arXiv:2305.02072v1 [cs.SC] 3 May 2023

除四元数代数上的多项式因式分解与求根

普热梅斯瓦夫·科普罗夫斯基

摘要。多项式因式分解与求根是计算数学中最常见的主题之一。然而，关于四元数代数上的多项式，相关研究仍然寥寥无几，唯一的例外是哈密顿四元数，针对它已有用于近似求多项式根的数值方法。本文的唯一目的，是介绍一种适用于数域上除四元数代数的多项式因式分解算法，并将其推广用于求根。

1. 引言

多项式因式分解是计算代数领域的经典课题之一。几十年来，人们已开发出众多算法，用于在各种基环上分解多项式，例如整数、有理数、有限域、局部域和整体域等。然而，仍有许多重要的环类尚无已知的多项式因式分解方法。四元数代数就是其中一个显著的空白。尽管四元数多项式是一个经典课题，自 20 世纪上半叶以来便一直受到研究，但其理论的算法方面仍极不发达。据我们所知，迄今开发的算法仅专注于实四元数代数上的多项式，尤其是哈密顿四元数（例如，[11, 12, 24, 29, 31] 中的求根算法，或 [21, 22, 30] 中的因式分解算法）。遗憾的是，为实四元数开发的方法无法应用于一般情形。根本原因在于，哈密顿四元数满足代数学基本定理，而一般的除四元数代数则不然。据作者所知，甚至没有一篇论文讨论一般四元数代数上的多项式因式分解。因此，本文唯一的目的就是部分弥补这一不足，并介绍用于分解数域上除四元数代数上的多项式的算法（见算法 3），以及用于求此类代数中多项式根的算法（见算法 4）。

定义一般结合环上的多项式有几种不同的方法。如果环是交换的，这些定义都一致；但当系数环是非交换环时，情况就不再如此。本文采用最经典的方法：在结合环 $\mathfrak{A}$ 上，多项式是指和式 $\mathfrak{p} = \mathfrak{a}_0 + \mathfrak{a}_1 x + \cdots + \mathfrak{a}_n x^n$，其中系数 $\mathfrak{a}_0$、……、$\mathfrak{a}_n$ 取自 $\mathfrak{A}$，且不定元 x 与这些系数交换。这类多项式在 [9, 10] 中称为 左多项式，在 [8, 12, 31] 等较新的文献中则称为 单侧多项式。

本文始终采用以下记号约定：交换环及其元素使用标准字体排印，而非交换环及其元素则使用哥特字体。此外，K 始终表示一个数域，即有理数域 $\mathbb{Q}$ 的有限扩张。回顾一下，若代数 $\mathfrak{A}$ 在 K 上具有一组基，

其形式为 $\{1, \mathfrak{i}, \mathfrak{j}, \mathfrak{k}\}$ ，并满足以下关系：

$$\mathfrak{i}^2 = \alpha, \qquad \mathfrak{j}^2 = \beta, \qquad \mathfrak{ij} = \mathfrak{k} = -\mathfrak{ji},$$

对于某些非零元素 $\alpha, \beta \in K$。代数 $\mathfrak{A}$ 因此记作 $\left(\frac{\alpha,\ \beta}{K}\right)$。关于四元数代数理论的深入介绍，请参阅[37] 和 [39]。我们始终将基域 K 视为 $\mathfrak{A}$的子代数 $K \cdot 1$；已知它构成了 $\mathfrak{A}$的中心 $Z(\mathfrak{A})$。我们用 $K^\times$ （分别用$\mathfrak{A}^\times$）表示 K 的非零元素乘法群（分别表示 $\mathfrak{A}$中可逆元素组成的群）。

每个四元数代数都配备有一种标准对合，下文用上划线表示。对于四元数 $\mathfrak{a} \in \mathfrak{A}$，乘积 $\mathfrak{a}\overline{\mathfrak{a}}$称为 $\mathfrak{a}$ 的范数 （在 [18]中）或约化范数 （在 [37, 39]中），记作 $N\mathfrak{a}$。同样，和 $\mathfrak{a} + \overline{\mathfrak{a}}$ 称为 $\mathfrak{a}$的（约化）迹，记作 $\mathrm{Tr}\ \mathfrak{a}$。自然包含 $\left(\frac{\alpha,\ \beta}{K}\right)[x] \hookrightarrow \left(\frac{\alpha,\ \beta}{K(x)}\right)$ 使我们能够将范数和标准对合的概念扩展到四元数多项式。特别地，若 $\mathfrak{p} = \mathfrak{a}_0 + \mathfrak{a}_1 x + \cdots + \mathfrak{a}_n x^n$，则 $\overline{\mathfrak{p}} = \overline{\mathfrak{a}_0} + \overline{\mathfrak{a}_1} x + \cdots + \overline{\mathfrak{a}_n} x^n$ 且 $N\mathfrak{p} = \mathfrak{p}\overline{\mathfrak{p}}$。我们将用同一符号 N 表示域扩张中的标准范数及其在多项式环上的自然延拓。如有歧义，我们会在范数的下标中标明相应的扩张。

四元数代数要么是除代数，要么同构于 2×2矩阵代数 $M_2 K$ （例如，参见 [39, 定理 5.4.4]）。当且仅当 2 重 Pfister 型 $\langle\langle -\alpha, -\beta \rangle\rangle = x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2$ 是各向同性的（即它有非平凡的零点）时，后一种情况才会发生。此时，四元数代数 $\left(\frac{\alpha,\ \beta}{K}\right)$ 称为分裂的。

2. 预备知识

注意，在分裂四元数代数上，每个多项式 $p \in K[x]$ 都有平凡的因式分解。事实上，若将 $\mathfrak{A}$ 与 $M_2 K$ 等同，并将 K 与其标量矩阵子域等同，则可写成

$$\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \cdot \overline{\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}}.$$

请注意，上述构造的 p 两个因子的次数都与多项式 p 本身的次数相同。这是因为除常数项外，它们的所有系数都是零因子。因此，在本文余下部分，我们将完全专注于除四元数代数上的多项式。

下面汇集一些关于除四元数代数上多项式的已知事实。这些事实都非常经典，但散见于文献之中，有时使用的术语也不尽相同。关于除环上的多项式环（包括除四元数代数）的概论，读者可参阅 [17, §16]。

定理 1 (Ore)。 *如果 $\mathfrak{A}$ 是一个除四元数代数，那么四元数多项式环 $\mathfrak{A}[x]$ 支持带余数的右除法以及右欧几里得算法。*

特别地，对于任意两个四元数多项式 $\mathfrak{p}$、$\mathfrak{q} \in \mathfrak{A}[x]$，都存在唯一的首一最大公右因子（下文记为 $\mathrm{gcrd}(\mathfrak{p}, \mathfrak{q})$）和最小公左倍数（记为 $\mathrm{lclm}(\mathfrak{p}, \mathfrak{q})$）。事实上，[25, 定理 I.8]给出了一个显式公式，可以根据右欧几里得算法计算出的右余数序列构造最小公左倍数。不过，在本文中我们不会使用这个公式。

定理 2 (Ore)。 *如果 $\mathfrak{A}$ 是除四元数代数，那么每个首一多项式 $\mathfrak{p} \in \mathfrak{A}[x]$ 都可以表示为不可约四元数多项式的乘积。 $\mathfrak{p}$ 的任意两种此类因式分解都具有相同数目的因子。*

上述两个定理的证明见 [25, 第一章，第 2 节和定理 II.1]。当然，一般而言，即使假设所有因子都是首一的，一个四元数多项式也可能有无穷多种不同的因式分解。为观察这一现象，取任意一个系数属于基域的非零首一多项式 $p \in K[x]$ 。假设 p 可分解为两个首一四元数多项式 $\mathfrak{pq} \in \mathfrak{A}[x]$的乘积 $p = \mathfrak{pq}$ ，它们不一定不可约。那么，对于每个可逆四元数 $\mathfrak{a} \in \mathfrak{A}$ ，都有

$$p = \mathfrak{a}p\mathfrak{a}^{-1} = (\mathfrak{apa}^{-1})(\mathfrak{aqa}^{-1}).$$

如果只有 $\mathfrak{p}, \mathfrak{q} \notin K[x]$，通过这种方式我们得到 p 的另一种因式分解，其中 $\mathfrak{apa}^{-1}$ 和 $\mathfrak{aqa}^{-1}$ 又是首一的。

命题 3 (Beck)**.** 设 $\mathfrak{A}$ 是 K 上的除四元数代数。那么每个多项式 $\mathfrak{p} \in \mathfrak{A}[x]$ 都可以唯一地表示为乘积 $\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q} \cdot p$，其中 $\mathfrak{c} \in \mathfrak{A}^\times$ 是 $\mathfrak{p}$ 的首项系数， p 是一个系数属于 K 的首一多项式，而 $\mathfrak{q} \in \mathfrak{A}[x]$ 是一个不能被来自 $K[x]$ 的任何非恒定多项式整除的首一四元数多项式。此外，如果将 $\mathfrak{A}[x]$ 视为 $K[x]$ 上秩为 4 的自由模，其一组基为 $\{1, \mathfrak{i}, \mathfrak{j}, \mathfrak{k}\}$，那么 p 是 $\mathfrak{p}$ 的坐标的最大公因式 (在 $K[x]$) 。

