Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Computations in the ring of quaternionic polynomials

Alberto Damiano[a,1], Graziano Gentili[b], Daniele Struppa[c]

[a] Department of Mathematics and Computer Science, Chapman University, One University Drive, Orange CA 92866, USA

[b] Dipartimento di Matematica "U. Dini", Università di Firenze, Viale Morgagni 67/A, 50134, Italy

[c] Department of Mathematics and Computer Science, Schmid College of Science, Chapman University, One University Drive, Orange CA 92866, USA

ARTICLE INFO

Article history:
Received 28 February 2009
Accepted 22 June 2009
Available online 27 June 2009

Keywords:
Quaternionic polynomials
Bezout theorem
Gröbner bases
Noncommutative syzygies

ABSTRACT

In this paper we study basic division properties in the ring of regular quaternionic polynomials. We obtain a Bezout-like theorem and we calculate the module syzygy for any vector of polynomials.

1. Introduction

In the early forties, Niven gave some fundamental contributions to the study of polynomials with quaternionic coefficients. His first work on quaternionic equations was Niven (1941), and later in Niven (1942) and Eilenberg and Niven (1944), coauthored with Eilenberg, he gave a first proof of the fundamental theorem of algebra in the ring of polynomials with quaternionic coefficients. After a few decades of relative oblivion, in recent years there has been a rebirth of interest in the study of such polynomials. This interest originated from the desire to extend fundamental properties of complex polynomials (see Pogorui and Shapiro, 2004; Serodio and Siu, 2001), but also received an impulse from the development of a new theory of regular functions of a quaternionic variable, of which quaternionic polynomials are an important example (see Gentili and Stoppato, 2008; Gentili and Struppa, 2006, 2007, 2008; Gentili et al., 2008). Most of these papers analyzed the structure of the set of zeros of such polynomials. In particular Gentili et al. (2008) offers a new proof of the fundamental theorem of algebra, while Gentili and Stoppato (2008), Pogorui and Shapiro (2004) and Serodio and Siu (2001) explain in detail the nature of such zeros; it was in Pogorui and Shapiro (2004), for example,

E-mail addresses: damiano@chapman.edu, alberto@tlc185.com (A. Damiano), gentili@math.unifi.it (G. Gentili), struppa@chapman.edu (D. Struppa).

[1] Tel.: +393498386632; fax: +3901841950166.

0747-7171/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2009.06.003

that the authors first identified the phenomenon of spherical zeros. Finally, Gentili and Struppa (2008) is a study of factorization of quaternionic polynomials and of the role that a nonstandard notion of multiplicity of zeros plays.

In this paper we continue this analysis but focus instead on issues of division within the ring of polynomials $\mathbb{H}[q]$. In the better known case of complex polynomials, divisibility and factorization are essentially equivalent, but this turns out not to be the case when we move to the noncommutative situation. In Section 2, we briefly describe the Euclidean division algorithm in $\mathbb{H}[q]$; our discussion here is a special case of the more general treatment given by Ore in Ore (1933), but we include it because of the simpler form it assumes in the quaternionic setting. In Section 3 we prove a version of the Bezout theorem, and we show its dependence on issues of commutativity.

Finally, we conclude with a short section in which we introduce Gröbner bases for the ideals in $\mathbb{H}[q]$, and we fully identify the module of syzygies for any list of polynomials, giving a minimal set of generators in the linear case.

2. Division algorithm for quaternionic polynomials

Let $\mathbb{H}$ denote the algebra of real quaternions. It is generated by three elements i, j, k, called imaginary units since they satisfy the relations $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i,$ and $ki = -ik = j$. Elements in $\mathbb{H}$ can be written as $q = x_0 + ix_1 + jx_2 + kx_3$ where the x_l are real. If we denote by S the 2-dimensional sphere of imaginary units of $\mathbb{H}$, i.e. $S = \{q \in \mathbb{H} \mid q^2 = -1\}$, then every nonreal quaternion q can be written in a unique way as $q = x + yI$, with $I \in S$ and $x, y \in \mathbb{R}, y > 0$. We will refer to $x = \text{Re}(q)$ as the real part of q and $y = \text{Im}(q)$ as the imaginary part of q. The algebra of quaternions is a division algebra in the sense that every nonzero element $q = x + yI \in \mathbb{H}^* = \mathbb{H} \setminus \{0\}$ has a (bilateral) inverse given by $\bar{q}/|q|^2$ where $\bar{q} = x - yI$ and $|q|^2 = x^2 + y^2$. Technically, polynomials over the quaternions could be finite sums of elements of the type aq^n or $q^n a$, with $a \in \mathbb{H}$, or, more in general, words of the type $a_0 q a_1 q \cdots a_{n-1} q a_n$ with $a_\ell \in \mathbb{H}$. However, only powers of q with right coefficients in $\mathbb{H}$ are regular quaternionic functions. In light of this observation, and consistently with the definition given in Lam (1991), we set

