The Roots of a Generalized Quaternion

Conference Paper · January 2010

1 author:

Marco Abrate
Politecnico di Torino

THE ROOTS OF A GENERALIZED QUATERNION

ABRATE MARCO

Abstract. Let $\left(\frac{u,v}{\mathbb{F}}\right)$ be a generalized quaternion algebra over an arbitrary field $\mathbb{F}$, that is a four dimensional vector space over $\mathbb{F}$ with the four basis elements $1, i_1, i_2, i_3$ satisfying the following multiplication laws:

$$i_1^2 = u, \quad i_2^2 = v, \quad i_3 = i_1 i_2 = -i_2 i_1,$$

and 1 acting as the unit element.
We first show the existence of a recurring relation on the powers of elements in $\left(\frac{u,v}{\mathbb{F}}\right)$, and then we show how Dickson polynomials of both first and second kind can be used to derive explicit formulas for computing the zeros of the polynomials of the form $P(x) = x^n - q$, where q lies in a generalized quaternion algebra over an arbitrary field $\mathbb{F}$ of characteristic not 2.

1. Introduction

The algebras of generalized quaternions over fields with characteristic not 2 are very important non-commutative algebras. Examples of quaternion algebras are the skew field of Hamilton's quaternions $\mathbb{H}$ or the square 2×2 matrices algebras $M_2(\mathbb{F})$ (cf. [1]).
It is well known that $\left(\frac{u,v}{\mathbb{F}}\right)$ is a four-dimensional associative algebra with central field $\mathbb{F}$.
Consider on $\left(\frac{u,v}{\mathbb{F}}\right)$ the anti-involution which sends a quaternion $x = (x_0, x_1, x_2, x_3)$ to its conjugate $\overline{x} = (x_0, -x_1, -x_2, -x_3)$; we define as usual *trace* and *norm* of a quaternion by

$$Tr(x) = x + \overline{x} \quad \text{ and } \quad N(x) = x\overline{x}.$$

The latter functions lead to a linear recurring relation between powers of generalized quaternions, as shown in the next Theorem:

Theorem 1.1. *Let be $q \in \left(\frac{u,v}{\mathbb{F}}\right)$. If $U_n = U_n(Tr(q), N(q))$ is the $n-$th term of the Fibonacci sequence with parameters $Tr(q)$ and $N(q)$ then the n-th power of $q \in \left(\frac{u,v}{\mathbb{F}}\right)$ is given by:*

$$q^n = qU_n - N(q)U_{n-1}. \tag{1.1}$$

Proof. The powers of a quaternion $q = (a_1, b_1, c_1, d_1)$ are recurring with characteristic polynomial:

$$p(x) = x^2 - Tr(q)x + N(q).$$

Let $q^n = (a_n, b_n, c_n, d_n)$: if $W_n(s, t, h, k)$ is the n-th term of the linear recurring sequence with initial values s and t and characteristic polynomial $x^2 - hx + k$, we set $U_n = W_n(0,1,h,k)$ and $T_n = W_n(1,0,h,k) = -kU_{n-1}$. Then for all $n > 1$:

$$\begin{aligned} a_n &= W_n(1, a_1, Tr(q), N(q)) = T_n + a_1 U_n = -N(q)U_{n-1} + a_1 U_n; \\ b_n &= W_n(0, b_1, Tr(q), N(q)) = b_1 U_n; \\ c_n &= W_n(0, c_1, Tr(q), N(q)) = c_1 U_n; \\ d_n &= W_n(0, d_1, Tr(q), N(q)) = d_1 U_n. \end{aligned}$$