上一命题中所述的多项式 p 称为 $\mathfrak{p}$ 的最大中心因子。命题 3 的证明可见 [2, Résultat 4]。根据该命题，显然，要分解四元数多项式，只需有一种方法分解在 $K[x]$中不可约的 $\mathfrak{A}[x]$ 多项式，以及另一种方法分解不能被来自 $K[x]$的多项式整除的四元数多项式。

引理 4. 设 $\mathfrak{A} = \left(\frac{\alpha, \beta}{K}\right)$ 是 K 上的除四元数代数，且 $\mathfrak{a}, \mathfrak{b} \in \mathfrak{A}$ 是两个四元数。若 $\mathfrak{ab} \in Z(\mathfrak{A}) = K$，则以下两个条件成立：

(1) $\mathfrak{ab} = \mathfrak{ba}$;(2) 存在标量 $c, d \in K$ 使得 $c \cdot \mathfrak{b} = d \cdot \overline{\mathfrak{a}}$

证明。 如果 $\mathfrak{a} = 0$ 或 $\mathfrak{b} = 0$，则结论显然成立。因此，不失一般性，我们可以假设 $\mathfrak{a}$、 $\mathfrak{b} \in \mathfrak{A}^\times$ ，从而它们的乘积 $d := \mathfrak{ab}$ 非零。计算

$$\mathfrak{ba} = \mathfrak{a}^{-1}\mathfrak{aba} = \mathfrak{a}^{-1} \cdot d \cdot \mathfrak{a} = d \cdot \mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{ab}.$$

这证明了第一个断言。第二个断言则立即可得。事实上，由$\mathfrak{ab} = d$ 可知

$$N(\mathfrak{a}) \cdot \mathfrak{b} = N(\mathfrak{a}) \cdot \mathfrak{a}^{-1} \cdot d = d \cdot \overline{\mathfrak{a}}. \qquad \square$$

注记 1. $\mathfrak{A}$ 是除代数这一假设不可或缺。为说明这一点，取分裂四元数代数 $\mathfrak{A} = M_2K$ ，并令

$$\mathfrak{a} := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \mathfrak{b} := \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

那么 $\mathfrak{ab}$ 是零矩阵，因此特别有 $\mathfrak{ab} \in Z(\mathfrak{A})$，但是

$$\mathfrak{ba} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \mathfrak{ab}.$$

命题 5. 设 $\mathfrak{A} = \left(\frac{\alpha, \beta}{K}\right)$ 是 K 上的四元数除环。此外，设 $p \in K[x]$ 是一个系数属于 K 的首一不可约多项式。那么， p 要么在 $\mathfrak{A}[x]$ 中仍不可约，要么分解为乘积 $p = \mathfrak{p}\overline{\mathfrak{p}}$ ，其中某个不可约四元数多项式为 $\mathfrak{p} \in \mathfrak{A}[x]$。

证明。假设 p 在 $\mathfrak{A}[x]$ 中不是不可约的。设 $p=\mathfrak{p}\mathfrak{q}$ 是 p 的某种因式分解，其中 $\mathfrak{p}$、$\mathfrak{q}\in\mathfrak{A}[x]$。将前一个引理应用于四元数代数$\left(\frac{\alpha,\beta}{K}\right)$，并利用 $\mathfrak{p}$、$\mathfrak{q}$ 和 p 都是多项式这一事实，我们得到

$$p=\mathfrak{p}\overline{\mathfrak{p}}\cdot q$$

对于某个多项式 $q\in K[x]$。由于范数 $N\mathfrak{p}=\mathfrak{p}\overline{\mathfrak{p}}$ 也属于 $K[x]$，因此根据 p 的不可约性，可得 $\deg q=0$，即 $q\in K$。

仍需证明 $\mathfrak{p}$ 在 $\mathfrak{A}[x]$ 中是不可约的。假设存在一些非零次多项式 $\mathfrak{q}$、$\mathfrak{r}\in\mathfrak{A}[x]$，使得 $\mathfrak{p}=\mathfrak{q}\mathfrak{r}$。因此

$$p=\mathfrak{q}\mathfrak{r}\cdot\overline{\mathfrak{q}\mathfrak{r}}=\mathfrak{q}\cdot\mathfrak{r}\overline{\mathfrak{r}}\cdot\overline{\mathfrak{q}}=\mathfrak{q}\overline{\mathfrak{q}}\cdot\mathfrak{r}\overline{\mathfrak{r}}.$$

但这与 p 作为 $\mathfrak{q}\overline{\mathfrak{q}}$、$\mathfrak{r}\overline{\mathfrak{r}}\in K[x]$ 的不可约性相矛盾。 □

现在我们可以给出 $\mathfrak{A}[x]$ 中的不可约性判据。

命题 6. 设 $\mathfrak{A}=\left(\frac{\alpha,\beta}{K}\right)$ 是数域 K上的除四元数代数。此外，设 $p\in K[x]$ 是首一不可约多项式，且 $L:=K[x]/(p)$。那么，p 在 $\mathfrak{A}[x]$ 中仍然不可约，当且仅当 $\mathfrak{A}\otimes L$ 不分裂。

证明。命题 5 断言，p 在 $\mathfrak{A}[x]$ 中不可约，当且仅当它不等于任何多项式 $\mathfrak{p}\in\mathfrak{A}[x]$的范数 $N\mathfrak{p}=\mathfrak{p}\overline{\mathfrak{p}}$。后一条件等价于：$p$ 不能由 Pfister 型$\langle\langle-\alpha,-\beta\rangle\rangle=\langle 1,-\alpha,-\beta,\alpha\beta\rangle$在 $K[x]$ 上表示，该型是 $\mathfrak{A}$的范数型。现在，由于根据假设 p是首一的，由 [26, 命题 3]（或 [27, 引理 17.3]）可知，p 不能由此型表示，当且仅当 L 不是 $\mathfrak{A}$的分裂域。□

备注 2. 文献 [38] 介绍了一种用于检验数域上的四元数代数是否分裂的程序，该程序也可在一些计算机代数系统中轻易获取，例如 Magna [4] 和 Sage [33]。因此，上述不可约性检验很容易实现。作者为计算机代数系统 Magma [4]编写了一个示例实现（见结尾部分）。

比较次数后，我们立即得到命题 6 的以下推论，可在检验不可约性的过程中用作快速退出条件。

推论 7. 设 $\mathfrak{A}$ 为除四元数代数，$p\in K[x]$ 为奇次数的首一不可约多项式，则 p 在 $\mathfrak{A}[x]$ 中仍然不可约。

最后，作为本节的总结，我们给出一个完整的四元数多项式不可约性判据，该判据可以直接在计算机代数系统中实现。

定理 8. 设 $\mathfrak{A}$ 是数域 K上的除四元数代数。此外，设 $\mathfrak{p}\in\mathfrak{A}[x]$ 是一个非常数多项式，$\mathfrak{p}=\mathfrak{c}\cdot\mathfrak{q}\cdot p$ 是其按照命题 *3* 所作的分解。

<escape>(1) *</escape>*如果 $\mathfrak{q}=1$，那么 $\mathfrak{p}$ 在 $\mathfrak{A}[x]$ 中不可约，当且仅当 p 在 $K[x]$ 中不可约，且 $\mathfrak{A}\otimes L$ 不分裂，其中 L *<escape>*$:=K[x]/(p)$.(2) *</escape>*如果 $p=1$，那么 $\mathfrak{p}$ 在 $\mathfrak{A}[x]$ 中不可约，当且仅当 $\mathfrak{q}$ 的范数 $N\mathfrak{q}$ 在 $K[x]$ 中不可约。*<escape>*(3) *</escape>*如果 $\mathfrak{q}\neq 1$ 且 $p\neq 1$，那么 $\mathfrak{p}$ 在 $\mathfrak{A}[x]$ 中可约。

证明。第一个断言直接由命题 6 得出，而第三个断言是显然的。我们只需证明断言（2）。不失一般性，设 $\mathfrak{p}$ 是首一的。因此，$\mathfrak{p}=\mathfrak{q}$。若 $\mathfrak{p}$ 可约，设 $\mathfrak{p}=\mathfrak{p}_1\mathfrak{p}_2$，那么 $N\mathfrak{q}=N\mathfrak{p}_1\cdot N\mathfrak{p}_2$ 在 $K[x]$ 中也可约。这就证明了一个方向。现在，设 $\mathfrak{p}$ 不可约，但 $N\mathfrak{q}$ 具有因式分解 $N\mathfrak{q}=q_1q_2$，其中 q_1、$q_2\in K[x]$ 是非常数多项式。根据假设，$\mathfrak{p}$ 的最大中心因子是平凡的。因此，和 都不被多项式 $\mathfrak{p}$、$\mathfrak{p}=\mathfrak{q}$ 中的任何一个整除。但我们有 $\mathfrak{p}$。

