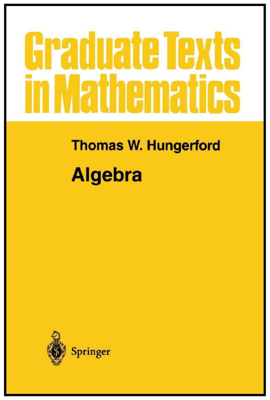
Modern Algebra

Supplement. Quaternions—An Algebraic View



Theorem A

Theorem A. The quaternions form a noncommutative division ring.

Proof. Tedious computations confirm that multiplication is associative and the distribution law holds. We now show that every nonzero element of $\mathbb{H}$ has a multiplicative inverse. Consider $q = a_0 + a_1 i + a_2 j + a_3 k$. Define $d = a_0^2 + a_1^2 + a_2^2 + a_3^2 \neq 0$. Notice that

$$\begin{aligned}
(a_0 + a_1 i + a_2 j + a_3 k)&((a_0/d) - (a_1/d)i - (a_2/d)j - (a_3/d)k) \\
&= (a_0(a_0/d) - a_1(-a_1/d) - a_2(-a_2/d) - a_3(-a_3/d)) \\
&+ (a_0(-a_1/d) + a_1(a_0/d) + a_2(-a_3/d) - a_3(-a_2/d))i \\
&+ (a_0(-a_2/d) + a_2(a_0/d) + a_3(-a_1/d) - a_1(-a_3/d))j \\
&+ (a_0(-a_3/d) + a_3(a_0/d) + a_1(-a_2/d) - a_2(-a_1/d))k \\
&= (a_0^2 + a_1^2 + a_2^2 + a_3^2)/d = 1.
\end{aligned}$$

So $(a_0 + a_1 i + a_2 j + a_3 k)^{-1} = (a_0/d) - (a_1/d)i - (a_2/d)j - (a_3/d)k$ where $d = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Therefore every nonzero element of $\mathbb{H}$ is a unit and so the quaternions form a noncommutative division ring. □

Theorem B

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 $p(x_0 + y_0 L) = 0$.

Proof. For any $n \in \mathbb{N}$ and any $L \in \mathbb{S}$ we have that $(x_0 + y_0 L)^n = \sum_{i=0}^n \binom{n}{i} x_0^{n-i} y_0^i L^i = \alpha_n + L\beta_n$ by the Binomial Theorem for a ring with identity (since $x_0 y_0 L = L x_0 y_0$ because $x_0, y_0 \in \mathbb{R}$; see Theorem III.1.6 of Hungerford) where

$$\alpha_n = \sum_{i \equiv 0 \pmod 4} \binom{n}{i} x_0^{n-i} y_0^i - \sum_{i \equiv 2 \pmod 4} \binom{n}{i} x_0^{n-i} y_0^i$$

and

$$\beta_n = \sum_{i \equiv 1 \pmod 4} \binom{n}{i} x_0^{n-i} y_0^i - \sum_{i \equiv 3 \pmod 4} \binom{n}{i} x_0^{n-i} y_0^i$$

Theorem B (continued 1)

Proof (continued). ...because $L^{0 \pmod 4} = 1$, $L^{1 \pmod 4} = L$, $L^{2 \pmod 4} = -1$, and $L^{3 \pmod 4} = -L$. We therefore have

$$0 = 0 - 0 = \sum_{n=0}^N (\alpha_n + I\beta_n) a_n - \sum_{n=0}^N (\alpha_n + J\beta_n) a_n$$

$$= \sum_{n=0}^N ((\alpha_n + I\beta_n) - (\alpha_n + J\beta_n)) a_n = \sum_{n=0}^N (I - J)\beta_n a_n = (I - J)\sum_{n=0}^N \beta_n a_n.$$

By hypothesis, $I - J \neq 0$ so (since $\mathbb{H}$ has no zero divisors) $\sum_{n=0}^N \beta_n a_n = 0$ and so

$$0 = p(x_0 + y_0 I) = \sum_{n=0}^N (x_0 + y_0 I)^n a_n = \sum_{n=0}^N (\alpha_n + I\beta_n) a_n$$

$$= \sum_{n=0}^N \alpha_n a_n + I \sum_{n=0}^N \beta_n a_n = \sum_{n=0}^N \alpha_n a_n.$$

Theorem B (continued 2)

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 $p(x_0 + y_0 L) = 0$.