Thus we have $q^n = U_n q - N(q)U_{n-1}$. □

Thanks to Theorem 1.1 we are now able to write a polynomial $P(x) \in \left(\frac{u,v}{\mathbb{F}}\right)[x]$ of the form $P(x) = x^n - q$ in a different way which is easier to study, that is

$$P(x) = x^n - q = U_n x - N(x)U_{n-1} - q.$$

We are concerned with polynomials of the form $P(x) = x^n - q$, where $q \in \left(\frac{u,v}{\mathbb{F}}\right)$ and $n \geq 2$. Our goal is to find the zeros of such polynomials in the algebra $\left(\frac{u,v}{\mathbb{K}}\right) \cong \mathbb{K} \otimes \left(\frac{u,v}{\mathbb{F}}\right)$ obtained by $\left(\frac{u,v}{\mathbb{F}}\right)$ extending components to $\mathbb{K}$, the algebraic closure of $\mathbb{F}$.

There is a Fundamental theorem of algebra for $\mathbb{H}$ (see [2] and [3]) which says that if the polynomial has only one term of highest degree then there exists a root in $\mathbb{H}$. The proof is topological, so it can't be extended to quaternion algebra over finite fields. Furthermore, a closed formula for the roots is unknown for general polynomials.

Gordon and Motzkin [6] considered the problem of constructing polynomials having specified numbers of roots, and proved the existence of a polynomial of degree n with exactly h roots, where $0 \leq h \leq n^4$ for quaternion algebra which are division rings.

Niven [4] and Brand [5] gave closed formulas for the roots of polynomials we are interested in, and more recently De Leo, Ducati and Leonardi [7] presented a matrix approach to find the solutions of more general unilateral polynomials, but all this results are in the special case of real quaternions $\mathbb{H}$.

Before we face the problem of finding roots of $P(x)$ we introduce some polynomials, closely related to Dickson polynomials, that will be helpful for the main results.

Definition 1.2. *Let $P(x) = x^n - q$ be a polynomial in $\left(\frac{u,v}{\mathbb{F}}\right)[x]$ of degree $n \in \mathbb{N}$. Let be*

$$D_k(y,\rho) = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-i} \binom{k-i}{i} (-\rho)^i y^{k-2i}$$

the Dickson polynomial of the first kind of degree k, and let

$$E_k(y,\rho) = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k-i}{i} (-\rho)^i y^{k-2i}$$

be the Dickson polynomials of second kind of degree k. We define polynomials

$$d_{n,q}(y,\rho) = D_n(y,\rho) - Tr(q), \qquad c_{n,q}(y) = y^n - N(q).$$

Theorem 1.3. *Let be $\mathbb{F}' \supseteq \mathbb{F}$ a field, and let $x \in \mathbb{F}' \otimes \left(\frac{u,v}{\mathbb{F}}\right)$ such that $P(x) = 0$. Then*

$$c_{n,q}(N(x)) = 0$$

and

$$d_{n,q}(Tr(x), N(x)) = 0.$$

Proof. The assumption $P(x) = 0$ implies $x^n = q$; hence

$$N(x)^n = N\left(x^n\right) = N(q),$$

that is $N(x)$ is a root of $c_{n,q}(y)$. Moreover, the Lagrange identity applied to $x^k + \overline{x}^k$ yields, for every k, to

$$\begin{aligned} Tr\left(x^k\right) = x^k + \overline{x}^k &= \sum_{i=0}^{\left\lfloor \frac{k}{2} \right\rfloor} (-1)^i \frac{k}{i} \binom{k-i-1}{i-1} x^i \overline{x}^i (x+\overline{x})^{k-2i} = \\ &= \sum_{i=0}^{\left\lfloor \frac{k}{2} \right\rfloor} \frac{k}{k-i} \binom{k-i}{i} \left(-N(x)\right)^i \left(Tr(x)\right)^{k-2i} = \\ &= D_k\left(Tr(x), N(x)\right). \end{aligned}$$

