FACTORIZATION AND ROOT-FINDING FOR POLYNOMIALS OVER DIVISION QUATERNION ALGEBRAS

PRZEMYSLAW KOPROWSKI

ABSTRACT. Polynomial factorization and root finding are among the most standard themes of computational mathematics. Yet still, little has been done for polynomials over quaternion algebras, with the single exception of Hamiltonian quaternions for which there are known numerical methods for polynomial root approximation. The sole purpose of the present paper is to present a polynomial factorization algorithm for division quaternion algebras over number fields, together with its adaptation for root finding.

1. INTRODUCTION

Polynomial factorization is one of the classical subjects in the realm of computational algebra. Over the decades, numerous algorithms have been developed for factoring polynomials over various base rings, like integers and rationals, finite fields, local and global fields, etc. Nonetheless, there are still many important classes of rings for which there are no known methods for polynomial factorization. One of these notable omissions is the class of quaternion algebras. Although quaternion polynomials are a classical subject that has been studied since the first half of the 20th century, the algorithmic side of the theory is strongly underdeveloped. To the best of our knowledge, the only algorithms developed so far concentrate exclusively on polynomials over real quaternion algebras with an emphasis on the Hamiltonian quaternions (see, e.g., [11, 12, 24, 29, 31] for root-finding algorithms, or [21, 22, 30] for factorization algorithms). Unfortunately, the methods developed for real quaternions cannot be applied in a general setting. The fundamental reason is that the Hamiltonian quaternions admit the fundamental theorem of algebra. It is not a case for general division quaternion algebras. The author is unaware of even a single paper addressing the factorization of polynomials over *general* quaternion algebras. Thus, the sole purpose of this paper is to partially remedy this situation and to present algorithms for factoring polynomials over division quaternion algebras over number fields (see Algorithm 3) and to compute roots of polynomials in such algebras (see Algorithm 4).

There are a few different ways how one can define polynomials over a general associative ring. If the ring is commutative, they all coincide, but no longer so when the ring of coefficients is non-commutative. In this paper, we follow the most classical approach, and by a polynomial, over an associative ring $\mathfrak{A}$, we understand a sum $\mathfrak{p} = \mathfrak{a}_0 + \mathfrak{a}_1 x + \cdots + \mathfrak{a}_n x^n$, where the coefficients $\mathfrak{a}_0, \ldots, \mathfrak{a}_n$ are taken from $\mathfrak{A}$ and the indeterminate x commutes with the coefficients. These are called *left polynomials* in [9, 10] or *unilateral polynomials* in more recent sources like [8, 12, 31].

Throughout this paper, we use the following notational convention. Commutative rings and their elements are typeset using the standard typeface, while for non-commutative rings and their elements, we use fraktur letters. Further, K will always denote a number field, i.e. a finite extension of the field $\mathbb{Q}$ of the rationals. Recall that an algebra $\mathfrak{A}$ over K is called a *quaternion algebra* if it has a basis of

the form $\{1, \mathfrak{i}, \mathfrak{j}, \mathfrak{k}\}$ subject to the relations

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

for some nonzero elements $\alpha, \beta \in K$. The algebra $\mathfrak{A}$ is then denoted $\left(\frac{\alpha,\beta}{K}\right)$. For an in-depth presentation of the theory of quaternion algebras, we refer the reader to [37] and [39]. We will always identify the base field K with the subalgebra $K \cdot 1$ of $\mathfrak{A}$, which is known to form the center $Z(\mathfrak{A})$ of $\mathfrak{A}$. We shall write $K^\times$ (respectively $\mathfrak{A}^\times$) to denote the multiplicative group of nonzero elements of K (resp. invertible elements in $\mathfrak{A}$).

Every quaternion algebra is equipped with a standard involution that will be denoted by an overbar in what follows. For a quaternion $\mathfrak{a} \in \mathfrak{A}$, the product $\mathfrak{a}\overline{\mathfrak{a}}$ is called the *norm* (in [18]) or the *reduced norm* (in [37, 39]) of $\mathfrak{a}$ and will be denoted $N\mathfrak{a}$. Likewise, the sum $\mathfrak{a} + \overline{\mathfrak{a}}$ is called the *(reduced) trace* of $\mathfrak{a}$, denoted $\mathrm{Tr}\,\mathfrak{a}$. The natural inclusion $\left(\frac{\alpha,\beta}{K}\right)[x] \hookrightarrow \left(\frac{\alpha,\beta}{K(x)}\right)$ let us extend the notion of the norm and standard involution to quaternionic polynomials. In particular, if $\mathfrak{p} = \mathfrak{a}_0 + \mathfrak{a}_1 x + \cdots + \mathfrak{a}_n x^n$, then $\overline{\mathfrak{p}} = \overline{\mathfrak{a}_0} + \overline{\mathfrak{a}_1} x + \cdots + \overline{\mathfrak{a}_n} x^n$ and $N\mathfrak{p} = \mathfrak{p}\overline{\mathfrak{p}}$. We will use the same symbol N to denote also the standard norm in a field extension and its natural prolongation to the polynomial rings. In case of ambiguity, we will indicate the corresponding extension in the norm's subscript.

A quaternion algebra is either a division algebra or is isomorphic to the 2×2 matrix algebra $M_2 K$ (see, e.g., [39, Theorem 5.4.4]). The latter case happens if and only if the 2-fold Pfister form $\langle\langle -\alpha, -\beta \rangle\rangle = x_0^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2$ is *isotropic* (i.e. it has a non-trivial zero). The quaternion algebra $\left(\frac{\alpha,\beta}{K}\right)$ is then said to be *split*.

2. Preliminaries

Observe that over a split quaternion algebra, every polynomial $p \in K[x]$ has a trivial factorization. Indeed, if we identify $\mathfrak{A}$ with $M_2 K$ and K with its subfield of scalar matrices, we can write

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

Notice that both divisors of p constructed above have the same degree as the polynomial p itself. This is due to the fact that all their coefficients, save the constant terms, are zero-divisors. Consequently, in the rest of the paper, we concentrate entirely on polynomials over division quaternion algebras.

Below we collect some known facts concerning polynomials over division quaternion algebras. They are all very classical but scattered throughout the literature and sometimes expressed using different terminology. For a general introduction to polynomial rings over division rings (including division quaternion algebras), we refer the reader to [17, §16].

Theorem 1 (Ore)**.** *If $\mathfrak{A}$ is a division quaternion algebra, then the ring $\mathfrak{A}[x]$ of quaternionic polynomials admits a right-hand division with a remainder and a right-hand Euclidean algorithm.*

In particular, for any two quaternionic polynomials $\mathfrak{p}, \mathfrak{q} \in \mathfrak{A}[x]$, there exists a unique monic greatest common right divisor (denoted $\mathrm{gcrd}(\mathfrak{p}, \mathfrak{q})$ hereafter) and the least common left multiple (denoted $\mathrm{lclm}(\mathfrak{p}, \mathfrak{q})$). In fact, [25, Theorem I.8] provides an explicit formula for constructing the least common left multiple from the sequence of the right reminders computed by the right-hand Euclidean algorithm. However, we will not use this formula in the present paper.

Theorem 2 (Ore)**.** *If $\mathfrak{A}$ is a division quaternion algebra, then every monic polynomial $\mathfrak{p} \in \mathfrak{A}[x]$ can be expressed as a product of irreducible quaternionic polynomials. Every two such factorizations of $\mathfrak{p}$ have the same number of factors.*

For proofs of the above two theorem see [25, Chapter I, §2 and Theorem II.1]. Of course, in general, a quaternionic polynomial may have infinitely many different factorizations, even assuming that all the factors are monic. To observe this phenomenon take any non-constant monic polynomial $p \in K[x]$ with coefficients in the ground field. Assume that p factors into a product $p = \mathfrak{p}\mathfrak{q}$ of two monic quaternionic polynomials $\mathfrak{p}\mathfrak{q} \in \mathfrak{A}[x]$, not necessarily irreducible. Then for every invertible quaternion $\mathfrak{a} \in \mathfrak{A}$ we have

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

If only $\mathfrak{p}, \mathfrak{q} \notin K[x]$, this way we obtain another factorization of p, where $\mathfrak{a}\mathfrak{p}\mathfrak{a}^{-1}$ and $\mathfrak{a}\mathfrak{q}\mathfrak{a}^{-1}$ are again monic.

