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 $M_2(\mathbb{F}_q)$, the vector space $\mathbb{F}_q^4$ with matrix multiplication. Such commutative subalgebras are themselves two dimensional vector subspaces with the inherited multiplication of $M_2(\mathbb{F}_q)$. We find that there are three isomorphism classes of maximal commutative subalgebras and give explicit formulas for the size of the isomorphism classes based on the size of $\mathbb{F}_q$.

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 $\mathbb{F}$ be a field, $\operatorname{char}\mathbb{F} \neq 2$, and fix $a, b \in \mathbb{F} - \{0\}$. Then define the *generalized quaternions* as

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

Analogous to the complex numbers, for $q = t + xi + yj + zk$ we denote the quaternion conjugate $\overline{q} = t - xi - yj - zk$ and we will call the additive subspace

$$\{xi + yj + zk : x, y, z \in \mathbb{F}\} \subseteq A_{a,b}(\mathbb{F})$$

the pure imaginary elements,

The generalized quaternions form what is known as a central simple algebra over $\mathbb{F}$. That is, it is a finite dimensional $\mathbb{F}$-algebra with center $\mathbb{F}$ and no nontrivial two-sided ideals. possibly insert proof that the generalized quaternions are a csa here

Date: June 11, 2021.

Definition 2 (Generalized Quaternion Norm)**.** We define the *generalized quaternion norm* from $A_{a,b}(\mathbb{F})$ to $\mathbb{F}$ to be the function

$$\begin{aligned} N_{a,b} : A_{a,b}(\mathbb{F}) &\to \mathbb{F} \\ q &\mapsto q\overline{q} = t^2 - ax^2 - by^2 + abz^2 \end{aligned}$$

For $q, w \in A_{a,b}(\mathbb{F})$, it is not difficult to show that $\overline{qw} = \overline{w}\overline{q}$. From this we note that the norm is multiplicative

$$N_{a,b}(qw) = qw\overline{qw} = qw\overline{w}\overline{q} = q\overline{q}w\overline{w} = N_{a,b}(q)N_{a,b}(w)$$

where the third equality holds since $w\overline{w} \in \mathbb{F}$ and therefore commutes with $\overline{q}$.

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. We will use the following two results to prove this.

Theorem 3 (Wedderburn [3, pg. 854])**.** *Let $\mathbb{F}$ be a field and A a central simple algebra. Then $A \simeq M_n(D)$ for some $\mathbb{F}$-division algebra D.*

Refer to [1] for a short proof of Wedderburn's Theorem.

Theorem 4 (Chevalley-Warning [2, pg. 5])**.** *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*

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

With these theorems, we now give a proof of the structure of the generalized quaternions over $\mathbb{F}_q$.

Theorem 5. $A_{a,b}(\mathbb{F}_q) \cong M_2(\mathbb{F}_q)$

Proof. We first make use of Theorem 4. Let

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

Here, $\deg f = 2 < 4$, so Chevalley-Warning holds and $|V| \equiv 0 \pmod{p}$, where V is the set of zeros of f. Note that $f(0,0,0,0) = 0$, so we must have p divides $|V|$. Therefore, f has a nontrivial zero.

It follows that there exists $q \in A_{a,b}(\mathbb{F}_q)$, $q \neq 0$, such that $N_{a,b}(q) = q\overline{q} = 0$. Therefore, q is a nontrivial zero divisor and $A_{a,b}(\mathbb{F}_q)$ is 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. Since $A_{a,b}(\mathbb{F}_q)$ is not a division algebra, we know $n \neq 1$. $A_{a,b}(\mathbb{F}_q)$ has $\mathbb{F}_q$-dimension 4, so $n = 2$ and D must have $\mathbb{F}_q$-dimension 1, so is isomorphic to $\mathbb{F}_q$.Therefore, $A_{a,b}(\mathbb{F}_q) \cong M_2(\mathbb{F}_q)$. □

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

Definition 6. For a matrix $A \in M_2(\mathbb{F}_q)$, define

(1) A's characteristic polynomial $p_A(X) = X^2 - \operatorname{tr}(A)X + \det(A)$.
(2) A's minimal polynomial $m_A(X)$ is the unique monic polynomial of smallest degree such that $m_A(A) = 0$.

By the Cayley-Hamilton Theorem [3, pg. 478], we know that $m_A(X)$ divides $p_A(X)$. So for nontrivial $A \in M_2(\mathbb{F}_q)$, we observe that if $A \in \mathbb{F}_q$, then $m_A(X) = X - A$. Otherwise, no minimal polynomial of degree 1 exists, and we have $m_A(X) = p_A(X)$.

