# An Abstract of the Thesis of 

Geoffrey Critzer for the Master's of Science in Mathematics presented on April 18, 2018 .

## Title Combinatorics of Vector Spaces over Finite Fields

Thesis Chair Daniel J. Miller


#### Abstract

Approved $\qquad$

Abstract In this writing we examine some known results concerning exact enumeration of vector spaces whose underlying fields are finite. We explore some of the many interesting analogies between subsets and subspaces. We derive some q-analogue identities and theorems. We link these results to some previously existing, as well as some newly added, sequences in the On Line Encyclopedia of Integer Sequences, OEIS. We give generating functions, formulas, recurrences, and Mathematica code that count various statistics concerning vector spaces over finite fields, linear operators, and subspace lattices.


Keywords $q$-binomial coefficient, $q$-exponential function, finite field, generating function, group action, general linear group.

# Combinatorics of Vector Spaces over Finite Fields 

A Thesis
Presented to
The Department of Mathematics and Economics EMPORIA STATE UNIVERSITY

In Partial Fulfillment
of the Requirements for the Degree
Master's of Science
by
Geoffrey Critzer
May 2018

Approved by the Department Chair

Approved by the Dean of the Graduate School and Distance Education

## Contents

1 Introduction ..... 1
2 The Number of Vectors in an $n$-Dimensional Vector Space over $\mathbb{F}_{q}$ ..... 2
3 The Number of Linearly Independent Lists of Vectors in $\mathbb{F}_{q}^{n}$. ..... 3
4 The Number of Subspaces of $\mathbb{F}_{q}^{n}$. ..... 8
5 The Number of $m \times n$ Matrices of a Given Rank with Entries in $\mathbb{F}_{q}$ ..... 11
6 A Closer Look at the $q$-Binomial Coefficients. ..... 23
7 A Group Theoretical Derivation of the $q$-Binomial Coefficients ..... 29
8 A Derivaton of the q-Binomial Coefficients via Generating Functions ..... 31
9 The Rogers-Szego polynomials ..... 38
10 Flags in Finite Vector Spaces ..... 41
11 The $q$-analog of the Exponential Function ..... 44
12 Direct Sum Decompositions ..... 49
13 The Number of $n \times n$ Diagonalizable Matrices ..... 55
14 Subgroups of $G L_{n}\left(\mathbb{F}_{q}\right)$ ..... 64
15 Subgroups of $G L_{n}\left(\mathbb{Z}_{m}\right)$ ..... 78

## List of Tables

$1 \quad\left((n)_{k}\right)_{2}$, Number of $k$-Tuples of Linearly Independent Vectors in $\mathbb{F}_{2}^{n}$ for $n \geq 0$ and $0 \leq k \leq n$. A2882535

2 Number of $n$-permutations having $k$ inversions for $n \geq 0,0 \leq k \leq\binom{ n}{2}$. A008302
$4 \quad \gamma_{n}(2)$ for $n \geq 0$. (The order of $\left.\mathrm{GL}_{n}\left(\mathbb{F}_{2}\right)\right) . A 002884 \ldots . . . . . . .$.
for $0 \leq k \leq n, n \geq 0$46

15 Number of ways to choose a $k$-dimensional subspace of a subspace of $\mathbb{F}_{3}^{n}$, for $0 \leq k \leq n, n \geq 0$47
16 Number of flags in $\mathbb{F}_{q}^{n}$ for $n \geq 0$. A289545 ..... 47
17 Number of flags of length m in $\mathbb{F}_{q}^{n}$ for $0 \leq m \leq n, n \geq 0$. A289946 ..... 48
18 Number of chains in $\mathbb{F}_{q}^{n}$ for $n \geq 0$. A293844 ..... 48
19 Number of chains of length k in $\mathbb{F}_{q}^{n}$ for $0 \leq k \leq n, n \geq 0$. A293845 ..... 49
2021$0 \leq k \leq n, n \geq 0 . \mathrm{A} 270880$51
22 Number of direct sum decompositions of $\mathbb{F}_{2}^{n}$, having exactly $k$ subspacesof dimension 1 for $0 \leq k \leq n, n \geq 0$. A28954451
23 number of direct sum decompositions of $\mathbb{F}_{q}^{n}$ into subspaces of dimension at $\operatorname{most} k, 1 \leq k \leq n$. A298561 ..... 52