Proposition 3 (Beck)**.** *Let $\mathfrak{A}$ be a division quaternion algebra over K. Then every polynomial $\mathfrak{p} \in \mathfrak{A}[x]$ can be uniquely expressed as a product $\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q} \cdot p$, where $\mathfrak{c} \in \mathfrak{A}^{\times}$ is the leading coefficient of $\mathfrak{p}$, p is a monic polynomial with coefficients in K and $\mathfrak{q} \in \mathfrak{A}[x]$ is a monic quaternionic polynomial not divisible by any non-constant polynomial from $K[x]$. Moreover, if $\mathfrak{A}[x]$ is treated as a free module of rank 4 over $K[x]$ with a basis $\{1, \mathfrak{i}, \mathfrak{j}, \mathfrak{k}\}$, then p is the greatest common divisor (in $K[x]$) of the coordinates of $\mathfrak{p}$.*

The polynomial p described in the last proposition is called the *maximal central factor* of $\mathfrak{p}$. A proof of Proposition 3 can be found in [2, Résultat 4]. In view of this proposition, it is clear that in order to factor quaternionic polynomials, it suffices to have a procedure that factors in $\mathfrak{A}[x]$ polynomials that are irreducible in $K[x]$, and another procedure that factors quaternionic polynomials not divisible by polynomials from $K[x]$.

Lemma 4. *Let $\mathfrak{A} = \left(\frac{\alpha, \beta}{K}\right)$ be a division quaternion algebra over K and $\mathfrak{a}, \mathfrak{b} \in \mathfrak{A}$ be two quaternions. If $\mathfrak{a}\mathfrak{b} \in Z(\mathfrak{A}) = K$, then the following two conditions hold:*

(1) $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$;
(2) *there are scalars $c, d \in K$ such that $c \cdot \mathfrak{b} = d \cdot \overline{\mathfrak{a}}$*

Proof. If $\mathfrak{a} = 0$ or $\mathfrak{b} = 0$, then the assertions hold trivially. Hence, without loss of generality, we can assume that $\mathfrak{a}, \mathfrak{b} \in \mathfrak{A}^{\times}$ and so their product $d := \mathfrak{a}\mathfrak{b}$ is nonzero. Compute

$$\mathfrak{b}\mathfrak{a} = \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b}\mathfrak{a} = \mathfrak{a}^{-1} \cdot d \cdot \mathfrak{a} = d \cdot \mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{a}\mathfrak{b}.$$

This proves the first assertion. The second one follows immediately. Indeed, from $\mathfrak{a}\mathfrak{b} = d$ we infer

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

Remark 1. The assumption that $\mathfrak{A}$ is a division algebra is indispensable. To observe that, take the split quaternion algebra $\mathfrak{A} = M_2 K$ and let

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

Then $\mathfrak{a}\mathfrak{b}$ is the zero matrix, hence in particular $\mathfrak{a}\mathfrak{b} \in Z(\mathfrak{A})$ but

$$\mathfrak{b}\mathfrak{a} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \mathfrak{a}\mathfrak{b}.$$

Proposition 5. *Let $\mathfrak{A} = \left(\frac{\alpha, \beta}{K}\right)$ be a quaternion division algebra over K. Further, let $p \in K[x]$ be a monic irreducible polynomial with coefficients in K. Then either p remains irreducible in $\mathfrak{A}[x]$ or it factors into a product $p = \mathfrak{p}\overline{\mathfrak{p}}$ for some irreducible quaternionic polynomial $\mathfrak{p} \in \mathfrak{A}[x]$.*

Proof. Suppose that p is not irreducible in $\mathfrak{A}[x]$. Let $p = \mathfrak{p}\mathfrak{q}$ be some factorization of p with $\mathfrak{p}, \mathfrak{q} \in \mathfrak{A}[x]$. Applying the previous lemma to the quaternion algebra $\left(\frac{\alpha,\beta}{K(x)}\right)$ and using the fact that $\mathfrak{p}$, $\mathfrak{q}$ and p are all polynomials we obtain that

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

for some polynomial $q \in K[x]$. Since, the norm $N\mathfrak{p} = \mathfrak{p}\overline{\mathfrak{p}}$ also sits in $K[x]$, it follows from the irreducibility of p that $\deg q = 0$, i.e. $q \in K$.

It remains to prove that $\mathfrak{p}$ is irreducible in $\mathfrak{A}[x]$. Suppose that there are some non-constant polynomials $\mathfrak{q}, \mathfrak{r} \in \mathfrak{A}[x]$, such that $\mathfrak{p} = \mathfrak{q}\mathfrak{r}$. Therefore

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

But this contradicts the irreducibility of p as $\mathfrak{q}\overline{\mathfrak{q}}, \mathfrak{r}\overline{\mathfrak{r}} \in K[x]$. $\square$

We may now present a criterion of irreducibility in $\mathfrak{A}[x]$.

Proposition 6. *Let* $\mathfrak{A} = \left(\frac{\alpha,\beta}{K}\right)$ *be a division quaternion algebra over a number field* K. *Further, let* $p \in K[x]$ *be a monic irreducible polynomial and* $L := {}^{K[x]}\!/\!_{(p)}$. *Then* p *remains irreducible in* $\mathfrak{A}[x]$ *if and only if* $\mathfrak{A} \otimes L$ *does not split.*

Proof. Proposition 5 asserts that p is irreducible in $\mathfrak{A}[x]$ if and only if it does not equal the norm $N\mathfrak{p} = \mathfrak{p}\overline{\mathfrak{p}}$ of any polynomial $\mathfrak{p} \in \mathfrak{A}[x]$. The latter condition is equivalent to the one that p is not represented over $K[x]$ by the Pfister form $\langle\langle -\alpha, -\beta \rangle\rangle = \langle 1, -\alpha, -\beta, \alpha\beta \rangle$, which is the norm form of $\mathfrak{A}$. Now, since p is monic by assumption, it follows from [26, Proposition 3] (or [27, Lemma 17.3]) that p is not represented by this form if and only if L is not the splitting field for $\mathfrak{A}$. $\square$

Remark 2. A procedure for testing if a quaternion algebra over a number field splits is described in [38] and readily available in some computer algebra systems like Magna [4] and Sage [33]. Hence, the above irreducibility test can be easily implemented. An example implementation for the computer algebra system MAGMA [4] was prepared by the author (see the closing section).

Comparing the degrees, we obtain the following immediate consequence of Proposition 6 that can be used as a quick-exit in the procedure for testing the irreducibility.

Corollary 7. *Let* $\mathfrak{A}$ *be a division quaternion algebra and* $p \in K[x]$ *be a monic, irreducible polynomial of odd degree, then* p *remains irreducible in* $\mathfrak{A}[x]$.

To conclude this section, we present a complete irreducibility criterion for quaternionic polynomials that can be directly implemented in a computer algebra system.

