QUATERNION ALGEBRAS: SET 2

KEITH CONRAD

Any F

1. Verify the multiplication table for u, v, w in $(a, b)_F$.

2. Verify that the map $(a, b)_F \to \mathrm{M}_2(F[t]_{t^2-a})$ given by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad u \mapsto \begin{pmatrix} t & 0 \\ 0 & -t \end{pmatrix}, \quad v \mapsto \begin{pmatrix} 0 & -1 \\ -b & 0 \end{pmatrix}, \quad w \mapsto \begin{pmatrix} 0 & -t \\ bt & 0 \end{pmatrix}$$

is an injective F-algebra homomorphism. (It is not onto.)

3. For $a \in F^\times$, let $E_a = F[t]_{t^2-a}$ (This is $F[\sqrt{a}]$ when a is not a square in F, but E_a even makes sense when a is a square in F, although in that case E_a is not a field.) Define the conjugate of $x + yt \in E_a$ to be $x - yt$ and the norm to be the product of an element with its conjugate: $\mathrm{N}(x + yt) = x^2 - ay^2 \in F$.

a) Check $\mathrm{N}\colon E_a \to F$ is multiplicative.

b) When a is a square in $F^\times$, show $\mathrm{N}(E_a^\times)$ equals $F^\times$ if $\mathrm{char}\, F \neq 2$ and ${F^\times}^2$ if $\mathrm{char}\, F = 2$. (Hint when $\mathrm{char}\, F \neq 2$: for $c, c' \in F$, notice that $(c+c')^2 - (c-c')^2 = 4cc'$, so any product can be written as a difference of squares.)

4. (Comparing scalars and non-scalars)

a) Show the center of a division ring is a field.

b) Let D be a division ring, with center F. If F doesn't have characteristic 2, show no element of $F^\times$ has the form x^2 and y^2 for $x \in F$ and $y \in D - F$. For instance, -1 is the only element of order 2 in $D^\times$. (This is false in the ring $\mathrm{M}_2(F)$, where $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and $-I_2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ all have order 2.)

c) Let D be a division ring, with center F. If F has characteristic 2, show no element of F has the form $x^2 + x$ and $y^2 + y$ for x in F and y in $D - F$. Give a counterexample in the ring $\mathrm{M}_2(F)$.

5. Let D be a division ring, with center F. Assume D is finite-dimensional over F. For every $d \in D^\times$, prove $d^{-1} \in F[d]$. (Hint: Look at the map $x \mapsto dx$ on $F[d]$.)

For remaining exercises, $\mathrm{char}\, F \neq 2$ and $B = (a, b)_F = F + Fu + Fv + Fw$

6. Show the center of B is F.

7. Show the set of elements of B which anti-commute with u is $Fv + Fw$, and the elements of B which anti-commute with u and square to b are those $xv + yw$ $(x, y \in F)$ such that $x^2 - ay^2 = 1$.

8. (Conjugation, trace, norm)

a) Check properties of conjugation on B: $\overline{\overline{q}} = q$, $\overline{q_1 + q_2} = \overline{q}_1 + \overline{q}_2$, $\overline{q_1 q_2} = \overline{q}_2 \overline{q}_1$, $\overline{cq} = c\overline{q}$ for $c \in F$, and $\overline{q} = q \Leftrightarrow q \in F$.

b) The trace and norm on B are defined, as in lecture, by $\mathrm{Tr}(q) = q + \overline{q}$ and $\mathrm{N}(q) = q\overline{q}$. Show q is a root of $T^2 - (\mathrm{Tr}q)T + \mathrm{N}(q) \in F[T]$, so $F[q] = F + Fq$ when $q \notin F$.

c) Show $\mathrm{Tr}(q) = \mathrm{N}(q + 1) - \mathrm{N}(q) - 1$, and more generally $\mathrm{Tr}(q_1\overline{q}_2) = \mathrm{N}(q_1 + q_2) - \mathrm{N}(q_1) - \mathrm{N}(q_2)$.