因此， [25, p。 494] 表明， $\mathfrak{p}$ 被 $\operatorname{lclm}(q_2, \overline{\mathfrak{p}}) \cdot \overline{\mathfrak{p}}^{-1} = q_2$ 右可除。这一矛盾意味着 $N\mathfrak{q}$ 必须是不可约的，从而证明了断言（2）。□

3. 中心多项式的因式分解

我们的首要任务是在 $\mathfrak{A}[x]$ 中分解一个系数属于基域 K 的不可约多项式 p。在全面讨论这个问题之前，我们先处理一个特殊情形。如果 K_* 有一个极大（交换）子域 K_*，且该子域嵌入到 $L := {}^{K[x]}\!/_{(p)}$ 中，那么在 $\mathfrak{A}[x]$ 中对 p 进行因式分解就格外容易。

引理9。设 $\mathfrak{A}$ 是数域 K 上的除四元数代数，且$p \in \mathfrak{A}[x]$ 是次数为 次数$p > 1$ 的首一不可约多项式。设 $L := {}^{K[x]}\!/_{(p)}$。如果存在 $\mathfrak{A}$ 的极大交换子域 K_*，使得对于某个多项式 $q \in K_*[x]$有 $p = N_{K_*/K}(q)$，那么

(1) K_* 嵌入到 L; (2) p在 $\mathfrak{A}[x]$ 中具有非平凡因式分解; (3) 四元数代数 $\mathfrak{A} \otimes L$ 是分裂的。

证明。令 $K_* = K(\sqrt{d})$ 满足对于某个 $q \in K_*[x]$，有 $p = N_{K_*/K}(q)$。设 $q = q_0 + q_1\sqrt{d}$。那么 $p = q_0^2 - q_1^2 d$。令 $a_i := q_i + (p) \in L$，其中 $i \in \{0, 1\}$。我们有

$$0 = a_0^2 - a_1^2 d$$

因此， d 是 L中的一个平方。这意味着 K_* 嵌入到 L中。现在， $p = (q_0 + q_1\sqrt{d})(q_0 - q_1\sqrt{d})$，其中 q_0、 $q_1 \in K_*[x] \subset \mathfrak{A}[x]$。因此， p 在 $\mathfrak{A}[x]$中具有非平凡因式分解。第三个断言现在由命题 6 得出。□

算法 1。设 $\mathfrak{A}$ 是数域 K 上的除四元数代数，并设 $p \in K[x]$ 是首一不可约多项式。如果存在一个 $\mathfrak{A}$ 的极大交换子域，使得 p 在其上可以进行因式分解，则该算法输出 p 在 $\mathfrak{A}$ 上的因式分解。否则，报告失败。

(1) 构造域扩张 $L := {}^{K[x]}\!/_{(p)}$。*(2)* 构造 L 的所有子域 $L_1, \ldots, L_n$，它们在 K 上的次数为 *2* （见下文注 *3* ）。*(3)* 对每个 L_i 重复以下步骤：*(a)* 检查四元数代数 $\mathfrak{A} \otimes L_i$ 是否分裂。若不分裂，则重新执行循环。*(b)* 求出一个嵌入 $\varphi : L_i \hookrightarrow \mathfrak{A}$ （见下文注*4*），并令 $K_* := \varphi(L_i)$。*(c)* 在 $K_*[x]$ 中将 p 因式分解为乘积 $p = \mathfrak{q} \cdot \overline{\mathfrak{q}}$，其中 $\mathfrak{q} \in K_*[x] \subset \mathfrak{A}[x]$。*(d)* 输出 $(\mathfrak{q}, \overline{\mathfrak{q}})$ 并退出。*(4)* 报告失败。

正确性证明。设 K_* 是 K 的一个极大（交换）子域，且 p 在 $K_*[x]$ 中有非平凡因式分解，则 $(K_* : K) = 2$，因此根据引理9， K_* 嵌入 L。因此， K_* 同构于算法第 (2) 步构造的域 $L_1, \ldots, L_n$ 中的一个。所以，第 (3d) 步会返回 p 的一个真因式分解。反过来，假设 L_i 是 L 的一个子域，它是 K 的二次扩张，且 $\mathfrak{A} \otimes L_i$ 分裂。那么， [37, Theorem I.2.8] 断言 L_i 嵌入 $\mathfrak{A}$。因此，在同构意义下，它是 $\mathfrak{A}$ 的一个极大子域。□

注3。在给定的域扩张 L/K 中找出所有次数固定的子域，是一个活跃的研究领域。有关解决这一问题的算法可见于 [7, 13, 14, 32, 35, 36]。

注记 4. 设 M 是 K 的一个二次扩张，使得 $\mathfrak{A}\otimes M$ 分裂。取一个元素 $d\in K$，它在 M 中是一个平方，但在 K中不是平方。则 $M=K(\sqrt{d})$。现在，[37, 定理 I.2.8] 断言， M 嵌入到 $\mathfrak{A}$中。因此， d 是某个纯四元数 $\mathfrak{a}\in\mathfrak{A}$的平方。于是，$a+b\sqrt{d}\mapsto a+b\mathfrak{a}$ 是从 M到 $\mathfrak{A}$的一个嵌入。通过求解两个范数方程，可以直接构造四元数 $\mathfrak{a}$ （参见例如 [16]）。

注记 5. 本文提出的所有算法都依赖于我们对数域上的多项式进行因式分解的能力，这些数域可以是基域 K ，也可以是它的二次扩张 K_*。幸运的是，数域上多项式的因式分解是一门研究成熟的学科。读者可参阅 [1, 3, 19, 20, 23, 28]。

现在我们将发展本节的主要过程：该过程接收一个在 $\mathfrak{A}$ 的每个交换子域中都不可约的多项式$p\in K[x]$，并构造一个四元数多项式 $\mathfrak{p}$ ，使得 $p=\mathfrak{p}\overline{\mathfrak{p}}$。总体思路是利用这一事实（见命题 6）： $\mathfrak{A}[x]$ 中存在 p 的非平凡因式分解，意味着 $\mathfrak{A}\otimes L$ 分裂，其中和之前一样， $L:=K[x]/(p)$。然后，我们可以利用 $\mathfrak{A}\otimes L$ 的零因子来找到一个多项式 $\mathfrak{p}\in\mathfrak{A}[x]$ ，使得 $\mathfrak{p}\overline{\mathfrak{p}}=pq$ ，其中带有某个无关因子 q。这可以被视为 p的“近似因式分解”。随后，我们将逐步改进这一“近似”，降低 q的次数。首先，我们证明一些预备引理。

引理 10. 设 $p,q\in K[x]$ 和 $\mathfrak{p}\in\mathfrak{A}[x]$ 为多项式，且设 $\mathfrak{r}\in\mathfrak{A}[x]$ 为 $\mathfrak{p}$ 模 q的余数。若 $pq=\mathfrak{p}\overline{\mathfrak{p}}$，则 q 整除多项式 $\mathfrak{r}\overline{\mathfrak{r}}$ 和 $\mathfrak{p}\overline{\mathfrak{r}}$。

证明. 存在某个四元数多项式 $\mathfrak{q}\in\mathfrak{A}[x]$，使得 $\mathfrak{p}=\mathfrak{q}\cdot q+\mathfrak{r}$。计算

$$\begin{aligned}\mathfrak{r}\overline{\mathfrak{r}}&=(\mathfrak{p}-\mathfrak{q}\cdot q)(\overline{\mathfrak{p}-\mathfrak{q}\cdot q})\\&=\mathfrak{p}\overline{\mathfrak{p}}-\mathfrak{p}\overline{\mathfrak{q}}\cdot q-\mathfrak{q}\overline{\mathfrak{p}}\cdot q+\mathfrak{q}\overline{\mathfrak{q}}\cdot q^2\\&=pq-\mathfrak{p}\overline{\mathfrak{q}}\cdot q-\mathfrak{q}\overline{\mathfrak{p}}\cdot q+\mathfrak{q}\overline{\mathfrak{q}}\cdot q^2\\&=(p-\mathfrak{p}\overline{\mathfrak{q}}-\mathfrak{q}\overline{\mathfrak{p}}+\mathfrak{q}\overline{\mathfrak{q}}\cdot q)\cdot q.\end{aligned}$$

这证明了第一个断言。对于第二个断言，写作

$$\mathfrak{p}\overline{\mathfrak{r}}=(\mathfrak{q}\cdot q+\mathfrak{r})\cdot\overline{\mathfrak{r}}=\mathfrak{q}\overline{\mathfrak{r}}\cdot q+\mathfrak{r}\overline{\mathfrak{r}}.$$