Theorem 8. *Let* $\mathfrak{A}$ *be a division quaternion algebra over a number field* K. *Further, Let* $\mathfrak{p} \in \mathfrak{A}[x]$ *be a non-constant polynomial and* $\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q} \cdot p$ *be its decomposition as in Proposition 3.*

(1) *If* $\mathfrak{q} = 1$, *then* $\mathfrak{p}$ *is irreducible in* $\mathfrak{A}[x]$ *if and only if* p *is irreducible in* $K[x]$ *and* $\mathfrak{A} \otimes L$ *does not split, where* $L := {}^{K[x]}\!/\!_{(p)}$.
(2) *If* $p = 1$, *then* $\mathfrak{p}$ *is irreducible in* $\mathfrak{A}[x]$ *if and only if the norm* $N\mathfrak{q}$ *of* $\mathfrak{q}$ *is irreducible in* $K[x]$.
(3) *If* $\mathfrak{q} \neq 1$ *and* $p \neq 1$, *then* $\mathfrak{p}$ *is reducible in* $\mathfrak{A}[x]$.

Proof. The first assertion follows immediately from Proposition 6, while the third one is trivial. We must prove only assertion (2). Without loss of generality, we can assume that $\mathfrak{p}$ is monic. Hence, $\mathfrak{p} = \mathfrak{q}$. If $\mathfrak{p}$ is reducible, say $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2$ then $N\mathfrak{q} = N\mathfrak{p}_1 \cdot N\mathfrak{p}_2$ is reducible in $K[x]$, too. This proves one implication. Now, suppose that $\mathfrak{p}$ is irreducible but $N\mathfrak{q}$ has a factorization $N\mathfrak{q} = q_1 q_2$ for some non-constant polynomials $q_1, q_2 \in K[x]$. The maximal central factor of $\mathfrak{p}$ is trivial by

assumption. Therefore, neither $\mathfrak{p}$ nor $\overline{\mathfrak{p}}$ is divisible by any of the polynomials q_1, q_2. But we have $\mathfrak{p}\overline{\mathfrak{p}} = N\mathfrak{q} = q_1q_2$. Therefore, [25, p. 494] says that $\mathfrak{p}$ is right-divisible by $\mathrm{lclm}(q_2, \overline{\mathfrak{p}}) \cdot \overline{\mathfrak{p}}^{-}1 = q_2$. This contradiction implies that $N\mathfrak{q}$ must be irreducible, proving assertion (2). $\qquad\square$

3. FACTORIZATION OF CENTRAL POLYNOMIALS

Our first task is to factor in $\mathfrak{A}[x]$ an irreducible polynomial p with coefficients in the base field K. Before we consider this problem in its full generality, we first deal with a special case. If there is a maximal (commutative) subfield K_* of $\mathfrak{A}$ such that K_* embeds into $L := {}^{K[x]}/_{(p)}$, then a factorization of p in $\mathfrak{A}[x]$ is exceptionally easy.

Lemma 9. *Let $\mathfrak{A}$ be a division quaternion algebra over a number field K and $p \in \mathfrak{A}[x]$ be a monic irreducible polynomial of degree $\deg p > 1$. Let $L := {}^{K[x]}/_{(p)}$. If there is a maximal commutative subfield K_* of $\mathfrak{A}$ such that $p = N_{K_*/K}(q)$ for some polynomial $q \in K_*[x]$, then*

(1) *K_* embeds into L;*
(2) *p has a non-trivial factorization in $\mathfrak{A}[x]$;*
(3) *the quaternion algebra $\mathfrak{A} \otimes L$ is split.*

Proof. Let $K_* = K(\sqrt{d})$ be such that $p = N_{K_*/K}(q)$ for some $q \in K_*[x]$. Write $q = q_0 + q_1\sqrt{d}$. Then $p = q_0^2 - q_1^2 d$. Let $a_i := q_i + (p) \in L$, for $i \in \{0, 1\}$. We have

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

and so d is a square in L. This means that K_* embeds into L. Now, $p = (q_0 + q_1\sqrt{d})(q_0 - q_1\sqrt{d})$, where $q_0, q_1 \in K_*[x] \subset \mathfrak{A}[x]$. Therefore, p has a non-trivial factorization in $\mathfrak{A}[x]$. The third assertion follows now from Proposition 6. $\qquad\square$

Algorithm 1. *Let $\mathfrak{A}$ be a division quaternion algebra over a number field K, and let $p \in K[x]$ be a monic irreducible polynomial. If there is a maximal commutative subfield of $\mathfrak{A}$ over which p factors, then this algorithm outputs a factorization of p over $\mathfrak{A}$. Otherwise, it reports a failure.*

(1) *Build a field extension $L := {}^{K[x]}/_{(p)}$.*
(2) *Construct all the subfields $L_1, \ldots, L_n$ of L of degree 2 over K (see Remark 3 below).*
(3) *Repeat the following steps for every L_i:*
   (a) *Check if the quaternion algebra $\mathfrak{A} \otimes L_i$ splits. If it does not, then reiterate the loop.*
   (b) *Find an embedding $\varphi : L_i \hookrightarrow \mathfrak{A}$ (see Remark 4 below) and let $K_* := \varphi(L_i)$.*
   (c) *Factor p in $K_*[x]$ into the product $p = \mathfrak{q} \cdot \overline{\mathfrak{q}}$, where $\mathfrak{q} \in K_*[x] \subset \mathfrak{A}[x]$.*
   (d) *Output $(\mathfrak{q}, \overline{\mathfrak{q}})$ and quit.*
(4) *Report a failure.*

Proof of correctness. Let K_* is a maximal (commutative) subfield of K such that p has a non-trivial factorization in $K_*[x]$, then $(K_* : K) = 2$ and so K_* embeds into L by Lemma 9. Hence, K_* is isomorphic to one of the fields $L_1, \ldots, L_n$ constructed in step (2) of the algorithm. Therefore, a proper factorization of p is returned in step (3d). Conversely, assume that L_i is a subfield of L, quadratic over K, and such that $\mathfrak{A} \otimes L_i$ is split. Then, [37, Theoreme I.2.8] asserts that L_i embeds into $\mathfrak{A}$. Hence, up to an isomorphism, it is a maximal subfield of $\mathfrak{A}$. $\qquad\square$

Remark 3. The problem of finding all the subfields of some fixed degree in a given field extension L/K is an active area of research. Algorithms for solving this problem can be found in [7, 13, 14, 32, 35, 36].

Remark 4. Let M be a quadratic extension of K such that $\mathfrak{A} \otimes M$ splits. Fix an element $d \in K$, which is a square in M but not in K. Then $M = K(\sqrt{d})$. Now, [37, Theoreme I.2.8] asserts that M embeds in $\mathfrak{A}$. Therefore, d is a square of some pure quaternion $\mathfrak{a} \in \mathfrak{A}$. Then $a + b\sqrt{d} \mapsto a + b\mathfrak{a}$ is an embedding of M into $\mathfrak{A}$. The quaternion $\mathfrak{a}$ can be directly constructed by solving two norm equations (see, e.g., [16]).

Remark 5. All the algorithms presented in this paper rely on our ability to factor polynomials over number fields, either the base field K or its quadratic extension K_*. Fortunately, the factorization of polynomials over number fields is a well-studied subject. We may refer the reader to [1, 3, 19, 20, 23, 28].

We will now develop the main procedure of this section that takes a polynomial $p \in K[x]$, irreducible in every commutative subfield of $\mathfrak{A}$, and constructs a quaternionic polynomial $\mathfrak{p}$ such that $p = \mathfrak{p}\overline{\mathfrak{p}}$. The general idea is to use the fact (see Proposition 6) that the existence of a non-trivial factorization of p in $\mathfrak{A}[x]$ implies that $\mathfrak{A} \otimes L$ splits, where as before $L := {}^{K[x]}\!/_{(p)}$. We can then use a zero-divisor of $\mathfrak{A} \otimes L$ to find a polynomial $\mathfrak{p} \in \mathfrak{A}[x]$ such that $\mathfrak{p}\overline{\mathfrak{p}} = pq$ for some extraneous factor q. This can be thought of as an "approximate factorization" of p. We will then successively improve this "approximation", reducing the degree of q. First, we show some preliminary lemmas.