Definition 1. The ring of *regular* quaternionic polynomials with *right* coefficients $\mathbb{H}[q]$ is the left $\mathbb{H}$-vector space whose elements are of the type $\left\{ \sum_{n=0}^{d} q^n a_n \mid a_n \in \mathbb{H}, d \in \mathbb{N} \right\}$ endowed with the noncommutative product defined by the (left) linear extension of

$$(q^n a_n) * (q^m a_m) := q^{n+m} a_n b_m.$$

Remark 2. It is important to note that the evaluation map $\epsilon_\alpha : \mathbb{H}[q] \to \mathbb{H}$ defined by $\epsilon_\alpha(F) = F(\alpha)$ is not an algebra homomorphism, since for example $\epsilon_\alpha((q - \beta) * (q - \alpha)) = \alpha^2 - \alpha(\alpha + \beta) + \beta\alpha \neq 0$, unless of course α and β commute.

The theory of zero sets for regular quaternionic polynomials is very different from that of complex polynomials. While the fundamental theorem of algebra still holds in $\mathbb{H}[q]$, (Gentili et al., 2008), quaternionic polynomial equations may admit an infinite number of solutions (see for example Gentili and Struppa, 2008).

Strictly related to the problem of finding roots of a regular polynomial is the factorization problem in $\mathbb{H}[q]$. Theorem 2.8 of Gentili and Struppa (2008) essentially says that every monic regular polynomials can be written as a product $P(q) * Q(q)$ where

$$P(q) = (q - \alpha_1) * \cdots * (q - \alpha_n)$$

is such that $\alpha_{i+1} \neq \bar{\alpha}_i$ for all $i = 1 \ldots n - 1$, so that its zero set is composed by isolated roots (see again (Gentili and Struppa, 2008) for a formula to find the roots given α_i), while $Q(q)$ is a commutative polynomial given by

$$Q(q) = (q^2 - q(2\text{Re}(\beta_1)) + |\beta_1|^2) \cdots (q^2 - q(2\text{Re}(\beta_m)) + |\beta_m|^2), \quad \text{for some } \beta_1, \ldots, \beta_m \in \mathbb{H}.$$

As in every noncommutative ring, ideals of $\mathbb{H}[q]$ can be left, right or bilateral, depending on which side one allows multiplication. For the sake of simplicity, most of the times we will consider *left* ideals only. Unless otherwise specified, our results on left ideals will translate into the corresponding ones for right ideals in a straightforward manner. Let us recall some basic definitions. If not differently indicated, all polynomials we consider will be monic.

Definition 3. We say that a regular polynomial G divides F on the left (resp. on the right) if there exists $A \in \mathbb{H}[q]$ such that $F = G * A$ (resp. $F = A * G$). Let $F_1, \ldots, F_n$ be polynomials of $\mathbb{H}[q]$. Their Greatest Common Left Divisor, shortly $GCLD(F_1, \ldots, F_n)$, is the unique monic element $D \in \mathbb{H}[q]$ such that D divides F_i on the left for every i, and such that every other left divisor of all F_i divides D on the left. Similarly one defines the greatest common right divisor $GCRD(F_1, \ldots, F_n)$.

In general it can be hard to calculate the *GCLD* of two polynomials due to the fact that one cannot rely on factorization. Performing a full factorization of a polynomial can be very difficult if one does not know its roots, even when the coefficients are chosen in a commutative field. Here we also have the issue of nonuniqueness. We need a better, algorithmic way of calculating the *GCLD*. As in the commutative case $\mathbb{K}[x]$, where $\mathbb{K}$ is a field, one can use the Euclidean Division algorithm. We first observe that $\mathbb{H}[q]$ is a (left and right) Euclidean domain.

