INVESTIGATING THE STRUCTURE OF $M_2(\mathbb{F}_q)$

IAN GALLAGHER
DR. ERIC BRUSSEL

Abstract. We present and prove a count of the maximal commutative subalgebras of $M_2(\mathbb{F}_q)$, as well as counts for the individual isomorphism classes.

1. Introduction

For a finite field of $q = p^m$ elements, $p \neq 2$, it is possible to count the number of vector subspaces of ${\mathbb{F}_q}^n$ of a given dimension. These counts arise in problems involving the number of points of $\mathbb{P}^n_q$, the Grassmannian, and further generalizations.

This paper is meant to address a similar problem. Namely, the structure and count of the maximal commutative subalgebras of $M_2(\mathbb{F}_q)$. Such subalgebras...

For the duration of the paper, $q = p^n$ for some prime $p \neq 2$.

2. Generalized Quaternions and $M_2(\mathbb{F}_q)$

Here, we introduce an alternative formulation of $M_2(\mathbb{F}_q)$ based on the generalized quaternions, an abstraction of the well-known quaternion algebra. This formulation lends itself nicely to a more general result detailing the structure of commutative subalgebras of $M_2(\mathbb{F}_q)$.

Definition 1 (Generalized Quaternions)**.** Let k be a field, $\operatorname{char} k \neq 2$, and fix $a, b \in k - \{0\}$. Then the *generalized quaternions* are a central simple k-algebra (CSA) of the form

$$A_{a,b}(k) = \{t + xi + yj + zl : t, x, y, z \in k\}$$
$$\text{where } i^2 = a, j^2 = b, \text{ and } ij = -ji = l$$

Definition 2 (Generalized Quaternion Norm)**.**

$$N_{a,b} : A_{a,b}(k) \to k$$
$$q \mapsto q\overline{q} = t^2 - ax^2 - by^2 + abz^2$$

It turns out that $M_2(\mathbb{F}_q)$ is the only isomorphism class of generalized quaternions over $\mathbb{F}_q$ but this fact is not immediately obvious. To prove this, we cite but do not prove the following results.

Theorem 3 (Wedderburn [1])**.** *Let k be a field and A a central simple algebra. Then $A \simeq M_n(D)$ for some k-division algebra D.*

Theorem 4 (Chevalley-Warning [2])**.** *Let $f_\alpha \in \mathbb{F}_q[X_1, \ldots, X_n]$ be polynomials in n variables such that $\sum_\alpha \deg f_\alpha < n$ and let V be the set of their common zeros in $\mathbb{F}_q^n$. One has*

$$|V| \equiv 0 \pmod{p}$$

Date: June 5, 2021.

With these theorems, we can now give a succint explanation for the structure of the generalized quaternions over $\mathbb{F}_q$

Lemma 5. *$N_{a,b}(X_1 + iX_2 + jX_3 + kX_4)$ has a nontrivial zero over $A_{a,b}(\mathbb{F}_q)$.*

Proof. For this, we make use of theorem 4. Let

$$\begin{aligned} f_1 &= N_{a,b}(X_1 + iX_2 + jX_3 + kX_4) \\ &= X_1^2 - aX_2^2 - bX_3^2 + abX_4^2 \\ &\in \mathbb{F}_q[X_1, X_2, X_3, X_4] \end{aligned}$$

Here, $\deg f_1 = 2 < 4$, so Chevalley-Warning holds and $|V| \equiv 0 \pmod{p}$. Note that $f(0,0,0,0) = 0$, so we must have p divides $|V|$. Therefore, f_1 has a nontrivial zero and this completes the proof. □