现在，由证明的前一部分可知，上述公式的右端可被 q 整除，因此 $\mathfrak{p}\overline{\mathfrak{r}}$也可被整除，证毕。□

引理 11. 保留前一个引理的假设，并设 $\mathfrak{q}:=\mathfrak{p}\overline{\mathfrak{r}}\cdot q^{-1}\in\mathfrak{A}[x]$。则 p整除 $\mathfrak{q}\overline{\mathfrak{q}}$。

证明. 计算

$$\begin{aligned}\mathfrak{q}\overline{\mathfrak{q}}&=(\mathfrak{p}\overline{\mathfrak{r}}\cdot q^{-1})\overline{(\mathfrak{p}\overline{\mathfrak{r}}\cdot q^{-1})}\\&=\mathfrak{p}\overline{\mathfrak{r}}\mathfrak{r}\overline{\mathfrak{p}}\cdot q^{-2}\\&=\mathfrak{p}\overline{\mathfrak{p}}\cdot\mathfrak{r}\overline{\mathfrak{r}}\cdot q^{-2}\\&=pq\cdot\mathfrak{r}\overline{\mathfrak{r}}\cdot q^{-2}\\&=(\mathfrak{r}\overline{\mathfrak{r}}\cdot q^{-1})\cdot p.\end{aligned}$$

该断言现由前述引理得出。 □

引理 12。 保留引理 *10* 和 *11* 的假设。记作 $r:=\mathfrak{q}\overline{\mathfrak{q}}\cdot p^{-1}\in K[x]$。则 次数$r<$次数 q。

证明。 所涉及多项式的次数之间具有以下关系：

- 度$r=2\cdot$度 $\mathfrak{q}-$度 p，因为$r=\mathfrak{q}\overline{\mathfrak{q}}\cdot p^{-1}$;

- 度$\mathfrak{q}=$度 $\mathfrak{p}+$度 $\mathfrak{r}-$度 q，因为 $\mathfrak{q}=\mathfrak{p}\overline{\mathfrak{r}}\cdot q^{-1}$;
- $2\cdot$度 $\mathfrak{p}=$度 $p+$度q，因为 $pq=\mathfrak{p}\overline{\mathfrak{p}}$;
- 度$\mathfrak{r}<$度 q，因为 $\mathfrak{r}$是 $\mathfrak{p}$模 q的余数。

综合这四个条件，我们得到如下结论：

$$\begin{aligned}\deg r &= 2\deg\mathfrak{q}-\deg p\\ &= 2\deg\mathfrak{p}+2\deg\mathfrak{r}-2\deg q-\deg p\\ &= \deg p+\deg q+2\deg\mathfrak{r}-2\deg q-\deg p\\ &= 2\deg\mathfrak{r}-\deg q\\ &< 2\deg q-\deg q=\deg q.\end{aligned}$$ □

现在，我们已经可以给出一种在 $\mathfrak{A}[x]$ 中分解系数属于 K 的不可约多项式 p 的算法。

算法 2. 设 $\mathfrak{A}=\left(\frac{\alpha,\ \beta}{K}\right)$ 是数域 K上的除四元数代数。给定一个首一不可约多项式 $p\in K[x]$，此算法输出其在 $\mathfrak{A}[x]$中的不可约因子。

(1) 构造域扩张 $L=K[x]/(p)$。*(2)* 检查四元数代数 $\mathfrak{A}\otimes L$ 是否分裂。如果不分裂，则输出 p并退出。*(3)* 执行算法 *1*。如果返回 p的因式分解 $(\mathfrak{p},\overline{\mathfrak{p}})$，则输出 $(\mathfrak{p},\overline{\mathfrak{p}})$并退出。*(4)* 求一个零因子 $\mathfrak{a}=a_0+a_1\mathfrak{i}+a_2\mathfrak{j}+a_3\mathfrak{k}\in\mathfrak{A}\otimes L$ （见备注 *6*）。*(5)* 令 $\mathfrak{p}\in\mathfrak{A}[x]$ 为 $\mathfrak{a}$ 在自然同态$\mathfrak{A}[x]\to\mathfrak{A}\otimes K[x]/(p)$下的原像，即 $\mathfrak{p}:=q_0+q_1\cdot\mathfrak{i}+q_2\cdot\mathfrak{j}+q_3\cdot\mathfrak{k}$，其中 q_0、.....、$q_3\in K[x]$是满足 $q_i+(p)=a_i$ （对 $i\le 3$）的多项式。*(6)* 设 $q:=\mathfrak{p}\overline{\mathfrak{p}}\cdot p^{-1}$。*(7)* 当 q 不是常数时，重复执行：*(a)* 计算 $\mathfrak{p}$模 q的余数 $\mathfrak{r}$。*(b)* 更新 $\mathfrak{p}$，令 $\mathfrak{p}:=\mathfrak{p}\overline{\mathfrak{r}}\cdot q^{-1}$。*(c)* 更新 q，令 $q:=\mathfrak{p}\overline{\mathfrak{p}}\cdot p^{-1}$。*(8)* 令 $\mathfrak{c}:=lc\,\mathfrak{p}$ 为 $\mathfrak{p}$的首项系数。*(9)* 输出 $(\mathfrak{p}\cdot\mathfrak{c}^{-1},\overline{\mathfrak{c}}^{-1}\cdot\overline{\mathfrak{p}})$。

正确性证明。 命题 6 断言， p 在 $\mathfrak{A}[x]$ 中不可约，当且仅当 $\mathfrak{A}\otimes L$ 不分裂。这证明了步骤 (2) 的正确性。假设算法在步骤 (2) 或 (3) 未终止。这意味着 $\mathfrak{A}\otimes L$ 分裂（即它与 M_2L同构），因此它包含一个零因子 $\mathfrak{a}=a_0+a_1\mathfrak{i}+a_2\mathfrak{j}+a_3\mathfrak{k}$。现在，$\mathfrak{a}$ 是零因子，当且仅当其范数为零（例如参见 [39, 练习 3.7]）：

$$N\mathfrak{a}=a_0^2-\alpha a_1^2-\beta a_2^2+\alpha\beta a_3^2=0.$$

令多项式 $\mathfrak{p}\in\mathfrak{A}[x]$ 按步骤 (5) 中的定义给出。现在，前一个公式可写为

$$\mathfrak{p}\overline{\mathfrak{p}}+(p)=q_0^2-\alpha q_1^2-\beta q_2^2+\alpha\beta q_3^2+(p)=0.$$

因此， p 整除 $\mathfrak{p}\overline{\mathfrak{p}}$，所以 q 是一个定义良好的多项式，满足条件$pq=\mathfrak{p}\overline{\mathfrak{p}}$。引理 10 表明， q 整除 $\mathfrak{p}\overline{\mathfrak{r}}$，其中 $\mathfrak{r}$ 是 $\mathfrak{p}$ 模 q所得的余数。因此，在步骤 (7b) 中更新 $\mathfrak{p}$ 后，我们再次得到一个（四元数）多项式。由引理 11 可知， p 整除更新后的多项式 $\mathfrak{p}$的范数 $N\mathfrak{p}=\mathfrak{p}\overline{\mathfrak{p}}$。因此，在步骤 (7c) 中再次更新 q 后，我们得到一个多项式，并且它显然满足条件 $pq=\mathfrak{p}\overline{\mathfrak{p}}$。此外，引理 12 断言，每次循环迭代后， q 的次数都会减小。因此，循环会在有限次迭代后停止，算法也就终止了。循环结束后，我们得到 $pq=\mathfrak{p}\overline{\mathfrak{p}}$ ，其中 q 是一个常数。根据假设， p 是首一的，

等式左边的首项系数为 $\mathrm{lc}(pq) = q \in K$，而右边的首项系数等于 $\mathrm{lc}(\mathfrak{p}) \cdot \mathrm{lc}(\overline{\mathfrak{p}}) = \mathfrak{c}\overline{\mathfrak{c}}$。因此，$\mathfrak{c}\overline{\mathfrak{c}} = q$，所以$p = \mathfrak{p} \cdot q^{-1} \cdot \overline{\mathfrak{p}} = (\mathfrak{p} \cdot \mathfrak{c}^{-1})(\overline{\mathfrak{c}}^{-1} \cdot \overline{\mathfrak{p}})$ 是 p的一个因式分解。□

注记 6。众所周知（参见 [38, 第 4] 节），在一个（必然是分裂的）四元数代数 $\left(\frac{\alpha,\ \beta}{L}\right)$ 中寻找零因子，等价于在由 $\alpha x^2 + \beta y^2 - \alpha\beta z^2 = 0$ 给出的射影圆锥曲线上寻找一个 L-有理点。这可以通过拉格朗日下降法的一个变体（参见 [6, 34] 和 [5, §127.5]）或求解范数方程（参见 [15]）来完成。特别地，总能找到一个纯四元数形式的零因子，即其形式为 $\mathfrak{a} = a_1\mathfrak{i} + a_2\mathfrak{j} + a_3\mathfrak{k}$。

