哈密尔顿数的矩阵实现

林磊

1 引子

若正整数 m, n 均能写成四个整数的平方和：

$$m = A^2 + B^2 + C^2 + D^2, \qquad n = a^2 + b^2 + c^2 + d^2,$$

则其积 mn 是否也能表成四个整数的平方和?

事实上

$$\begin{aligned} mn &= (A^2 + B^2 + C^2 + D^2)(a^2 + b^2 + c^2 + d^2) \\ &= (Aa - Bb - Cc - Dd)^2 + (Ab + Ba - Cd + Dc)^2 \\ &\quad +(Ac + Ca - Db + Bd)^2 + (Ad + Da - Bc + Cb)^2. \end{aligned}$$

只要对上式左右两边展开就可验证该式子的正确性, 但要写出这个式子就不那么容易. 下面我们将从哈密尔顿四元数知识入手来解决这类问题.

注: 在数论中有这样的一个结论: 每个正整数都可以表示成四个整数的平方和. 因此借助以上的引子, 只要证明该结论对所有素数成立即可.

高斯曾证明了: 形如 $4n + 1$ 的素数可以表示为两个整数的平方和(即可表为四个整数的平方和, 后两个为零的平方). 例如: $5 = 4 \cdot 1 + 1 = 2^2 + 1^2$.

2 哈密尔顿四元数及其矩阵的实现

设

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

则 $\mathbb{H}$ 是哈密尔顿四元数体[1]. 它为 $\mathbb{R}$ 上的结合代数, $1, i, j, k$ 为其一组基, 称为哈密尔顿四元数. 其运算如下:

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j.$$

我们定义:

$$R = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C}).$$

则 R 为 $M_2(\mathbb{C})$ 的 R 结合子代数(有单位元 E_2).

简略证明: 因为 $E_2 \in R$, 所以 R 是非空集合. 又

$$\alpha\alpha_1 - \beta\bar{\beta_1} = \overline{\bar{\alpha}\bar{\alpha_1} - \bar{\beta}\beta_1}\ , \quad \alpha\beta_1 + \beta\bar{\alpha_1} = -(\overline{-\bar{\beta}\alpha_1 - \bar{\alpha}\bar{\beta_1}}),$$

$$\overline{\alpha - \alpha_1} = \bar{\alpha} - \bar{\alpha_1}\ , \quad \overline{\beta - \beta_1} = -\bar{\beta} + \bar{\beta_1}.$$

则

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \alpha_1 & \beta_1 \\ -\bar{\beta_1} & \bar{\alpha_1} \end{pmatrix} = \begin{pmatrix} \alpha\alpha_1 - \beta\bar{\beta_1} & \alpha\beta_1 + \beta\bar{\alpha_1} \\ -\bar{\beta}\alpha_1 - \bar{\alpha}\bar{\beta_1} & \bar{\alpha}\bar{\alpha_1} - \bar{\beta}\beta_1 \end{pmatrix} \in R,$$

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} - \begin{pmatrix} \alpha_1 & \beta_1 \\ -\bar{\beta_1} & \bar{\alpha_1} \end{pmatrix} = \begin{pmatrix} \alpha - \alpha_1 & \beta - \beta_1 \\ -\bar{\beta} + \bar{\beta_1} & \bar{\alpha} - \bar{\alpha_1} \end{pmatrix} \in R.$$

所以 R 为 $M_2(\mathbb{C})$ 的子环, 运用矩阵的运算性质, 容易证明 $(R, +)$ 为一 $\mathbb{R}$ -模且满足:

$$r(xy) = (rx)y = x(ry) \quad \forall r \in \mathbb{R}, \forall x, y \in R.$$

故 R 为 $\mathbb{R}$ -代数.

记

$$E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ I = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix},\ J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in R.$$

令 $\alpha = a + bi,\ \beta = c + di$, 则下式成立:

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = aE_2 + bI + cJ + dK.$$

所以 $E_2,\ I,\ J,\ K$ 为 R 的一组基. 又容易计算:

$$I^2 = J^2 = K^2 = -E_2,\ IJ = K,\ JK = I,\ KI = J,\ JI = -K,\ KJ = -I,\ IK = -J.$$

[1] R 是一个有单位元的环，若 R 中每个非零元都可逆，则称 R 为一个除环. 非交换的除环称为体.

