QUATERNION ALGEBRAS: SET 1

KEITH CONRAD

Matrices

1. Let R be a ring with identity, possibly *noncommutative*. Check the 2×2 matrices over R, denoted $\mathrm{M}_2(R)$, form a ring with identity $I_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ using the usual addition and multiplication rules. In the case of multiplication, entries from the left matrix always come first. That is, the matrix product is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

2. When R is *commutative*, the trace, determinant, and transpose of a matrix in $\mathrm{M}_2(R)$ are defined by

$$\mathrm{Tr}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a + d, \quad \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\top} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Check, for all $A, B \in \mathrm{M}_2(R)$, that the trace satisfies

$$\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B), \quad \mathrm{Tr}(AB) = \mathrm{Tr}(BA),$$

the determinant satisfies

$$\det(AB) = \det(A)\det(B),$$

and the transpose satisfies

$$(A^{\top})^{\top} = A, \quad (A + B)^{\top} = A^{\top} + B^{\top}, \quad (AB)^{\top} = B^{\top}A^{\top}, \quad \mathrm{Tr}(A^{\top}) = \mathrm{Tr}(A), \quad \det(A^{\top}) = \det(A).$$

Also, verify that A is a root of the quadratic polynomial $T^2 - (\mathrm{Tr}A)T + \det A \in R[T]$. That is, $A^2 - (\mathrm{Tr}A)A + (\det A)I_2 = O$.

3. When R is commutative, show $\mathrm{M}_2(\mathrm{M}_2(R))$ is isomorphic as a ring to $\mathrm{M}_4(R)$ by "erasing the borders."

4. Determine which parts of the previous two exercises remain true when R is noncommutative (*e.g.*, $R = \mathbf{H}$ or $R = \mathrm{M}_2(\mathbf{R})$).

5. Let R be a commutative ring. For $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(R)$, show $A \in \mathrm{M}_2(R)^{\times} \iff \det A \in R^{\times}$, in which case $A^{-1} = \left(\begin{smallmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{smallmatrix}\right)$, where $\Delta = \det A$. Also check, for any $A, B \in \mathrm{M}_2(R)$ with B invertible, that BAB^{-1} has the same trace and determinant as A. (A matrix of the form BAB^{-1} is called a *conjugate* of A, which is not to be confused with the use of this term in the sense of complex or quaternionic conjugate on $\mathbf{C}$ and $\mathbf{H}$.)

6. Let $A \in \mathrm{M}_2(\mathbf{Q})$. If $A \in \mathrm{M}_2(\mathbf{Z})$, its trace and determinant are in $\mathbf{Z}$, but not conversely, *e.g.*, $\left(\begin{smallmatrix} 0 & 2/3 \\ 0 & 0 \end{smallmatrix}\right)$. By exercise 5, any matrix in $\mathrm{M}_2(\mathbf{Q})$ which is conjugate to a matrix in $\mathrm{M}_2(\mathbf{Z})$ has integral trace and determinant. Is $\left(\begin{smallmatrix} 0 & 2/3 \\ 0 & 0 \end{smallmatrix}\right)$ conjugate to a matrix in $\mathrm{M}_2(\mathbf{Z})$?

7. (Inverting quaternionic matrices)

a) In $\mathrm{M}_2(\mathbf{H})$, show the three matrices $\left(\begin{smallmatrix} i & j \\ j & k \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} i & j \\ j & i \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} i & i \\ -j & j \end{smallmatrix}\right)$ are all invertible (that is, each has a 2-sided multiplicative inverse) by computing the inverse. Notice that the second matrix has determinant $i^2 - j^2 = 0$, yet it is invertible.

b) Pick any $q_1, q_2 \in \mathbf{H}$ such that $q_1q_2 \neq q_2q_1$. Show the matrix $\left(\begin{smallmatrix} 1 & q_1 \\ q_2 & q_1q_2 \end{smallmatrix}\right)$ is invertible (with determinant 0) but its transpose $\left(\begin{smallmatrix} 1 & q_2 \\ q_1 & q_1q_2 \end{smallmatrix}\right)$ is not invertible (with non-zero determinant).