Theorem 6. *$A_{a,b}(\mathbb{F}_q) \cong M_2(\mathbb{F}_q)$*

Proof. By lemma 5, there exists $q \in A_{a,b}(\mathbb{F}_q)$, $q \neq 0$, such that $N_{a,b}(q) = q\overline{q} = 0$. In other words, $A_{a,b}(\mathbb{F}_q)$ has nontrivial zero divisors and is therefore not a $\mathbb{F}_q$-division algebra. By theorem 3 we must have $A_{a,b}(\mathbb{F}_q) \cong M_n(D)$ for some $\mathbb{F}_q$-division algebra D and natural number n. However, $\dim_{\mathbb{F}_q} A_{a,b}(\mathbb{F}_q) = 4$, so $n = 2$ and D must have $\mathbb{F}_q$-dimension 1.
$\therefore D \cong \mathbb{F}_q$ and $A_{a,b}(\mathbb{F}_q) \cong M_2(\mathbb{F}_q)$. □

3. Planes in $M_2(\mathbb{F}_q)$

For a matrix $A \in M_2(\mathbb{F}_q)$, we know

(1) A's characteristic polynomial: $p_A(X) = X^2 - \operatorname{tr}(A)X + \det(A)$.
(2) A's minimum polynomial: $m_A(X) = X - A$ if $A \in \mathbb{F}_q$. Otherwise, $m_A(X) = p_A(X)$.

This gives an evaluation map $\epsilon_A : \mathbb{F}_q[X] \to M_2(\mathbb{F}_q)$ taking $f(X)$ to $f(A)$, which is a $\mathbb{F}_q$-linear ring homomorphism with image $\mathbb{F}_q[A] \subseteq M_2(\mathbb{F}_q)$. The kernel is nontrivial, since $M_2(\mathbb{F}_q)$ has finite $\mathbb{F}_q$-dimension and $\mathbb{F}_q[X]$ does not. It follows that $ker(\epsilon_A) = (m_A(X))$. By the First Isomorphism Theorem,

$$\frac{\mathbb{F}_q[X]}{(m_A(X))} \cong \mathbb{F}_q[A]$$

So if $A \in M_2(\mathbb{F}_q) - \mathbb{F}_q$, we know $m_A(X) = p_A(X)$ is degree 2 and $\mathbb{F}_q[A]$ has $\mathbb{F}_q$-dimension 2.

Thus, we have that each such A generates the unique 2 dimensional commutative sub-algebra of $M_2(\mathbb{F}_q)$ containing A. All possible 2 dimensional commutative sub-algebra's are therefore of the form

$$\frac{\mathbb{F}_q[X]}{(m_A(X))}$$

for some $A \in M_2(\mathbb{F}_q) - \mathbb{F}_q$. The set of two dimensional commutative sub-algebra's of $M_2(\mathbb{F}_q)$ must then be composed of exactly three isomorphism classes based on $m_A(X)$

(1) If $m_A(X)$ is irreducible, define $K_{-1} = \mathbb{F}_q[A] \cong \mathbb{F}_{q^2}$.
(2) If $m_A(X)$ is reducible but not separable, define $K_1 = \mathbb{F}_q[A] \cong \mathbb{F}_q \times \mathbb{F}_q$.
(3) If $m_A(X)$ is separable, define $K_0 = \mathbb{F}_q[A] \cong \mathbb{F}_{q_{nil}}^2$ the degenerate nilpotent case.

It is worth noting that the case that $m_A(X)$ is both separable and irreducible does not require consideration seeing as finite fields are perfect.

4. Identifying maximal commutative subalgebras

At this point, we have shown that each matrix $A \in M_2(\mathbb{F}_q) - \mathbb{F}_q$ can be identified with the unique plane generated by taking the linear span of 1 and A, and that this plane belongs to one of three given isomorphism classes. It is reasonable to ask whether this is the maximal commutative sub-algebra of $M_2(\mathbb{F}_q)$ containing A. Indeed, if we drop the restriction of commutativity, we may easily find subalgebras of dimension 3. The set of all upper triangular matrices is one such example.