Proposition 4 (*Euclidean Division*). *Let F, G be regular polynomials. Then there exist Q, R, Q' and R' in $\mathbb{H}[q]$, with $\max(\deg(R), \deg(R')) < \deg(G)$, such that*

$$F = Q * G + R \quad \text{and} \quad F = G * Q' + R'.$$

Moreover, such polynomials are uniquely determined.

Proof. The existence is proved by performing Euclidean division on F and G in the same way one would do it in the commutative case. Note that the two polynomials can always be chosen to be monic, so the division of the terms of F by the leading power of G is unambiguous. The only difference with the commutative case is that in order to get Q and R versus Q' and R', one has to perform multiplications of partial quotient respectively to the right or to the left by G. Uniqueness follows easily from the fact that $(\mathbb{H}[q], *, +)$ is an integral domain, and from the fact that the degrees of R and R' are both smaller than the degree of G. □

Corollary 5 (*Remainder Theorem*). *Let $F(q)$ be a regular polynomial and let $\alpha \in \mathbb{H}$. Then there exists $Q \in \mathbb{H}[q]$ such that $F(q) = (q - \alpha) * Q(q) + F(\alpha)$.*

Because of Remark 2, the usual remainder theorem holds only for left division (see also Wedderburn, 1921), which is an immediate consequence of Proposition 4.

3. Bezout's theorem

In order to give an algorithm for the calculation of the greatest common divisor using Euclidean division, we introduce the following notation. If $F = Q * G + R$ and $F = G * Q' + R'$ as in Proposition 4, we define

$$mod_r(F, G) = R, \quad div_r(F, G) = Q, \quad mod_l(F, G) = R', \quad div_l(F, G) = Q'.$$

Note that the subscripts refer to the side with respect to which division is performed, although Q and Q' are, technically speaking, left and right quotients respectively.

Theorem 6 (*Calculation of GCLD*). *Let F, G be nonzero regular polynomials. Then the following list of instructions returns their greatest common left divisor in a finite number of steps:*

```
Input: $F, G \in \mathbb{H}[q] \setminus \{0\}$
Output: GCLD(F,G)
Initialization: $a := F$, $b := G$
• While $b \neq 0$ Do
    $t := b$
    $b := mod_l(a, b)$
    $a := t$
• Return $a$.
```

Proof. The proof is formally the same as in the commutative case, only one needs to keep all factors in the correct position, either to the left or to the right. Note that termination is guaranteed by the fact that the remainder sequence has strictly decreasing degrees. □

Remark 7. In order to calculate the greatest common *right* divisor, the situation is completely symmetric. It is indeed sufficient to replace the second step of the "while" loop in Algorithm 6 with $b := mod_r(a, b)$.

Remark 8. A different algorithm based on the use of Gröbner bases will be provided in the next section.

Euclidean division is a very powerful tool that also allows to express the greatest common divisor as an explicit combination of the two polynomials. This is true in every commutative Euclidean domain, and the corresponding algorithm in $\mathbb{H}[q]$ is virtually identical. After completing all the iterated divisions of Algorithm 6, one "climbs" back up to the top with simple algebraic steps. The only important observation is that quotients of the iterated divisions are *right* multiples, so that one ends up with a *right* linear combination of F and G. We do not prove the following result, which also appears in Wedderburn (1921), giving rather an example of calculation which illustrates the procedure.

Proposition 9. *Let F and G be nonzero regular polynomials. Then there exist $A, B \in \mathbb{H}[q]$ such that $GCLD(F, G) = F * A + G * B$.*

Example 10. Consider $F(q) = q*(q-i)*(q-j) = q^3 - q^2(i+j) + qk$ and $G(q) = q*(q-k) = q^2 - qk$. In order to find $mod_l(F, G)$ we need to perform *left* division of F by G. This gives

$$F = G * (q - i - j + k) + q(k - j + i - 1). \tag{1}$$

Since the first remainder $R_1 = q(k + j - i - 1)$ is not zero, we need to perform yet another division. We use the remainder to divide G and we see that

$$G = R_1 * (q - k)(k + j - i - 1)^{-1}, \tag{2}$$

which ends the iteration since the new remainder is zero. Keeping the common divisor monic, and from (1), we have

$$\begin{aligned} q &= GCLD(F, G) = R_1(k + j - i - 1)^{-1} = F * (k + j - i - 1)^{-1} \\ &\quad - G * (k + j - i - 1)^{-1}(q - i - j + k). \end{aligned}$$

Definition 11. Given n polynomials in $\mathbb{H}[q]$, we define recursively

$$GCLD(F_1, \ldots, F_n) = GCLD(GCLD(F_1, F_2), F_3, \ldots, F_n).$$

We are now ready to state the following theorem.

