Polynomial Functions and the Quaternions

Serge Ballif
ballif@math.psu.edu

The Pennsylvania State University

January 18, 2008

Outline

Rings

Definition

A ring R is a set together with two binary operations "$+$" and "$\times$" such that the following three properties hold.

1. $(R, +)$ form an additive group.
2. Multiplication is associative (i.e. $(ab)c = a(bc)$ for all $a, b, c \in R$).
3. The left and right distributive laws hold:

$$a(b + c) = ab + ac \quad \text{and} \quad (a + b)c = ac + bc.$$

Convention

For the purposes of this talk, we will assume that all rings have an identity element 1 such that $1r = r$ for all $r \in R$.

Examples of Rings

Example

The following rings are familiar to all mathematicians.

- $\mathbb{R}$ — the real numbers
- $\mathbb{C}$ — the complex numbers
- $\mathbb{Z}$ — the integers
- $\mathrm{Mat}_n(\mathbb{R})$ — the ring of $n \times n$ real-valued matrices

Division Rings

Definition

A ring R is a division ring iff every nonzero element of R has a two-sided inverse element iff $(R - \{0\}, \times)$ is a group.

Remark

A field is a commutative division ring.

Example

- $\mathbb{R}$ and $\mathbb{C}$ are division rings.
- $\mathbb{Z}$ and $\mathrm{Mat}_n(\mathbb{R})$ are not division rings.

The Real Quaternions

Definition

The ring of real quaternions $\mathbb{H}$ is a 4-dimensional real vector space with basis $\{1, i, j, k\}$. $\mathbb{H}$ is a division ring with multiplication structure determined by the relations

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

An element q of $\mathbb{H}$ is of the form

$$q = a + bi + cj + dk,$$

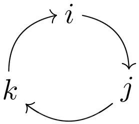
where $a, b, c, d \in \mathbb{R}$. The real part of q is a, and the purely imaginary part of q is $bi + cj + dk$.

Quaternion Multiplication

Remark

Multiplication of quaternions is not commutative. We have $ij = k$, but $ji = -k$.

Mnemonic



Practice

Multiply the following quaternions:

$$(1 + 2i + 3j + 4k)(4 + 3i + 2j + k)$$

Polynomials

Definition

For any ring R, we let $R[\mathrm{x}]$ denote the polynomial ring with indeterminate x and coefficients from the ring R.

Remark

Each polynomial $f(\mathrm{x}) \in R[\mathrm{x}]$ is of the form

$$f(\mathrm{x}) = \sum_{i=0}^{n} a_i \mathrm{x}^i.$$

Since the indeterminate x commutes with the coefficients, we also have

$$f(\mathrm{x}) = \sum_{i=0}^{n} \mathrm{x}^i a_i.$$

Right Evaluation

Definition

Let $f(\mathrm{x}) = \sum_{i=0}^{n} a_i \mathrm{x}^i \in R[\mathrm{x}]$. For each element $r \in R$, we define (right) evaluation of f at r to be the map $R[\mathrm{x}] \to R$ that maps $f(\mathrm{x})$ to

$$f(r) := \sum_{i=0}^{n} a_i r^i.$$

An element r is a (right) root of $f(\mathrm{x})$ if $f(r) = 0$.

Factoring Does Not Preserve Evaluation

Caution

If R is noncommutative, then evaluation is not a ring homomorphism. That is,

$$f(\mathrm{x}) = g(\mathrm{x})h(\mathrm{x}) \quad \text{does not imply} \quad f(r) = g(r)h(r).$$

Example

Consider

$$f(\mathrm{x}) = (\mathrm{x} - i)(\mathrm{x} - j) \in \mathbb{H}[\mathrm{x}].$$

We might expect i and j to be roots of $f(\mathrm{x})$. However, we note that $f(\mathrm{x}) = \mathrm{x}^2 - (i + j)\mathrm{x} + k$, so $f(i) = i^2 - (i + j)i + k = -1 - i^2 - ij + k = 2k \neq 0$ and $f(j) = j^2 - (i + j)j + k = -1 - ij - j^2 + k = 0$. Hence, j is a right root of $f(\mathrm{x})$, but i is not.