Theorem 7. *The set of two dimensional commutative subalgebras of $M_2(\mathbb{F}_q)$ is composed of exactly three isomorphism classes based on $m_A(X)$.*

1. *If $m_A(X)$ is irreducible, define $\mathbb{F}_q[A] \cong \mathbb{F}_{q^2}$.*
2. *If $m_A(X)$ is reducible but not separable, define $\mathbb{F}_q[A] \cong \mathbb{F}_q \times \mathbb{F}_q$.*
3. *If $m_A(X)$ is separable, define $\mathbb{F}_q[A] \cong \mathbb{F}^2_{q_{nil}}$.*

Proof. Define the evaluation map $\varepsilon_A : \mathbb{F}_q[X] \to M_2(\mathbb{F}_q)$ taking $f(X)$ to $f(A)$, which is a $\mathbb{F}_q$-algebra 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. $m_A(A) = 0$ by definition so $m_A(X) \subseteq \ker(\varepsilon_A)$. Since $\mathbb{F}_q[X]$ is a principal ideal domain, and the minimal polynomial is defined to be the smallest degree polynomial with A as a root, $\ker(\varepsilon_A) = (m_A(X))$. By the First Isomorphism Theorem,

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

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. A then generates the 2 dimensional commutative subalgebra of $M_2(\mathbb{F}_q)$ containing A. Let K be an arbitrary 2 dimensional subalgebra of $M_2(\mathbb{F}_q)$. Then there exists $B \in K - \mathbb{F}_q$ whose minimal polynomial is degree 2 and we must have $K = \mathbb{F}_q[B]$. All possible 2 dimensional commutative subalgebras 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 subalgebras 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 $\mathbb{F}_q[A] \cong \mathbb{F}_{q^2}$.
2. If $m_A(X)$ is reducible but not separable, define $\mathbb{F}_q[A] \cong \mathbb{F}_q \times \mathbb{F}_q$.
3. If $m_A(X)$ is separable, define $\mathbb{F}_q[A] \cong \mathbb{F}^2_{q_{nil}}$.

□

The commutative subalgebra generated when $m_A(X)$ is separable can be considered a degenerate case due to the presence of nontrivial nilpotent elements which square to 0. Since $m_A(X)$ is separable and reducible, we have $m_A(X) = (X - x)^2$ for some $x \in \mathbb{F}_q$. By the definition of the minimal polynomial, we must have that $(A - x)^2 = 0$. A is not an element of $\mathbb{F}_q$, so $A - x$ is nonzero and is therefore a nontrivial nilpotent element. It is worth noting that the case that $m_A(X)$ is both separable and irreducible does not require consideration since finite fields are perfect.

Definition 8. We refer to the two dimensional commutative subalgebras of $M_2(\mathbb{F}_q)$ as the *commutative planes* of the matrix ring.

4. Identifying maximal commutative subalgebras

We have shown that each matrix $A \in M_2(\mathbb{F}_q) - \mathbb{F}_q$ generates a commutative plane containing it, $\mathbb{F}_q[A]$, and that this plane belongs to one of three given isomorphism classes.

Since there exists subalgebras of dimension three, such as the set of upper triangular matrices, it is reasonable to ask whether this is the maximal commutative subalgebra of $M_2(\mathbb{F}_q)$ containing A.

To prove that there are no commutative subalgebras of dimension 3, and that $\mathbb{F}_q[A]$ is therefore maximal, we return to the generalized quaternions formulation. We first introduce a useful vector notation for the generalized quaternions.

Definition 9 (Generalized Quaternions, Vector Notation)**.** Let $p, q \in A_{a,b}(\mathbb{F})$. Write $p = (s, \mathbf{v})$, and $q = (t, \mathbf{w})$, using the vector notation $\mathbf{v} = \langle v_1 i, v_2 j, v_3 k\rangle$ and $\mathbf{w} = \langle w_1 i, w_2 j, w_3 k\rangle$ with coefficients in $A_{a,b}(\mathbb{F})$. Modified dot and cross product formulas compute

$$\begin{aligned}
\mathbf{v} \cdot_{a,b} \mathbf{w} &= v_1 w_1 a + v_2 w_2 b - ab v_3 w_3 \\
\mathbf{v} \times_{a,b} \mathbf{w} &= \left\langle \begin{vmatrix} v_2 j & v_3 k \\ w_2 j & w_3 k \end{vmatrix}, \begin{vmatrix} v_1 i & v_3 k \\ w_1 i & w_3 k \end{vmatrix}, \begin{vmatrix} v_1 i & v_2 j \\ w_1 i & w_2 j \end{vmatrix} \right\rangle \\
&= \langle (-v_2 w_3 + v_3 w_2) bi, (v_1 w_3 - v_3 w_1) aj, (v_1 w_2 - v_2 w_1) k\rangle
\end{aligned}$$