In particular, if $k = n$ it follows that $Tr\left(x^n\right) = Tr(q)$ and

$$D_n\left(Tr(x), N(x)\right) - Tr(q) = 0;$$

thus $Tr(x)$ is a root of $d_{n,q}(y, N(x))$. □

Theorem 1.4. *Let be ν and τ roots of $c_{n,q}(y)$ and $d_{n,q}(y,\nu)$ respectively. If $V_k = V_k(\tau,\nu)$ is the Lucas sequence with parameters τ and ν then for all $n \geq 1$*

$$Tr(q) = V_n.$$

Proof. Let be $r, s \in \mathbb{K}$. We know by [8] that Dickson polynomials of first kind have the property

$$D_k(r,s) = V_k(r,s), \qquad \forall k \in \mathbb{N}.$$

If τ is a root of $d_{n,q}(y,\nu)$ then

$$0 = d_{n,q}(\tau,\nu) = D_n(\tau,\nu) - Tr(q) = V_n(\tau,\nu) - Tr(q).$$

□

2. The Roots of a Generalized Quaternion

In this section we see how the roots of polynomials $c_{n,q}(y)$ and $d_{n,q}(y,\rho)$ of Definition 1.2 can be used to derive explicit formulas for direct computation of all the zeros of $P(x)$.

Theorem 2.1. *Let be ν and τ roots of polynomials $c_{n,q}(y)$ and $d_{n,q}(y,\nu)$ respectively. If the n-th term of the Fibonacci sequence with parameters τ and ν is in $\mathbb{K}^*$ then*

$$x = \left(q + \nu U_{n-1}(\tau,\nu)\right) U_n(\tau,\nu)^{-1} \tag{2.1}$$

is a zero for $P(x)$.

Proof. Let be $x = (q + \nu U_{n-1}(\tau,\nu))\, U_n(\tau,\nu)^{-1}$. Using the properties of Fibonacci and Lucas sequences $U_n = U_n(\tau,\nu)$ and $V_n = V_n(\tau,\nu)$, the trace of x is

$$\begin{aligned} Tr(x) &= U_n^{-1}\left(Tr(q) + 2\nu U_{n-1}\right) = U_n^{-1}\left(V_n + 2\nu U_{n-1}\right) = \\ &= U_n^{-1}\left(V_n + U_n V_1 - U_1 V_n\right) = U_n^{-1}\left(V_n + U_n\tau - V_n\right) = \tau, \end{aligned}$$

and the norm of x is

$$\begin{aligned} N(x) &= U_n^{-2}\left(N(q) + \nu U_{n-1} Tr(q) + \nu^2 U_{n-1}^2\right) = \\ &= U_n^{-2}\left(\nu^n + \nu U_{n-1} V_n + \nu^2 U_{n-2} U_n + \nu^n\right) = \\ &= U_n^{-2}\left(2\nu^n + \nu U_{n-1} U_{n+1} - \nu\tau U_n U_{n-1} + \nu^2 U_{n-2} U_n\right) = \\ &= U_n^{-2}\left(2\nu^n + 2\nu U_{n-1} U_{n+1} - \nu U_n(\tau U_{n-1} - \nu U_{n-2})\right) = \\ &= U_n^{-2}\nu\left(2(\nu^{n-1} + U_{n-1}U_{n+1}) - U_n^2\right) = U_n^{-2}\nu(2U_n^2 - U_n^2) = \nu. \end{aligned}$$

Hence for all $k \in \mathbb{N}$ $U_k\left(Tr(x), N(x)\right) = U_k(\tau,\nu) = U_k$ and

$$x^n = U_n x - \nu U_{n-1} = q + \nu U_{n-1} - \nu U_{n-1} = q.$$

□

Theorem 2.2. *Let be ν a root of $c_{n,q}(y)$ and τ a root of $d_{n,q}(y,\nu)$. If $E_{n-1}(\tau,\nu) \neq 0$ then*

$$x = (q + \nu U_{n-1}(\tau,\nu))\, U_n(\tau,\nu)^{-1}$$

is a zero of $P(x)$.

