Quaternionic polynomials in Magma

Przemysław Koprowski
Institute of Mathematics
University of Silesia
ul. Bankowa 14, 40-007 Katowice, Poland
przemyslaw.koprowski@us.edu.pl

Abstract

This paper provides a brief introduction to the package qPoly for the Magma computer algebra system, which enables computations with univariate polynomials over division quaternion algebras. The package substantially extends existing functionality, bringing the support for quaternionic polynomials to a level comparable to that currently available for polynomials over fields.

Polynomials over non-commutative rings were introduced over ninety years ago and have remained an active area of research ever since. The theory of polynomials over non-commutative division rings is particularly well developed, as it largely parallels the theory over fields. For a survey of classical results, we refer the reader to [5, §16]. Nonetheless, despite this maturity, support for non-commutative polynomials in mainstream computer algebra systems remains rudimentary, typically limited to basic arithmetic and evaluation.

The package qPoly addresses this gap in functionality by extending Magma with a comprehensive suite of tools for handling left unilateral polynomials over division quaternion algebras. The ultimate goal is to offer a level of functionality comparable to that available for univariate polynomials over fields. The software already implements most of the intended features; the primary remaining limitation concerns functional decomposition (i.e., there is no non-commutative analog of the `Decomposition(f)` command). A comprehensive description of the package, including its performance results, can be found in [4].

A central design principle of qPoly is to provide seamless integration with Magma. Consequently, function names and input-output specifications closely follow the conventions of the native system whenever mathematically meaningful. The main exception is that some qPoly commands include the qualifiers `Left` or `Right` in their names, reflecting the non-commutativity of quaternionic polynomial multiplication.

At the time of writing, the list of commands provided by qPoly comprises over thirty functions, ranging from basic arithmetic routines (e.g., `Coordinates`, `Euclidean[Left|Right]Division`, `Norm`, `Trace`), through one-sided greatest common divisors, least common multiples, and the computation of Bézout coefficients (e.g., `GreatestCommon[Left|Right]Divisor`, `LeastCommon[Left|Right]Multiple`), to non-commutative interpolation (`BrayWhaplesPolynomial`, `Interpolation`), root finding (e.g., `HasRoot`, `Roots`), irreducibility testing and factorization (e.g., `IsIrreducible`, `Factorization`, `CentralDecomposition`), and resultant computation (`Resultant`). All commands are fully documented in the manual distributed with the package. Some of the algorithms implemented in qPoly were presented at previous ISSAC meetings (see [2, 3]).

The package is released as open-source software under the MIT License and is available from the author's webpage (`http://www.pkoprowski.eu/qpoly`) as well as the ACM Collected Algorithms Repository (`https://calgo.acm.org/1056.zip`). It is distributed as a zip archive that should be extracted into a directory accessible to MAGMA. The package is then loaded by attaching its specification:

```
> AttachSpec("path_to_package/qpoly.spec");
```

This paper demonstrates the usage of the package through three illustrative examples. As is well known, polynomials over non-commutative division rings may have infinitely many roots. Nevertheless, the number of conjugacy classes of roots is finite and bounded by the degree of the polynomial (see, e.g., [1, Theorem 2] or [5, Theorem 16.4]). This phenomenon necessitates a refined notion of multiplicity.

Let $\mathscr{A} = \left(\frac{\alpha,\beta}{K}\right)$ be a division quaternion algebra. Each root $a \in \mathscr{A}$ of a quaternionic polynomial $p \in \mathscr{A}[x]$ possesses two associated multiplicities: the *isolated multiplicity* and the *spherical multiplicity*. A nonzero spherical multiplicity indicates that p vanishes not only at a, but on its entire conjugacy class $\{bab^{-1} \mid b \in \mathscr{A}^\times\}$.

This refined notion of multiplicity is reflected in the specification of the root-related routines. Specifically, the `Roots` command in qPoly differs from its counterpart in standard MAGMA. Instead of returning pairs (*root*, *multiplicity*), it returns triples of the form (*root*, *isolated multiplicity*, *spherical multiplicity*).