d) Show $\mathrm{Tr}(q^2) = (\mathrm{Tr}q)^2 - 2\mathrm{N}(q)$ for every $q \in B$.

e) When $q \in B - F$, show $T^2 - (\mathrm{Tr}q)T + \mathrm{N}(q)$ is the unique monic quadratic in $F[T]$ with q as a root. Conclude that under any isomorphism $\varphi\colon B \to B'$ of quaternion algebras over F, q and $\varphi(q)$ have the same trace and norm. In particular, if $B \cong \mathrm{M}_2(F)$, then any such isomorphism carries the trace on B to the trace on $\mathrm{M}_2(F)$ and the norm on B to the determinant on $\mathrm{M}_2(F)$.

f) For $q = x_0 + x_1u + x_2v + x_3w$, $\mathrm{N}(q) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$. This is a quadratic form. Another quadratic form on B is the function $\frac{1}{2}\mathrm{Tr}(q^2)$. Write this out explicitly in terms of the coordinates x_i of q and compare it with $\mathrm{N}(q)$.

9. For all q, q' in B, check qq' and $q'q$ have the same scalar part. (What is its formula?) Thus $qq' - q'q$ is pure, *i.e.*, $\mathrm{Tr}(qq') = \mathrm{Tr}(q'q)$. Give a second proof that qq' and $q'q$ have the same trace by using part c of the previous exercise and the fact that $\mathrm{N}(\overline{q}) = \mathrm{N}(q)$.

10. For $q \in B$ with $q \notin F$, show $\{r \in B : rq = qr\} = F[q]$. When B is a division ring and $q, q' \in B^\times$, show $qrq^{-1} = q'rq'^{-1}$ for all $r \in B$ if and only if $q' \in qF[r]$.

11. If $e_1, e_2 \in B$ satisfy the conditions $e_1^2 \in F^\times, e_2^2 \in F^\times$, $e_1e_2 = -e_2e_1$, and e_1^2 and e_2^2 are not in ${F^\times}^2$, show $\{1, e_1, e_2, e_1e_2\}$ is a linearly independent set. Remember, F has characteristic $\neq 2$. (Hint: If $c_0 + c_1e_1 + c_2e_2 + c_3e_1e_2 = 0$ where $c_i \in F$, write this as $(c_0 + c_1e_1) + (c_2 + c_3e_1)e_2 = 0$ and multiply on the left by $c_2 - c_3e_1$. Note $c_2^2 - c_3^2e_1^2 \neq 0$ unless $c_2 = c_3 = 0$, since $e_1^2 \notin {F^\times}^2$.)

12. Under the isomorphism $(1, b)_F \cong \mathrm{M}_2(F)$ determined by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad u \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad v \mapsto \begin{pmatrix} 0 & -1 \\ -b & 0 \end{pmatrix}, \quad w \mapsto \begin{pmatrix} 0 & -1 \\ b & 0 \end{pmatrix}$$

what quaternion in $(1, b)_F$ corresponds to the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$?

13. Under the isomorphism $(1, 1)_F \cong \mathrm{M}_2(F)$ as in the previous exercise (with $a = 1$), let the quaternion $c_0+c_1u+c_2v+c_3w$ correspond to the matrix $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. Write $\alpha, \beta, \gamma, \delta$ in terms of c_0, c_1, c_2, c_3 and vice versa. Check that, under this isomorphism, the norm corresponds to the determinant, the trace corresponds to the trace, but conjugation does *not* correspond to the transpose. What operation on matrices does conjugation correspond to?

14. When $a \neq -b$ in $F^\times$, check $\{1, u+v, w, (u+v)w\}$ is a quaternionic basis of $(a, b)_F$. Therefore $(a, b)_F \cong (a + b, -ab)$. For example, $(2, 3)_{\mathbf{Q}} \cong (5, -6)_{\mathbf{Q}}$.