Remainder Theorem

Theorem (Commutative Case)

Let R be a commutative ring. An element $r \in R$ is a root of a nonzero polynomial $f(\mathrm{x}) \in R[\mathrm{x}]$ iff $f(\mathrm{x}) = g(\mathrm{x})(\mathrm{x} - r)$ for some polynomial $g(\mathrm{x}) \in R[\mathrm{x}]$.

Theorem (Noncommutative Case)

Let R be a noncommutative ring. An element $r \in R$ is a right root of a nonzero polynomial $f(\mathrm{x}) \in R[\mathrm{x}]$ iff ...

Remainder Theorem

Theorem (Commutative Case)

Let R be a commutative ring. An element $r \in R$ is a root of a nonzero polynomial $f(\mathrm{x}) \in R[\mathrm{x}]$ iff $f(\mathrm{x}) = g(\mathrm{x})(\mathrm{x} - r)$ for some polynomial $g(\mathrm{x}) \in R[\mathrm{x}]$.

Theorem (Noncommutative Case)

Let R be a noncommutative ring. An element $r \in R$ is a right root of a nonzero polynomial $f(\mathrm{x}) \in R[\mathrm{x}]$ iff $f(\mathrm{x}) = g(\mathrm{x})(\mathrm{x} - r)$ for some polynomial $g(\mathrm{x}) \in R[\mathrm{x}]$.

Proof of Remainder Theorem

Proof.

($\Leftarrow$) Let

$$f(\mathrm{x}) = \left(\sum_{i=0}^{n} a_i \mathrm{x}^i\right)(\mathrm{x} - r) = \sum_{i=0}^{n} a_i \mathrm{x}^{i+1} - \sum_{i=0}^{n} a_i r \mathrm{x}^i.$$

Then

$$f(r) = \sum_{i=0}^{n} a_i (r)^{i+1} - \sum_{i=0}^{n} a_i r (r)^i = 0,$$

so r is a root of $f(\mathrm{x})$.

($\Rightarrow$) Suppose that $f(r) = 0$. Then by the division algorithm (on the right), we can write

$$f(\mathrm{x}) = g(\mathrm{x})(\mathrm{x} - r) + s$$

for some $g(\mathrm{x}) \in R[\mathrm{x}]$ and some $s \in R$. The first part shows that r is a root of $g(\mathrm{x})(\mathrm{x} - r)$. Thus $f(r) = s = 0$. □

Factor Theorem

Theorem (Commutative Case)

Let D be a field, and let $f(\mathrm{x}) = g(\mathrm{x})h(\mathrm{x})$. An element $d \in D$ is a root of $f(\mathrm{x})$ iff d is a root of either $g(\mathrm{x})$ or $h(\mathrm{x})$.

Theorem (Noncommutative Case)

Let D be a division ring, and let $f(\mathrm{x}) = g(\mathrm{x})h(\mathrm{x})$. An element $d \in D$ is a root of $f(\mathrm{x})$ iff . . .

Factor Theorem

Theorem (Commutative Case)

Let D be a field, and let $f(\mathrm{x}) = g(\mathrm{x})h(\mathrm{x})$. An element $d \in D$ is a root of $f(\mathrm{x})$ iff d is a root of either $g(\mathrm{x})$ or $h(\mathrm{x})$.

Theorem (Noncommutative Case)

Let D be a division ring, and let $f(\mathrm{x}) = g(\mathrm{x})h(\mathrm{x})$. An element $d \in D$ is a root of $f(\mathrm{x})$ iff one of the following holds.

1. *d is a root of $h(\mathrm{x})$, or*
2. *a conjugate of d is root of $g(\mathrm{x})$.*

Proof of Factor Theorem

Proof.