Theorem 12 (*Bezout Theorem for Regular Polynomials*). *Let $F_1, \ldots, F_n$, $n > 1$, be nonzero regular quaternionic polynomials. The following facts are equivalent:*
(a) *$F_1, \ldots, F_n$ have no common roots in $\mathbb{H}$*
(b) *$GCLD(F_1, \ldots, F_n) = 1$*
(c) *There exist $A_1, \ldots, A_n$ regular polynomials such that $F_1 * A_1 + \cdots + F_n * A_n = 1$.*

Proof. (a) ⇒ (b) Let $D := GCLD(F_1, \ldots, F_n)$. If $D \notin \mathbb{H}$, then it has at least a root $\alpha \in \mathbb{H}$, so we can write $D = (q - \alpha) * D'$. This implies that α is a common root for the polynomials, which is a contradiction. Hence $D \in \mathbb{H}$ and since it is monic, $D = 1$.
(b) ⇒ (c) The case $n = 2$ is an instance of Proposition 9. For $n > 2$, consider the $n - 1$ polynomials $GCLD(F_1, F_2)$ and $F_3, \ldots, F_n$ which have no common roots. Using induction on n and then again Proposition 9, one obtains

$$\begin{aligned} 1 &= GCLD(F_1, F_2) * A + F_3 * A_3 + \cdots + F_n * A_n = (F_1 * A_1' + F_2 * A_2') * A + F_3 * A_3 \\ &\quad + \cdots + F_n * A_n, \end{aligned}$$

which is the thesis with $A_i := A_i' * A$, $i = 1, 2$.

(c) $\Rightarrow$ (a) Suppose the polynomials have a common root $\alpha \in \mathbb{H}$. Then, using Corollary 5, we have that for every index i, $F_i(q) = (q - \alpha) * F_i'(q)$ for some F_i'. We can write then

$$(q - \alpha) * (F_1' * A_1 + \cdots + F_n' * A_n) = 1$$

which is absurd, because the degree of a regular product is the sum of the degrees. □

It is immediate to verify, as a consequence of the previous considerations, that every left or right ideal of $\mathbb{H}[q]$ is principal. We give the statement for left ideals.

Corollary 13. *Let I be a left ideal in $\mathbb{H}[q]$ and let $F_1, \ldots, F_n$ be its generators. Let $D = GCRD(F_1, \ldots, F_n)$. Then $I = \mathbb{H}[q]\langle D\rangle$.*

Remark 14. Observe that a completely symmetric version of Theorem 12 using the greatest common right divisor could not be given. Indeed, only the equivalence of (b) and (c) can be proved. If $GCRD(F_1, \ldots, F_n) = 1$, one uses again (right) Euclidean divisions to find a combination $\sum_i A_i * F_i = 1$, while the opposite implication is immediate to prove. The fact that such conditions are not equivalent to condition (a) is due to the noncommutativity of the $*$-product and to the fact that roots of regular polynomials only correspond to left linear factors. The next example will illustrate the situation.

Example 15. Consider $F = q^2 - q(i + j) + k$ and $G = q^2 - q(j + k) - i$. The polynomial F vanishes only at $q = i$, while the only root of Q is $q = k$. However, performing iterative right divisions, one gets that $GCRD(F, G) = q - j = (k - i)^{-1} * F - (k - i)^{-1} * G$.

4. Gröbner bases for quaternionic polynomials

The theory of Gröbner bases provides a powerful tool to perform effective computations in any commutative polynomial ring. A classical reference is Kreuzer and Robbiano (2000). Recently, this theory has been extended to a wider collection of algebras, including the so-called *solvable algebras*, or *G-algebras*. Thanks to the work of Levandovskyy (2005), Gröbner basis algorithms have been implemented on Singular (Greuel et al., 2005). The libraries for calculations in noncommutative rings are grouped in its subsystem called Plural (Greuel et al., 2003). A G-algebra A is essentially a quotient of the ring of noncommutative polynomials $\mathbb{K}\langle x_1, \ldots, x_n\rangle$ modulo a two-sided ideal of relations. Relations in a G-algebra are of the type