Compare this to $\langle v_1, v_2, v_3\rangle \times \langle w_1, w_2, w_3\rangle = \langle v_2 w_3 - v_3 w_2, -v_1 w_3 + v_3 w_1, v_1 w_2 - v_2 w_1\rangle$. Thus

$$\begin{aligned}
pq &= (st + v_1 w_1 a + v_2 w_2 b - ab v_3 w_3) + (s w_1 + t v_1 - v_2 w_3 b + v_3 w_2 b) i \\
&\quad + (s w_2 + t v_2 + v_1 w_3 a - v_3 w_1 a) j + (s w_3 + t v_3 + v_1 w_2 - v_2 w_1) k \\
&= (st + \mathbf{v} \cdot_{a,b} \mathbf{w}, s\mathbf{w} + t\mathbf{v} + \mathbf{v} \times_{a,b} \mathbf{w})
\end{aligned}$$

Lemma 10. *Let $p = (0, \mathbf{v})$, and $q = (0, \mathbf{w})$. Then $pq = qp$ if and only if $\mathbf{v} \times_{a,b} \mathbf{w} = 0$ 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 $pq - qp = 2\mathbf{v} \times_{a,b} \mathbf{w}$, and since i, j, k are linearly independent and char $k \neq 2$, $pq = qp$ if and only if $\mathbf{v} \times_{a,b} \mathbf{w} = 0$.

Additionally, setting $\langle t_1, t_2, t_3\rangle = \langle v_1, v_2, v_3\rangle \times \langle w_1, w_2, w_3\rangle$, we observe $\mathbf{v} \times_{a,b} \mathbf{w} = \langle (-bi) t_1, (-aj) t_2, (k) t_3\rangle$. Also, i, j, k are all not roots of the norm polynomial and are therefore units.

$$\begin{aligned}
N_{a,b}(i) &= i * (-i) = -a \\
N_{a,b}(j) &= j * (-j) = -b \\
N_{a,b}(k) &= k * (-k) = ab
\end{aligned}$$

Since i, j, k are units in $M_2(\mathbb{F}_q)$, they cannot be zero divisors, and we have that $\mathbf{v} \times_{a,b} \mathbf{w} = 0$ if and only if $\langle v_1, v_2, v_3\rangle \times \langle w_1, w_2, w_3\rangle = 0$, as desired. □

Theorem 11. *If $K \subseteq A_{a,b}(\mathbb{F})$ is a commutative plane, then $K = \mathbb{F}[\mathbf{w}]$ for some nonzero pure imaginary $\mathbf{w} \in A_{a,b}(\mathbb{F})$, and $\dim_{\mathbb{F}} K = 2$.*

Proof. If $q = (t, \mathbf{w}) \in K - \mathbb{F}$, then $q - t = \mathbf{w}$ is in $\mathbb{F}[q]$, hence $\mathbb{F}[\mathbf{w}] = \mathbb{F}[q] \subseteq K$. If $p = (s, \mathbf{v}) \in K$ then since $pq = qp$, $\mathbf{v}$ is a scalar multiple of $\mathbf{w}$ by Lemma 10. Therefore, $K \subseteq \mathbb{F}[\mathbf{w}]$. It follows that $K = \mathbb{F}[\mathbf{w}]$. Finally, since $w \notin \mathbb{F}$, we must have $m_{\mathbf{w}}(X) = p_{\mathbf{w}}(X)$, so $\deg(m_{\mathbf{w}}(X)) = 2$ and this completes the proof. □

Now, $A_{a,b}(\mathbb{F}_q) \cong M_2(\mathbb{F}_q)$, so Theorem 11 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 12. *$M_2(\mathbb{F}_q)$ has q^2+q+1 unique commutative planes.*

