Quaternions—An Algebraic View

Note. You likely first encounter the quaternions in Introduction to Modern Algebra. John Fraleigh's *A First Course in Abstract Algebra*, 7th edition (Addison Wesley, 2003), defines the quaternions in Part IV (Rings and Fields), Section 24 (Noncommutative Examples—see pages 224 and 225). However, this is an "optional" section for Introduction to Modern Algebra 1 (MATH 4127/5127). In Modern Algebra 1 (MATH 5410) Thomas Hungerford's *Algebra* (Springer-Verlag, 1974) defines them in his Chapter III (Rings), Section III.1. Rings and Homomorphisms). We now initially follow definitions of Hungerford.

Definition (Hungerford's III.1.1). A *ring* is a nonempty set R together with two binary operations (denoted $+$ and multiplication) such that:

(i) $(R, +)$ is an abelian group.

(ii) $(ab)c = a(bc)$ for all $a, b, c \in R$ (i.e., multiplication is associative).

(iii) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ (left and right distribution of multiplication over $+$).

If in addition,

(iv) $ab = ba$ for all $a, b \in R$,

then R is a *commutative ring*. If R contains an element 1_R such that

(v) $1_R a = a 1_R = a$ for all $a \in R$,

then R is a *ring with identity* (or *unity*).

Note. An obvious "shortcoming" of rings is the possible absence of inverses under multiplication. We adopt the standard notation from $(R, +)$. We denote the $+$ identity as 0 and for $n \in \mathbb{Z}$ and $a \in R$, na denotes the obvious repeated addition.

Definition (Hungerford's III.1.3). A nonzero element a in the ring R is a *left* (respectively, *right*) *zero divisor* if there exists a nonzero $b \in R$ such that $ab = 0$ (respectively, $ba = 0$). A *zero divisor* is an element of R which is both a left and right zero divisor.

Definition (Hungerford's page 117). Let $S = \{1, i, j, k\}$. Let $\mathbb{H}$ be the additive abelian group $\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$ and write the elements of $\mathbb{H}$ as formal sums $(a_0, a_1, a_2, a_3) = a_0 1 + a_1 i + a_2 j + a_3 k$. We often drop the "1" in "$a_0 1$" and replace it with just a_0. Addition in $\mathbb{H}$ is as expected:

$$(a_0+a_1i+a_2j+a_3k)+(b_0+b_1i+b_2j+b_3k) = (a_0+b_0)+(a_1+b_1)i+(a_2+b_2)j+(a_3+b_3)k.$$

We turn $\mathbb{H}$ into a ring by defining multiplication as

$$(a_0 + a_1 i + a_2 j + a_3 k)(b_0 + b_1 i + b_2 j + b_3 k) = (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3)$$

$$+(a_0b_1+a_1b_0+a_2b_3-a_3b_2)i+(a_0b_2+a_2b_0+a_3b_1-a_1b_3)j+(a_0b_3+a_3b_0+a_1b_2-a_2b_1)k.$$

This product can be interpreted by considering:

(i) multiplication in the formal sum is associative,

(ii) $ri = ir$, $rj = jr$, $rk = kr$ for all $r \in \mathbb{R}$,

(iii) $i^2 = j^2 = k^2 = ijk = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

This ring is called the *real quaternions* and is denoted $\mathbb{H}$ in commemoration of Sir William Rowan Hamilton (1805–1865) who discovered them in 1843.

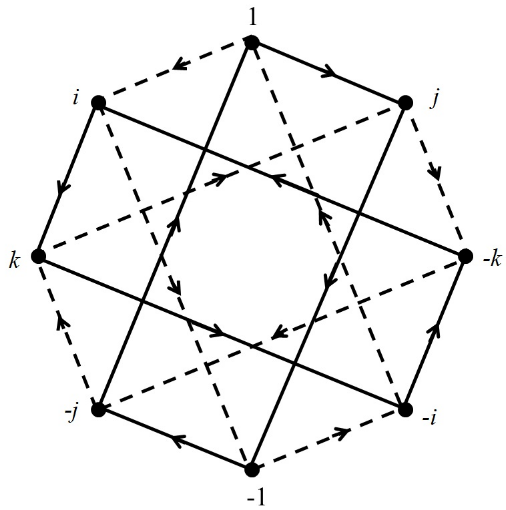
Definition (Hungerford's III.1.5). A commutative ring R with (multiplicative) identity 1_R and no zero divisors is an *integral domain*. A ring D with identity $1_D \neq 0$ in which every nonzero element is a unit is a *division ring*. A *field* is a commutative division ring.