Proof. This corollary follows immediately from Theorem 2.1, using the fact that for all $k \in \mathbb{N}$ one has $E_{k-1}(\tau,\nu) = U_k(\tau,\nu)$ (cf. [8] for example). □

Theorem 2.3. *Let be $q \in \left(\frac{u,v}{\mathbb{F}}\right)$. If $q \notin \mathbb{F}$ then for all x such that $x^n = q$*

$$U_n = U_n(Tr(x), N(x)) \neq 0.$$

Proof. Suppose that exists x such that $x^n = q$ and $U_n^{(x)} = 0$. Then

$$q = x^n = U_n x - N(x) U_{n-1} = U_{n+1} \in \mathbb{K}.$$

Being $q \in \left(\frac{u,v}{\mathbb{F}}\right)$

$$q \in \mathbb{K} \cap \left(\frac{u,v}{\mathbb{F}}\right) = \mathbb{F},$$

a contradiction. □

Theorem 2.3 says that if $q \notin \mathbb{F}$ then $P(x)$ has at most n^2 distinct roots in $\left(\frac{u,v}{\mathbb{K}}\right)$ given by Equation (2.1).

We now investigate what happens when $q \in \mathbb{F}$. Let $q \in \left(\frac{u,v}{\mathbb{F}}\right)$ be a quaternion, and $d_{n,q}(y,\rho)$ and $E_{n-1}(y,\rho)$ polynomials as in Definition 1.2. Let us introduce the polynomial

$$m(y,\rho) = GCD(d_{n,q}(y,\rho), E_{n-1}(y,\rho)).$$

We have the following Theorem:

Theorem 2.4. *Let be ν a root of $c_{n,q}(y)$. If τ is a zero of $m(y,\nu)$ then every element of the set*

$$\mathbb{S}_{\tau,\nu} = \left\{ x \in \left(\frac{u,v}{\mathbb{K}}\right) | Tr(x) = \tau, N(x) = \nu \right\} \tag{2.2}$$

is a zero of $x^n - q$.

Proof. Since τ is a root of $E_{n-1}(y,\nu)$ then $U_n(\tau,\nu) = 0$. Thus, if $x \in \mathbb{S}_{\tau,\nu}$ and τ is a zero of $d_{n,q}(y,\nu)$ one has

$$x^n = U_n x - \nu U_{n-1} = U_{n+1} = 2^{-1} V_n = q.$$

□

Example 2.5. *Let $\mathbb{F} = \mathbb{F}_{31}$ be the finite field with 31 elements and let $\left(\frac{-1,-1}{\mathbb{F}_{31}}\right)$ be the quaternion algebra over $\mathbb{F}_{31}$. Let us consider the quaternion $q = (23, 17, 27, 24)$ and the equation $x^3 = (23, 17, 27, 24)$. The polynomial $c_{3,(23,17,27,24)}(y)$ has three distinct roots in $\mathbb{F}_{31}$: $\nu_1 = 17, \nu_2 = 22, \nu_3 = 23$. Thus we have three polynomials*

$$d_{3,(23,17,27,24)}(y, 17) = (17 + y)(18 + y)(27 + y),$$
$$d_{3,(23,17,27,24)}(y, 22) = (11 + y)(23 + y)(28 + y),$$
$$d_{3,(23,17,27,24)}(y, 23) = (16 + y)(22 + y)(24 + y).$$

We can now apply Equation (2.1) to nine couples of parameters: $(14, 17)$, $(13, 17)$, $(4, 17)$, $(20, 22)$, $(8, 22)$, $(3, 22)$, $(15, 23)$, $(9, 23)$, $(7, 23)$ getting the solutions of the equation $x^3 = (23, 17, 27, 24)$:

$$\begin{array}{ll} x_{(14,17)} = (7, 2, 5, 1), & x_{(13,17)} = (22, 15, 22, 23), \\ x_{(4,17)} = (2, 14, 4, 7), & x_{(20,22)} = (10, 8, 20, 4), \\ x_{(8,22)} = (4, 10, 25, 5), & x_{(3,22)} = (17, 13, 17, 22), \\ x_{(15,23)} = (23, 3, 23, 17), & x_{(9,23)} = (20, 19, 1, 25), \\ x_{(7,23)} = (19, 9, 7, 20). & \end{array}$$

