QUATERNION ALGEBRAS: SET 4

KEITH CONRAD

1. Call a ring $R \neq 0$ simple if any ring homomorphism $R \to S$ ($S \neq 0$) is injective.
   a) Prove the commutative simple rings are the fields.
   b) By exercise 8 on set 1, $M_2(F)$ is a simple ring for any field $F$. Is $M_2(D)$ a simple ring if $D$ is any division ring?
   c) When char $F \neq 2$, show $(a,0)_F$ is not a simple ring, as follows: map $(a,0)_F$ to $F[t]_{t^2-a}$ by
   $$c_0 + c_1 u + c_2 v + c_3 w \mapsto c_0 + c_1 t.$$ Show this is a ring homomorphism; it is not, however, injective. What does this homomorphism correspond to when you view $(a,0)_F$ inside $M_2(F[t]_{t^2-a})$ by the embedding from exercise 2 on set 2?

All about characteristic 2

Unless indicated otherwise, from now on char $F = 2$. For $a \in F$ and $b \in F^\times$, we define the quaternion algebra $[a,b]_F$ as
   $$[a,b]_F = F + Fu + Fv + Fw,$$
where
   • $u^2 + u = a$,
   • $v^2 = b$,
   • $w = uv = v(u+1)$.

2. Check the multiplication table for $u, v, w$ in $[a,b]_F$ from lecture.

3. Show the map $[a,b]_F \to M_2(F[t]_{t^2+t+a})$ determined by
   $$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad u \mapsto \begin{pmatrix} t & 0 \\ 0 & t+1 \end{pmatrix}, \quad v \mapsto \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}, \quad w \mapsto \begin{pmatrix} 0 & t \\ b(t+1) & 0 \end{pmatrix}$$
is an injective ring homomorphism. Check this even holds when $b = 0$, but show $[a,0]_F$ is not a simple ring. (For all of the remaining exercises, the notation $[a,b]_F$ is understood to mean $b \neq 0$.)

4. Show the center of $[a,b]_F$ is $F$.

5. (Conjugation in characteristic 2) For $q = x_0 + x_1 u + x_2 v + x_3 w$ in $[a,b]_F$, set
   $$\overline{q} = x_0 + x_1 (u+1) + x_2 v + x_3 w.$$ That is, $\overline{u} = u + 1$ and $\overline{v} = v$, $\overline{w} = w$. Check $\overline{q} = \overline{q}$, $\overline{q_1+q_2} = \overline{q_1} + \overline{q_2}$, $\overline{q_1q_2} = \overline{q_1}\overline{q_2}$, and $\overline{cq} = \overline{c} \overline{q}$ for $c \in F$. However, it is no longer true that $\overline{q} = q \iff q \in F$!

6. Define the trace and norm on $[a,b]_F$ by $\text{Tr}(q) = q + \overline{q}$ and $N(q) = q\overline{q}$.
   a) For $q = x_0 + x_1 u + x_2 v + x_3 w$, confirm that
   $$\text{Tr}(q) = x_1, \quad N(q) = x_0^2 + x_0 x_1 + ax_1^2 + b(x_2^2 + x_2 x_3 + x_3^2).$$
   b) Show trace is additive, $\text{Tr}(qq') = \text{Tr}(q'q)$ for any $q$ and $q'$ (what is an explicit formula for $\text{Tr}(qq')$ in terms of the coordinates of $q$ and $q'$?), and the norm is multiplicative. Since $q$ is a root of $T^2 - (\text{Tr}q)T + N(q) \in F[T]$, once again we see that $F[q] = F + Fq$ for $q \notin F$.
   c) For $a \in F$ and $b \in F^\times$, show $[a,b]_F$ is either isomorphic to $M_2(F)$ or is a division ring.
7. When \( q \in [a, b)_F \) is not in \( F \), does \( \{ r \in [a, b)_F \mid rq = qr \} = F[q] \)? For the particular element \( u \), check \( ur = ru = (u + 1)r \). Does \( ur = (u + 1)r \) imply \( r \in Fv + Fw \)?