Note. First, it is straightforward to show that $1 = (1, 0, 0, 0)$ is the identity in $\mathbb{H}$. However, since $ij = -ji \neq ji$, then $\mathbb{H}$ is not commutative and so $\mathbb{H}$ is not an integral domain nor a field.

Theorem A. The quaternions form a noncommutative division ring.

Note. Since every nonzero element of $\mathbb{H}$ is a unit, the $\mathbb{H}$ contains no left zero divisors: If $q_1 q_2 = 0$ and $q_1 \neq 0$, then $q_2 = q_1^{-1} 0 = 0$. Similarly, $\mathbb{H}$ has no right zero divisors.

Note. I use the 8-element multiplicative group $\{\pm 1, \pm i, \pm j, \pm k\}$ (called by Hungerford the "quaternion group"; see his Exercise I.2.3) to illustrate Cayley digraphs of groups in Introduction to Modern Algebra (MATH 4127/5127); see my online notes for that class on Section I.7. Generating Sets and Cayley Digraphs. Consider the Cayley digraph given below. This is the Cayley digraph for a multiplicative group of order 8, denoted Q_8. The dotted arrow represents multiplication on the right by i and the solid arrow represents multiplication on the right by j. The problem is to use this diagram to create a multiplication table for Q_8.



Solution. For multiplication on the right by i we have: $1 \cdot i = i$, $i \cdot i = -1$, $-1 \cdot i = -i$, $-i \cdot i = 1$, $j \cdot i = -k$, $-k \cdot i = -j$, $-j \cdot i = k$, and $k \cdot i = j$. For multiplication on the right by j we have: $1 \cdot j = j$, $j \cdot j = -1$, $-1 \cdot j = -j$, $-j \cdot j = 1$, $i \cdot j = k$, $k \cdot j = -i$, $-i \cdot j = -k$, and $-k \cdot j = i$. This gives us 16 of the entries in the multiplication table for Q_8. Since 1 is the identity, we get another 15 entries. All entries can be found from this information. For example, $k \cdot k = k \cdot (i \cdot j) = (k \cdot i) \cdot j = (j) \cdot j = -1$. The multiplication table is:

$\cdot$	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

This group is addressed in Hungerford in Exercises I.2.3, I.4.14, and III.1.9(a). Notice that each of i, j, and k are square roots of -1. So the quaternions are, in a sense, a generalization of the complex numbers $\mathbb{C}$. The Galois group $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\alpha)$, where $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$, is isomorphic to Q_8 (see page 584 of D. Dummit and R. Foote's *Abstract Algebra*, 3rd edition, John Wiley and Sons (2004)).

Note. The quaternions may also be interpreted as a subring of the ring of all 2×2 matrices over $\mathbb{C}$. This is Exercise III.1.8 of Hungerford (see page 120): "Let R be the set of all 2×2 matrices over the complex field $\mathbb{C}$ of the form $\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}$, where $\overline{z}, \overline{w}$ are the complex conjugates of a and w, respectively. Prove that R is a division ring and that R is isomorphic to the division ring of real quaternions." In fact, the quaternion group, Q_8, can be thought of as the group of order 8 generated by $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, under matrix multiplication (see Hungerford's Exercise I.2.3).

Note. In fact, the complex numbers can be similarly represented as the field of all 2×2 matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ where $a, b \in \mathbb{R}$ (see Exercise I.3.33 of Fraleigh).

