsopanidis, *Zhi-Wei Sun's 1-3-5 Conjecture and Variations*, Journal of Number Theory **222** (2021) 1–20.
- Zhi-Wei Sun, *Refining Lagrange's Four-Square Theorem*, Journal of Number Theory **175** (2017) 167–190.
- John Voight, *Quaternion Algebras*, post-publication version v.1.0.6u, October 6, 2025 (available online).