Lemma 10. *Let $p, q \in K[x]$ and $\mathfrak{p} \in \mathfrak{A}[x]$ be polynomials and let $\mathfrak{r} \in \mathfrak{A}[x]$ be the reminder of $\mathfrak{p}$ modulo q. If $pq = \mathfrak{p}\overline{\mathfrak{p}}$, then q divides the polynomials $\mathfrak{r}\overline{\mathfrak{r}}$ and $\mathfrak{p}\overline{\mathfrak{r}}$.*

Proof. We have $\mathfrak{p} = \mathfrak{q} \cdot q + \mathfrak{r}$ for some quaternionic polynomial $\mathfrak{q} \in \mathfrak{A}[x]$. Compute

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

This proves the first assertion. For the second one, write

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

Now, it follows from the previous part of the proof that the right-hand side of the above formula is divisible by q and so is $\mathfrak{p}\overline{\mathfrak{r}}$, as claimed. $\square$

Lemma 11. *Keep the assumptions of the previous lemma and let $\mathfrak{q} := \mathfrak{p}\overline{\mathfrak{r}} \cdot q^{-1} \in \mathfrak{A}[x]$. Then p divides $\mathfrak{q}\overline{\mathfrak{q}}$.*

Proof. Compute

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

The assertion follows now from the preceding lemma. $\square$

Lemma 12. *Keep the assumptions of Lemmas 10 and 11. Denote $r := \mathfrak{q}\overline{\mathfrak{q}} \cdot p^{-1} \in K[x]$. Then $\deg r < \deg q$.*

Proof. We have the following relations between the degrees of the polynomials in question:

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

- $\deg \mathfrak{q} = \deg \mathfrak{p} + \deg \mathfrak{r} - \deg q$, since $\mathfrak{q} = \mathfrak{p}\overline{\mathfrak{r}} \cdot q^{-1}$;
- $2 \cdot \deg \mathfrak{p} = \deg p + \deg q$, since $pq = \mathfrak{p}\overline{\mathfrak{p}}$;
- $\deg \mathfrak{r} < \deg q$, since $\mathfrak{r}$ is the reminder of $\mathfrak{p}$ modulo q.

Combining these four conditions, we obtain the following:

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

We are now ready to present an algorithm that factors in $\mathfrak{A}[x]$ an irreducible polynomial p with coefficients in K.

Algorithm 2. *Let $\mathfrak{A} = \left(\frac{\alpha, \beta}{K} \right)$ be a division quaternion algebra over a number field K. Given a monic irreducible polynomial $p \in K[x]$, this algorithm outputs its irreducible factors in $\mathfrak{A}[x]$.*

(1) *Construct the field extension $L = {}^{K[x]}/_{(p)}$.*

(2) *Check if the quaternion algebra $\mathfrak{A} \otimes L$ splits. If it does not split, output p and quit.*

(3) *Execute Algorithm 1. If it returns a factorization $(\mathfrak{p}, \overline{\mathfrak{p}})$ of p, then output $(\mathfrak{p}, \overline{\mathfrak{p}})$ and quit.*

(4) *Find a zero-divisor $\mathfrak{a} = a_0 + a_1 \mathfrak{i} + a_2 \mathfrak{j} + a_3 \mathfrak{k} \in \mathfrak{A} \otimes L$ (see Remark 6).*

(5) *Let $\mathfrak{p} \in \mathfrak{A}[x]$ be an inverse image of $\mathfrak{a}$ under the natural homomorphism $\mathfrak{A}[x] \to \mathfrak{A} \otimes {}^{K[x]}/_{(p)}$, i.e. $\mathfrak{p} := q_0 + q_1 \cdot \mathfrak{i} + q_2 \cdot \mathfrak{j} + q_3 \cdot \mathfrak{k}$, where $q_0, \dots, q_3 \in K[x]$ are polynomials such that $q_i + (p) = a_i$ for $i \leq 3$.*

(6) *Set $q := \mathfrak{p}\overline{\mathfrak{p}} \cdot p^{-1}$.*

(7) *While q is non-constant do:*

    (a) *Compute the reminder $\mathfrak{r}$ of $\mathfrak{p}$ modulo q.*

    (b) *Update $\mathfrak{p}$ setting $\mathfrak{p} := \mathfrak{p}\overline{\mathfrak{r}} \cdot q^{-1}$.*

    (c) *Update q setting $q := \mathfrak{p}\overline{\mathfrak{p}} \cdot p^{-1}$.*

(8) *Let $\mathfrak{c} := \mathrm{lc}\, \mathfrak{p}$ be the leading coefficient of $\mathfrak{p}$.*

(9) *Output $(\mathfrak{p} \cdot \mathfrak{c}^{-1}, \overline{\mathfrak{c}}^{-1} \cdot \overline{\mathfrak{p}})$.*

Proof of correctness. Proposition 6 asserts that p is irreducible in $\mathfrak{A}[x]$ if and only if $\mathfrak{A} \otimes L$ does not split. This proves the correctness of step (2). Assume that the algorithm does not terminate at step (2) or (3). This means that $\mathfrak{A} \otimes L$ splits (i.e. it is isomorphic to $M_2 L$) and so it contains a zero-divisor $\mathfrak{a} = a_0 + a_1 \mathfrak{i} + a_2 \mathfrak{j} + a_3 \mathfrak{k}$. Now, $\mathfrak{a}$ is a zero-divisor if and only if its norm vanishes (see, e.g., [39, Exercise 3.7]):

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

Let the polynomial $\mathfrak{p} \in \mathfrak{A}[x]$ be defined as in step (5). The previous formula reads now as

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

Therefore, p divides $\mathfrak{p}\overline{\mathfrak{p}}$ and so q is a well defined polynomial satisfying the condition $pq = \mathfrak{p}\overline{\mathfrak{p}}$. Lemma 10 says that q divides $\mathfrak{p}\overline{\mathfrak{r}}$, where $\mathfrak{r}$ is the reminder of $\mathfrak{p}$ modulo q. Hence, updating $\mathfrak{p}$ in step (7b), we again obtain a (quaternionic) polynomial. It follows from Lemma 11 that p divides the norm $N\mathfrak{p} = \mathfrak{p}\overline{\mathfrak{p}}$ of the updated polynomial $\mathfrak{p}$. Consequently, after updating q in step (7c) once again, we have a polynomial, and it clearly satisfies the condition $pq = \mathfrak{p}\overline{\mathfrak{p}}$. Further, Lemma 12 asserts that the degree of q diminishes after every iteration of the loop. It follows that the loop stops after finitely many iterations, and so the algorithm terminates. After the loop is finished we have $pq = \mathfrak{p}\overline{\mathfrak{p}}$ where q is a constant. Since p is monic by assumption,

the leading coefficient of the left-hand side is $\mathrm{lc}(pq) = q \in K$, while the leading coefficient of the right-hand side equals $\mathrm{lc}(\mathfrak{p}) \cdot \mathrm{lc}(\overline{\mathfrak{p}}) = \mathfrak{c}\overline{\mathfrak{c}}$. Therefore, $\mathfrak{c}\overline{\mathfrak{c}} = q$ and so $p = \mathfrak{p} \cdot q^{-1} \cdot \overline{\mathfrak{p}} = (\mathfrak{p} \cdot \mathfrak{c}^{-1})(\overline{\mathfrak{c}}^{-1} \cdot \overline{\mathfrak{p}})$ is a factorization of p. $\square$

Remark 6. It is well known (see [38, Section 4]) that finding a zero-divisor in a (necessarily split) quaternion algebra $\left(\frac{\alpha,\beta}{L}\right)$ is equivalent to finding an L-rational point on a projective conic curve given by $\alpha x^2 + \beta y^2 - \alpha\beta z^2 = 0$. This can be done either by a variant of a Lagrange descent (see [6, 34] and [5, §127.5]) or by solving a norm equation (see [15]). In particular, it is always possible to find a zero-divisor which is a pure quaternion, i.e. it has a form $\mathfrak{a} = a_1\mathfrak{i} + a_2\mathfrak{j} + a_3\mathfrak{k}$.