To prove that there are no commutative subalgebras of dimension 3, we return to the generalized quaternions formulation. We first introduce an alternative vector notation for the generalized quaternions that is useful for cleaner computations.

Definition 7 (Generalized Quaternions, Vector Notation)**.** Let $p = (s, \mathbf{v})$, and $q = (t, \mathbf{w})$, using the vector notation $v = \langle v_1 i, v_2 j, v_3 l\rangle$ and $w = \langle w_1 i, w_2 j, w_3 l\rangle$ with coefficients in $A_{a,b}(k)$. The usual dot and cross product formulas compute

$$\begin{aligned}\mathbf{v}\cdot\mathbf{w} &= v_1w_1a + v_2w_2b - abv_3w_3\\ \mathbf{v}\times\mathbf{w} &= \left\langle \begin{vmatrix} v_2j & v_3l\\ w_2j & w_3l\end{vmatrix}, \begin{vmatrix} v_1i & v_3l\\ w_1i & w_3l\end{vmatrix}, \begin{vmatrix} v_1i & v_2j\\ w_1i & w_2j\end{vmatrix}\right\rangle\\ &= \langle(-v_2w_3 + v_3w_2)bi, (v_1w_3 - v_3w_1)aj, (v_1w_2 - v_2w_1)l\rangle\end{aligned}$$

Compare this to $\langle v_1, v_2, v_3\rangle \times \langle w_1, w_2, w_3\rangle = \langle v_2w_3 - v_3w_2, -v_1w_3 + v_3w_1, v_1w_2 - v_2w_1\rangle$. Thus

$$\begin{aligned}pq &= (st + v_1w_1a + v_2w_2b - abv_3w_3) + (sw_1 + tv_1 - v_2w_3b + v_3w_2b)i\\ &\quad + (sw_2 + tv_2 + v_1w_3a - v_3w_1a)j + (sw_3 + tv_3 + v_1w_2 - v_2w_1)l\\ &= (st + \mathbf{v}\cdot\mathbf{w}, s\mathbf{w} + t\mathbf{v} + \mathbf{v}\times\mathbf{w})\end{aligned}$$

Lemma 8. *Let $p = (0, \mathbf{v})$, and $q = (0, \mathbf{w})$. Then $pq = qp$ if and only if $\mathbf{v}\times\mathbf{w} = 0$ if and only if $\langle v_1, v_2, v_3\rangle \times \langle w_1, w_2, w_3\rangle = 0$.*

Proof. We have $pq - qp = 2\mathbf{v}\times\mathbf{w}$, and since i, j, k are linearly independent and $\operatorname{char} k \neq 2$, $pq = qp$ if and only if $\mathbf{v}\times\mathbf{w} = 0$ if and only if $\langle v_1, v_2, v_3\rangle \times \langle w_1, w_2, w_3\rangle = 0$. □

Theorem 9. *If $K \subseteq A_{a,b}(k)$ is a commutative subalgebra, then $K = k[\mathbf{w}]$ for some pure imaginary $\mathbf{w} \in A_{a,b}(k)$, and $\dim_k K = 1$ or 2.*

Proof. If $q = (t, \mathbf{w}) \in K$, then $q - t = \mathbf{w}$ is in $k[q]$, hence $k[\mathbf{w}] = k[q] \subseteq K$. If $p = (s, \mathbf{v}) \in K$ then since $pq = qp$, $\mathbf{v}$ is a scalar multiple of $\mathbf{w}$ by lemma 8. Therefore $K = k[\mathbf{w}]$. Since $\deg(m_{\mathbf{w}}(X))$ is either 1 or 2, this completes the proof. □

Now, $A_{a,b}(\mathbb{F}_q) \cong M_2(\mathbb{F}_q)$, so theorem 9 suffices to show that no commutative subalgebra of dimension 3 exists and we may conclude that the three isomorphism classes of commutative planes are the maximal commutative subalgebras of $M_2(\mathbb{F}_q)$