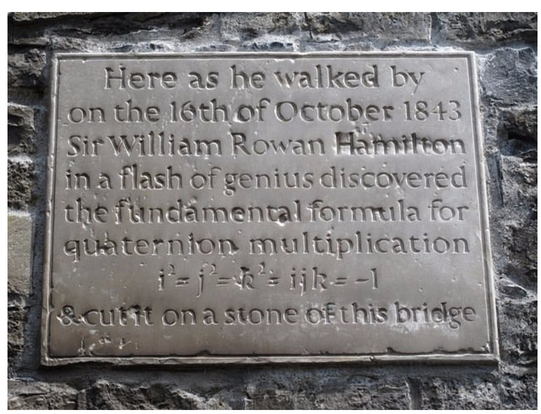
Note. The complex numbers can be defined as ordered pairs of real numbers, $\mathbb{C} = \{(a,b) \mid a,b \in \mathbb{R}\}$, with addition defined as $(a,b) = (c,d) = (a+c, b+d)$ and multiplication defined as $(a,b)(c,d) = (ac - bd, bc + ad)$. We then have that $\mathbb{C}$ is a field with additive identity $(0,0)$ and multiplicative identity $(1,0)$. The additive inverse of (a,b) is $(-a,-b)$ and the multiplicative inverse of $(a,b) \neq (0,0)$ is $(a/(a^2+b^2), -b/(a^2+b^2))$. We commonly denote (a,b) as "$a+ib$" so that $i = (0,1)$ and we notice that $i^2 = -1$. In fact, this is the definition of the complex field in our graduate level Complex Analysis 1 (MATH 5510); see my online notes for that class on Section I.2. The Field of Complex Numbers. The complex numbers are visualized as the "complex plane" where $a + ib \in \mathbb{C}$ is associated with $(a,b) \in \mathbb{R}^2$. During the early decades of the 19th century, the complex numbers became an accepted part of mathematics (in large part due to the development of complex function theory by Augustin Cauchy). Since the complex numbers have an interpretation as a sort of "two dimensional" number system, a natural question to ask is: "Is there a three (or higher) dimensional number system?"

Note. Sir William Rowan Hamilton (1805–1865) spent the years 1835 to 1843 trying to develop a three dimensional number system based on triples of real numbers. He never succeeded. However, he did succeed in developing a four dimensional number system, now called the quaternions and denoted "$\mathbb{H}$" in his honor. In a letter he wrote late in his life to his son Archibald Henry, Hamilton tells the story of his discovery:

"Every morning in the early part of [October 1843], on my coming down to breakfast, your little brother, William Edwin, and yourself, used to ask me, 'Well, papa, can you multiply triplets?' Whereto I was always obliged to reply, with a sad shake of the head: 'No, I can only add and subtract them.' But on the 16th day of that some month... An electric circuit seemed to close; and a spark flashed forth the herald (as I foresaw immediately) of many long years to come of definitely directed through and work by myself, is spared, and, at all events, on the part of others if I should even be allowed to live long enough distinctly to communicate the discovery. Nor could I resist the impulse—unphilosophical as it may have been—to cut with a knife on a stone of Brougham Bridge [in Dublin, Ireland; now called "Broom Bridge"], as we passed it, the fundamental formula with the symbols i, j, k:

$$i^2 = j^2 = k^2 = ijk = -1$$

which contains the Solution of the Problem, but, of course, the inscription has long wince mouldered away."



Images from the MacTutor biography webpage for Hamilton and the Tripadvisor website (both accessed 1/5/2024)

So the exact date of the birth of the quaternions is October 16, 1843. [This note is based on *Unknown Quantity: A Real and Imaginary History of Algebra* by John Derbyshire, John Henry Press (2006).]

Note. You are probably familiar with the Factor Theorem which relates roots of a polynomial to linear factor of the polynomial. You might not recall that it requires commutivity, though:

The Factor Theorem. (Hungerford's Theorem III.6.6). Let R be a commutative ring with identity and $f \in R[x]$. Then $c \in R$ is a root of f if and only if $x - c$ divides f.

