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 $M_2(\mathbb{F}_q)$

Need to include information here about the different plane types and how to determine the plane type based on the minimum polynomial of a nontrivial element of the plane.

3. IDENTIFYING MAXIMAL COMMUTATIVE SUB-ALGEBRAS

Include theorem from Jacobson paper.

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 subalgebra created by the span of 1 and x. Label $N = |\{E_x \mid x \in M_2(\mathbb{F}_q) - \mathbb{F}_q\}|$.

$$N(q^2 - q) + q = q^4$$
$$N(q - 1) + 1 = q^3$$
$$N(q - 1) = q^3 - 1$$
$$N = q^2 + q + 1$$

$\square$

Date: April 30, 2021.

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 $S = \{\lambda^2 \det(A) \mid \lambda \in k^\times\} = k^\times - k^{\times 2}$. $\qquad\square$

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 $G_y = \{A \in GL_2(\mathbb{F}_q) \mid Ay = yA\}$ 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.

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

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

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

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 $\operatorname{char}(\mathbb{F}_q) \neq 2$ 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 cite previous lemma using Cref later we know that each plane...

By theorem 1, ... □