Let $g(\mathrm{x}) = \sum_{i=0}^{n} b_i \mathrm{x}^i$. Then

$$f(\mathrm{x}) = \left(\sum_{i=0}^{n} b_i \mathrm{x}^i\right) h(\mathrm{x}) = \sum_{i=0}^{n} b_i h(\mathrm{x})\mathrm{x}^i.$$

If $h(d) = 0$, then $f(d) = 0$. Suppose that $h(d) = a \neq 0$ and $f(d) = 0$. Then

$$\begin{aligned} f(d) &= \sum_{i=0}^{n} b_i h(d) d^i \\ &= \sum_{i=0}^{n} b_i a d^i a^{-1} a \\ &= \sum_{i=0}^{n} b_i \left(ada^{-1}\right)^i a \\ &= g(ada^{-1}) h(d). \end{aligned}$$

Since $f(d) = 0$, but $h(d) \neq 0$, we must have $g(ada^{-1}) = 0$. □

The Number of Roots

Theorem (Commutative Case)

Let D be a field. A polynomial in $D[\mathrm{x}]$ of degree n has at most n distinct roots in D.

Theorem (Noncommutative Case,)

Let D be a division ring. A polynomial in $D[\mathrm{x}]$ of degree n has at most . . .

The Number of Roots

Theorem (Commutative Case)

Let D be a field. A polynomial in $D[\mathrm{x}]$ of degree n has at most n distinct roots in D.

Theorem (Noncommutative Case, Gordon, Motzkin, 1965)

Let D be a division ring. A polynomial in $D[\mathrm{x}]$ of degree n has at most ∞ roots. However, these roots will come from at most n distinct conjugacy classes of D.

A Familiar Polynomial

Example

In the division ring $\mathbb{H}$ of real quaternions, i, j, and k are each roots of second degree polynomial

$$\mathrm{x}^2 + 1.$$

In fact, each of the infinitely many conjugates of i is a root of $\mathrm{x}^2 + 1$.

Proof of Roots in at Most n Conjugacy Classes

Proof.

1. We prove by induction. The case $n = 1$ is immediately true.
2. For $n \geq 2$, let c be a root of $f(\mathrm{x})$. Then $f(\mathrm{x}) = g(\mathrm{x})(\mathrm{x} - c)$.
3. Suppose that $d \neq c$ is another root of $f(\mathrm{x})$. Then a conjugate of d is a root of $g(\mathrm{x})$.
4. By the induction hypothesis, d lies in at most one of the (at most) $n - 1$ conjugacy classes of roots of $g(\mathrm{x})$.

□

Algebraically Closed Division Rings

Definition

A division ring is said to be right algebraically closed if every nonconstant polynomial has a right root.

Theorem (Niven, Jacobson, 1941)

The real quaternions $\mathbb{H}$ *are right (and left) algebraically closed.*

Quaternionic Conjugates

Definition

The quaternionic conjugate of $q = a + bi + cj + dk$ is $\bar{q} = a - bi - cj - dk$.

Definition

The conjugate polynomial of a polynomial

$$f(\mathrm{x}) = \sum_{i=0}^{n} q_i \mathrm{x}^i \quad \text{is} \quad \bar{f}(\mathrm{x}) = \sum_{i=0}^{n} \bar{q}_i \mathrm{x}^i.$$

Useful Facts

For $p, q \in \mathbb{H}$, $\overline{pq} = \bar{q}\bar{p}$. Similarly, for $f(\mathrm{x}), g(\mathrm{x}) \in \mathbb{H}[\mathrm{x}]$, $\overline{fg} = \bar{g}\bar{f}$. Also, $q\bar{q} \in \mathbb{R}$, while $f\bar{f} \in \mathbb{R}[\mathrm{x}]$.

Proof of "Fundamental Theorem"

Sketch of Proof.

Let $f(\mathrm{x}) = \sum_{i=0}^{n} q_i \mathrm{x}^i$.

1. $\bar{f}f \in \mathbb{R}[\mathrm{x}]$ must have a root a in $\mathbb{C}$.
2. Either a is a root of f, or a conjugate b of a is a root of $\bar{f}$.
3. Note that $\sum_{i=0}^{n} \bar{q}_i b^i = 0 \Rightarrow \sum_{i=0}^{n} q_i \bar{b}^i = 0$, so $\bar{b}$ is a left root of $f(\mathrm{x})$.
4. Thus, $f(\mathrm{x}) = (\mathrm{x} - \bar{b})g(\mathrm{x})$ for some $g(\mathrm{x}) \in D[\mathrm{x}]$.
5. Note that $\deg g < \deg f$, so by induction on the degree of f, $g(\mathrm{x})$ has a right root.
6. Therefore, f has a right root. □