从而我们可以定义以下同构:

$$\rho \ : \ \mathbb{H} \longrightarrow R$$

$$a + bi + cj + dk \longmapsto \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = aE_2 + bI + cJ + dK.$$

简略证明: 只要作如下基之间的对应:

$$1 \mapsto E_2,\ i \mapsto I,\ j \mapsto J,\ k \mapsto K.$$

显然: $\rho(x + y) = \rho(x) + \rho(y)$, $\rho(rx) = r\rho(y)$. 又由基之间运算的相似性能得到 $\rho(xy) = \rho(x)\rho(y)$ 成立, 且 ρ 是同构的. 因为它们都是 $\mathbb{R}$ 结合代数, 故 ρ 为 $\mathbb{H} \longrightarrow R$ 的 $\mathbb{R}$ 结合代数同构. 由此, 我们把四元数体用矩阵的形式加以了表示.

仍然记 $\alpha = a + bi$, $\beta = c + di$, 则

$$\det\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = |\alpha|^2 + |\beta|^2 = a^2 + b^2 + c^2 + d^2 = n.$$

记 $\alpha_1 = A + Bi$, $\beta_1 = C + Di$, 则

$$\det\begin{pmatrix} \alpha_1 & \beta_1 \\ -\bar{\beta}_1 & \bar{\alpha}_1 \end{pmatrix} = |\alpha_1|^2 + |\beta_1|^2 = A^2 + B^2 + C^2 + D^2 = m,$$

$$\begin{aligned} \det\left(\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}\begin{pmatrix} \alpha_1 & \beta_1 \\ -\bar{\beta}_1 & \bar{\alpha}_1 \end{pmatrix}\right) &= \begin{pmatrix} \alpha\alpha_1 - \beta\bar{\beta}_1 & \alpha\beta_1 + \beta\bar{\alpha}_1 \\ -\bar{\beta}\alpha_1 - \bar{\alpha}\bar{\beta}_1 & \bar{\alpha}\bar{\alpha}_1 - \bar{\beta}\beta_1 \end{pmatrix} = |\alpha\alpha_1 - \beta\bar{\beta}_1|^2 + |\alpha\beta_1 + \beta\bar{\alpha}_1|^2 \\ &= (Aa - Bb - Cc - Dd)^2 + (Ab + Ba - Cd + Dc)^2 \\ &\quad +(Ac + Ca - Db + Bd)^2 + (Ad + Da - Bc + Cb)^2. \end{aligned}$$

又在行列式运算中有 $\det(X)\det(Y) = \det(XY)$, 所以

$$\det\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}\det\begin{pmatrix} \alpha_1 & \beta_1 \\ -\bar{\beta}_1 & \bar{\alpha}_1 \end{pmatrix} = \det\left(\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}\begin{pmatrix} \alpha_1 & \beta_1 \\ -\bar{\beta}_1 & \bar{\alpha}_1 \end{pmatrix}\right).$$

故可得到引子中等式成立.

下面我们借助矩阵的运算来寻找 $\mathbb{H}$ 上的运算性质.

令 $x = a + bi + cj + dk$, 则 $\bar{x} = a - bi - cj - dk$, 故

$$\rho(\bar{x}) = \begin{pmatrix} a-bi & -c-di \\ c-di & a+bi \end{pmatrix} = \begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix} = \overline{\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}'} = \overline{\rho(x)}'.$$

则

$$\rho(\bar{y}\bar{x}) = \rho(\bar{y})\rho(\bar{x}) = (\overline{\rho(y)})'(\overline{\rho(x)})' = ((\overline{\rho(x)})(\overline{\rho(y)}))' = \overline{\rho(x)\rho(y)}' = \overline{\rho(xy)}' = \rho(\overline{xy}).$$

因为 ρ 同构, 所以, $\overline{xy} = \bar{y}\bar{x}$. (这与一般的复数的共轭运算不一样)

因为

$$|x|^2 = x \cdot \bar{x} = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2.$$

所以

$$\det(\rho(x)) = \det\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = a^2 + b^2 + c^2 + d^2 = |x|^2.$$

则由

$$\det(\rho(x))\det(\rho(y)) = \det(\rho(xy)).$$

知, $|x|^2|y|^2 = |xy|^2$, 即 $|x|\,|y| = |xy|$.

