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 $\mathbb{P}^n_q$, the Grassmannian, and further generalizations.

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

2. Identifying maximal commutative sub-algebras

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

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 $N = |\{E_x \mid x \in M_2(\mathbb{F}_q) - \mathbb{F}_q\}|$.

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

A 2D commutative subalgebra E must be such that $|E| = p^2$ and $\mathbb{F}_q \subseteq E$. ∎

Date: April 30, 2021.

Lemma 2. *Let* $A \in M_2(k)$. *Let* $S = \det(kA)$. *Then*

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

Proof. Let $A \in M_2(k)$. Then $\det(\lambda A) = \det(\lambda I)\det(A) = \lambda^2 \det(A)$ where $\lambda \in k$.

Case (1) Suppose $\det(A) = 0$. Then $\lambda^2 \det(A) = 0$ for all $\lambda \in k$ and we have $S = 0$.

Case (2) Suppose $\det(A) = \alpha^2$ where $\alpha \in k^{\times}$. Then $\lambda^2 \det(A) = \lambda^2\alpha^2 = (\lambda\alpha)^2 \in {k^{\times}}^2$. It follows that $S \subseteq {k^{\times}}^2$. Now, let $\sigma \in k^{\times}$. Then $\det(\frac{\sigma}{\alpha}A) = \frac{\sigma^2}{\alpha^2}\alpha^2 = \sigma^2$. So $\sigma^2 \in S$ and we have shown ${k^{\times}}^2 \subseteq S$. Therefore, $S = {k^{\times}}^2$.

Case (3) Suppose $\det(A) = \beta$ where $\beta \in k^{\times} - {k^{\times}}^2$. Then $\lambda^2 \det(A) = \lambda^2\beta \in k^{\times} - {k^{\times}}^2$. It follows that $S \subseteq k^{\times} - {k^{\times}}^2$. Since $|k^{\times}/{k^{\times}}^2| = 2$, if $\sigma, \gamma \notin {k^{\times}}^2$, we know there exists $\lambda \in k^{\times}$ such that $\sigma\lambda^2 = \gamma$. So $k^{\times} - {k^{\times}}^2 \subseteq S$ is clear and we have shown $S = k^{\times} - {k^{\times}}^2$.

∎

Theorem 3. *This is a theorem.*

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

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

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

Proof. We shall consider the conjugation action of $GL_2(\mathbb{F}_q)$ on $M_2(\mathbb{F}_q)$ for the matrices,

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

These are the rational canonical forms for matrices with minimum polynomials $X^2 - 1$ and X^2 respectively. We want to compute the size of their orbits, G_x, G_y, using the orbit coset correspondence theorem. Now,

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

Clearly, matrices of the form $sx + tI$ 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 these 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,

$$[G : G_x] = \frac{(q^2-1)(q^2-q)}{(q-1)^2} = q(q-1)$$

By the orbit coset correspondence theorem should cite/include prior we have that $\#\,\mathrm{orbit}(x) = q(q+1)$

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 $q^2 - q = q(q-1)$ elements of G_y. Therefore,

$$[G : G_y] = \frac{(q^2-1)(q^2-q)}{q^2-1} = q(q-1)$$

and we have $\#orbit(y) = q^2 - 1$

Now, referring to cite previous lemma using Cref later we know that each plane

□