5. Plane Counts

Theorem 10. *$M_2(\mathbb{F}_q)$ has $q^2 + q + 1$ unique nontrival commutative subalgebras.*

Proof. Let E_x for $x \in M_2(\mathbb{F}_q) - \mathbb{F}_q$ be the commutative subalgebra created by the span of 1 and x. Label $\Sigma = \{E_x \mid x \in M_2(\mathbb{F}_q) - \mathbb{F}_q\}$ and set $N = |\Sigma|$, the number of unique 2D commutative subalgebras. Let $x, y \in M_2(\mathbb{F}_q) - \mathbb{F}_q$. E_x, E_y are both two dimensional $\mathbb{F}_q$ algebras so we know that $E_x \cap E_y$ is also a $\mathbb{F}_q$-algebra. By dimension arguments, either

$E_x = E_y$ or $E_x \cap E_y = \mathbb{F}_q$. Since $\bigcup_{E\in\Sigma} E = M_2(\mathbb{F}_q)$, $\{E_x - \mathbb{F}_q \mid x \in M_2(\mathbb{F}_q) - \mathbb{F}_q\}$ is a partition of $M_2(\mathbb{F}_q) - \mathbb{F}_q$. The following then holds,

$$\begin{aligned} N(|E_x| - |\mathbb{F}_q|) &= |M_2(\mathbb{F}_q)| - |\mathbb{F}_q| \\ N(q^2 - q) &= q^4 - q \\ N(q-1) &= q^3 - 1 \\ N &= q^2 + q + 1 \end{aligned}$$

□

Lemma 11. *Consider the following elements of $M_2(\mathbb{F}_q)$.*

$$x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Under the conjugation action of $GL_2(\mathbb{F}_q)$ on $M_2(\mathbb{F}_q)$,

$$|\mathcal{O}_x| = q(q+1)$$
$$|\mathcal{O}_y| = (q+1)(q-1)$$

Proof. We may compute the size of the orbits of x, y by first computing the size of their stabilizers, G_x, G_y, and then applying the orbit-coset correspondence theorem. Now,

$$\begin{aligned} G_x &= \{A \in GL_2(\mathbb{F}_q) \mid A \cdot x = x\} \\ &= \{A \in GL_2(\mathbb{F}_q) \mid AxA^{-1} = x\} \\ &= \{A \in GL_2(\mathbb{F}_q) \mid Ax = xA\} \end{aligned}$$

Inevitably, matrices of the form $sx+tI$ commute with x for $s, t \in \mathbb{F}_q$, so if $sx+tI \in GL_2(\mathbb{F}_q)$, then $sx + tI \in G_x$. These are also the only possible matrices in G_x since they are the elements of the maximal commutative subalgebra containing x (Theorem 9). It now suffices to determine when $\det(sx + tI) = 0$.

$$\det(sx + tI) = \begin{vmatrix} t & s \\ s & t \end{vmatrix} = t^2 - s^2$$

Therefore, $\det(sx + tI) = 0$ when $t^2 = s^2$, so when $t = \pm s$. We have thus found precisely $q^2 - 2q + 1 = (q-1)^2$ elements of G_x. It follows that,

$$[GL_2(\mathbb{F}_q) : G_x] = \frac{(q^2-1)(q^2-q)}{(q-1)^2} = q(q+1)$$

By the orbit coset correspondence theorem [3] we have that $|\mathcal{O}_x| = q(q+1)$

Similarly we have $G_y = \{A \in GL_2(\mathbb{F}_q) | Ay = yA\}$ and the only possible elements of G_y are those of the form $sy + tI$ for $s, t \in \mathbb{F}_q$ where $sy + tI \in GL_2(\mathbb{F}_q)$.