Example 2.6. *Let us consider the algebra of Hamilton's quaternion $\mathbb{H}$ and the equation $x^4 = -4$. The polynomial $c_{4,-4}(y)$ has four distinct roots: $-2, 2, -2i, 2i$. Then we have the four polynomials*

$$d_{4,-4}(y,-2) = y^4 + 8y^2 + 16,$$
$$d_{4,-4}(y,2) = y^4 - 8y^2 + 16,$$
$$d_{4,-4}(y,-2i) = y^4 + 8iy^2,$$
$$d_{4,-4}(y,2i) = y^4 - 8iy^2.$$

Since $E_3(y,-2) = y^3 + 4y$ and $E_3(y,2) = y^3 - 4y$, we have $m(y,-2) = y^2 + 4$ and $m(y,2) = y^2 - 4$. Thus by Theorem 2.4 we know that the roots of $x^4 + 4 = 0$ having norm -2 are all in the sets $\mathbb{S}_{-2i,-2}$ and $\mathbb{S}_{2i,-2}$, and those having norm 2 are all in the sets $\mathbb{S}_{-2,2}$ and $\mathbb{S}_{2,2}$.
For $\nu = -2i$ we have $m(y,-2i) = y$. Then the root $\tau_1 = 0$ of $d_{4,-4}(y,-2i)$ give the set $\mathbb{S}_{0,-2i}$, while the other two roots namely $\tau_2 = -2 + 2i$ and $\tau_3 = 2 - 2i$ allow to write two distinct roots of $x^4 = -4$ using Equation (2.1):

$$x_{(\tau_1,-2i)} = (-1 + i, 0, 0, 0), \quad x_{(\tau_2,-2i)} = (1 - i, 0, 0, 0).$$

Similarly, for $\nu = 2i$ *we have* $m(y, 2i) = y$. *Then we have* $\tau_4 = 0$ *and we find the set of solutions* $\mathbb{S}_{0,2i}$, *and the two roots* $\tau_5 = -2 - 2i$ *and* $\tau_6 = 2 + 2i$ *allow to write the roots:*

$$x_{(\tau_5, 2i)} = (-1 - i, 0, 0, 0), \quad x_{(\tau_6, 2i)} = (1 + i, 0, 0, 0).$$

References

[1] A. J. Hahn, *Quadratic algebras, Clifford algebras, and arithmetic Witt groups*, Springer - New York, 2002.
[2] S. Eilenberg and I. Niven, *The Fundamental Theorem of Algebra for Quaternions*, Bull AMS, **50** (1944), 246–248.
[3] I. Niven, *Equations in Quaternions*, American Math. Monthly, **48** No. 10 (1941), 654–661.
[4] I. Niven, *The Roots of a Quaternion*, American Math. Monthly **49** No. 6 (1942), 386–388.
[5] L. Brand, *The Roots of a Quaternion*, American Math. Monthly **49** No. 8 (1942), 519–520.
[6] B. Gordon and T. S. Motzkin, *On the Zeros of Polynomials over Division Rings*, Transactions of the American Mathematical Society, Vol. 116. (Apr. 1965), 218–226.
[7] S. De Leo, G. Ducati and V. Leonardi, *Zeros of Unilateral Quaternionic Polynomials*, Electronic Journal of Linear Algebra, **15** (2006), 297–313.
[8] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, Vol. 65, Longman Scientific and Technical, 1993.

AMS Classification Numbers: 11B39, 11E88

Dipartimento di Matematica, Università di Torino, Via C. Alberto 10, 10123 Torino, Italy

E-mail address: marco.abrate@unito.it