例 1。下面通过一个简单示例说明上述算法的工作方式。固定有理数域上的四元数代数 $\mathfrak{A} := \left(\frac{-1,\ -1}{\mathbb{Q}}\right)$ 并令

$$p = x^4 + 11x^2 + 16x + 6.$$

域 $L = K[x]/(p)$ 分裂了 $\mathfrak{A}$，因此 p 在 $\mathfrak{A}[x]$ 中因式分解。步骤 (5) 中构造的多项式 $\mathfrak{p}$ 具有如下形式 $\mathfrak{p} = 0 + q_1\mathfrak{i} + q_2\mathfrak{j} + q_3\mathfrak{k}$，其中：

$$\begin{aligned} q_1 &= 19x^3 - 12x^2 + 211x + 154, \\ q_2 &= 13x^3 - 11x^2 + 136x + 97, \\ q_3 &= 53. \end{aligned}$$

因此，最初多项式 $q = \mathfrak{p}\overline{\mathfrak{p}} \cdot p^{-1}$ 等于

$$q = 530x^2 - 742x + 5989.$$

在这个特定例子中，循环只执行一次，停止后我们得到

$$\mathfrak{p} = \left(\frac{29}{50} + \frac{11}{25}\mathfrak{k}\right) \cdot x^2 + \left(\frac{11}{25} - \frac{13}{10}\mathfrak{i} + \frac{19}{10}\mathfrak{j} - \frac{29}{50}\mathfrak{k}\right) \cdot x + \frac{11}{25} - \frac{18}{25}\mathfrak{i} + \frac{73}{50}\mathfrak{j} - \frac{29}{50}\mathfrak{k}.$$

将 $\mathfrak{p}$ 右除以其首项系数，得到所求的 p 因子：

$$\mathfrak{q}_0 := \mathfrak{p} \cdot \mathrm{lc}(\mathfrak{p})^{-1} = x^2 - (3\mathfrak{i} - \mathfrak{j} + \mathfrak{k}) \cdot x - 2\mathfrak{i} + \mathfrak{j} - \mathfrak{k}$$

直接计算即可验证 $p = \mathfrak{q}_0\overline{\mathfrak{q}_0}$。

4. Factoring general polynomials

现在我们将介绍一种算法，用于对任意四元数多项式进行因式分解。首先，我们证明下面这个辅助引理，它可以在一定程度上缓解因缺乏交换性而造成的不便。

引理 13. 设 $\mathfrak{p}$，$\mathfrak{q} \in \mathfrak{A}[x]$ 为不可约首一多项式。若范数 $N\mathfrak{p}$ 和$N\mathfrak{q}$ 在 $K[x]$中互素，则存在不可约多项式 $\mathfrak{p}_1$，$\mathfrak{q}_1 \in \mathfrak{A}[x]$，使得 $N\mathfrak{p}_1 = N\mathfrak{p}$、$N\mathfrak{q}_1 = N\mathfrak{q}$ 和 $\mathfrak{p}\mathfrak{q} = \mathfrak{q}_1\mathfrak{p}_1$。

证明。根据假设，多项式 $N\mathfrak{p}$ 和 $N\mathfrak{q}$ 互素。因此，根据贝祖恒等式，存在多项式 p、$q \in K[x]$，使得

$$p \cdot N\mathfrak{p} + 1 = q \cdot N\mathfrak{q}.$$

令 $\mathfrak{p}_* := \overline{\mathfrak{p}} \cdot p$ 和 $\mathfrak{q}_* := \overline{\mathfrak{q}} \cdot q$。则

$$\mathfrak{p}_*\mathfrak{p} + 1 = \mathfrak{q}\mathfrak{q}_*.$$

这意味着 $\mathfrak{q}$ 是右可逆的[1]模 $\mathfrak{p}$。令

$$\mathfrak{p}_1 := \mathfrak{a} \cdot \mathrm{lclm}(\mathfrak{p}, \mathfrak{q}_*) \cdot \mathfrak{q}_*^{-1},$$

[1]注意到，$\mathfrak{q}$ 在模 $\mathfrak{p}$ 下也是左可逆的。然而，为了证明后一个断言，只需采用一个较弱的假设，即 $\mathrm{gcrd}(\mathfrak{p}, \mathfrak{q}) = 1$，并结合 [25, 定理 I.5]。

其中选取四元数 $\mathfrak{a}$，使得 $\mathfrak{p}_1$ 为首一多项式。重新排列该项（见 [25, 定理 I.13]）可得

$$\mathfrak{p} = \mathrm{lclm}(\mathfrak{p}_1, \mathfrak{q}) \cdot \mathfrak{q}^{-1}.$$

根据假设，$\gcd(N\mathfrak{p}, N\mathfrak{q}) = 1$，我们可以推断 $\mathrm{gcrd}(\mathfrak{p}, \mathfrak{q}) = 1$。因此，$\mathfrak{p}$ 和 $\mathfrak{p}_1$ 的范数相同。我们有

$$\mathfrak{p}\mathfrak{q} = \mathrm{lclm}(\mathfrak{p}_1, \mathfrak{q}) \cdot \mathfrak{q}^{-1} \cdot \mathfrak{q} = \mathrm{lclm}(\mathfrak{p}_1, \mathfrak{q}).$$

因此，乘积 $\mathfrak{p}\mathfrak{q}$ 可被 $\mathfrak{p}_1$右可除。取 $\mathfrak{q}_1 := \mathfrak{p}\mathfrak{q} \cdot \mathfrak{p}_1^{-1}$。显然，$N\mathfrak{q}_1 = N\mathfrak{q}$ 和 $\mathfrak{q}_1\mathfrak{p}_1 = \mathfrak{p}\mathfrak{q}$。□

算法 3. 设 $\mathfrak{A}$ 为数域 K 上的除四元数代数。给定一个非零多项式 $\mathfrak{p} \in \mathfrak{A}[x]$，该算法输出一个四元数 $\mathfrak{c} \in \mathfrak{A}$ 和一个首一不可约四元数多项式的列表 $\mathscr{L} = (\mathfrak{q}_1, \ldots, \mathfrak{q}_n)$，使得$\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_n$。

(1) 令 $\mathfrak{c} := lc(\mathfrak{p})$ 并更新 $\mathfrak{p}$，设置 $\mathfrak{p} := \mathfrak{c}^{-1} \cdot \mathfrak{p}$。初始化 $\mathscr{L} := ()$。*(2)* 令 $p_0, \ldots, p_4 \in K[x]$ 为 $\mathfrak{p}$ 关于基 $\{1, \mathfrak{i}, \mathfrak{j}, \mathfrak{k}\}$ 的坐标，其中 $\mathfrak{A}[x]$ 被视为关于 $K[x]$ 的自由模。*(3)* 计算 $\mathfrak{p}$ 的最大中心因子 $p := gcd(p_0, \ldots, p_4)$，并设置 $\mathfrak{q} := \mathfrak{p} \cdot p^{-1}$。*(4)* 将 p 在 $K[x]$ 中分解为不可约多项式 $r_1, \ldots, r_m \in K[x]$ 的乘积 $p = r_1^{e_1} \cdots r_m^{e_m}$。*(5)* 使用算法 *2* 分解 $\mathfrak{A}[x]$ 中的每个多项式 r_i。将该算法的输出追加 e_i 份到列表 $\mathscr{L}$ 中。*(6)* 将 $N\mathfrak{q} = \mathfrak{q}\overline{\mathfrak{q}}$ 的范数在 $K[x]$ 中分解为首一不可约多项式 $q_1, \ldots, q_k \in K[x]$ 的乘积 $N\mathfrak{q} = q_1^{\varepsilon_1} \cdots q_k^{\varepsilon_k}$。*(7)* 只要多项式 $\mathfrak{q}$ 仍为非常数，就重复以下步骤：*(a)* 计算最大公右因子 $\mathfrak{r} := gcrd(\mathfrak{q}, q_k)$。*(b)* 更新列表 $\mathscr{L}$，将 $\mathfrak{r}$ 前置于列表开头。*(c)* 更新多项式 $\mathfrak{q}$，设置 $\mathfrak{q} := \mathfrak{q} \cdot \mathfrak{r}^{-1}$。*(d)* 将指数 ε_k 减 *1*。*(e)* 若 $\varepsilon_k = 0$，则将索引 k 减 *1*。*(8)* 输出 $\mathfrak{c}$ 和列表 $\mathscr{L}$。