$$\det(sy + tI) = \begin{vmatrix} t & 0 \\ s & t \end{vmatrix} = t^2$$

So $\det(sy + tI) = 0$ if and only if $t = 0$. There are then $q^2 - q$ elements of G_y. Therefore,

$$[GL_2(\mathbb{F}_q) : G_y] = \frac{(q^2-1)(q^2-q)}{q^2-q} = q^2 - 1$$

and we have $|\mathcal{O}_y| = q(q-1)$ □

Theorem 12.

$$|[K_{-1}]| = \binom{q}{2} \tag{1}$$

$$|[K_1]| = \binom{q+1}{2} \tag{2}$$

$$|[K_0]| = q+1 \tag{3}$$

Proof. The elements x, y from lemma 11 are the rational canonical forms for all matrices with minimum polynomials X^2-1 and X^2 respectively. Note that two matrices in $M_2(k)$ are conjugate if and only if they have the same rational canonical form [3].

Since $X^2-1 = (X+1)(X-1)$ is reducible and not separable over $\mathbb{F}_q$, and $\text{char}(\mathbb{F}_q) \neq 2$, all of the elements of $\mathcal{O}_x$ generate an embedding K_1.

Any embedding K_1 must also contain an element of $\mathcal{O}_x$. To see this, pick a nontrivial element $A \in K_1$ such that A is orthogonal to the identity. Then $\text{tr}(A) = 0$, and $m_A(X) = p_A(X) = X^2 + \det(A)$. We picked $A \in K_1$, which means that $m_A(X)$ must also be reducible and not separable. It follows that $\det(A) = -\lambda^2$ for some $\lambda \in \mathbb{F}_q$. Let $B = A/\lambda \in K_1$ and observe $\text{tr}(B) = \text{tr}(A)/\lambda = 0$, $\det(B) = \det(A)/\lambda^2 = -\lambda^2/\lambda^2 = -1$. Therefore, $m_B(X) = p_B(X) = X^2 - \text{tr}(B)X + \det(B) = X^2 - 1$ as desired.

Furthermore, suppose $B' \in K_1$ has minimum polynomial X^2-1. Then B' is orthogonal to the identity as well and $B' = \alpha B$ for some $\alpha \in \mathbb{F}_q^\times$ due to K_1 being dimension 2. We have $-1 = \det(B') = \alpha^2 \det(B) = -\alpha^2$, so $\alpha = \pm 1$ and $B' = \pm B$. We have therefore shown that each embedding K_1 contains exactly 2 elements of $\mathcal{O}_x$. Applying lemma 11,

$$|[K_1]| = \frac{1}{2}|\mathcal{O}_x| = \frac{q(q+1)}{2} = \binom{q+1}{2}$$

Similarly, since X^2 is separable over $\mathbb{F}_q$, all of the elements of $\mathcal{O}_y$ generate an embedding of K_0. Any embedding K_0 will always contain exactly $q-1$ elements of $\prime_y$. These are precisely the nontrivial elements of K_0 that are orthogonal to the identity. Applying lemma 11,

$$|[K_0]| = \frac{1}{q-1}|\mathcal{O}_x| = \frac{q^2-1}{q-1} = q+1$$

It remains to show $|[K_{-1}]| = \binom{q}{2}$. We may use the previous counts and theorem 10 to do so.

$$\begin{aligned}
|[K_{-1}]| &= q^2 + q + 1 - |[K_1]| - |[K_0]| \\
&= q^2 + q + 1 - \binom{q+1}{2} - (q+1) \\
&= q^2 - \frac{q(q+1)}{2} \\
&= \frac{q(q-1)}{2} \\
&= \binom{q}{2}
\end{aligned}$$

This completes the proof.

□

References

[1] D. W. Henderson, *A short proof of Wedderburn's theorem*, Amer. Math. Monthly **72** (1965), 385–386.
[2] Jean-Pierre Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.
[3] D. S. Dummit and R. M. Foote, *Abstract Algebra*, third edition, John Wiley & Sons, Inc., Hoboken, New Jersey, 2004.