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 sub-algebras 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, 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 $\mathbb{P}_q^n$, the Grassmannian, and further generalizations.

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

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

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

(1) A's characteristic polynomial: $p_A(X) = X^2 - \mathrm{tr}(A)X + \det(A)$.
(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, then $\mathbb{F}_q[A] \cong \mathbb{F}_q^2$
(2) If $m_A(X)$ is reducible but not separable, then $\mathbb{F}_q[A] \cong \mathbb{F}_q \times \mathbb{F}_q$
(3) If $m_A(X)$ is separable, then $\mathbb{F}_q[A] \cong \mathbb{F}_{q_{nil}}^2$ the degenerate nilpotent case.

Date: May 14, 2021.

3. Identifying maximal commutative sub-algebras

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 sub-algebra's of dimension 3. The set of all upper triangular matrices is one such example.

To address this we state, but do not prove, a related result by Jacobson.

Theorem (Jacobson [1])**.** For an arbitrary field k, the maximum number $N(n)$ of linearly independent commutative matrices of n rows and columns is given by the formula $N(n) = \lfloor n^2/4 \rfloor + 1$.

In the case of $M_2(\mathbb{F}_q)$, $n = 2$ and we have that $N(2) = \lfloor 2^2/4 \rfloor + 1 = 2$. Therefore, these planes containing A are indeed maximal.

4. Plane Counts

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

Proof outline notes:

- Each plane has q^2 elements.
- Each plane shares the q elements of $\mathbb{F}_q$.
- Each plane has trivial intersection.
- The planes cover all of $M_2(\mathbb{F}_q)$.

Proof. Let E_x for $x \in M_2(\mathbb{F}_q) - \mathbb{F}_q$ be the commutative subalgbra created by the span of 1 and x. Label $N = |\{E_x \mid x \in M_2(\mathbb{F}_q) - \mathbb{F}_q\}|$.

$$\begin{aligned} N(q^2 - q) + q &= q^4 \\ N(q-1) + 1 &= q^3 \\ N(q-1) &= q^3 - 1 \\ N &= q^2 + q + 1 \end{aligned}$$

□

Lemma 2. *Let k be a field such that $\left[k : k^{\times 2}\right] = 2$ and $A \in M_2(k)$. Define $S = \{\det(\lambda A) \mid \lambda \in k^\times\}$.*

$$S = \begin{cases} \{0\} & \text{if } \det(A) = 0 \\ k^{\times 2} & \text{if } \det(A) \in k^{\times 2} \\ k^\times - k^{\times 2} & \text{if } \det(A) \in k^\times - k^{\times 2} \end{cases}$$

Proof. Let $A \in M_2(k)$. Then $\det(\lambda A) = \det(\lambda I)\det(A) = \lambda^2 \det(A)$ where $\lambda \in k$. If $\det(A) = 0$, then $\det(\lambda A) = 0$ for $\lambda \in k$ and $S = \{0\}$ follows. Otherwise, we know that the quotient group $k^\times / k^{\times 2}$ has only the two cosets $k^{\times 2}, k^\times - k^{\times 2}$. So if $\det(A) \in k^{\times 2}$, we have $S = \{\lambda^2 \det(A) \mid \lambda \in k^\times\} = k^{\times 2}$ and similarly, if $\det(A) \in k^\times - k^{\times 2}$, then $S = \{\lambda^2 \det(A) \mid \lambda \in k^\times\} = k^\times - k^{\times 2}$. □

Lemma 3. *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 requires result citation/prior inclusion. 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 should cite/include prior 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 4.

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

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

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

Proof. The elements x, y from lemma 3 are the rational canonical forms for all matrices with minimum polynomials $X^2 - 1$ and X^2 respectively.

Since $X^2 - 1 = (X+1)(X-1)$ in $M_2(\mathbb{F}_q)$ and $\mathrm{char}(\mathbb{F}_q) \neq 2$ this must be included in the introductory sections, all of the elements of $\mathcal{O}_x$ belong to an embedding of $\mathbb{F}_q \times \mathbb{F}_q$. Additionally any embedding of $\mathbb{F}_q \times \mathbb{F}_q$ must be of this form...

Now, referring to lemma 2 we know that each plane isomorphic to $\mathbb{F}_q \times \mathbb{F}_q$

By theorem 1, ... $\square$

References

[1] Nathan Jacobson, *Schur's Theorems on Commutative Matrices*, Bull. Amer. Math. Soc. **50** (1944), 431–436.