Consider the quaternion algebra $\mathscr{A} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and a polynomial $p \in \mathscr{A}[x]$ defined by the list of coefficients:

```
> A<i,j,k> := QuaternionAlgebra<Rationals() | -1, -1>;
> P<x> := PolynomialRing(A);
> p := P![ 6+6*i-36*j+24*k, 18-12*i-6*j+30*k, 23+5*i-30*j+20*k,
>        15-10*i-5*j+25*k, 16+i-6*j+4*k, 3-2*i-j+5*k, 3 ];
```

We find the roots of p in $\mathscr{A}$ as follows:

```
> Roots( p );
[ <-i - j, 0, 2>, <i + j - k, 1, 2>, <-1 + i, 1, 0> ]
```

In this example, p has a single isolated root at $i-1$, vanishes on the entire conjugacy class of $i+j$, and admits a root $i+j-k$ that exhibits both types of multiplicity.

The polynomial ring $\mathscr{P} = \mathscr{A}[x]$ is *similarity-factorial* (see [6, 8]): every non-constant polynomial possesses a factorization into irreducibles that is unique up to similarity. More precisely, any two factorizations consist of the same number of factors, which correspond pairwise under the similarity relation. Here, two quaternionic polynomials $p, q \in \mathscr{P}$ are called *similar* if the left $\mathscr{P}$-modules $\mathscr{P}/(\mathscr{P}p)$ and $\mathscr{P}/(\mathscr{P}q)$ are isomorphic.

We illustrate this property with the following example. Let p be defined as follows:

```
> A<i,j,k> := QuaternionAlgebra<QuadraticField(7) | -1, -1>;
> p := (x^2 - (3+i)*x - k)*(x - j)*(x^2 + (1-k)*x + (1-k))*(k*x - (1+k));
```

We factor this polynomial using the `Factorization` command provided by qPoly. This command has the same output specification as its commutative counterpart in MAGMA. Given a polynomial

$p \in \mathscr{P}$, it returns a list of pairs (q_i, k_i), where q_i is a monic irreducible factor and k_i is its multiplicity, followed by the leading coefficient c. These components satisfy $p = c \cdot q_1^{k_1} \cdots q_n^{k_n}$.

Because multiplication is non-commutative, the order of factors is critical. Specifically, the leading coefficient must be the leftmost factor, and the irreducible polynomials must be multiplied in the exact order they appear in the list. In our example, we obtain:

```
> fp, c := Factorization(p); fp; c;
[
    <x^2 + (-3 + i)*x + -k, 1>,
    <x^2 + (1 + 2/3*i + 4/3*j - 1/3*k)*x + 1/3 + 2/3*i + 2/3*j - k, 1>,
    <x + -1 - 2/3*i + 2/3*j + 1/3*k, 1>,
    <x + -j, 1>
]
k
```

Note that the factorization returned by $q\mathcal{P}oly$ differs from the one used to define p. For instance, the factor $x - j$, which originally appeared in the second position, was shifted to the final position. Consequently, the two factors it "jumped over" have been transformed. We can verify that the command's output remains a valid factorization of p:

```
> c*FactorisationToPolynomial(fp) eq p;
true
```

As previously noted, the factors are determined only up to similarity. To demonstrate this, consider the polynomial $\mathfrak{r}_1 := x^2 + (1-k)x + (1-k)$ from the initial definition of p, and let $\mathfrak{r}_2$ be the second factor returned by `Factorization`. We can verify their similarity as follows:

```
> r1 := x^2 + (1-k)*x + (1-k); r2 := fp[2][1];
> test, lambda := IsSimilar(r1, r2 : Isomorphism := true); test;
true
```

The second return value, λ, provides an explicit isomorphism between the left $\mathscr{P}$-modules $\mathscr{P}/(\mathscr{P}\mathfrak{r}_1)$ and $\mathscr{P}/(\mathscr{P}\mathfrak{r}_2)$, thereby certifying the similarity of the two factors.

Finally, we consider an application to sums of squares. According to Pourchet's Theorem (see, e.g., [7, Theorem 17.2]), a polynomial $p \in \mathbb{Q}[x]$ is a sum of four squares if and only if it is non-negative everywhere and, in the factorization of p over $\mathbb{Q}_2[x]$, each irreducible factor has either even multiplicity or even degree. Such polynomials are precisely the norms of quaternionic polynomials over $\left(\frac{-1,-1}{\mathbb{Q}}\right)$.