$$x_j x_i = c_{ij} \cdot x_i x_j + d_{ij}, \quad 1 \le i < j \le n, \tag{3}$$

where $c_{ij} \in \mathbb{K}$ and $d_{ij} \in A$ satisfy certain “nondegeneracy" conditions, for which we refer to the manual of Plural. In particular, a vector space basis for any G-algebra is given by the standard monomials $x_1^{a_1} \cdots x_n^{a_n}$, a fact which allows one to carry over many of the concepts and algorithms from the commutative theory of Gröbner bases. A key condition which guarantees the termination of Buchberger algorithm for G-algebras is the fact that, with respect to a given term ordering on the set of standard monomials, we have that the leading term (LT) of the polynomials d_{ij} satisfies

$$LT(d_{ij}) < x_i x_j, \quad 1 \le i < j \le n.$$

Examples of G-algebras (and quotients of G-algebras) include the Weyl algebra, the exterior algebra over a finite-dimensional vector space, the Clifford algebra, and all universal enveloping algebras associated with simple Lie algebras. The ring of regular polynomials is also a quotient of a G-algebra, as the following propositions shows. We omit their proofs since they are straightforward.

Proposition 16. *Let $\mathcal{H}$ be the $\mathbb{R}$-algebra generated by q, i, j, k and satisfying the following relations*
(1) $qi = iq$, $qj = jq$, $qk = kq$
(2) $ij = -ji$, $jk = -kj$, $ik = -ki$.
Then $\mathcal{H}$ is a G-algebra.

Notice that the relations of (2) in the above proposition make i, j and k into anticommutative variables, while (1) says that q behaves like an indeterminate in a commutative polynomial ring. If we then introduce the relations $i^2 = j^2 = k^2 = -1$, we can state the next result.

Proposition 17. *Let $\mathcal{H}$ be as above and let $\mathcal{I}$ be the two-sided ideal of $\mathcal{H}$ generated by $(i^2 + 1, j^2 + 1, k^2 + 1, ij - k, jk - i, ik + j)$. Then $\mathbb{H}[q] \simeq \mathcal{H}/\mathcal{I}$.*

We recall the following definition, which we present only for left ideals.

Definition 18. Let I be a left ideal in a G-algebra A, and let σ be an order relation on the set of standard monomials which is compatible with multiplication (i.e., a *term order*) and such that $t > 1$ for every monomial t (i.e., a *well order*). Denote by $LT_\sigma(F)$ the leading term of an element of A with respect to such relation. A subset $\mathcal{G} \subset A$ is called a left Gröbner basis for I if $LT(\mathcal{G}) = \{LT_\sigma(g) \mid g \in \mathcal{G}\}$ generates the left monoid $(LT_\sigma(f) \mid f \in I)$. Moreover, we say that $\mathcal{G}$ is *reduced* if the leading term of every element g of $\mathcal{G}$ does not divide the monomials of $\mathcal{G} \setminus \{g\}$.

Since $\mathbb{H}[q]$ is a quotient of a G-algebra, every left or right ideal admits a unique reduced Gröbner basis with respect, for instance, to the term order given by the extension of $q > i > j > k$ to the set of terms. Corollary 13 implies the following result.

Proposition 19. *Let $I = (F_1, \dots, F_n)$ be a right (resp. left) ideal of $\mathbb{H}[q]$. Then the reduced right (resp. left) Gröbner basis of any system of generators for I, with respect to any term ordering, is $\{GCLD(F_1, \dots, F_n)\}$ (resp. $\{GCRD(F_1, \dots, F_n)\}$).*

Proof. Let us prove the statement for a right ideal. If the generators have no common root, Bezout theorem shows that $D = 1$ is their greatest common left divisor and $I = (1)$. It is clear that $\{1\}$ is the reduced Gröbner basis of I. Suppose now that $D := GCLD(F_1, \dots, F_n)$ is not a constant. Since D divides all generators, then $LT(D)$ divides all their leading terms, which shows that $\{D\}$ is a Gröbner basis for I. The fact that it is reduced is obvious since it contains only one element. □