设

$$X = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix},$$

则

$$\begin{aligned} X\overline{X}' &= \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}\begin{pmatrix} a-bi & -c-di \\ c-di & a+bi \end{pmatrix} \\ &= \begin{pmatrix} a^2+b^2+c^2+d^2 & 0 \\ 0 & a^2+b^2+c^2+d^2 \end{pmatrix} \\ &= (\det X)E_2 = \overline{X}'X. \end{aligned}$$

所以, $X^* = \overline{X}'$ 则 $X^{-1} = \dfrac{1}{\det X}X^* = \dfrac{1}{\det X}\overline{X}'$. 即 $x^{-1} = \dfrac{1}{|x|^2}\bar{x}$. 于是我们可以得到

$$(xy)^{-1} = \frac{1}{|xy|^2}\overline{xy} = \frac{1}{|x|^2|y|^2}\bar{y}\bar{x} = \frac{1}{|y|^2}\bar{y}\frac{1}{|x|^2}\bar{x} = y^{-1}x^{-1}.$$

例题: 在 $\mathbb{H}$ 中求解 $x^2 = a$ $(a \in \mathbb{R})$.

解: 设 $x = e + bi + cj + dk \in \mathbb{H}$.

1. 当$a > 0$ 时:

   令
   $$y = \frac{x}{\sqrt{a}} = \frac{e + bi + cj + dk}{\sqrt{a}}.$$
   则方程变为 $y^2 = 1$. 此时, $|y|^2 = 1$, 故
   $$y = y^{-1} \cdot y \cdot y = y^{-1} \cdot y^2 = y^{-1} \cdot 1 = y^{-1} = \frac{1}{|y|^2}\bar{y} = \bar{y}.$$
   从而得
   $$y = \frac{e}{\sqrt{a}}, \quad b = c = d = 0.$$
   因此, $\frac{e}{\sqrt{a}} = \pm 1$, 所以, $x = e = \pm\sqrt{a}$, 故原方程的解集为 $\{\sqrt{a}, -\sqrt{a}\}$.

2. 当$a < 0$ 时:

   令
   $$y = \frac{x}{\sqrt{-a}} = \frac{e + bi + cj + dk}{\sqrt{-a}}.$$
   则方程变为 $y^2 = -1$. 此时, $|y|^2 = 1$, 故
   $$y = y^{-1} \cdot y \cdot y = y^{-1} \cdot y^2 = y^{-1} \cdot (-1) = -y^{-1} = -\frac{1}{|y|^2}\bar{y} = -\bar{y}.$$
   从而得
   $$y = \frac{bi + cj + dk}{\sqrt{a}}, \quad e = 0.$$
   因此
   $$1 = |y|^2 = \frac{b^2 + c^2 + d^2}{-a}.$$
   所以 $b^2 + c^2 + d^2 = -a$. 故原方程的解集为 $\{bi + cj + dk \mid b^2 + c^2 + d^2 = -a,\ b, c, d \in \mathbb{R}\}$.

3. 当$a = 0$ 时:

   $x^2 = 0$, 因为, $\mathbb{H}$ 为一个除环, 故, $\mathbb{H}$ 上没有非零零因子, 所以 $x = 0$, 即此时方程解集为 $\{0\}$.