Example 1. We will illustrate how the above algorithm works using the following toy example. Fix the quaternion algebra $\mathfrak{A} := \left(\frac{-1,-1}{\mathbb{Q}}\right)$ over the rationals and let

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

The field $L = {}^{K[x]}\!/_{(p)}$ splits $\mathfrak{A}$, hence p factors in $\mathfrak{A}[x]$. The polynomial $\mathfrak{p}$ constructed in step (5) has a form $\mathfrak{p} = 0 + q_1\mathfrak{i} + q_2\mathfrak{j} + q_3\mathfrak{k}$, where:

$$q_1 = 19x^3 - 12x^2 + 211x + 154,$$
$$q_2 = 13x^3 - 11x^2 + 136x + 97,$$
$$q_3 = 53.$$

It follows that initally the polynomial $q = \mathfrak{p}\overline{\mathfrak{p}} \cdot p^{-1}$ equals

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

In this particular example, the loop is executed only once, and after it stops, we have

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

Dividing $\mathfrak{p}$ on the right by its leading coefficient, we obtain the sought factor of p:

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

It can be verified by a direct computation that $p = \mathfrak{q}_0\overline{\mathfrak{q}_0}$.

4. Factoring general polynomials

We will now present an algorithm that factors an arbitrary quaternionic polynomial. First, we prove the following auxiliary lemma that may, to some extent, mitigate inconveniences caused by the lack of commutativity.

Lemma 13. *Let* $\mathfrak{p}, \mathfrak{q} \in \mathfrak{A}[x]$ *be irreducible monic polynomials. If the norm* $N\mathfrak{p}$ *and* $N\mathfrak{q}$ *are relatively prime in* $K[x]$, *then there are irreducible polynomials* $\mathfrak{p}_1, \mathfrak{q}_1 \in \mathfrak{A}[x]$ *such that* $N\mathfrak{p}_1 = N\mathfrak{p}$, $N\mathfrak{q}_1 = N\mathfrak{q}$ *and* $\mathfrak{p}\mathfrak{q} = \mathfrak{q}_1\mathfrak{p}_1$.

Proof. The polynomials $N\mathfrak{p}$ and $N\mathfrak{q}$ are relatively prime by assumption. Hence, by Bézout identity, there are polynomials $p, q \in K[x]$ such that

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

Set $\mathfrak{p}_* := \overline{\mathfrak{p}} \cdot p$ and $\mathfrak{q}_* := \overline{\mathfrak{q}} \cdot q$. Then

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

This means that $\mathfrak{q}$ is right-invertible[1] modulo $\mathfrak{p}$. Set

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

---

[1]Notice that $\mathfrak{q}$ is also left-invertible modulo $\mathfrak{p}$. However, to prove the latter assertion it suffices to use a weaker asumption that $\mathrm{gcrd}(\mathfrak{p}, \mathfrak{q}) = 1$ together with [25, Theorem I.5].

where the quaternion $\mathfrak{a}$ is selected in such a way that $\mathfrak{p}_1$ is monic. Rearranging the term (see [25, Theorem I.13]) we obtain

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

From the assumption $\gcd(N\mathfrak{p}, N\mathfrak{q}) = 1$ we infer $\mathrm{gcrd}(\mathfrak{p}, \mathfrak{q}) = 1$. Hence, the norms of $\mathfrak{p}$ and $\mathfrak{p}_1$ coincide. We have

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

Therefore, the product $\mathfrak{p}\mathfrak{q}$ is right-divisible by $\mathfrak{p}_1$. Take $\mathfrak{q}_1 := \mathfrak{p}\mathfrak{q} \cdot \mathfrak{p}_1^{-1}$. It is clear that $N\mathfrak{q}_1 = N\mathfrak{q}$ and $\mathfrak{q}_1 \mathfrak{p}_1 = \mathfrak{p}\mathfrak{q}$. $\qquad\square$

Algorithm 3. *Let it $\mathfrak{A}$ be a division quaternion algebra over a number field K. Given a nonzero polynomial $\mathfrak{p} \in \mathfrak{A}[x]$, this algorithm outputs a quaternion $\mathfrak{c} \in \mathfrak{A}$ and a list $\mathscr{L} = (\mathfrak{q}_1, \ldots, \mathfrak{q}_n)$ of monic irreducible quaternionic polynomials such that $\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_n$.*

   (1) *Let $\mathfrak{c} := \mathrm{lc}(\mathfrak{p})$ and update $\mathfrak{p}$ setting $\mathfrak{p} := \mathfrak{c}^{-1} \cdot \mathfrak{p}$. Initialize $\mathscr{L} := ()$.*
   (2) *Let $p_0, \ldots, p_4 \in K[x]$ be the coordinates of $\mathfrak{p}$ with respect to the basis $\{1, \mathfrak{i}, \mathfrak{j}, \mathfrak{k}\}$ of $\mathfrak{A}[x]$ treated as a free module over $K[x]$.*
   (3) *Compute the maximal central factor $p := \gcd(p_0, \ldots, p_4)$ of $\mathfrak{p}$ and set $\mathfrak{q} := \mathfrak{p} \cdot p^{-1}$.*
   (4) *Factor p in $K[x]$ into the product $p = r_1^{e_1} \cdots r_m^{e_m}$ of irreducible polynomials $r_1, \ldots, r_m \in K[x]$.*
   (5) *Factor every polynomial r_i in $\mathfrak{A}[x]$ using Algorithm 2. Append e_i copies of the output of that algorithm to the list $\mathscr{L}$.*
   (6) *Factor the norm $N\mathfrak{q} = \mathfrak{q}\overline{\mathfrak{q}}$ in $K[x]$ into the product $N\mathfrak{q} = q_1^{\varepsilon_1} \cdots q_k^{\varepsilon_k}$ of monic irreducible polynomials $q_1, \ldots, q_k \in K[x]$.*
   (7) *Repeat the following steps as long as the polynomial $\mathfrak{q}$ remains non-constant:*
      (a) *Compute the greatest common right divisor $\mathfrak{r} := \mathrm{gcrd}(\mathfrak{q}, q_k)$.*
      (b) *Update the list $\mathscr{L}$ prepending $\mathfrak{r}$ to it at the beginning.*
      (c) *Update the polynomial $\mathfrak{q}$ setting $\mathfrak{q} := \mathfrak{q} \cdot \mathfrak{r}^{-1}$.*
      (d) *Decrement the exponent ε_k by 1.*
      (e) *If $\varepsilon_k = 0$, then decrement the index k by 1.*
   (8) *Output $\mathfrak{c}$ and the list $\mathscr{L}$.*