15. We saw during the lecture that for $a, b \in F^\times$,

$$b = x^2 - ay^2 \text{ for some } x, y \in F \Longrightarrow (a, b)_F \cong \mathrm{M}_2(F)$$

by passing from the basis $\{1, u, v, w\}$ to the basis $\{1, u, xv + yw, u(xv + yw)\}$. What is wrong with the following alternate proof?

If $x = 0$, then $y \neq 0$ and $(a, b)_F = (a, -ay^2)_F \cong (a, -a)_F \cong \mathrm{M}_2(F)$.

If $x \neq 0$, then $(yu + v)^2 = x^2$ and the set $\{1, u, yu + v, u(yu + v)\}$ is a basis of $(a, b)_F$, so $(a, b)_F \cong (a, x^2)_F \cong \mathrm{M}_2(F)$.

16. We saw in lecture that for $a, b \in F^\times$,

$$(a, b)_F \cong \mathrm{M}_2(F) \Longleftrightarrow b = x^2 - ay^2 \text{ for some } x, y \in F.$$

The left side looks symmetric in a and b since $(a, b)_F \cong (b, a)_F$. The right side does not appear to be symmetric in a and b. Show the right side can be written in the following more symmetric form:

$$ax^2 + by^2 = 1 \text{ for some } x, y \in F.$$

17. When $\mathbf{F}$ is a finite field with odd characteristic, show no quaternion algebra over $\mathbf{F}$ is a division ring. (This is a special instance of Wedderburn's theorem.)

18. Suppose -1 is a sum of three squares in F: $-1 = x^2 + y^2 + z^2$ for some $x, y, z \in F$. Then $\mathrm{N}(1 + xi + yj + zk) = 0$, so the ring $\mathbf{H}(F) = (-1, -1)_F$ is not a division ring and therefore $\mathbf{H}(F) \cong \mathrm{M}_2(F)$.

We know an isomorphism $(-1, -1)_F \cong \mathrm{M}_2(F)$ implies -1 is a sum of two squares in F. Thus, if -1 is a sum of three squares in a field (of characteristic $\neq 2$) then it is already a sum of two squares in the field. Can you prove this without using quaternion algebras?

19. When B has an element of norm 0, it is not a division ring, so it is isomorphic to $\mathrm{M}_2(F)$. Prove $(a, -a)_F$, for $a \neq 0$, and $(a, 1-a)_F$, for $a \neq 0, 1$, are isomorphic to $\mathrm{M}_2(F)$ by finding specific non-zero elements with norm 0.

20. When $q \in B^\times$, let $R_q(r) = qrq^{-1}$ for $r \in B$. Show that when r is pure, so is $R_q(r)$. Repeat in this setting exercise 15 on the previous set.

21. (Generalized dot and cross products)

In exercise 19 of the previous set, you saw multiplication on $\mathbf{H}^0$ is related to the dot product and cross product on $\mathbf{R}^3$: two quaternions in $\mathbf{H}^0$ have a product in $\mathbf{H}^0$ if and only if their dot product is 0 (that is, they are perpendicular), in which case their product as quaternions equals their cross product as vectors. For any quaternion algebra $B = (a, b)_F$, describe a dot product and cross product on F^3 which is related to multiplication in B^0. (Formulas for these new products will depend on a and b.)

Quaternion algebras over $\mathbf{Q}$

22. Suppose $a, b \in \mathbf{R}^\times$ are not both negative. Show $(a, b)_{\mathbf{Q}}$ becomes a subring of $\mathrm{M}_2(\mathbf{R})$ by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad u \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \quad v \mapsto \begin{pmatrix} 0 & -1 \\ -b & 0 \end{pmatrix}, \quad w \mapsto \begin{pmatrix} 0 & -\sqrt{a} \\ \sqrt{a}b & 0 \end{pmatrix},$$

where without loss of generality we take a to be positive.