8. (Homomorphisms) This exercise gives a common property of $\mathbf{H}$ and $\mathrm{M}_2(\mathbf{R})$: any ring homomorphism from either of these rings to a non-zero ring is injective.

a) Let D be a division ring and let R be any non-zero ring (with identity). Show any ring homomorphism $f\colon D \to R$ is injective. (By definition, ring homomorphisms preserve the multiplicative identity.)

b) Let F be a field and let R be any non-zero ring (with identity). Show any ring homomorphism $f\colon \mathrm{M}_2(F) \to R$ is injective. (Hint: If $f(M) = 0$, also $f(AMB) = 0$ for any $A, B \in \mathrm{M}_2(F)$. When $M \neq O$, choose A and B suitably to conclude $f(I_2) = 0$, a contradiction.)

Quaternions

9. Check all the multiplicative rules for i, j, k in $\mathbf{H}$ follow from $i^2 = -1, j^2 = -1, k = ij = -ji$, and associativity.

10. Verify properties of quaternionic conjugation: $\overline{\overline{q}} = q, \overline{q_1 + q_2} = \overline{q}_1 + \overline{q}_2$, $\overline{q_1 q_2} = \overline{q}_2 \overline{q}_1$, $\overline{cq} = c\overline{q}$ for $c \in \mathbf{R}$, and $\overline{q} = q \Leftrightarrow q \in \mathbf{R}$.

11. For $q \in \mathbf{H}$, its trace and norm are $\mathrm{Tr}(q) = q + \overline{q}$ and $\mathrm{N}(q) = q\overline{q}$.

a) Show every $q \in \mathbf{H}$ is a root of the quadratic polynomial $T^2 - (\mathrm{Tr} q)T + \mathrm{N}(q) \in \mathbf{R}[T]$. Thus $\mathbf{R}[q] = \mathbf{R} + \mathbf{R}q$ for $q \notin \mathbf{R}$.

b) Call $q \in \mathbf{H}$ *integral* if $\mathrm{Tr}(q) \in \mathbf{Z}$ and $\mathrm{N}(q) \in \mathbf{Z}$. (For example, every quaternion with integer coordinates is integral.) Let $q_1 = 1/2 + i/6 + j/6 + 5k/6$ and $q_2 = k$. Show q_1 is integral, but $q_1 + q_2$ and $q_1 q_2$ are not integral. Is q_1 conjugate to a quaternion with integral coordinates? (That is, does $q q_1 q^{-1}$ have integral coordinates for some nonzero q?)

12. (Matrix embeddings)

a) Show the maps $\mathbf{C} \to \mathrm{M}_2(\mathbf{R})$ given by $a + bi \mapsto \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ and $\mathbf{H} \to \mathrm{M}_2(\mathbf{C})$ given by $z + wj \mapsto \left(\begin{smallmatrix} z & -w \\ \overline{w} & \overline{z} \end{smallmatrix}\right)$ are injective ring homomorphisms.

b) What operations on $\mathrm{M}_2(\mathbf{R})$ correspond to conjugation and norm on the subring $\mathbf{C}$? Similarly for $\mathrm{M}_2(\mathbf{C})$ and the subring $\mathbf{H}$.

c) Following the pattern in part a, can you say anything worthwhile about the set of quaternionic matrices $\left(\begin{smallmatrix} q_1 & -q_2 \\ \overline{q}_2 & \overline{q}_1 \end{smallmatrix}\right)$ in $\mathrm{M}_2(\mathbf{H})$?

13. Verify that the images of $\mathbf{C}$ in $\mathrm{M}_2(\mathbf{R})$ and $\mathbf{H}$ in $\mathrm{M}_2(\mathbf{C})$ from the previous exercise can be described as follows: $\mathbf{C} = \{A \in \mathrm{M}_2(\mathbf{R}) : \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)A = A\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\}$ and $\mathbf{H} = \{A \in \mathrm{M}_2(\mathbf{C}) : \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)A = \overline{A}\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\}$, where $\overline{A}$ is the matrix with complex conjugate entries to A.