Proof of correctness. Fix a nonzero polynomial $\mathfrak{p} \in \mathfrak{A}[x]$. Proposition 3 asserts that $\mathfrak{p}$ can be uniquely expressed as $\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q} \cdot p$, where p is the greatest common divisor (in $K[x]$) of the coordinates of $\mathfrak{p}$, constructed in step (2) of the algorithm. It is clear that by factoring $\mathfrak{q}$ and p into products of irreducible quaternionic polynomials, we obtain a factorization of the original polynomial $\mathfrak{p}$. Factorization of p is performed in steps (4–5) using Algorithm 2. It remains to factor $\mathfrak{q}$. Assume that $\mathfrak{q} = \mathfrak{r}_1 \cdots \mathfrak{r}_l$ is some factorization of $\mathfrak{q}$. Then $N\mathfrak{q} = N\mathfrak{r}_1 \cdots N\mathfrak{r}_l$ is a factorization in $K[x]$ of the norm of $\mathfrak{q}$. But now, $K[x]$ is a (commutative) unique factorization domain, hence every $N\mathfrak{r}_i$ must equal precisely one of the irreducible factors $q_1, \ldots, q_k \in K[x]$ of $N\mathfrak{q}$. Repeatedly applying Lemma 13 we see that there is another factorization $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_l$ such that $N\mathfrak{q}_l = q_k$. Consequently, we can extract the right-most factor $\mathfrak{q}_l = \mathrm{gcrd}(\mathfrak{q}, q_k)$. A simple induction shows that the loop in step (7) will eventually produce all the irreducible factors. $\qquad\square$

Remark 7. One may wonder why we have to use a dedicated method when dealing with polynomials having coefficients in the center of the algebra. The reason is that the norm of a central polynomial $p \in K[x]$ is just its square $Np = p^2$. Consequently $\mathrm{gcrd}(p, Np) = \gcd(p, p^2) = p$. Hence, even if p factors in $\mathfrak{A}[x]$ into a product $p = \mathfrak{p}\overline{\mathfrak{p}}$, step (7a) of Algorithm 3 cannot extract its factors. The same phenomenon is observed when factoring polynomials in a finite field extension using Trager's

algorithm. Say, $L = K(\vartheta)$ is a finite extension of K and $p \in L[x]$. In Trager's algorithm, to factor p, we "shift" it and compute the norm of $p(x + k\vartheta)$ for some $k \in \mathbb{Z}$. Unfortunately, in the case of quaternionic polynomials, this trick no longer works due to the lack of commutativity. That is why we need to recourse to the more complex method described in Section 3. Therefore, factorization of polynomials over division quaternion algebras (hence algebras of degree two) is much more time-consuming than factorization over degree two field extensions. Nonetheless, detailed complexity analysis needs to be a subject of further research.

Example 2. We will illustrate Algorithm 3 with another toy example. Take again the quaternion algebra $\mathfrak{A} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and let

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

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

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

Computing the greatest common divisor of these four polynomials, we obtain the maximal central factor of $\mathfrak{p}$:

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

The polynomial p is precisely the one that was factored already in the previous example. It remains to factor the polynomial $\mathfrak{q} := (1 + \mathfrak{k})^{-1} \cdot \mathfrak{p} \cdot p^{-1}$, that is not divisible by any polynomial with coefficients in K. The norm of $\mathfrak{q}$ factors in $K[x]$ into a product $N\mathfrak{q} = q_1 q_2 q_3$, where

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

Computing the successive greatest common right divisors, we obtain factors of $\mathfrak{q}$:

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

This yields a factorization $\mathfrak{p} = (1 + \mathfrak{k}) \cdot \mathfrak{q}_1 \mathfrak{q}_2 \mathfrak{q}_3 \cdot \mathfrak{q}_0 \overline{\mathfrak{q}_0}$, where $\mathfrak{q}_0$ is the factor of p constructed in Example 1.

5. Root finding

Polynomial factorization is closely related to the problem of root finding. For quaternionic polynomials, the latter question was studied already 80 years ago by Niven in the case of Hamiltonian quaternions (see [24]) and 40 years ago by Beck for arbitrary quaternion algebras (see [2]). Nevertheless, so far, computational methods have concentrated exclusively on Hamiltonian quaternions (see, e.g., [11, 12, 24, 29, 31]). In this section, we show how to adapt Algorithm 3 to find roots in $\mathfrak{A}$ of a polynomial $\mathfrak{p} \in \mathfrak{A}[x]$, where $\mathfrak{A}$ is a division quaternion algebra over a number field.

It is known that the Fundamental Theorem of Algebra holds for the Hamiltonian quaternions (see, e.g., [12, 24, 29]). Hence, every non-constant polynomial with coefficients in $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ has a root in $\mathbb{H}$. This property no longer holds if we replace $\mathbb{H}$ by a split quaternion algebra over the reals. Similarly, it is completely unsurprising that, in the situation considered in this paper, there are polynomials with coefficients in division quaternion algebras over number fields that do not have roots in their rings of coefficients. If it is the case, then the algorithm must of course return an empty set.

In a commutative world, finding roots in $L \supseteq K$ of a polynomial $p \in K[x]$ is equivalent to finding linear factors of p in $L[x]$. It no longer works when we leave the commutative playpen and consider polynomials over non-commutative division rings. Here we encounter two immediate obstacles. First, a quaternionic polynomial may have infinitely many zeros. Secondly, the evaluation map $\mathfrak{A}[x] \to \mathfrak{A}$, $\mathfrak{p} \mapsto \mathfrak{p}(\mathfrak{a})$ for some fixed $\mathfrak{a}$ is no longer a ring homomorphism if $\mathfrak{a} \notin Z(\mathfrak{A})$. In particular, $\mathfrak{p} = \mathfrak{q}\mathfrak{r}$ and $\mathfrak{q}(\mathfrak{a}) = 0$ does not yet imply that $\mathfrak{p}(\mathfrak{a}) = 0$. Fortunately, both these inconveniences are easy to overcome. First, however, for the reader's convenience, let us cite two very classical facts concerning the roots of quaternionic polynomials. Recall that two nonzero quaternions $\mathfrak{a}$, $\mathfrak{b}$ are said to be *conjugate* if there is a quaternion $\mathfrak{c} \in \mathfrak{A}^\times$ such that $\mathfrak{a} = \mathfrak{c}\mathfrak{b}\mathfrak{c}^{-1}$. Clearly, conjugacy is an equivalence relation.

Theorem 14 (Gordon–Motzkin). *Let $\mathfrak{A}$ be a division quaternion algebra and $\mathfrak{p} \in \mathfrak{A}[x]$. Then:*

(1) *A quaternion $\mathfrak{a} \in \mathfrak{A}$ is a root of $\mathfrak{p}$ if and only if $\mathfrak{p}$ is right-divisible by $x - \mathfrak{a}$.*
(2) *At most $\deg \mathfrak{p}$ conjugacy classes of $\mathfrak{A}$ contains roots of $\mathfrak{p}$.*
(3) *If $\mathfrak{p} = (x - \mathfrak{a}_1) \cdots (x - \mathfrak{a}_n)$, then every root of $\mathfrak{p}$ is conjugate to some $\mathfrak{a}_i$.*
(4) *If a conjugacy class of $\mathfrak{A}$ contains more than one root of $\mathfrak{p}$, then $\mathfrak{p}$ has infinitely many roots in this class.*

For a proof of the above theorem we refer the reader to [10] or [17, §16]. For a nonzero quaternion $\mathfrak{a} \in \mathfrak{A}$ we denote its *characteristic polynomial* by $\chi_\mathfrak{a} = N(x - \mathfrak{a}) = x^2 - \mathrm{Tr}(\mathfrak{a}) \cdot x + N(\mathfrak{a}) \in K[x]$. It is obvious that $\chi_\mathfrak{a} = \chi_{\overline{\mathfrak{a}}} = \chi_\mathfrak{b}$ for every conjugate $\mathfrak{b}$ of $\mathfrak{a}$. Conversely, Dickson's theorem (see e.g., [17, Theorem 16.8]) asserts that $\chi_\mathfrak{a} = \chi_\mathfrak{b}$ implies that $\mathfrak{a}$ and $\mathfrak{b}$ are conjugate. The next theorem is taken from [2].