23. Can the norm on $(a, b)_{\mathbf{Q}}$ ever take only values ≤ 0? What about the norm on $(a, b)^0_{\mathbf{Q}}$?

24. (Checking division rings)

a) For any prime $p \neq 2$ and integer a such that the Legendre symbol $(\frac{a}{p})$ equals -1, prove $(a, p)_{\mathbf{Q}}$ is a division ring.

b) Show the following are division rings: $(-1, p)_{\mathbf{Q}}$ when $p \equiv 3 \bmod 4$, $(2, 3)_{\mathbf{Q}}$, and $(11, 3)_{\mathbf{Q}}$.

c) For $a \in \mathbf{Z}$, formulate a condition on a mod 8 which implies $(a, 2)_{\mathbf{Q}}$ is a division ring.

25. We know from the previous exercise that $(11, 3)_{\mathbf{Q}}$ is a division ring. By symmetry (*i.e.*, $(11, 3)_{\mathbf{Q}} \cong (3, 11)_{\mathbf{Q}}$), $(3, 11)_{\mathbf{Q}}$ is a division ring. However, since $(\frac{3}{11}) = 1$, the previous exercise does not apply directly. Find a proof that $(3, 11)_{\mathbf{Q}}$ is a division ring which does not rely on the symmetry.

26. Decide if the following are division rings: $(2, 5)_{\mathbf{Q}}$, $(2, -5)_{\mathbf{Q}}$, $(6, 10)_{\mathbf{Q}}$, $(6, -10)_{\mathbf{Q}}$, $(5, 11)_{\mathbf{Q}}$, $(5, -11)_{\mathbf{Q}}$. (None of the examples have both entries negative, since $(a, b)_{\mathbf{Q}}$ is trivially a division ring when $a, b < 0$: the norm is positive at any non-zero element.)

27. Decide if $(2 - \sqrt{2}, 3 + \sqrt{2})_{\mathbf{Q}[\sqrt{2}]}$ and $(-1, 2 - \sqrt{2})_{\mathbf{Q}[\sqrt{2}]}$ are division rings by a generalization of exercise 24 from $\mathbf{Q}$ to $\mathbf{Q}[\sqrt{2}]$.

28. Let L be a field with characteristic different from 2. For an irreducible π in $L[t]$ and an $f \in L[t]$ such that $f \not\equiv \square \bmod \pi$, prove $(f, \pi)_{L(t)}$ is a division ring. In particular, if $a \in L^\times$ is not a square in $L^\times$ then $(a, t)_{L(t)}$ is a division ring. (For example, $(-1, t)_{\mathbf{Q}(t)}$ is a division ring.)

29. Is $(t, t^2 + 1)_{\mathbf{F}_3(t)}$ a division ring?

30. (QR, CRT, and all that)

a) Use Jacobi QR and the Chinese remainder theorem to prove: if $a \in \mathbf{Z}$ is squarefree and not 1, then $(\frac{a}{p}) = -1$ for some prime p. Treat separately the case when a is odd and even (and perhaps also when a is positive and negative).

b) Show, for any $a \in \mathbf{Q}^\times$, that $(a, b)_{\mathbf{Q}} \cong \mathrm{M}_2(\mathbf{Q})$ for every b in $\mathbf{Q}^\times$ if and only if a is a rational square.

c) Based on one of the equivalent conditions for a quaternion algebra to be isomorphic to a matrix algebra, part b shows that for $a \in \mathbf{Q}^\times$, the equation $a = x^2 - by^2$ has a $\mathbf{Q}$-solution for every $b \in \mathbf{Q}^\times$ if and only if a is a rational square. Can you prove this without mentioning quaternion algebras?

d) Show part b is equivalent to: $\{x^2 - ay^2 \neq 0 : x, y \in \mathbf{Q}\} = \mathbf{Q}^\times$ if and only if $a \in \mathbf{Q}^{\times 2}$.