14. View $\mathrm{M}_n(\mathbf{C}) \subset \mathrm{M}_{2n}(\mathbf{R})$ and $\mathrm{M}_n(\mathbf{H}) \subset \mathrm{M}_{2n}(\mathbf{C})$ in the "obvious" way using the embeddings from exercise 12. Is the generalization of the previous exercise for $\mathrm{M}_n(\mathbf{C})$ and $\mathrm{M}_n(\mathbf{H})$ true if $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is replaced by the $2n \times 2n$ matrix $\left(\begin{smallmatrix} O & -I_n \\ I_n & O \end{smallmatrix}\right)$?

15. For $q \in \mathbf{H}^\times$, let $R_q\colon \mathbf{H} \to \mathbf{H}$ by $R_q(r) = qrq^{-1}$.

a) Show R_q is a ring homomorphism.

b) Show $R_{q_1} \circ R_{q_2} = R_{q_1 q_2}$. Would this be true if we used the function $r \mapsto q^{-1}rq$ instead? Does $R_{q_1 + q_2} = R_{q_1} + R_{q_2}$?

c) For $q, q' \in \mathbf{H}^\times$, show $R_q(r) = R_{q'}(r)$ for all $r \in \mathbf{H}$ if and only if $q = cq'$ for some $c \in \mathbf{R}$. Is this conclusion still true if we only know $R_q(r) = R_{q'}(r)$ for all pure quaternions r?

d) For any $f(T) \in \mathbf{R}[T]$ and $r \in \mathbf{H}$, show $f(r) = 0 \Rightarrow f(R_q(r)) = 0$.

16. As in lecture, let $\mathbf{H}^0 = \mathbf{R}i + \mathbf{R}j + \mathbf{R}k$.

a) Show $\mathbf{H}^0 = \{q \in \mathbf{H} : q^2 \leq 0\}$, and use this to give another proof that $R_q(\mathbf{H}^0) \subset \mathbf{H}^0$ when $q \in \mathbf{H}^\times$.

b) For $q \in \mathbf{H}$, show $q^2 = -1$ if and only if $q = bi + cj + dk$ with $b^2 + c^2 + d^2 = 1$. That is, the roots of $T^2 + 1$ in $\mathbf{H}$ form a sphere of pure quaternions.

c) Writing $\mathbf{H}^0 = \{q \in \mathbf{H} : \mathrm{Tr}(q) = 0\}$ suggests the analogue of pure quaternions in $\mathrm{M}_2(\mathbf{R})$ is $\{A \in \mathrm{M}_2(\mathbf{R}) : \mathrm{Tr}(A) = 0\}$. As with pure quaternions, is it true that the square of a "pure matrix" is a scalar (matrix)? In $\mathbf{H}$, $q^2 \in \mathbf{R} \Leftrightarrow q \in \mathbf{R}$ or $q \in \mathbf{H}^0$. Is the analogous statement true in $\mathrm{M}_2(\mathbf{R})$?

17. Let $q = 1 + 2k$. View $R_q \colon \mathbf{H}^0 \to \mathbf{H}^0$ as a map from $\mathbf{R}^3$ to $\mathbf{R}^3$ by the identification

$$x_1 i + x_2 j + x_3 k \longleftrightarrow \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

Compute $R_q(\mathbf{v})$ when $\mathbf{v}$ is either of the vectors

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

18. In $\mathbf{C}[T]$, $T^2 + 1 = (T + i)(T - i)$. Viewing $\mathbf{C}[T]$ inside $\mathbf{H}[T]$, this polynomial identity is not true when we substitute $T = j$. What does this mean?