正确性证明。固定一个非零多项式 $\mathfrak{p} \in \mathfrak{A}[x]$。命题 3 断言，$\mathfrak{p}$ 可以唯一地表示为 $\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q} \cdot p$，其中 p 是 $\mathfrak{p}$各坐标的最大公因式（在 $K[x]$中），该最大公因式是在算法的步骤（2）中构造的。显然，通过将 $\mathfrak{q}$ 和 p 分解为不可约四元数多项式的乘积，我们可以得到原多项式 $\mathfrak{p}$的一个因式分解。p 的因式分解在步骤（4–5）中使用算法 2 完成。接下来需要对 $\mathfrak{q}$进行因式分解。假设 $\mathfrak{q} = \mathfrak{r}_1 \cdots \mathfrak{r}_l$是 $\mathfrak{q}$的某种因式分解。那么，$N\mathfrak{q} = N\mathfrak{r}_1 \cdots N\mathfrak{r}_l$ 就是 $\mathfrak{q}$的范数在 $K[x]$ 中的一个因式分解。但此时，$K[x]$ 是一个（交换）唯一因式分解整环，因此每个 $N\mathfrak{r}_i$ 都必须恰好等于 $N\mathfrak{q}$的不可约因子 q_1、……、$q_k \in K[x]$中的一个。通过反复应用引理 13，我们可以看到，存在另一个因式分解 $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_l$，使得 $N\mathfrak{q}_l = q_k$。因此，我们可以提取最右侧的因子$\mathfrak{q}_l = \mathrm{gcrd}(\mathfrak{q}, q_k)$。通过简单的归纳法可以证明，步骤（7）中的循环最终将生成所有不可约因子。□

注记 7. 有人可能会疑惑，为什么在处理系数属于代数中心的多项式时，我们必须采用专门的方法。原因在于，中心多项式 $p \in K[x]$ 的范数恰好就是其平方 $Np = p^2$。因此，$\gcd(p, Np) = \gcd(p, p^2) = p$。由此，即使 p 在 $\mathfrak{A}[x]$ 中可以分解为乘积$p = \mathfrak{p}\overline{\mathfrak{p}}$，算法 3 的步骤 (7a) 也无法提取其因子。在使用 Trager 方法对有限域扩张中的多项式进行因式分解时，也会观察到相同的现象。

算法。设 $L = K(\vartheta)$ 是 K 和 $p \in L[x]$ 的有限扩张。在 Trager 算法中，为了因式分解 p，我们将其“平移”，并计算某个 $k \in \mathbb{Z}$ 下 $p(x + k\vartheta)$ 的范数。遗憾的是，对于四元数多项式，由于缺乏交换性，这种技巧不再奏效。因此，我们需要采用第 3 节所述的更复杂方法。因此，在除四元数代数（也就是次数为二的代数）上进行多项式因式分解，比在次数为二的域扩张上进行因式分解耗时得多。尽管如此，详细的复杂度分析仍有待进一步研究。

例子 2. 我们将用另一个简单示例来说明算法 3。再次取四元数代数 $\mathfrak{A} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ 并令

$$\begin{aligned}\mathfrak{p} := (1+\mathfrak{k})\cdot x^8 + (-2+\mathfrak{i}-\mathfrak{j}-2\mathfrak{k})\cdot x^7 + (9+11\mathfrak{k})\cdot x^6 \\ + (-6+12\mathfrak{i}-6\mathfrak{j}-2\mathfrak{k})\cdot x^5 + (-45+10\mathfrak{i}-18\mathfrak{j}-27\mathfrak{k})\cdot x^4 \\ + (-44+17\mathfrak{i}+49\mathfrak{j}+32\mathfrak{k})\cdot x^3 + (21-50\mathfrak{i}+58\mathfrak{j}+53\mathfrak{k})\cdot x^2 \\ + (48-90\mathfrak{i}-2\mathfrak{j}+8\mathfrak{k})\cdot x + 18 - 36\mathfrak{i} - 12\mathfrak{j} - 6\mathfrak{k}.\end{aligned}$$

然后 $\mathfrak{p} = (1+\mathfrak{k})\cdot(p_0 + p_1\mathfrak{i} + p_2\mathfrak{j} + p_3\mathfrak{k})$，其中

$$\begin{aligned}p_0 &= x^8 - 2x^7 + 10x^6 - 4x^5 - 36x^4 - 6x^3 + 37x^2 + 28x + 6,\\ p_1 &= 3x^5 - 4x^4 + 33x^3 + 4x^2 - 46x - 24,\\ p_2 &= -x^7 - 9x^5 - 14x^4 + 16x^3 + 54x^2 + 44x + 12,\\ p_3 &= x^6 + 2x^5 + 9x^4 + 38x^3 + 16x^2 - 20x - 12.\end{aligned}$$

计算这四个多项式的最大公因式，我们得到 $\mathfrak{p}$ 的最大中心因子：

$$p := \gcd(p_0, \ldots, p_4) = x^4 + 11x^2 + 16x + 6.$$

多项式 p 正是前一个例子中已经分解过的多项式。接下来需要分解多项式 $\mathfrak{q} := (1+\mathfrak{k})^{-1}\cdot\mathfrak{p}\cdot p^{-1}$，它不能被任何系数属于 K 的多项式整除。$\mathfrak{q}$ 的范数在 $K[x]$ 中分解为乘积 $N\mathfrak{q} = q_1q_2q_3$，其中

$$\begin{aligned}q_1 &= x^2 + 1,\\ q_2 &= x^2 - 4x + 5,\\ q_3 &= x^4 - 3x^2 + 5.\end{aligned}$$

计算连续的最大公右因子，得到 $\mathfrak{q}$ 的因子：

$$\begin{aligned}\mathfrak{q}_3 &:= \operatorname{gcrd}(\mathfrak{q}, q_3) = x^2 + \mathfrak{i}x - 2 - \mathfrak{k},\\ \mathfrak{q}_2 &:= \operatorname{gcrd}(\mathfrak{q}\cdot\mathfrak{q}_3^{-1}, q_2) = x - 2 - \mathfrak{j},\\ \mathfrak{q}_1 &:= \operatorname{gcrd}(\mathfrak{q}\cdot\mathfrak{q}_3^{-1}\cdot\mathfrak{q}_2^{-1}, q_1) = x - \mathfrak{i}.\end{aligned}$$

由此得到因式分解 $\mathfrak{p} = (1+\mathfrak{k})\cdot\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\cdot\mathfrak{q}_0\overline{\mathfrak{q}_0}$，其中 $\mathfrak{q}_0$ 是示例 1 中构造的 p 的因子。

5. 求根

多项式因式分解与求根问题密切相关。早在 80 年前，Niven 就研究了哈密顿四元数情形下四元数多项式的求根问题（见 [24]）；40 年前，Beck 则研究了任意四元数代数情形（见 [2]）。然而，迄今为止，计算方法一直只关注哈密顿四元数（例如，见 [11, 12, 24, 29,31]）。本节将说明如何调整算法 3，以求出 $\mathfrak{A}$ 中多项式 $\mathfrak{p} \in \mathfrak{A}[x]$ 的根，其中 $\mathfrak{A}$ 是数域上的除四元数代数。

众所周知，代数学基本定理对哈密顿四元数成立（例如，见 [12, 24, 29]）。因此，系数属于 $\mathbb{H} = \left(\frac{-1,\ -1}{\mathbb{R}}\right)$ 的每个非恒定多项式在 $\mathbb{H}$ 中都有一个根。若将 $\mathbb{H}$ 换成实数域上的分裂四元数代数，这一性质便不再成立。同样，在本文所讨论的情形下，数域上的除四元数代数中存在一些系数所在环内没有根的多项式，这完全不足为奇。如果确实如此，那么算法当然必须返回空集。

在交换的世界中，求多项式 $p \in K[x]$ 在 $L \supseteq K$ 中的根，等价于求 p 在 $L[x]$ 中的一次因子。离开交换的游乐场，转而考虑非交换除环上的多项式时，这种方法便不再适用。此时我们会立即遇到两个障碍。首先，四元数多项式可能有无穷多个零点。其次，对于某个固定的 $\mathfrak{a}$，求值映射 $\mathfrak{A}[x] \to \mathfrak{A},\ \mathfrak{p} \mapsto \mathfrak{p}(\mathfrak{a})$在 $\mathfrak{a} \notin Z(\mathfrak{A})$ 时不再是环同态。特别是，$\mathfrak{p} = \mathfrak{q}\mathfrak{r}$ 和 $\mathfrak{q}(\mathfrak{a}) = 0$ 尚不能推出 $\mathfrak{p}(\mathfrak{a}) = 0$。幸运的是，这两个问题都很容易解决。不过，为了方便读者，我们先列举两个关于四元数多项式根的经典事实。回想一下，若存在一个四元数 $\mathfrak{c} \in \mathfrak{A}^{\times}$ 使得 $\mathfrak{a} = \mathfrak{c}\mathfrak{b}\mathfrak{c}^{-1}$，则称两个非零四元数 $\mathfrak{a}$、$\mathfrak{b}$ 互为共轭。显然，共轭关系是一种等价关系。

定理 14 (Gordon–Motzkin)。设 $\mathfrak{A}$ 是一个除四元数代数，且 $\mathfrak{p} \in \mathfrak{A}[x]$。那么：