number of direct sum decompositions of $\mathbb{F}_{2}^{n}$ with maximal subspace of di
mension $k, 1 \leq k \leq n$. A298399 ..... 52
Number of ordered direct sum decompositions of $\mathbb{F}_{2}^{n}$ for $n \geq 0$ ..... 53
Number of ordered direct sum decompositions of $\mathbb{F}_{2}^{n}$ containing exactly $k$subspaces for $1 \leq k \leq n, n \geq 0$.53
Number of direct sum decompositions of $\mathbb{F}_{2}^{n}$ containing a given nonzerovector for $n \geq 1$. A27088355Number of direct sum decompositions of $\mathbb{F}_{2}^{n}$ that contain a given nonzerovector and that contain exactly $k$ subspaces for $1 \leq k \leq n, n \geq 1$. A270882 55
Number of $n \times n$ diagonalizable matrices over $\mathbb{F}_{q}$ for $n \geq 0$. A132186 ..... 57
Number of $n \times n$ diagonalizable matrices over $\mathbb{F}_{3}$ for $n \geq 0$. A290516 ..... 57
Number of $n \times n$ diagonalizable operators $T$ over $\mathbb{F}_{2}$ such that range $(T)=$$k$ for $0 \leq k \leq n, n \geq 0$. A29654858
32
$k$ for $0 \leq k \leq n, n \geq 0 . \mathrm{A} 297892$ ..... 58
Number of $n \times n$ projections over $\mathbb{F}_{3}$ for $n \geq 0$. A053846 ..... 60
Number of $n \times n$ matrices over $\mathbb{F}_{3}$ that are invertible and diagonalizable for$n \geq 0$. A05384660
Number of $n \times n$ diagonalizable matrices over $\mathbb{F}_{3}$ having $k$ distinct eigen- values $0 \leq k \leq 3, n \geq 0$. A296605 ..... 61
Order of $P G L_{n}\left(\mathbb{F}_{3}\right)$ for $n \geq 1$. A003787 ..... 72
Order of $P G L_{n}\left(\mathbb{F}_{4}\right)$ for $n \geq 1$. A003788 ..... 72
Order of $P S L_{n}\left(\mathbb{F}_{3}\right)$ for $n \geq 1$. A003793 ..... 76
Order of $G L_{n}\left(\mathbb{Z}_{4}\right)$ for $n \geq 0$. A065128 ..... 82
Order of $G L_{n}\left(\mathbb{Z}_{6}\right)$ for $n \geq 0$. A065498 ..... 83
41 Order of $G L_{2}\left(\mathbb{Z}_{m}\right)$ for $m \geq 1$. A000252 ..... 83

43 Order of $S L_{2}\left(\mathbb{Z}_{m}\right)$ for $m \geq 1$. A000056
$44 \quad$ Order of $S L_{3}\left(\mathbb{Z}_{m}\right)$ for $m \geq 1$. A011785
45 Order of $P S L_{2}\left(\mathbb{Z}_{m}\right)$ for $m \geq 1$. A300915 87

## 1. Introduction

The Euclidian space, $\mathbb{R}^{n}$, is oftentimes held up as the quintessential example of a vector space. However, the consideration of vector spaces over finite fields is not only a serious endeavor for both pure and applied mathematicians but also provides a veritable playground for the recreational combinatorialist. In [11], Joseph Gallian states that "finite fields were first introduced by Galois in 1830 in his proof of the unsolvability of quintics. When Cayley invented matrices a few decades later, it was natural to investigate groups of matrices over finite fields." Today, finite matrices over finite fields are studied extensively. They play a very important role in the theory of finite groups. They have applications in "computer science, coding theory, information theory, and cryptography" [11]. It is also asserted in [11] (albeit without proof) that yet another important reason for researching vector spaces over finite fields is that "they are just plain fun!".

In this writing we examine some known results concerning exact enumeration of characteristics associated with vector spaces whose underlying fields are finite. We explore some of the many interesting analogies between subsets of $n$-element sets and subspaces of $n$-dimensional vector spaces. We derive some $q$-analogue identities, expressions and theorems. We link these results to some previously existing, as well as some newly added, sequences in the On Line Encyclopedia of Integer Sequences, OEIS. We give generating functions, formulas, recurrences, and Mathematica code that count various statistics concerning vector spaces over finite fields, linear operators, and subspace lattices. We examine some group properties of a finite dimensional vector space over a finite field, exposing it as an elementary abelian group.

In particular, we derive the probability generating function for the probability (in the limit as $n \rightarrow \infty$ ) that a random linear operator $T$ on an $n$-dimensional vector space over a field with $q$ elements is such that dim null $T=j$ for $j \in\{0,1,2, \ldots\}$. We give an original
proof of a well known recurrence defining the Galois numbers. We give a bijection between the number of diagonalizable $n \times n$ matrices with entries in $\mathbb{F}_{q}$ and the number of weak decompositions of $\mathbb{F}_{q}$ into exactly $q$ subspaces. We determine the order of some interesting subgroups of the general linear group as well as some subgroups of the group of invertible matrices over the ring of integers modulo $m$.