The `Factorization` command, discussed above, provides a means of decomposing a rational polynomial into a sum of squares. Consider, for instance, the polynomial $p = x^6 + 6x^5 + 8x^4 - 26x^3 + 50x^2 - 22x + 9$:

```
> P<x> = PolynomialRing(Rationals());
> p := x^6 + 6*x^5 + 8*x^4 - 26*x^3 + 50*x^2 - 22*x + 9; p;
x^6 + 6*x^5 + 8*x^4 - 26*x^3 + 50*x^2 - 22*x + 9
```

We factor p over the algebra $\mathscr{A} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$:

```
> A<i,j,k> := QuaternionAlgebra<Rationals() | -1, -1>;
> factors := Factorization( PolynomialRing(A)! p ); factors;
[
    <$.1^3 + (3 + 434/47841*i - 4952/47841*j - 89251/47841*k)*$.1^2 +
        (-107431/47841 - 8047/15947*i - 25963/47841*j + 234545/47841*k)*$.1 +
        45151/15947 - 6952/47841*i + 15520/47841*j - 44296/47841*k, 1>,
```

```
    <$.1^3 + (3 - 434/47841*i + 4952/47841*j + 89251/47841*k)*$.1^2 +
        (-107431/47841 + 8047/15947*i + 25963/47841*j - 234545/47841*k)*$.1 +
        45151/15947 + 6952/47841*i - 15520/47841*j + 44296/47841*k, 1>
]
```

The ring $\mathscr{P} = \mathscr{A}[x]$ is a free module of rank 4 over $\mathbb{Q}[x]$ with basis $\{1, \imath, \jmath, \Bbbk\}$. The coordinates (extracted with the `Coordinates` command) of either of the two factors obtained above provide the four squares we are looking for:

```
> Coordinates(factors[1][1]);
[
    x^3 + 3*x^2 - 107431/47841*x + 45151/15947,
    434/47841*x^2 - 8047/15947*x - 6952/47841,
    -4952/47841*x^2 - 25963/47841*x + 15520/47841,
    -89251/47841*x^2 + 234545/47841*x - 44296/47841
]
```

Consequently, p can be expressed as a sum $p = q_0^2 + q_1^2 + q_2^2 + q_3^2$, where:

$$q_0 = x^3 + 3x^2 - \tfrac{107431}{47841}x + \tfrac{45151}{15947}, \qquad q_1 = \tfrac{434}{47841}x^2 - \tfrac{8047}{15947}x - \tfrac{6952}{47841},$$
$$q_2 = -\tfrac{4952}{47841}x^2 - \tfrac{25963}{47841}x + \tfrac{15520}{47841}, \qquad q_3 = -\tfrac{89251}{47841}x^2 + \tfrac{234545}{47841}x - \tfrac{44296}{47841}.$$

The correctness of this result can be verified directly:

```
> &+ [ q^2 : q in Coordinates(factors[1][1]) ] eq p;
true
```

References

[1] B. Gordon and T. S. Motzkin. On the zeros of polynomials over division rings. *Trans. Amer. Math. Soc.*, 116:218–226, 1965.

[2] P. Koprowski. Factorization and root-finding for polynomials over division quaternion algebras. In *Proceedings of the International Symposium on Symbolic & Algebraic Computation (ISSAC 2023)*, pages 417–424. ACM, New York, [2023] ©2023.

[3] P. Koprowski. Computing resultant of quaternionic polynomials. *ACM Commun. Comput. Algebra*, 58(3):89–92, 2024.

[4] P. Koprowski. Algorithm 1056: q*Poly*—a Magma package for working with quaternionic polynomials. *ACM Trans. Math. Software*, 51(2):Art. 13, 14, 2025.

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

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

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

[8] D. Smertnig. Factorizations of elements in noncommutative rings: a survey. In *Multiplicative ideal theory and factorization theory*, volume 170 of *Springer Proc. Math. Stat.*, pages 353–402. Springer, [Cham], 2016.