(1) 四元数 $\mathfrak{a} \in \mathfrak{A}$ 是 $\mathfrak{p}$ 的根，当且仅当 $\mathfrak{p}$ 可被 $x - \mathfrak{a}$右除。(2) 至多有$\deg \mathfrak{p}$ 个 $\mathfrak{A}$ 的共轭类包含 $\mathfrak{p}$ 的根。(3) 若 $\mathfrak{p} = (x - \mathfrak{a}_1)\cdots(x - \mathfrak{a}_n)$，则 $\mathfrak{p}$ 的每个根都与某个 $\mathfrak{a}_i$共轭。(4) 若 $\mathfrak{A}$ 的一个共轭类包含 $\mathfrak{p}$的多个根，则 $\mathfrak{p}$ 在该共轭类中有无穷多个根。

关于上述定理的证明，请参阅 [10] 或 [17, §16]。对于非零四元数 $\mathfrak{a} \in \mathfrak{A}$，我们将其特征多项式记为 $\chi_{\mathfrak{a}} = N(x - \mathfrak{a}) = x^2 - \mathrm{Tr}(\mathfrak{a}) \cdot x + N(\mathfrak{a}) \in K[x]$。显然，对于 $\mathfrak{a}$的任意共轭 $\mathfrak{b}$，都有 $\chi_{\mathfrak{a}} = \chi_{\overline{\mathfrak{a}}} = \chi_{\mathfrak{b}}$。反过来，Dickson 定理（例如参见 [17, 定理 16.8]）断言，$\chi_{\mathfrak{a}} = \chi_{\mathfrak{b}}$ 蕴含 $\mathfrak{a}$ 与 $\mathfrak{b}$ 共轭。下一个定理引自 [2]。

定理 15 (Beck)。设 $\mathfrak{A}$ 为一个除四元数代数，$\mathfrak{p} \in \mathfrak{A}[x]$ 为一个非常数多项式。则：

(1) 四元数 $\mathfrak{a}$ 与 $\mathfrak{p}$ 的一个根 $\mathfrak{b}$ 共轭，当且仅当 $\chi_{\mathfrak{a}}$ 在 $K[x]$ 中整除 $N\mathfrak{p}$，当且仅当 $\mathfrak{a}$ 是 $N\mathfrak{p}$ 的一个根。(2) 如果 $\chi_{\mathfrak{a}}$ 整除 $\mathfrak{p}$，其中 $\mathfrak{a} \in \mathfrak{A}^{\times}$，那么 $\mathfrak{a}$ 的每一个共轭都是 $\mathfrak{p}$ 的根。

设一个非零四元数多项式 $\mathfrak{p} \in \mathfrak{A}[x]$。将其重新写成乘积$\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q} \cdot p$，其中 $\mathfrak{c}$ 是首项系数，p 是 $\mathfrak{p}$的最大中心因子，且 $\mathfrak{q}$ 不能被 $K[x]$中的任何非常数多项式整除。鉴于上述两个定理，显然，要找出 $\mathfrak{p}$的根，我们只需找出它的线性右因子。为此，只需考察 p 的线性因子和二次因子，以及 $N\mathfrak{q}$的二次因子。此外，由于 $\mathfrak{p}$ 可能有无穷多个根，我们所能做的最好办法就是按共轭关系枚举根。这正是算法 4 所做的。不过，首先我们需要陈述以下引理。该引理广为人知，但我们尚未找到合适的参考文献。

引理 16. 四元数 $\mathfrak{a} \in \mathfrak{A} \setminus K$ 是多项式 $p \in K[x]$ 的根，当且仅当 $\chi_{\mathfrak{a}}$ 整除 p。

证明。 假设 $p(\mathfrak{a}) = 0$。那么 [17, 定理 16.6] 断言，存在某个多项式 $\mathfrak{q} \in \mathfrak{A}[x]$，使得 $p = \mathfrak{q} \cdot \chi_{\mathfrak{a}}$。但是 p 和 $\chi_{\mathfrak{a}}$ 都属于 $K[x]$，因此 $\mathfrak{q} \in K[x]$ 也属于其中（例如参见[17, 练习 16.1]）。反向推论显然成立。□

现在，我们可以给出求根算法。该算法是对算法 3 中所述因式分解过程的一种简单改编。

算法 4. 给定一个非零多项式 $\mathfrak{p} \in \mathfrak{A}[x]$，此算法输出一个集合 $\mathscr{R} \subset \mathfrak{A}$，使得 $\mathscr{R}$ 的每个元素都是 $\mathfrak{p}$ 的根，并且 $\mathfrak{p}$ 的每个根都与 $\mathscr{R}$ 中唯一的一个元素共轭。

(1) 令 $\mathfrak{c} := lc(\mathfrak{p})$，并通过设定 $\mathfrak{p} := \mathfrak{c}^{-1} \cdot \mathfrak{p}$ 来更新 $\mathfrak{p}$。*(2)* 令 $p_0, \ldots, p_4 \in K[x]$ 为 $\mathfrak{p}$ 相对于 $\mathfrak{A}[x]$ 的 $\{1, \mathfrak{i}, \mathfrak{j}, \mathfrak{k}\}$ 基的坐标，其中 $\mathfrak{A}[x]$ 被视为有理数域 $K[x]$ 上的自由模。*(3)* 计算 $\mathfrak{p}$ 的最大中心因子 $p := gcd(p_0, \ldots, p_4)$，并令 $\mathfrak{q} := \mathfrak{p} \cdot p^{-1}$。*(4)* 将 p 在 $K[x]$ 中因式分解为不可约多项式 $r_1, \ldots, r_m \in K[x]$ 的乘积 $p = r_1^{e_1} \cdots r_m^{e_m}$。*(5)* 将 $\mathscr{R}$ 初始化为 p 的所有一次因子的根（在 K 中）组成的集合：

$$\mathscr{R} := \big\{a \in K : r_i = x - a \text{ for some } i \le k\big\}.$$

(6) 对于每个次数为 *2* 的多项式 r_i：（*a*）以 r_i 为输入执行算法 *1*；如果报告失败，则重新执行循环。（*b*）否则，如果算法 *1* 返回因式分解 $r_i = (x - \mathfrak{a}_i)(x - \overline{\mathfrak{a}_i})$，则检查 $\mathscr{R}$ 是否包含一个与 $\mathfrak{a}_i$ 共轭的元素。（*c*）如果不包含，则将 $\mathfrak{a}_i$ 添加到 $\mathscr{R}$ 中。（*7*）将 $N\mathfrak{q} = \mathfrak{q}\overline{\mathfrak{q}}$ 的范数在 $K[x]$ 中分解为首一不可约多项式 q_1、……、$q_k \in K[x]$ 的乘积 $N\mathfrak{q} = q_1^{\varepsilon_1} \cdots q_k^{\varepsilon_k}$。（*8*）对于每个次数为 *2* 的多项式 q_j：（*a*）计算最大公右因子 $x - \mathfrak{b}_j = gcrd(q_j, \mathfrak{q})$。（*b*）检查 $\mathscr{R}$ 是否包含一个与 $\mathfrak{b}_j$ 共轭的元素。（*c*）如果不包含，则将 $\mathfrak{b}_j$ 添加到 $\mathscr{R}$ 中。（*9*）输出集合 $\mathscr{R}$。

正确性证明。 固定一个四元数多项式 $\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q} \cdot p$，并令 $\mathscr{R}$ 为通过该算法构造的集合。首先，我们将证明 $\mathscr{R}$ 的每个元素都是 p 的根。如果某个元素 $a \in \mathscr{R}$ 是在步骤 (5) 中构造的，那么显然 $\mathfrak{p}(a) = p(a) = 0$。同样，如果 $\mathfrak{a}_i \in \mathscr{R}$ 是在步骤 (6b) 中构造的，那么 $\chi_{\mathfrak{a}_i} = (x - \mathfrak{a}_i)(x - \overline{\mathfrak{a}_i})$ 整除 p。因此，$\mathfrak{a}_i$ 再次是 $\mathfrak{p}$ 的一个根（根据定理 15，它的所有共轭也都是根）。现在，取一个在步骤 (8a) 中构造的元素 $\mathfrak{b}_j \in \mathscr{R}$。那么，$x - \mathfrak{b}_j$ 作为 $\mathfrak{q}$ 和 q_j 的最大公右因子，特别地，是 $\mathfrak{p}$ 的一个右因子，因为 p 是中心的。因此可得，$\mathfrak{b}_j$ 是 $\mathfrak{p}$ 的一个根。