8. Define the pure quaternions \( [a, b)_F^0 \) as the elements with trace 0 (that is, \( \overline{q} = -q = q \)). Concretely, \( [a, b)_F^0 = F + Fv + Fw \). If \( r \) is pure and \( q \) is invertible, show \( qrq^{-1} = pure \).

9. The characteristic 2 analogue of \( x \mapsto x^2 \) is \( x \mapsto x^2 + x \). The former is multiplicative while the latter is (in characteristic 2) additive. Denote this operation by \( \mathcal{P} \). Let \( F \) be the product of it and its conjugate: \( N(x) = x^2 + x \). This is an additive subgroup of \( F \). (This is analogous to the multiplicative subgroup \( F^{\times 2} \) of \( F^{\times} \) when \( \text{char } F \neq 2 \).)

Define the ring \( \tilde{E}_a \) to be \( F[t]_{t^2 + t + a} \), when \( a \in F \). This is a characteristic 2 analogue of \( E_a = F[t]_{t^2 - a} \), for \( a \neq 0 \) from characteristic not 2.

a) Show \( \tilde{E}_a \) is a field if and only if \( a \notin \nu(F) \).

b) Show \( \tilde{E}_a \cong F \times F \) if \( a \in \nu(F) \) (e.g., if \( a = 0 \)).

c) Let the conjugate of \( x + yt \) in \( \tilde{E}_a \) be \( x + y(t + 1) \), and the norm of an element of \( \tilde{E}_a \) is defined to be the product of it and its conjugate: \( N(x + yt) = x^2 + xy + ay^2 \). Check the norm is multiplicative, so \( F^{\times 2} \subset N(\tilde{E}_a^{\times}) \subset F^{\times} \).

d) Show \( N(\tilde{E}_a^{\times}) = F^{\times} \) when \( a \in \nu(F) \). (Hint: \( c^2 + cc' = cc' \), so every product has the form \( x^2 + xy \).)

10. Verify the following properties in characteristic 2, and identify what they are analogues of in characteristic not 2:

- \( [a, b)_F \cong [a + b, b)_F \)
- \( [a, b)_F \cong [a, b(x^2 + xy + ay^2)]_F \) when \( x^2 + xy + ay^2 \neq 0 \)
- \( [a, b)_F \cong [a, be^c]_F \) for \( c \in F^{\times} \)
- \( [a, b)_F \cong [a + c^2 + c, b)_F \)
- \( [a, 1)_F \cong M_2(F) \)
- \( [0, b)_F \cong M_2(F) \)
- \( [a, c^2)_F \cong [a, c^2 + c, b)_F \) for \( [a, a)_F \) are all isomorphic to \( M_3(F) \)
- \( [a, b)_F \cong [a, b)_F \) if and only if \( \overline{b} \in N(\tilde{E}_a^{\times}) \), and in particular \( [a, b)_F \cong M_2(F) \) if \( b \in N(\tilde{E}_a^{\times}) \)
- \( \mathcal{P} \) \( (a, b)_F \) is a division ring and \( c \in F \), \( [a, b)_F \cong [c, c)_F \) if and only if \( \overline{c} \in \nu(F) \).

11. Choose a field \( L \) with characteristic 2. Let \( \pi \) be irreducible in \( L[t] \) and let \( f \in L[t] \) satisfy \( f \neq q^2 + g \) mod \( \pi \) for any \( g \). Conclude that \( (\overline{f}, \pi)_{L(t)} \) is a division ring. In particular, \( (1, t)_{L(t)} \) is a non-commutative division ring with characteristic 2.

12. Show the only quaternion algebra over a finite field with characteristic 2 is the \( 2 \times 2 \) matrix algebra over that field.

13. If you know quadratic reciprocity in characteristic 2 (e.g., if you attended my lectures last summer and have the notes), show for \( a \in F(t) \) that \( [a, b]_{F(t)} \cong M_2(F(t)) \) for all \( b \) if and only if \( a \in \nu(F(F(t))) \). Here \( F \) is a finite field of characteristic 2.