Theorem 15 (Beck). *Let $\mathfrak{A}$ be a division quaternion algebra and $\mathfrak{p} \in \mathfrak{A}[x]$ a non-constant polynomial. Then:*

(1) *A quaternion $\mathfrak{a}$ is conjugate to a root $\mathfrak{b}$ of $\mathfrak{p}$ if and only if $\chi_\mathfrak{a}$ divides $N\mathfrak{p}$ in $K[x]$ if and only if $\mathfrak{a}$ is a root of $N\mathfrak{p}$.*
(2) *If $\chi_\mathfrak{a}$ divides $\mathfrak{p}$, for some $\mathfrak{a} \in \mathfrak{A}^\times$ then every conjugate of $\mathfrak{a}$ is a root of $\mathfrak{p}$.*

Fix a nonzero quaternionic polynomial $\mathfrak{p} \in \mathfrak{A}[x]$. Write it again as a product $\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q} \cdot p$, where $\mathfrak{c}$ is the leading coefficient, p the maximal central factor of $\mathfrak{p}$, and $\mathfrak{q}$ is not divisible by any non-constant polynomial from $K[x]$. In view of the above two theorems, it is clear that to find roots of $\mathfrak{p}$, all we need to do is to find its linear right factors. To this end, it suffices to consider just the linear and quadratic factors of p together with the quadratic factors of $N\mathfrak{q}$. Moreover, since $\mathfrak{p}$ may have infinitely many roots, the best we can do is to enumerate roots up to conjugacy relation. This is precisely what Algorithm 4 does. First, however, we need to state the following lemma, which is widely known, but we are not aware of any convenient reference.

Lemma 16. *A quaternion $\mathfrak{a} \in \mathfrak{A} \setminus K$ is a root of a polynomial $p \in K[x]$ if and only if $\chi_\mathfrak{a}$ divides p.*

Proof. Assume that $p(\mathfrak{a}) = 0$. Then [17, Theorem 16.6] asserts that $p = \mathfrak{q} \cdot \chi_{\mathfrak{a}}$ for some polynomial $\mathfrak{q} \in \mathfrak{A}[x]$. But p and $\chi_{\mathfrak{a}}$ sit in $K[x]$, hence also $\mathfrak{q} \in K[x]$ (see e.g., [17, Exercise 16.1]). The opposite implication is trivial.   □

We are now ready to present the root finding algorithm, which is an easy adaptation of the factorization procedure presented in Algorithm 3.

Algorithm 4. *Given a nonzero polynomial $\mathfrak{p} \in \mathfrak{A}[x]$, this algorithm outputs a set $\mathscr{R} \subset \mathfrak{A}$ such that every element of $\mathscr{R}$ is a root of $\mathfrak{p}$ and every root of $\mathfrak{p}$ is conjugate to a unique element of $\mathscr{R}$.*

  (1) *Let $\mathfrak{c} := \mathrm{lc}(\mathfrak{p})$ and update $\mathfrak{p}$ setting $\mathfrak{p} := \mathfrak{c}^{-1} \cdot \mathfrak{p}$.*
  (2) *Let $p_0, \ldots, p_4 \in K[x]$ be the coordinates of $\mathfrak{p}$ with respect to the basis $\{1, \mathfrak{i}, \mathfrak{j}, \mathfrak{k}\}$ of $\mathfrak{A}[x]$ treated as a free module over $K[x]$.*
  (3) *Compute the maximal central factor $p := \gcd(p_0, \ldots, p_4)$ of $\mathfrak{p}$ and set $\mathfrak{q} := \mathfrak{p} \cdot p^{-1}$.*
  (4) *Factor p in $K[x]$ into the product $p = r_1^{e_1} \cdots r_m^{e_m}$ of irreducible polynomials $r_1, \ldots, r_m \in K[x]$.*
  (5) *Initialize $\mathscr{R}$ to be the set of roots (in K) of all the linear factors of p:*
$$\mathscr{R} := \big\{ a \in K : r_i = x - a \text{ for some } i \leq k \big\}.$$
  (6) *For every polynomial r_i of degree 2:*
    (a) *Execute Algorithm 1 with input r_i, if it reports a failure, then reiterate the loop.*
    (b) *Otherwise, if Algorithm 1 returns a factorization $r_i = (x - \mathfrak{a}_i)(x - \overline{\mathfrak{a}_i})$, then check if $\mathscr{R}$ contains an element conjugate to $\mathfrak{a}_i$.*
    (c) *If it does not, then add $\mathfrak{a}_i$ to $\mathscr{R}$.*
  (7) *Factor the norm $N\mathfrak{q} = \mathfrak{q}\overline{\mathfrak{q}}$ in $K[x]$ into the product $N\mathfrak{q} = q_1^{\varepsilon_1} \cdots q_k^{\varepsilon_k}$ of monic irreducible polynomials $q_1, \ldots, q_k \in K[x]$.*
  (8) *For every polynomial q_j of degree 2:*
    (a) *Compute the greatest common right divisor $x - \mathfrak{b}_j = \gcd(q_j, \mathfrak{q})$.*
    (b) *Check if $\mathscr{R}$ contains an element conjugate to $\mathfrak{b}_j$.*
    (c) *If it does not, then add $\mathfrak{b}_j$ to $\mathscr{R}$.*
  (9) *Output the set $\mathscr{R}$.*

Proof of correctness. Fix a quaternionic polynomial $\mathfrak{p} = \mathfrak{c} \cdot \mathfrak{q} \cdot p$ and let $\mathscr{R}$ be the set constructed by the algorithm. First, we will prove that every element of $\mathscr{R}$ is a root of p. If an element $a \in \mathscr{R}$ was constructed in step (5), then it is clear that $\mathfrak{p}(a) = p(a) = 0$. Likewise, if $\mathfrak{a}_i \in \mathscr{R}$ was constructed in step (6b), then $\chi_{\mathfrak{a}_i} = (x - \mathfrak{a}_i)(x - \overline{\mathfrak{a}_i})$ divides p. Hence, $\mathfrak{a}_i$ is again a root of $\mathfrak{p}$ (and so are all its conjugates by Theorems 15). Now, take an element $\mathfrak{b}_j \in \mathscr{R}$ constructed in step (8a). Then $x - \mathfrak{b}_j$, being the greatest common right divisor of $\mathfrak{q}$ and q_j, is, in particular, a right divisor of $\mathfrak{p}$, since p is central. It follows that $\mathfrak{b}_j$ is a root of $\mathfrak{p}$.

Conversely, we will now show that every root of $\mathfrak{p}$ is conjugate to some element of $\mathscr{R}$. Assume that $\mathfrak{a} \in \mathfrak{A}$ is a root of $\mathfrak{p}$. Then $x - \mathfrak{a}$ is a right divisor of $\mathfrak{p}$, by Theorem 14. We need to consider three cases. If $\mathfrak{a}$ sits in K, then $x - \mathfrak{a}$ divides p and so $\mathfrak{a}$ is one of the elements constructed in step (5) of the algorithm. Hence, without loss of generality, we can assume that $\mathfrak{a} \notin K$. If $x - \mathfrak{a}$ divides p, then the characteristic polynomial $\chi_{\mathfrak{a}}$ of $\mathfrak{a}$ divides p, by Lemma 16. Thus, $\chi_{\mathfrak{a}}$ is one of the factors r_i of degree 2 considered in step (6). Consequently, either $\mathfrak{a}$ is added to $\mathscr{R}$, or $\overline{\mathfrak{a}}$ is added to $\mathscr{R}$, or $\mathscr{R}$ already contains an element conjugate to one of these two. But, $\mathfrak{a}$ and $\overline{\mathfrak{a}}$ are conjugate by Dickson's theorem (see e.g., [17, Theorem 16.8]). Therefore, either way, $\mathscr{R}$ contains an element conjugate to $\mathfrak{a}$.