19. Identify $\mathbf{H}^0$ with $\mathbf{R}^3$ in the usual way, as in exercise 17.

a) Show multiplication of *pure* quaternions can be described in terms of the dot product and cross product on $\mathbf{R}^3$: $q_1, q_2 \in \mathbf{H}^0 \Longrightarrow q_1 q_2 = -(\mathbf{q}_1 \cdot \mathbf{q}_2) + \mathbf{q}_1 \times \mathbf{q}_2$, where we write bold $\mathbf{q}$ for the vector in $\mathbf{R}^3$ corresponding to the pure quaternion q in $\mathbf{H}^0$. In particular, observe that $\mathbf{q}_1$ and $\mathbf{q}_2$ are perpendicular if and only if q_1 and q_2 anti-commute (that is, $q_1 q_2 = -q_2 q_1$).

b) What are the constraints on the coordinates of $x_1 i + x_2 j + x_3 k$ in order for it to anti-commute with $i + j$?

c) For $q_1, q_2, q_3 \in \mathbf{H}^0$, show

$$\mathbf{q}_1 \times (\mathbf{q}_2 \times \mathbf{q}_3) = \frac{1}{2}(q_1 q_2 q_3 - q_2 q_3 q_1).$$

20. When Hamilton was looking for a multiplication on $\mathbf{R}^3$, he wanted a product, call it $\odot$, which preserves length: $|\mathbf{v}_1||\mathbf{v}_2| = |\mathbf{v}_1 \odot \mathbf{v}_2|$ for $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{R}^3$. Squaring both sides, this amounts to seeking a multiplication rule for sums of three squares: can products of sums of three squares be given again as a sum of three squares by a polynomial expression in the original coordinates, say with integer coefficients? What about with real coefficients? This would generalize the two-square identity $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$, where the coefficients are ± 1.

21. Write $\mathbf{C} = \mathbf{R} + \mathbf{R}\sqrt{-1}$. Show $\mathbf{H}(\mathbf{C}) \cong \mathrm{M}_2(\mathbf{C})$ if we identify $1 \leftrightarrow \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $i \leftrightarrow \left(\begin{smallmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{smallmatrix}\right)$, $j \leftrightarrow \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and $k \leftrightarrow \left(\begin{smallmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{smallmatrix}\right)$.

22. (The quaternionic exponential function) For $q \in \mathbf{H}$, set $e^q = \sum_{n \geq 0} q^n/n!$.

a) Write $q = a + bq_0$, where $a, b \in \mathbf{R}$ and q_0 is pure of length 1. Show $e^q = e^a e^{bq_0}$.

b) With the notation as in part a, show $e^{bq_0} = \cos b + (\sin b)q_0$. In particular, e^{bq_0} has length 1, so $|e^q| = e^a$.

c) For $q, q' \in \mathbf{H}$, does $e^q e^{q'} = e^{q+q'}$ if and only if $qq' = q'q$?

Linear Algebra

23. In $\mathbf{R}^n$, let $\mathbf{v}_1$ and $\mathbf{v}_2$ be linearly independent. For $a, b, c, d \in \mathbf{R}$, show $a\mathbf{v}_1 + b\mathbf{v}_2$ and $c\mathbf{v}_1 + d\mathbf{v}_2$ are linearly independent if and only if the determinant $\left|\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right| = ad - bc$ is non-zero.

24. Prove there is no way to make $\mathbf{R}^3$ into a field such that the usual scalar multiplication $c\mathbf{v}$ ($c \in \mathbf{R}$, $\mathbf{v} \in \mathbf{R}^3$) equals $(ce) \odot \mathbf{v}$, where e is the identity for the hypothetical multiplication $\odot$ in the field. (Hint: Pick any $\mathbf{w} \neq \mathbf{0}$ in $\mathbf{R}^3$, and let $T_\mathbf{w} \colon \mathbf{R}^3 \to \mathbf{R}^3$ by $T_\mathbf{w}(\mathbf{v}) = \mathbf{w} \odot \mathbf{v}$. Show $T_\mathbf{w}$ is $\mathbf{R}$-linear, so it can be represented by a 3×3 matrix. This matrix has an eigenvalue in $\mathbf{R}$, say λ. Conclude $\mathbf{w} = \lambda e$ if $\mathbf{R}^3$ is a field. Therefore every $\mathbf{w} \in \mathbf{R}^3$ is a scalar multiple of e, which is a contradiction.)