14. Show conjugation on \( [a, b)_F \) is the unique involution \( q \mapsto q^* \) which fixes \( F \) pointwise and satisfies \( qq^* \in F \) for every \( q \in [a, b)_F \).

15. (An alternate basis for quaternion algebras in characteristic 2) For any \( a, b \in F \), let \( ((a, b))_F = F + Fr + Fs + Frs \) with the rules \( r^2 = a, s^2 = b, rs = rs + 1 \). Remember, \( \text{char } F = 2 \).

a) For \( a \in F \) and \( b \in F^{\times} \), check that in \( ((a, b))_F \) the choice \( u = rs \) and \( v = s \) shows \( (a, b)_F \cong [ab, b)_F \).

b) What can you say about \( ((a, 0))_F \)?
16. Recall from lecture, for a separable quadratic field extension $K/F$, and $b \in F^\times$, the quaternion algebra $(K/F, b)$ is defined to be $K + K v$ where $v^2 = b$ and $v \alpha = \sigma(\alpha)v$ for all $\alpha \in K$. (We write $\sigma$ for the conjugation on $K$ that fixes $F$.) Find $K \supset \mathbb{F}_2(t)$ such that $[1, t]_{\mathbb{F}_2(t)} = (K/\mathbb{F}_2(t), t)$.

17. In a quaternion algebra of characteristic not 2, the equation $q_1q_2 - q_2q_1 = 1$ has no solution, since the left side has trace 0 for any $q_1$ and $q_2$, while the right side has trace $2 \neq 0$. But in characteristic 2, where $2 = 0$, this obstruction does not occur. Is there a solution to $q_1q_2 - q_2q_1 = 1$ in the split quaternion algebra $M_2(F)$ when $\text{char } F = 2$? What about in the quaternion division algebra $[1, t]_{\mathbb{F}_2(t)}$?

18. Let $F$ be a field of any characteristic. Let $K/F$ be a separable quadratic field extension. For a quaternion algebra $D$ over $F$, show $K$ is isomorphic to a subfield of $D$ if and only if $D \cong (K/F, b)$ for some $b \in F^\times$.

19. Let $F$ be a field of any characteristic and let $K/F$ be a separable quadratic field extension. On $(K/F, b)$, set $(\alpha_1 + \alpha_2 v)^* = \alpha_1 - \sigma(\alpha_2)v$. Show this operation is an involution on $(K/F, b)$, but $qq^* \notin F$ for some $q$. For the particular example $(K/F, 1) \cong M_2(F)$, is this operation the transpose on matrices?

20. Fill in the details of the following proof of Noether’s theorem: for $F$ of characteristic 2 and $D$ a 4-dimensional $F$-division algebra, some $q \in D - F$ has $q^2 \notin F$.

Suppose there is some $d \in D - F$ such that $d^2 \in F$ (otherwise we're certainly done). Some $\alpha \in D$ satisfies $d\alpha \neq \alpha d$. Let $\beta = d\alpha d^{-1} - \alpha \neq 0$. Then $d$ and $\beta$ commute. Let $q = \beta^{-1} \alpha$. Then looking at $dqd^{-1}$ and $dq^2d^{-1}$ shows $q \in D - F$ and $q^2 \in D - F$.

21. Let $F$ be a field of any characteristic. Let $B$ be a 4-dimensional simple $F$-algebra which is not a division ring. In the lectures we saw a proof that $B \cong M_2(F)$. Fill in the details of the following alternate proof.

Pick $q \in B$ with $q \neq 0$, $q \notin B^\times$. Set $M = Bq$ (the left multiples of $q$). Then $1 \leq \dim_F M \leq 3$.

Let $B$ act on $M$ by left multiplications. Check this yields an $F$-algebra homomorphism $B \to \mathcal{L}(M, M)$, so $\dim_F M \geq 2$. Then let $B$ act on $B/M$ by left multiplications to get a reverse inequality, so $\dim_F M = 2$ and our homomorphism $B \to \mathcal{L}(M, M) \cong M_2(F)$ is the desired isomorphism. That proves the result. (If instead $\dim_F(B) = n^2$ where $n > 2$, what lower and upper bounds on $\dim_F M$ do we get by this argument?)