Proof. By Theorem 11, each commutative plane is of the form $\mathbb{F}_q[\mathbf{w}]$ for some pure imaginary $\mathbf{w} \in M_2(\mathbb{F}_q)$, and is therefore uniquely determined by the line $\mathbb{F}_q\mathbf{w}$ by Lemma 10. The number of commutative planes is then the same as the number of pure imaginary lines through the origin. Since there are q^3-1 choices of pure imaginaries in $M_2(\mathbb{F}_q)$ and $\mathbf{w}$ has $q-1$ nonzero scalar multiples in $\mathbb{F}_q$, there must then be

$$\frac{q^3-1}{q-1} = q^2+q+1$$

unique commutative planes in $M_2(\mathbb{F}_q)$. □

Lemma 13. *Consider the following elements of $M_2(\mathbb{F}_q)$.*

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

Let $\mathcal{O}_x, \mathcal{O}_Y$ denote the orbits of x, y under the conjugation action of $GL_2(\mathbb{F}_q)$ on $M_2(\mathbb{F}_q)$. Then

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

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 [3, pg. 114]. Now

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

Since matrix multiplication is distributive, 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 11). 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 $t=\pm s$. This eliminates the q scalar multiples of $x+I$ and the q scalar multiples of $x-I$, of which only 0 is shared between them. We have thus found precisely $q^2-2q+1=(q-1)^2$ elements of G_x. It follows that

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

where $[GL_2(\mathbb{F}_q) : G_x]$ is the index of G_x in $GL_2(\mathbb{F}_q)$. By the Orbit-Coset Correspondence Theorem 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 14. *The orbits of the commutative planes in $M_2(\mathbb{F}_q)$ under the conjugation action of $GL_2(\mathbb{F}_q)$ are precisely the three isomorphism classes of planes.*

Proof. Let K, K' be commutative planes in $M_2(\mathbb{F}_q)$ such that $K \cong K'$. That is, K, K' are the same plane type. Let $A \in K$, $B \in K'$ be nonzero elements orthogonal to the identity. Then $K = \mathbb{F}_q[A]$, $K' = \mathbb{F}_q[B]$ and

$$m_A(X) = p_A(X) = X^2 + \alpha$$
$$m_B(X) = p_B(X) = X^2 + \beta$$

where $\alpha = \det(A)$, $\beta = \det(B)$. Furthermore, we must have that $\alpha\mathbb{F}_q^{\times 2} = \beta\mathbb{F}_q^{\times 2}$ since K, K' belong to the same plane type. It follows that there exists $\delta \in \mathbb{F}_q^\times$ such that $\alpha = \delta^2\beta$. Let $C = \delta B$. Then C is a nonzero element of K' orthogonal to the identity with $\mathbb{F}_q[C] = \mathbb{F}_q[B] = K'$ and

$$\det(C) = \det(\delta I)\det(B) = \delta^2\beta = \alpha$$

and we have that $m_A(X) = m_C(X) = X^2 + \alpha$. Therefore

$$\begin{pmatrix} 0 & -\alpha \\ 1 & 0 \end{pmatrix}$$

is the rational canonical form for both A and C. Two matrices in $M_2(\mathbb{F})$ conjugate if and only if they have the same rational canoncial form [3, pg. 476]. Therefore A and C are conjugate, so the commutative planes $K = \mathbb{F}_q[A]$ and $K' = \mathbb{F}_q[C]$ are conjugate.

We have thus shown that two commutative planes are conjugate if they are of the same isomorphism class. We also know that two conjugate commutative planes are isomorphic, so we may conclude that the orbits of the commutative planes of $M_2(\mathbb{F}_q)$ under the conjugation action of $GL_2(\mathbb{F}_q)$ are precisely the three isomorphism classes, as desired. □

Theorem 15. *The size of the orbits of the commutative planes in $M_2(\mathbb{F}_q)$ under the conjugation action of $GL_2(\mathbb{F}_q)$ are as follows Maybe should continue using the orbit notation?*

$$|[\mathbb{F}_{q^2}]| = \binom{q}{2} \tag{1}$$

$$|[\mathbb{F}_q \times \mathbb{F}_q]| = \binom{q+1}{2} \tag{2}$$

$$|[\mathbb{F}^2_{q_{nil}}]| = q + 1 \tag{3}$$

Proof. The elements x, y from Lemma 13 are the rational canonical forms for all matrices with minimal polynomials $X^2 - 1$ and X^2 respectively. Note again that two matrices in $M_2(\mathbb{F})$ are conjugate if and only if they have the same rational canonical form.