Proof (continued). Now for any $L \in \mathbb{S}$ we have that

$$p(x_0 + y_0 L) = \sum_{n=0}^{N} (x_0 + y_0 L)^n a_n = \sum_{n=0}^{N} (\alpha_n + L\beta_n) a_n$$

$$= \sum_{n=0}^{N} \alpha_n a_n + L \sum_{n=0}^{N} \beta_n a_n = 0 + 0 = 0.$$

□

Proposition 16.2 of Lam

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 $R[t]$.

Proof. We give a proof for left roots and divisors with the proof for right being similar. First, if

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

then

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

Proposition 16.2 of Lam (continued)

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 $R[t]$.

Proof. Second, suppose $f(r) = \sum_{i=0}^{n} r^i a_i = 0$. By the Remainder Theorem (Hungerford's Corollary III.6.3 which is stated for $x - r$ on the right, but the result also holds for $x - r$ on the left; this result holds in rings with unity) there is a unique $g(t) \in R[t]$ such that

$$f(t) = (t - r) g(t) + f(r) = (t - r) g(t) + 0 = (t - r) g(t).$$

So $t - r$ is a left divisor of $f(t)$. □

Proposition 16.3 of Lam

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.

Proof. Let $g(t) = \sum_{i=0}^{n} t^i b_i$. Then $f(t) = h(t)g(t) = \sum_{i=0}^{n} t^i h(t) b_i$ and so

$$f(d) = \sum_{i=0}^{n} d^i h(d) b_i = \sum_{i=0}^{n} d^i a b_i = \sum_{i=0}^{n} a a^{-1} d^i a b_i$$

$$= \sum_{i=0}^{m} a (a^{-1} d a)^i b_i = a g(a^{-1} d a) = h(d) g(a^{-1} d a).$$

If d is a left root of f but not a left root of h then, since D has no zero divisors, $a^{-1}da$ must be a left root of g. □

Proposition 16.4 of Lam

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.

Proof. We prove this using induction. In the base case, $n = 1$ and so f has exactly one left root and so the left roots lie in $n = 1$ conjugacy class. Now suppose that if a polynomial is of degree $n - 1$, then its left roots lie in at most $n - 1$ conjugacy classes. Let f be degree n and let c be a left root of f. Then by Proposition 16.2, $f(t) = (t - c)g(t)$ where g is of degree $n - 1$. Suppose $d \neq c$ is any other left root of f. Then by Proposition 16.3, d is a conjugate to a left root of $g(t)$ (in particular, $(d-c)^{-1}d(d-c) = r$ is a left root of g so $d = (d-c)r(d-c)^{-1}$).

Proposition 16.4 of Lam (continued)

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.

Proof (continued). Since by the induction hypothesis the left roots of g lie in at most $n - 1$ conjugacy classes, then this arbitrary left root of f (arbitrary except that is is not c) must lie in one of these $n - 1$ conjugacy classes. Adding in the conjugacy class containing c, we have that the left roots of f lie in at most n conjugacy classes. The result now follows in general by induction.

The proof of the second claim follows similarly by induction. The result for right roots is similar. □

Lemma A

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

Proof. Let $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ and $q_2 = a_2 + b_2 i + c_2 j + d_2 k$. Then

$$\begin{aligned}
\overline{q_1 q_2} &= \overline{(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k)} \\
&= \overline{(a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i} \\
&\quad \overline{+ (a_1 c_2 + c_1 a_2 + d_1 b_2 - b_1 d_2) j + (a_1 d_2 + d_1 a_2 + b_1 c_2 - c_1 b_2) k} \\
&= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) - (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i \\
&\quad - (a_1 c_2 + c_1 a_2 + d_1 b_2 - b_1 d_2) j - (a_1 d_2 + d_1 a_2 + b_1 c_2 - c_1 b_2) k \\
&= ((a_2)(a_1) - (-b_2)(-b_1) - (-c_2)(-c_1) - (-d_2)(-d_1)) \\
&\quad + ((-b_2)(a_1) + (-b_1)(a_2) - (-d_2)(-c_1) + (-c_2)(-d_1) i \\
&\quad + ((-c_2)(a_1) + (a_2)(-c_1) - (-b_2) - d_1) + (-d_2)(-b_1)) j \\
&\quad + ((-d_2)(a_1) + (a_2)(-d_1) - (-c_2)(-b_1) + (-b_2)(-c_1)) k
\end{aligned}$$

Lemma A (continued)

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

Proof (continued). ...