Remark 20. Note that, in particular, this proposition allows to calculate greatest common divisors using Gröbner bases, which is an alternative to Algorithm 6. If one uses Singular, the algebra $\mathbb{H}[q]$ can be introduced via the sequence of commands

```
ring r=0,(q,i,j,k),dp;
matrix C[4][4]=0,1,1,1,0,0,-1,-1,0,0,0,-1,0,0,0,0;
LIB "nctools.lib";
ncalgebra(C,0);
ideal a=i2+1,j2+1,k2+1,ij-k,jk-i,ik+j;
qring H=twostd(a);
```

Then only *right* greatest common divisors can be calculated with the command `std` which returns a *left* Gröbner basis. However, define the following $\mathbb{H}$-antilinear map in $\mathbb{H}[q]$

$$c\left(\sum_i q^i a_i\right) := \sum_i q^i \bar{a}_i$$

which clearly satisfies the usual property of a conjugation: $c(f * g) = c(g) * c(f)$, which in turn allows to transform a *right* Gröbner basis calculation into the calculation of a *left* Gröbner basis for the ideal generated by the conjugates. In particular, one has

$$GCLD(f_1, \dots, f_n) = c(GCRD(c(f_1), \dots, c(f_n))).$$

Given a (not necessarily commutative) ring R the question of whether some given elements $f_1, \dots, f_n$ of R satisfy relations of the type

$$a_1 f_1 + \cdots + a_n f_n = 0, \quad a_i \in \mathcal{R},$$

is highly nontrivial (Bluhm and Kreuzer, 2006). n-tuples $(a_1, \dots, a_n)$ are called (left) *syzygies* of $f_1, \dots, f_n$ and clearly form a (left) R-module. When R is the ring of commutative polynomials, the algorithm to explicitly construct the syzygies of a set of polynomials is a classical application of the theory of Gröbner bases. The algorithm has been extended to the case of G-algebras (see Levandovskyy, 2005 and references therein). For two-sided syzygies see also the paper Bluhm and Kreuzer (2006) where the authors present a general technique for noncommutative polynomials and their quotients. Here we make some observation on the nature of the module of syzygies for polynomials in $\mathbb{H}[q]$ without exploiting such general algorithms. First, note that thanks to the conjugation defined in the previous paragraph, we have that left syzygy computations are equivalent to right syzygy computations. We will then only focus on left syzygies. We start with a result on the nature of syzygies of linear polynomials.

Proposition 21. *For every integer $i = 1, \dots, n$, $n > 1$, let $f_i = q - a_i \in \mathbb{H}[q]$ where a_i are distinct quaternions. Then the $\mathbb{H}[q]$ left module of syzygies of $(f_1, \dots, f_n)$ is generated by*

$$s_{12} = (q - a_2)(\bar{a}_1 - \bar{a}_2)\mathbf{e}_1 + (q - a_1)(\bar{a}_2 - \bar{a}_1)\mathbf{e}_2,$$

together with, if $n > 2$, the $n - 2$ polynomials

$$t_i = f_i(a_1 - a_2)^{-1}\mathbf{e}_1 + f_i(a_2 - a_1)^{-1}\mathbf{e}_2 + \mathbf{e}_i, \quad 3 \le i \le n.$$

Proof. The fact that the above vectors are syzygies is a straightforward calculation. Notice that the syzygies t_i come from the fact that $(x - a_1) - (x - a_2) = a_2 - a_1$ which implies that $(a_2 - a_1)^{-1}(x - a_1) - (a_2 - a_1)^{-1}(x - a_2) = 1$. This in particular says that the ideal (f_1, f_2) is actually the whole ring. What we only need to prove, then, is the statement for $n = 2$: the module of left syzygies $Syz(f_1, f_2)$ is such that $Syz(f_1, f_2) = \langle s_{12} \rangle$. Let $f, g \in \mathbb{H}[q]$ be two polynomials such that $f * f_1 + g * f_2 = 0$. Let us consider the linear polynomial $L(q) = f_2 * (\bar{a}_1 - \bar{a}_2)$ and let us divide f to the right by L. We obtain

$$f(q) = Q(q) * L(q) + R,$$

where $R \in \mathbb{H}$. This implies

$$\begin{aligned} f(q) * (q - a_1) &= Q(q) * L(q) * (q - a_1) + R * (q - a_1) \\ &= Q(q) * (q - a_2) * (\bar{a}_1 - \bar{a}_2) * (q - a_1) + R * (q - a_1), \end{aligned} \tag{4}$$

and using the fact that both s_{12} and (f, g) are syzygies of the pair (f_1, f_2) we have

$$-g(q) * (q - a_2) = Q(q) * (q - a_1) * (\bar{a}_1 - \bar{a}_2) * (q - a_2) + R * (q - a_1) \tag{5}$$

from which it follows that

$$-[g(q) + Q(q) * (q - a_1) * (\bar{a}_1 - \bar{a}_2)] * (q - a_2) = R * (q - a_1). \tag{6}$$