Note. The Factor Theorem is used to prove the following, which might remind you of the Fundamental Theorem of Algebra:

Hungerford's Theorem III.6.7. If D is an integral domain contained in an integral domain E and $f \in D[x]$ has degree n, then f has at most n distinct roots in E.

So in an integral domain, an n degree polynomial at most n roots. Surprisingly in a division ring, this can be violated.

Note. It is easy to see that the polynomial $q^2 + 1 \in \mathbb{H}[q]$ has more than two roots. Along with $\pm i$ are the roots $\pm j$ and $\pm k$. In fact, the polynomial has an *infinite* number of roots in $\mathbb{H}$! Let $x_1, x_2, x_3 \in \mathbb{R}$ with $x_1^2 + x_2^2 + x_3^2 = 1$. Then

$$\begin{aligned}
(x_1 i + x_2 j + x_3 k)^2 &= x_1^2 i^2 + x_1 x_2 ij + x_1 x_3 ik + x_2 x_1 ji + x_2^2 j^2 + x_2 x_3 jk \\
&\quad + x_3 x_1 ki + x_3 x_2 kj + x_3^2 k^2 \text{ by the definition of multiplication} \\
&= -x_1^2 - x_2^2 - x_3^2 \text{ since } ij = -ji, ik = -ki, jk = -kj \\
&= -1 \text{ since } x_1^2 + x_2^2 + x_3^2 = 1.
\end{aligned}$$

Note. We now turn our attention to polynomials in $\mathbb{H}[x]$. We are particularly interested in roots of such polynomials, a version of the Factor Theorem, and the concept of algebraic closure. Much of this material is of fairly recent origins. The remainder of the supplement is mostly based on the following references:

1. T. Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics #131, Springer-Verlag (1991).

2. G. Gentili and D. C. Struppa, A New Theory of Regular Functions of a Quaternionic Variable, *Advances in Mathematics* **216** (2007), 279–301.

Definition. We denote by $\mathbb{S}$ the two dimensional sphere (as a subset of the four dimensional quaternions $\mathbb{H}$) $\mathbb{S} = \{q = x_1 i + x_2 j + x_3 k \mid x_1^2 + x_2^2 + x_3^2 = 1\}$. As observed above, for any $I \in \mathbb{S}$ we have $I^2 = -1$. For $x, y \in \mathbb{R}$ we let $x + y\mathbb{S}$ denote the two dimensional sphere $x + y\mathbb{S} = \{x + yI \mid I \in \mathbb{S}\}$. (We might think of $x + y\mathbb{S}$ as a two dimensional sphere centered at $(x, 0, 0, 0)$ with radius $|y|$.)

Note. We take q as the indeterminate in the ring of polynomials $\mathbb{H}[q]$. Since $\mathbb{H}$ is not commutative, we are faced with the case that a monomial of the form $aq^n \in \mathbb{H}[q]$ is the same as monomial $a_1qa_1qa_2q\cdots qa_n \in \mathbb{H}[q]$ where $a = a_0a_1\cdots a_n$, but if we evaluate aq^n at some element of $\mathbb{H}$, we may get a different value than if we evaluate $a_qqa_1q\cdots qa_n$ at the same element of $\mathbb{H}$. That is, evaluation of an element of $\mathbb{H}[q]$ at $r \in \mathbb{H}$ is not a homomorphism (recall that Fraleigh deals with the evaluation homomorphism for field theory in Theorem 22.4). In the remainder of this supplement, we consider polynomials with the powers of the indeterminate on the left and the coefficients on the right: $p(q) = \sum_{i=0}^n q^i a_i$. We will call p a "quaternionic polynomial."

Definition. For two quaternionic polynomials $p_1(q) = \sum_{i=0}^n q^i a_i$ and $p_2(q) = \sum_{i=0}^m q^i b_i$ in $\mathbb{H}[q]$, define the product

$$(p_1p_2)(q) = \sum_{i=0,1,\ldots,n;j=0,1,\ldots,m} q^{i+j} a_i b_j.$$

Note. We now explore roots of quaternionic polynomials. The following result is originally due to A. Pogorui and M. V. Shapiro (in "On the Structure of the Set of Zeros of Quaternionic Polynomials," *Complex Variables* **49**(6) (2004), 379–389) but we present an easier proof due to Gentili and Struppa in 2007.