3 复数的矩阵实现

最后我们再看一些有趣的结果: 易知,

$$\mathbb{R}+\mathbb{R}I,\mathbb{R}+\mathbb{R}J,\mathbb{R}+\mathbb{R}K\cong\mathbb{C}.$$

只要分别定义 $I\mapsto i,\ J\mapsto i,\ K\mapsto i$ 即可. 于是

$$M=\left\{\begin{pmatrix}a & b\\ -b & a\end{pmatrix}\mid a,b\in\mathbb{R}\right\}=\mathbb{R}+\mathbb{R}J\cong\mathbb{C},$$

$$a+bi\mapsto aE_2+bJ=\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}+\begin{pmatrix}0 & b\\ -b & 0\end{pmatrix}=\begin{pmatrix}a & b\\ -b & a\end{pmatrix}=X\in M.$$

这是复数的矩阵实现.(对称分解)

注: 在矩阵的学习中, 我们知道, 任何一个矩阵都可以分解成一个对称矩阵和一个反对称矩阵的和, 这一结论的证明非常简单即:

$$X=\frac{X+X'}{2}+\frac{X-X'}{2}.$$

这个结论看起来无足轻重，但事实上它正好对应着复数 $x=a+bi$ 的实部和虚部的分解. (在其上可以讨论它们的和、 乘、 逆、 共轭、 模等) 令$x=a+\vec{u},\ y=a'+\vec{v}$, 定义

$$x\cdot y=aa'-(\vec{u},\vec{v})+(a\vec{v}+a'\vec{u}+\vec{u}\times\vec{v}).$$

This is a wonderful formula ! (它包含了向量的全部运算)

问题思考:

1、设 $P\subset\mathbb{R}$ 是子域

$$\mathbb{H}_P=\{a+bi+cj+dk\mid a,b,c,d\in P\}.$$

则 $\mathbb{H}_P$ 为 $\mathbb{H}$ 的子除环.

2、若上述的 $P=\mathbb{Z}_p$, 则 $\mathbb{H}_P$ 还是除环吗?

3、 $I=\{a+bi+cj+dk\mid a,b,c,d\in\mathbb{C}\}$, 则 I 是否为除环?

证明： 1、因为 P 非空, 故存在一元 $a\in P\subset\mathbb{H}_P$, 故 $\mathbb{H}_P$ 非空. 又 P 为一个域, 所以 $ab\in P$, $a-b\in P\quad\forall a,b\in P$, 则易证

$$xy=(a+bi+cj+dk)(e+fi+sj+tk)\in\mathbb{H}_P,$$

$$x-y=(a+bi+cj+dk)-(e+fi+sj+tk)\in\mathbb{H}_P.$$

其中 $a,b,c,d,e,f,s,t\in P$, 所以, $\mathbb{H}_P$ 为 $\mathbb{H}$ 的子环. 显然 P 中的单位元即为 $\mathbb{H}_P$ 中单位元.又因为

$$x\cdot\bar{x}=(a+bi+cj+dk)(a-bi-cj-dk)=a^2+b^2+c^2+d^2.$$

而$P\subset\mathbb{R}$ 是子域, 若 $x\neq 0$ 则 $l=a^2+b^2+c^2+d^2\neq 0$， 且

$$\frac{\pm a}{l},\ \frac{\pm b}{l},\ \frac{\pm c}{l},\ \frac{\pm d}{l}\in P.$$

因此,

$$x^{-1}=\frac{\bar{x}}{l}=\frac{a}{l}+\frac{-b}{l}i+\frac{-c}{l}j+\frac{-d}{l}k\in\mathbb{H}_P.$$

即 $\mathbb{H}_P$ 中非零元有逆元, 所以 $\mathbb{H}_P$ 为一除环.

2、因为 p 为素数, 由引子中的注知道 p 可表为四个整数的和, 即有 $a,b,c,d\in\mathbb{Z}_+$ 使 $p=a^2+b^2+c^2+d^2$. 其中, a,b,c,d 中至少有三个元小于 p , 不妨设 $a<p$, 则在域 $P=\mathbb{Z}_p$ 上 $a\neq 0$, 故 $x=a+bi+cj+dk\neq 0$, 但 $x\bar{x}=a^2+b^2+c^2+d^2=p=0$, 所以 x 无逆元, 故此时, $\mathbb{H}_P$ 不是除环.

3、取 $0\neq x=1+\sqrt{-1}i+0j+0k\in I$, 但 $x\cdot\bar{x}=a^2+b^2+c^2+d^2=1+(-1)=0$ 所以 x 是非零零因子(x 无逆元), 故 I 不是除环.