The previous equation can hold only if the term $g(q) + Q(q) * (q - a_1) * (\bar{a}_1 - \bar{a}_2)$ is a constant. However, it is easy to see that the only constants $R, S \in \mathbb{H}$ satisfying $S * (q - a_2) = R * (q - a_1)$ are $R = S = 0$ which, combined with equation (4) proves the statement. □

The proof of the above result only uses Euclidean division. We now present a more general result whose proof is based on a classical method due to Schreyer for the construction of syzygies of the generators of an ideal given a Gröbner basis for the ideal. This is well known in the commutative case (Kreuzer and Robbiano, 2000), and has been extended to G-algebras (Levandovskyy, 2005).

Consider some nonzero polynomials $F_1, \dots, F_t \in \mathbb{H}[q]$ with degrees $n_1 \dots n_t$, and calculate $D = GCRD(F_1, \dots, F_t)$. We can suppose that F_i is monic and that $n_1 \ge \dots \ge n_t$, so we can define $d_{ij} := n_i - n_j$ for all $1 \le i < j \le t$. Using Corollary 13 we can write $F_i = H_i * D$ for all i, and find polynomials A_i such that $\sum_{i=1}^{t} A_i * F_i = D$ with the Euclidean algorithm. For all $1 \le i < j \le t$, put moreover $G_{ij} := F_i - q^{d_{ij}} F_j$, and let C_{ij} be such that $G_{ij} = C_{ij} * D$. With this notation, we state the following

Theorem 22. *The module of left syzygies $Syz(F_1, \dots, F_t)$ is generated by the following $\binom{t}{2}$ vectors*

$$v_{ij} := \mathbf{e}_i - q^{d_{ij}}\mathbf{e}_j - C_{ij} * \sum_{k=1}^{t} A_k \mathbf{e}_k, \quad 1 \le i < j \le t, \tag{7}$$

where $\mathbf{e}_i$ is the ith element of the canonical basis of $\mathbb{H}[q]^t$, together with the vectors

$$w_i := \mathbf{e}_i - H_i * \sum_{k=1}^{t} A_k \mathbf{e}_k, \quad 1 \le i \le t. \tag{8}$$

Proof. As a consequence of Proposition 19, the set $\mathcal{G} = \{F_1, \dots, F_t, D\}$ is a left Gröbner basis for the ideal $I := \mathbb{H}[q](F_1, \dots, F_t)$, although not a reduced one. We have chosen the Gröbner basis so that it contains the generators of I, because in this case it is easier to “lift” the syzygies of $\mathcal{G}$ to those of I. It suffices indeed to calculate the S-polynomials of all pairs in $\mathcal{G}$, express them as a combination of the basis (which amounts to writing them as multiples of D wince this is the minimal one), and then read the relations obtained as combinations of $F_1, \ldots, F_t$. Given $i < j$, take

$$S(F_i, F_j) = F_i - q^{d_{ij}} F_j = C_{ij} * D.$$

Since $D = \sum_k A_k F_k$, we can rewrite the above equality as

$$F_i - q^{d_{ij}} F_j - C_{ij} \sum_{k=1}^{t} A_k * F_k = 0,$$

which says that $v_{ij} \cdot (F_1, \ldots, F_t) = 0$. For the second set of syzygies, let d be the degree of D, and remember that D is monic by definition. Therefore, for all $1 \leq i \leq t$ we have

$$S(F_i, D) = F_i - q^{n_i - d} * D = H_i * D - q^{n_i - d} * D = (H_i - q^{n_i - d}) * D.$$

Comparing the second and the last quantity in the above chain of equalities, and rewriting again D, we obtain the following relation

$$F_i - q^{n_i - d} * D - (H_i - q^{n_i - d}) * D = F_i - H_i * \sum_{k=1}^{n} A_k * F_k,$$

which means that $w_i \cdot (F_1, \ldots, F_t) = 0$. Based on the the discussion in Levandovskyy (2005) (with an adaptation to the noncommutative case of, for example, Theorem 3.1.8 of Kreuzer and Robbiano (2000)), these vectors generate the module of left syzygies. □