$$\begin{aligned}
\overline{q_1 q_2} &= ((a_2)(a_1) - (-b_2)(-b_1) - (-c_2)(-c_1) - (-d_2)(-d_1)) \\
&\quad + ((-b_2)(a_1) + (-b_1)(a_2) - (-d_2)(-c_1) + (-c_2)(-d_1) i \\
&\quad + ((-c_2)(a_1) + (a_2)(-c_1) - (-b_2) - d_1) + (-d_2)(-b_1)) j \\
&\quad + ((-d_2)(a_1) + (a_2)(-d_1) - (-c_2)(-b_1) + (-b_2)(-c_1)) k \\
&= ((a_2)(a_1) - (-b_2)(-b_1) - (-c_2)(-c_1) - (-d_2)(-d_1)) \\
&\quad + ((a_2)(-b_1) + (-b_2)(a_1) + (-c_2)(-d_1) - (-d_2)(-c_1)) i \\
&\quad + ((a_2)(-c_1) + (-c_2)(a_1) + (-d_2)(-b_1) - (-b_2)(-d_1)) j \\
&\quad + ((a_2)(-d_1) + (-d_2)(a_1) + (-b_2)(-c_1) - (c_1)(-b_1)) k \\
&= (a_2 + (-b_2) i + (-c_2) j + (-d_2) k)(a_1 + (-b_1) i \\
&\quad + (-c_1) j + (-d_1) k) \\
&= \overline{q_2}\,\overline{q_1}.
\end{aligned}$$

□

Theorem 16.14 of Lam

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.

Proof. For $f(q) = \sum_{r=0}^n g^r a_r \in \mathbb{H}[q]$, define $\overline{f}(q) = \sum_{r=0}^n r^r \overline{qa_r} \in \mathbb{H}[q]$. For $f, g \in \mathbb{H}[q]$ with $f(q) = \sum_{i=0}^n q^i a_i$ and $g(q) = \sum_{j=0}^m q^j b_j$ we have

$$\begin{aligned}
\overline{fg} &= \overline{\left(\sum_{i=0}^n q^i a_i\right)\left(\sum_{j=0}^m q^j b_i\right)} \\
&= \overline{\left(\sum_{i=0,1,\ldots,n;j=0,1,\ldots,m} q^{i+j} a_i b_j\right)} \\
&= \sum_{i=0,1,\ldots,n;j=0,1,\ldots,m} q^{i+j}\overline{a_i b_j}
\end{aligned}$$

Theorem 16.14 of Lam (continued 1)

Proof (continued). . . .

$$\begin{aligned}
\overline{fg} &= \sum_{i=0,1,\ldots,n;j=0,1,\ldots,m} q^{i+j}\overline{a_i b_j} \\
&= \sum_{i=0,1,\ldots,n;j=0,1,\ldots,m} q^{i+j}\overline{b_j}\,\overline{a_i} \text{ by Lemma A} \\
&= \left(\sum_{j=0}^m q^j \overline{b_j}\right)\left(\sum_{i=0}^n q^i \overline{a_i}\right) \\
&= \overline{g}\,\overline{f}.
\end{aligned}$$

So, in particular, $\overline{f\overline{f}} = \overline{\overline{f}}\,\overline{f} = f\overline{f}$, and so $f\overline{f}$ equals its own quaternionic conjugate. Therefore the coefficients of $f\overline{f}$ must be real and $f\overline{f} \in \mathbb{R}[q]$ for all $f \in \mathbb{H}[q]$.

Theorem 16.14 of Lam (continued 2)

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

Proof (continued). We now use mathematical induction on $n = \deg(f)$ to prove that f has a left root in $\mathbb{H}$. For $n = 1$, f clearly has a left root. Suppose $n \geq 2$ and that every polynomial of degree less than n has a left root in $\mathbb{H}$. Since $\mathbb{R}(i) = \mathbb{C} \subset \mathbb{H}$ is algebraically closed and $f\overline{f} \in \mathbb{R}[q]$ then $f\overline{f}$ has a root α in $\mathbb{R}(i) = \mathbb{C}$. By Proposition 16.3, either α is a left root or f or a conjugate β of α is a left root of $\overline{f}$. In the former case we are done. In the latter case, if $f(q) = \sum_{r=0}^n q^r a_r$ then $\overline{f}(q) = \sum_{n=0}^n q^r \overline{a_r}$ and so $\overline{f}(\beta) = \sum_{r=0}^n \beta^r \overline{a_r} = 0$ or $\sum_{r=0}^n a_r \overline{\beta}^r = 0$. That is, $\overline{\beta}$ is a right root of $f(q)$. By Theorem 16.2 (applied to a right roots) we can write $f(q) = (q - \overline{\beta})g(q)$ where $g(q) \in \mathbb{H}$ has degree $n-1$. By the induction hypothesis, $g(q)$ has a left root $\gamma \in \mathbb{H}$. But then γ is also a left root of $f(q)$ and the general result now follows by induction. The result for right algebraic closure is similar. □