反过来，我们现在将证明，$\mathfrak{p}$ 的每个根都与 $\mathscr{R}$中的某个元素共轭。假设 $\mathfrak{a} \in \mathfrak{A}$ 是 $\mathfrak{p}$的一个根。根据定理 14，$x - \mathfrak{a}$ 是 $\mathfrak{p}$的一个右因子。我们需要考虑三种情况。如果 $\mathfrak{a}$ 属于 K，那么 $x - \mathfrak{a}$ 整除 p，因此 $\mathfrak{a}$ 是算法步骤 (5) 中构造出的元素之一。于是，不失一般性，我们可以假设 $\mathfrak{a} \notin K$。如果 $x - \mathfrak{a}$ 整除 p，那么根据引理 16，$\mathfrak{a}$ 的特征多项式 $\chi_{\mathfrak{a}}$ 整除 p。因此，$\chi_{\mathfrak{a}}$ 是步骤 (6) 中考察的次数为 2 的因子 r_i 之一。于是，要么将 $\mathfrak{a}$ 加入 $\mathscr{R}$，要么将 $\overline{\mathfrak{a}}$ 加入 $\mathscr{R}$，要么 $\mathscr{R}$ 已包含一个与这两个元素之一共轭的元素。但是，根据 Dickson 定理（例如参见 [17, 定理 16.8]），$\mathfrak{a}$ 与 $\overline{\mathfrak{a}}$ 共轭。因此，无论哪种情况，$\mathscr{R}$ 都包含一个与 $\mathfrak{a}$共轭的元素。

最后，假设 $x - \mathfrak{a}$不整除 p。由于 p 是中心元素，因此 $x - \mathfrak{a}$必定是 $\mathfrak{q}$ 的右因子。但这样一来，范数 $N(x - \mathfrak{a}) = \chi_{\mathfrak{a}}$ 在 $K[x]$中不可约

并且整除 $N\mathfrak{q}$。因此， $\chi_{\mathfrak{a}} = q_j$ 对于某个 $j \le k$ 成立，从而 $x - \mathfrak{a} =$ 是$\mathfrak{q}$和 q_j的最大公右因子。因此，要么 $\mathfrak{a}$ 本身在步骤 (8c) 中被添加到 $\mathscr{R}$ ，要么 $\mathscr{R}$ 包含一个与 $\mathfrak{a}$共轭的元素。这样，我们就证明了 $\mathfrak{p}$ 的每个根都与 $\mathscr{R}$中的某个元素共轭。该元素是唯一确定的，因为 $\mathscr{R}$ 中的元素两两不共轭。□

6. 结论与进一步研究

我们提出了一种显式算法，用于对系数属于数域上的除四元数代数的单边多项式进行因式分解。如前所述，一般而言，一个四元数多项式可能有无穷多种不同的不可约因子分解。本文提出的算法只输出其中一种分解。这一事实使得该算法的复杂度相当难以分析。作者通过实证观察发现，算法输出可能是“次优的”，也就是说，系数的大小可能变得任意大。这种现象主要出现在分解中心多项式时，因为算法 2 可能会遇到系数急剧膨胀的问题，这在多项式环上的欧几里得类算法中很常见。通过选择系数较小的因子（或限制系数增长）来克服这一障碍的方法，值得进一步研究。

本文介绍的算法已由作者在计算机代数系统 Magma 的软件包 $\mathfrak{qPoly}$ 中实现。该软件包依据 MIT 许可证发布，可从作者的网页 http://www.pkoprowski.eu/qpoly 免费下载。

参考文献

[1] Ali Ayad. 关于整体域上多项式因式分解复杂度的讲座。国际数学论坛，5(9-12):477–486，2010。[2] Bernard Beck. 四元数中的多项式方程。数学教学（第二辑），25(3- 4):193–201（1980），1979。[3] Karim Belabas、Mark van Hoeij、Jürgen Klüners 和 Allan Steel。整体域上的多项式因式分解。波尔多数论杂志，21(1):15–39，2009。[4] Wieb Bosma、John Cannon 和 Catherine Playoust。Magma 代数系统。I. 用户语言。符号计算杂志，24(3-4):235–265，1997。计算代数与数论（伦敦，1993）。[5] John Cannon、Wieb Bosma、Claus Fieker 和 Allan Steel（编）。*Magma* 函数手册，第 2.27-7 版，2022。[6] John E. Cremona 和 D. Rusin。有理二次曲线的高效求解。数学计算，72(243):1417–1441，2003。[7] Andreas-Stephan Elsenhans 和 Jürgen Klüners。数域子域的计算及其在伽罗瓦群计算中的应用。符号计算杂志，93:1–20，2019。[8] Maria Irene Falcão、Fernando Miranda、Ricardo Severino 和 Maria Joana Soares。四元数多项式环中的求值方案。*BIT*，58(1):51–72，2018。[9] Basil Gordon 和 Theodore Samuel Motzkin。除环上多项式的零点。美国数学会汇刊，116:218–226，1965。[10] Basil Gordon 和 Theodore Samuel Motzkin。对论文“除环上多项式的零点”的更正。美国数学会汇刊，122:547，1966。[11] Drahoslava Janovská 和 Gerhard Opfer。关于简单四元数多项式全部零点计算的注记。*SIAM* 数值分析杂志，48(1):244–256，2010。[12] Bahman Kalantari。四元数多项式求根算法。复杂度杂志，29(3- 4):302–322，2013。[13] Jürgen Klüners。关于子域的计算：算法的详细说明。波尔多数论杂志，10(2):243–271，1998。[14] Jürgen Klüners 和 Michael E. Pohst。关于子域的计算。符号计算杂志，24(3- 4):385–397，1997。计算代数与数论（伦敦，1993）。[15] Przemysław Koprowski。整体域上的各向同性向量，2021。arXiv https://arxiv.org/abs/2111.08569。

[16] Przemysław Koprowski。《四元数代数中的平方根计算》，2023年。arXiv https://arxiv.org/abs/2301.00743。[17] Tsit-Yuen Lam。《非交换环初阶课程》，数学研究生教材第131卷。Springer-Verlag，纽约，第二版，2001年。[18] Tsit-Yuen Lam。《域上的二次型导论》，数学研究生研究丛书第67卷。美国数学会，罗得岛州普罗维登斯，2005年。[19] Susan Landau。《代数数域上的多项式因式分解》。SIAM计算杂志，14(1)：184–195，1985年。[20] Arjen K. Lenstra。《代数数域上的多项式因式分解》。载于《计算机代数》（伦敦，1983年），计算机科学讲义第162卷，第245–254页。Springer，柏林，1983年。[21] Johanna Lercher、Daniel Scharler、Hans-Peter Schröcker和Johannes Siegele。《双次数为(n,1)的四元数多项式的因式分解》。Beiträge zur Algebra und Geometrie，64(1)：209–232，2023年。[22] Zijia Li、Daniel F. Scharler和Hans-Peter Schröcker。《某些结合实代数中左多项式的因式分解结果：研究现状、应用与开放问题》。计算与应用数学杂志，349：508–522，2019年。[23] José Méndez Omaña和Michael E. Pohst。《整体域上的多项式因式分解。II》。符号计算杂志，40(6)：1325–1339，2005年。[24] Ivan Niven。《四元数方程》。美国数学月刊，48：654–661，1941年。[25] Oystein Ore。《非交换多项式理论》。数学年刊（第二辑）（2 508，1933 34 3 480），（）：–。[26] Yves Pourchet。《代数数域上一元多项式表示为平方和的问题》。Acta Arithmetica，19：89–104，1971年。[27] A. R. Rajwade。《平方数》，伦敦数学会讲义丛书第171卷。剑桥大学出版社，剑桥，1993年。[28] Xavier-François Roblot。《数域上的多项式因式分解算法》。符号计算杂志，38(5)：1429–1443，2004年。[29] Takis Sakkalis、Kwanghee Ko和Galam Song。《四元数多项式的根：理论与计算》。理论计算机科学，800：173–178，2019年。[30] Daniel F. Scharler和Hans-Peter Schröcker。《一种分裂四元数多项式的因式分解算法》。Advances in Applied Clifford Algebras，31(3)：论文编号29，共23页，2021年。[31] Rogério Serôdio、Edgar Pereira和Jose Vitória。《四元数多项式零点的计算》。计算数学与应用，42(8-9)：1229–1237，2001年。数值方法与计算力学（米什科尔茨，1998年）。[32] Jonas Szutkoski和Mark van Hoeij。《计算代数数域所有子域的复杂度》。符号计算杂志，93：161–182，2019年。[33] Sage开发团队。《SageMath，Sage数学软件系统》（9.5版），2022年。https://www.sagemath.org。[34] Mark van Hoeij和John Cremona。《函数域上的圆锥曲线求解》。波尔多数论杂志，18(3)：595–606，2006年。http://jtnb.cedram.org/item?id=JTNB_2006__18_3_595_0。[35] Mark van Hoeij、Jürgen Klüners和Andrew Novocin。《生成子域》。载于《ISSAC 2011——第36届国际符号与代数计算研讨会论文集》，第345–352页。ACM，纽约，2011年。[36] Mark van Hoeij、Jürgen Klüners和Andrew Novocin。《生成子域》。符号计算杂志，52：17–34，2013年。[37] Marie-France Vignéras。《四元数代数的算术》，数学讲义第800卷。Springer，柏林，1980年。[38] John Voight。《矩阵环的识别：四元数代数与二次型算法》。载于《二次型与高次型》，数学发展丛书第31卷，第255–298页。Springer，纽约，2013年。[39] John Voight。《四元数代数》，数学研究生教材第288卷。Springer，Cham，[2021] ©2021。