Theorem B. Let $p(q) = \sum_{n=0}^N q^n a_n$ be a given quaternionic polynomial. Suppose that there exist $x_0, y_0 \in \mathbb{R}$ and $I, J \in \mathbb{S}$ with $I \neq J$ such that $p(x_0 + y_0 I) = 0$ and $p(x_0 + y_0 J) = 0$. Then for all $L \in \mathbb{S}$ we have $p(x_0 + y_0 L) = 0$.

Note. In fact, Gentili and Struppa develop a theory of analytic functions of a quaternionic variable and show that the previous result holds for an analytic function.

Note. In a ring of polynomials, $R[t]$, each element of R commutes with indeterminate t (see Hungerford's Theorem III.5.2(ii)). So in $R[t]$ we have that $f(r) = \sum_{i=0}^n a_i t^i = \sum_{i=0}^n t^i a_i$. However, for $r \in R$ where R is not commutative we likely have $\sum_{i=0}^n a_i r^i \neq \sum_{i=0}^n r^i a_i$. So in order to evaluate $f(r)$, we must decide on a standard representation of $f(t)$. In this supplement, we use the form $f(t) = \sum_{i=0}^n t^i a_i \in R[t]$. Additionally, we may have $f(t) = g(t)h(t)$ in $R[t]$, but we may not have $f(r) = g(r)h(r)$. Consider $g(t) = t-a$ and $h(t) = t-b$ where $a, b \in R$ do not commute (so $ab \neq ba$). Then we have by the definition of multiplication that $f(t) = g(t)h(t) = (t-a)(t-b) = t^2 - t(a+b) + ab$. But

$$f(a) = a^2 - a(a+b) + ab = ab - ba \neq 0 = g(a)h(a).$$

(This "sneaky" behavior results from the term at being expressed as ta in the representation of $g(t)h(t)$.)

Definition 16.1 of Lam. Let R be a ring and $f(t) = \sum_{i=0}^n t^i a_i \in R[t]$. An element $r \in R$ is a *left root* of f if $f(r) = \sum_{i=0}^n r^i a_i = 0$. If $g(t) = \sum_{i=0}^n a_i t^i \in R[t]$. An element $r \in R$ is a *right root* of g if $g(r) = \sum_{i=0}^n a_i r^i = 0$.

Proposition 16.2 of Lam. (The Factor Theorem in a Ring with Unity). An element $r \in R$ is a left (right) root of a nonzero polynomial $f(t) = \sum_{i=0}^n t^i a_i \in R[t]$ if and only if $t - r$ is a left (right) divisor of $f(t)$ in $R[t]$.

Note. Recall a *right ideal* of a ring R is a subring I of R such that for all $r \in R$ and $x \in I$ we have $xr \in I$ (Hungerford's Definition III.2.1). We see from the Factor Theorem in a Ring with Unity that the set of polynomials in $R[t]$ having r as a left root is precisely the right ideal $(t-r)R[t] = \{(t-r)g(t) \mid g(t) \in R[t]\}$.

Proposition 16.3 of Lam. Let D be a division ring and let $f(t) = h(t)g(t)$ in $D[t]$. Let $d \in D$ be such that $a = h(d) \neq 0$. Then $f(d) = h(d)g(a^{-1}da)$. In particular, if d is a left root of f but not of h then the conjugate of d, $a^{-1}da$, is a left root of g.

Note. A result similar to Proposition 16.3 holds for right roots.

Note. If D is an integral domain and $p \in D[x]$ is of degree n, then p has at most n roots in D (see Hungerford's Theorem III.6.7, mentioned above). This is not the case in a division ring as illustrated by $p(q) = q^2 + 1 \in \mathbb{H}[q]$, as described above. The following result is analogous to Hungerford's Theorem III.6.7, but for division rings. It does not imply at most n roots, but roots from at most n conjugacy classes.