Remark 23. The generators presented in the previous theorem may not be minimal. The linear syzygies constructed in Proposition 21 are in fact fewer than the ones provided by Theorem 22. Consider for example the case $t = 2$, and $F_i = q - a_i$, with $a_1 \neq a_2 \in \mathbb{H}$. While the proposition only gives the syzygy $s_{12} = (q - a_2)(\bar{a}_1 - \bar{a}_2)\mathbf{e}_1 + (q - a_1)(\bar{a}_2 - \bar{a}_1)\mathbf{e}_2$, the previous theorem would give 3 redundant generators. However, since $D = 1$ in this case, we have $H_i = F_i, A_i = (-1)^i (a_2 - a_1)^{-1}$ and $C_{12} = (a_2 - a_1)$. Therefore, $v_{12} = 0$ and

$$w_1 = w_2 = ((a_2 - a_1 - F_1)\mathbf{e}_1 - F_1\mathbf{e}_2)(a_2 - a_1)^{-1} = |a_2 - a_1|^2 s_{12}.$$

Acknowledgments

The first two authors are grateful to Chapman University for the hospitality during the period in which this paper was written. The authors are also grateful to the Editor and the anonymous referees for pointing out the work of Ore, and for other helpful suggestions.

References

Bluhm, H., Kreuzer, M., 2006. Gröbner basis techniques in the computation of two-sided syzygies. In: Combinatorial Group Theory, Discrete Groups, and Number Theory. In: Contemp. Math., vol. 421. Amer. Math. Soc., Providence, RI, pp. 45–64.
Eilenberg, S., Niven, I., 1944. The f̈undamental theorem of algebraf̈or quaternions. Bull. Amer. Math. Soc. 50, 246–248.
Gentili, G., Stoppato, C., 2008. Zeros of regular functions and polynomials of a quaternionic variable. Michigan Math. J. 56 (3), 655–667.
Gentili, G., Struppa, D.C., 2006. A new approach to Cullen-regular functions of a quaternionic variable. C. R. Math. Acad. Sci. Paris, Ser. I 342, 741–744.
Gentili, G., Struppa, D.C., 2007. A new theory of regular functions of a quaternionic variable. Adv. Math. 216, 279–301.
Gentili, G., Struppa, D.C., 2008. On the multiplicity of zeroes of polynomials with quaternionic coefficients. Milan J. Math. 76, 15–25.
Gentili, G., Struppa, D.C., Vlacci, F., 2008. The fundamental theorem of algebra for Hamilton and Cayley numbers. Math. Z. 259 (4), 895–902.
Greuel, G.-M., Pfister, G., Schönemann, H., 2005. Singular 3.0. A computer algebra system for polynomial computations. Centre for Computer Algebra, University of Kaiserslautern. http://www.singular.uni-kl.de.
Greuel, G.-M., Levandovskyy, V., Schönemann, H., 2003. Singular::Plural 2.1. A computer algebra system for noncommutative polynomial algebras. Centre for Computer Algebra, University of Kaiserslautern. http://www.singular.uni-kl.de/plural.
Kreuzer, M., Robbiano, L., 2000. Computational Commutative Algebra 1. Springer.
Lam, T.Y., 1991. A first course in noncommutative rings. In: Graduate Texts in Mathematics, vol. 123. Springer-Verlag, New York.
Levandovskyy, V., 2005. Non-commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation. Ph.D. Thesis.
Niven, I., 1941. Equations in quaternions. Amer. Math. Monthly 48, 654–661.
Niven, I., 1942. The roots of a quaternion. Amer. Math. Monthly 49, 386–388.
Ore, O., 1933. Theory of non-commutative polynomials. Ann. Math. 34 (3), 480–508.
Pogorui, A., Shapiro, M.V., 2004. On the structure of the set of zeros of quaternionic polynomials. Complex Var. 49 (6), 379–389.
Serodio, R., Siu, L.S., 2001. Zeros of quaternionic polynomials. Appl. Math. Lett. 14, 237–239.
Wedderburn, J.H.M., 1921. On division algebras. Trans. Amer. Math. Soc. 22 (2), 129–135.