Finally, assume that $x - \mathfrak{a}$ does not divide p. It follows that $x - \mathfrak{a}$ must be a right divisor of $\mathfrak{q}$ since p is central. But then the norm $N(x - \mathfrak{a}) = \chi_{\mathfrak{a}}$ is irreducible in $K[x]$

and divides $N\mathfrak{q}$. Consequently, $\chi_\mathfrak{a} = q_j$ for some $j \leq k$ and so $x - \mathfrak{a} = \operatorname{gcrd}(\mathfrak{q}, q_j)$. Therefore, either $\mathfrak{a}$ itself is added to $\mathscr{R}$ in step (8c) or $\mathscr{R}$ contains an element conjugate to $\mathfrak{a}$. This way, we have proved that every root of $\mathfrak{p}$ is conjugate to some element of $\mathscr{R}$. This element is uniquely determined since the elements of $\mathscr{R}$ are pairwise non-conjugate. □

6. Conclusion and further studies

We have presented an explicit algorithm for factorization of unilateral polynomials with coefficients in division quaternion algebras over number fields. As mentioned earlier, in general, a quaternionic polynomial may have infinitely many different factorizations into irreducible factors. The algorithm presented in the paper outputs just one of these factorizations. This fact makes the complexity of the algorithm rather tricky. It has been empirically observed by the author that the output can be "suboptimal" in the sense that the sizes of coefficients can become arbitrarily large. This phenomenon occurs mostly when factoring central polynomials since Algorithm 2 may suffer from the explosive growth of coefficients that is typical to Euclidean-like algorithms over polynomial rings. Methods to overcome this obstacle by selecting factors with small coefficients (or restricting the growth of the coefficients) should be a subject for further studies.

The algorithms introduced in the paper were implemented by the author in a package $_q\mathcal{P}ol_y$ for the computer algebra system Magma. The package is distributed under the MIT license and can be freely downloaded from the author's web page `http://www.pkoprowski.eu/qpoly`.

References

[1] Ali Ayad. A lecture on the complexity of factoring polynomials over global fields. *Int. Math. Forum*, 5(9-12):477–486, 2010.
[2] Bernard Beck. Sur les équations polynomiales dans les quaternions. *Enseign. Math. (2)*, 25(3-4):193–201 (1980), 1979.
[3] Karim Belabas, Mark van Hoeij, Jürgen Klüners, and Allan Steel. Factoring polynomials over global fields. *J. Théor. Nombres Bordeaux*, 21(1):15–39, 2009.
[4] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
[5] John Cannon, Wieb Bosma, Claus Fieker, and Allan Steel (eds.). *Handbook of Magma Functions*, 2.27-7 edition, 2022.
[6] John E. Cremona and D. Rusin. Efficient solution of rational conics. *Math. Comp.*, 72(243):1417–1441, 2003.
[7] Andreas-Stephan Elsenhans and Jürgen Klüners. Computing subfields of number fields and applications to Galois group computations. *J. Symbolic Comput.*, 93:1–20, 2019.
[8] Maria Irene Falcão, Fernando Miranda, Ricardo Severino, and Maria Joana Soares. Evaluation schemes in the ring of quaternionic polynomials. *BIT*, 58(1):51–72, 2018.
[9] Basil Gordon and Theodore Samuel Motzkin. On the zeros of polynomials over division rings. *Trans. Amer. Math. Soc.*, 116:218–226, 1965.
[10] Basil Gordon and Theodore Samuel Motzkin. Correction to the paper "On the zeros of polynomials over division rings". *Trans. Amer. Math. Soc.*, 122:547, 1966.
[11] Drahoslava Janovská and Gerhard Opfer. A note on the computation of all zeros of simple quaternionic polynomials. *SIAM J. Numer. Anal.*, 48(1):244–256, 2010.
[12] Bahman Kalantari. Algorithms for quaternion polynomial root-finding. *J. Complexity*, 29(3-4):302–322, 2013.
[13] Jürgen Klüners. On computing subfields. A detailed description of the algorithm. *J. Théor. Nombres Bordeaux*, 10(2):243–271, 1998.
[14] Jürgen Klüners and Michael E. Pohst. On computing subfields. *J. Symbolic Comput.*, 24(3-4):385–397, 1997. Computational algebra and number theory (London, 1993).
[15] Przemysław Koprowski. Isotropic vectors over global fields, 2021. arXiv `https://arxiv.org/abs/2111.08569`.

[16] Przemysław Koprowski. Computing square roots in quaternion algebras, 2023. arXiv https://arxiv.org/abs/2301.00743.

[17] Tsit-Yuen Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.

[18] Tsit-Yuen Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[19] Susan Landau. Factoring polynomials over algebraic number fields. *SIAM J. Comput.*, 14(1):184–195, 1985.

[20] Arjen K. Lenstra. Factoring polynomials over algebraic number fields. In *Computer algebra (London, 1983)*, volume 162 of *Lecture Notes in Comput. Sci.*, pages 245–254. Springer, Berlin, 1983.

[21] Johanna Lercher, Daniel Scharler, Hans-Peter Schröcker, and Johannes Siegele. Factorization of quaternionic polynomials of bi-degree (n,1). *Beitr. Algebra Geom.*, 64(1):209–232, 2023.

[22] Zijia Li, Daniel F. Scharler, and Hans-Peter Schröcker. Factorization results for left polynomials in some associative real algebras: state of the art, applications, and open questions. *J. Comput. Appl. Math.*, 349:508–522, 2019.

[23] José Méndez Omaña and Michael E. Pohst. Factoring polynomials over global fields. II. *J. Symbolic Comput.*, 40(6):1325–1339, 2005.

[24] Ivan Niven. Equations in quaternions. *Amer. Math. Monthly*, 48:654–661, 1941.

[25] Oystein Ore. Theory of non-commutative polynomials. *Ann. of Math. (2)*, 34(3):480–508, 1933.

[26] Yves Pourchet. Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. *Acta Arith.*, 19:89–104, 1971.

[27] A. R. Rajwade. *Squares*, volume 171 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1993.

[28] Xavier-François Roblot. Polynomial factorization algorithms over number fields. *J. Symbolic Comput.*, 38(5):1429–1443, 2004.

[29] Takis Sakkalis, Kwanghee Ko, and Galam Song. Roots of quaternion polynomials: theory and computation. *Theoret. Comput. Sci.*, 800:173–178, 2019.

[30] Daniel F. Scharler and Hans-Peter Schröcker. An algorithm for the factorization of split quaternion polynomials. *Adv. Appl. Clifford Algebr.*, 31(3):Paper No. 29, 23, 2021.

[31] Rogério Serôdio, Edgar Pereira, and Jose Vitória. Computing the zeros of quaternion polynomials. *Comput. Math. Appl.*, 42(8-9):1229–1237, 2001. Numerical methods and computational mechanics (Miskolc, 1998).

[32] Jonas Szutkoski and Mark van Hoeij. The complexity of computing all subfields of an algebraic number field. *J. Symbolic Comput.*, 93:161–182, 2019.

[33] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.5)*, 2022. https://www.sagemath.org.

[34] Mark van Hoeij and John Cremona. Solving conics over function fields. *J. Théor. Nombres Bordeaux*, 18(3):595–606, 2006. http://jtnb.cedram.org/item?id=JTNB_2006__18_3_595_0.

[35] Mark van Hoeij, Jürgen Klüners, and Andrew Novocin. Generating subfields. In *ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, pages 345–352. ACM, New York, 2011.

[36] Mark van Hoeij, Jürgen Klüners, and Andrew Novocin. Generating subfields. *J. Symbolic Comput.*, 52:17–34, 2013.

[37] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[38] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. In *Quadratic and higher degree forms*, volume 31 of *Dev. Math.*, pages 255–298. Springer, New York, 2013.

[39] John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, [2021] ©2021.