Note. Quaternion a is a *conjugate* of quaternion b (in the algebraic sense) if $a = cbc^{-1}$ for some quaternion c. Notice that if $a = c_1b_1c_1^{-1}$ and $a = c_2b_2c_2^{-1}$, then $b_1 = c_1^{-1}ac_1$ so that $b_1 = c_1^{-1}(c_2b_2c_2^{-1})c_1 = (c_1^{-1}c_2)b_2(c_1^{-1}c_2)^{-1}$. So conjugation is an equivalence relation and the conjugacy classes partition $\mathbb{H}$.

Theorem 16.4 of Lam. **(Gordon-Motzkin Theorem.)** Let D be a division ring and let f be a polynomial of degree n in $D[t]$. Then the left (right) roots of f lie in at most n conjugacy classes of D. If $f(t) = (t - a_1)(t - a_2) \cdots (t - a_n)$ where $a_1, a_2, \ldots, a_n \in D$, then any left (right) root of f is conjugate to some a_i.

Definition. For $q = a + bi + cj + dk \in \mathbb{H}$, we define the *quaternionic conjugate* $\overline{q} = a - bi - cj - dk$.

Note. For $q = a + bi + cj + dk \in \mathbb{H}$, we have

$$\begin{aligned} q\overline{q} &= (a + bi + cj + dk)(a + (-b)i + (-c)j + (-d)k) \\ &= ((a)(a) - (b)(-b) - (c)(-c) - (d)(-d)) \\ &\quad +((a)(-b) + (b)(a) + (c)(-d) - (d)(-c))i \\ &\quad +((a)(-c) + (c)(a) + (d)(-b) - (b)(-d))j \\ &\quad +((a)(-d) + (d)(a) + (b)(-c) - (c)(-b))k \\ &= a^2 + b^2 + c^2 + d^2. \end{aligned}$$

We define the *modulus* of $a \in \mathbb{H}$ as $\sqrt{q\overline{q}}$.

Lemma A. For $q_1, q_2 \in \mathbb{H}$ we have $\overline{q_1 q_2} = \overline{q_2}\,\overline{q_1}$.

Note. Recall that a field is algebraically closed if every nonconstant polynomial over the field has a root in the field. This is the motivation for the following definition.

Definition (Lam, page 169). A division ring D is left (right) algebraically closed if every nonconstant polynomial in $D[t]$ has a left (right) root in D.

Note. By Proposition 16.2, if $f \in D[t]$ for left or right algebraically closed division ring D, then f can by factored into a product of linear factors in $D[t]$ (that is, f splits in $D[t]$).

Note. The following is the Fundamental Theorem of Algebra for Quaternions. The result originally appeared in I. Nivens' "Equations in Quaternions," *American Mathematical Monthly*, **48** (1941), 654–661.

Theorem 16.14 of Lam. ("Niven-Jacobson" in Lam) Fundamental Theorem of Algebra for Quaternions. The quaternions, $\mathbb{H}$, are left (and right) algebraically closed.

Note. Now that we have our Fundamental Theorem of Algebra, we conclude with a brief exploration of the structure of the set of quaternions for which a polynomial has a left (right) root. The following result is from A. Pogorui and M. Shapiro's "On the Structure of the Set of Zeros of Quaternionic Polynomials," *Complex Variables: Theory and Applications* **49**(6) (2004), 379–389.

Theorem (Pogorui and Shapiro). For f a (nonzero) polynomial in $\mathbb{H}[q]$. The set of left (right) roots of f consists of isolated points or isolated two dimensional spheres of the form $S = x + y\mathbb{S}$ for $x, y \in \mathbb{R}$. The number of isolated roots plus twice the number of isolated spheres is less than or equal to n.

Note. We would hope that the "less than or equal to n" of Pogorui and Shapiro's theorem could simply be replaced with "equal to n." The punch-line is that we cannot have "the number... equal to the degree n," but with a well thought-out definition of multiplicity, we can get the multiplicities of the roots to sum to the degree. This is explored in another supplement to these notes on Quaternions—The Degree of a Polynomial versus the Number of Zeros.

Revised and Updated: 1/11/2024