Since $X^2 - 1 = (X+1)(X-1)$ is reducible and not separable over $\mathbb{F}_q$, and $\operatorname{char}(\mathbb{F}_q) \neq 2$, all of the elements of $\mathcal{O}_x$ generate a commutative plane isomorphic to $\mathbb{F}_q \times \mathbb{F}_q$.

Any copy of $K \subseteq M_2(\mathbb{F}_q)$ isomorphic to $\mathbb{F}_q \times \mathbb{F}_q$ must also contain an element of $\mathcal{O}_x$. To see this, pick a nontrivial element $A \in K$ such that A is orthogonal to the identity. Then $\operatorname{tr}(A) = 0$, and $m_A(X) = p_A(X) = X^2 + \det(A)$. We picked $A \in K$, 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 $B = A/\lambda \in K$ and observe $\operatorname{tr}(B) = \operatorname{tr}(A)/\lambda = 0$, $\det(B) = \det(A)/\lambda^2 = -\lambda^2/\lambda^2 = -1$. Therefore, $m_B(X) = p_B(X) = X^2 - \operatorname{tr}(B)X + \det(B) = X^2 - 1$ as desired.

Furthermore, suppose $B' \in K$ 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 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 possible choice of K contains exactly 2 elements of $\mathcal{O}_x$. Applying Lemma 13, notational abuse here replacing K with $\mathbb{F}_q \times \mathbb{F}_q$.

$$|[\mathbb{F}_q \times \mathbb{F}_q]| = \frac{1}{2}|\mathcal{O}_x| = \frac{q(q+1)}{2} = \binom{q+1}{2}$$

Similarly, since X^2 is separable over $\mathbb{F}_q$, all of the elements of $\mathcal{O}_y$ generate a commutative subalgebra isomorphic to $\mathbb{F}^2_{q_{nil}}$. Any isomorphic copy K will contain exactly $q-1$ elements of $\prime_y$. These are precisely the nontrivial elements of K that are orthogonal to the identity. Applying Lemma 13,

$$|[\mathbb{F}^2_{q_{nil}}]| = \frac{1}{q-1}|\mathcal{O}_x| = \frac{q^2-1}{q-1} = q+1$$

To show $|[\mathbb{F}_{q^2}]| = \binom{q}{2}$, we apply Theorem 12 and compute.

$$\begin{aligned}
|[\mathbb{F}_{q^2}]| &= q^2 + q + 1 - |[\mathbb{F}_q \times \mathbb{F}_q]| - |[\mathbb{F}^2_{q_{nil}}]| \\
&= q^2 + q + 1 - \binom{q+1}{2} - (q+1) \\
&= q^2 - \frac{q(q+1)}{2} \\
&= \frac{q(q-1)}{2} \\
&= \binom{q}{2}
\end{aligned}$$

This completes the proof. □

From Theorem 15 we can also find the limiting ratios of these commutative planes

Corollary 16. *As $q \to \infty$, the ratio of commutative subalgebras of $M_2(\mathbb{F}_q)$*

$$|[\mathbb{F}_{q^2}]| : |[\mathbb{F}_q \times \mathbb{F}_q]| : |[\mathbb{F}^2_{q_{nil}}]|$$

approaches $1 : 1 : 0$.

Proof. It suffices to show that the limit of $|[\mathbb{F}_{q^2}]|/|[\mathbb{F}_q \times \mathbb{F}_q]|$ approaches 1 and that the limit of $|[\mathbb{F}^2_{q\,nil}]|/|[\mathbb{F}_q \times \mathbb{F}_q]|$ approaches 0. cite something here?

$$\lim_{q\to\infty} \frac{|[\mathbb{F}_{q^2}]|}{|[\mathbb{F}_q \times \mathbb{F}_q]|} = \lim_{q\to\infty} \frac{\binom{q}{2}}{\binom{q+1}{2}} = \lim_{q\to\infty} \frac{q(q-1)}{2}\frac{2}{q(q+1)} = \lim_{q\to\infty} \frac{(q-1)}{(q+1)} = 1$$

$$\lim_{q\to\infty} \frac{|[\mathbb{F}^2_{q\,nil}]|}{|[\mathbb{F}_q \times \mathbb{F}_q]|} = \lim_{q\to\infty} \frac{q+1}{\binom{q+1}{2}} = \lim_{q\to\infty} (q+1)\cdot\frac{2}{q(q+1)} = \lim_{q\to\infty} \frac{2}{q} = 0$$

□

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.