An underlying theme of this thesis is to demonstrate the pleasantly "surprising efficiency of generating functions in combinatorial enumeration problems" associated with vector spaces. The quote is from Flajolet and Sedgwick's, Analytic Combinatorics [9], where a "symbolic method" for deriving counting generating functions is determined, along with a "systematic translation mechanism between combinatorial constructions and operations on generating functions". Throughout this thesis we employ the calculus of generating functions developed in [9] to derive, with much economy of thought, generating functions that enumerate many interesting questions we may ask about linear mappings on a vector space whose underlying field has only finitely many elements.

## 2. The Number of Vectors in an $n$-Dimensional Vector Space over $\mathbb{F}_{q}$

A field is a set along with two operations satisfying a handful of axioms. A finite field containing $q$ elements exists if and only if $q$ is a prime power, meaning that $q=p^{n}$ for some prime integer $p$ and positive integer $n$; C.f. [3]. Moreover, if $q$ is a prime power, then up to isomorphism, there is exactly one field of size $q$. This field is denoted by $\mathbb{F}_{q}$.

A vector space is an Abelian group acted upon by a field satisfying a handful of axioms. A nonzero finite dimensional vector space over an infinite field contains infinitely many vectors. A finite dimensional vector space over a finite field contains finitely many vectors and we are compelled to count them. Since every $n$-dimensional vector space over $\mathbb{F}_{q}$ shares the same isomorphism class, we can resign ourselves to count statistics related to
the coordinate vector space $\mathbb{F}_{q}^{n}=\left\{\left(a_{1}, \ldots, a_{n}\right): a_{i} \in \mathbb{F}_{q} \forall i=1, \ldots, n\right\}$ without any loss of generality, and we shall do so throughout this paper. However, the reader should note that since all of our results depend only on the isomorphism classes of our vector spaces, any of our theorems formulated for $\mathbb{F}_{q}^{n}$ may be freely applied to any vector space over $\mathbb{F}_{q}$ of dimension $n$. Thus the notation $\mathbb{F}_{q}^{n}$ merely serves as a compact way of denoting the dimension of the vector space and the size of the field of scalars under consideration.

Theorem 2.1. The number of vectors in $\mathbb{F}_{q}^{n}$ is equal to $q^{n}$ for any $n \geq 1$.
Proof. There are $q$ elements in the field $\mathbb{F}_{q}$. To form a coordinate vector, i.e., an $n$-tuple of field elements, we make $n$ independent choices for a field element. So by the product rule there are $q^{n}$ vectors in $\mathbb{F}_{q}^{n}$.

## 3. The Number of Linearly Independent Lists of Vectors in $\mathbb{F}_{q}^{n}$.

In this section we describe a very well known and rudimentary method of counting the number of bases of a $k$-dimensional subspace in an $n$-dimensional vector space. We define the $q$-number and the $q$-factorial. We follow [14] to show that the $q$-factorial is the polynomial generating function counting the number of $n$-permutations having a specified number of inversions.

A basis for a $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$ is an ordered list (tuple) of $k$ linearly independent vectors in $\mathbb{F}_{q}^{n}$. Each linearly independent list of $k$ vectors in $\mathbb{F}_{q}^{n}$ corresponds to exactly one basis of a $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$. So the number of bases over all the $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ is precisely the number of $k$-tuples, $\left(v_{1}, v_{2}, \ldots, v_{k}\right)$ of linearly independent vectors in $\mathbb{F}_{q}^{n}$.

Definition 3.1. The number of length $k$ linearly independent lists of vectors in $\mathbb{F}_{q}^{n}$ is called the $q$-falling factorial number and is denoted $\left((n)_{k}\right)_{q}{ }^{1}$.

[^0]To form a list of $k$ linearly independent vectors in $\mathbb{F}_{q}^{n}$ we may choose the first vector, $v_{1}$, from any of the $q^{n}$ vectors in $\mathbb{F}_{q}^{n}$ except for the zero vector. This means we have $q^{n}-1$ choices for $v_{1}$. The second vector, $v_{2}$, must be linearly independent from $v_{1}$. In other words, $v_{2}$ must not be in the span of $v_{1}$. Since there are $q$ elements in $\mathbb{F}_{q}$, then there are $q$ scalar multiples of $v_{1}$. So there are $q$ vectors in span $v_{1}$. So there are $q^{n}-q$ choices for $v_{2}$. Now $v_{3}$ must be chosen from the vectors that are not in $\operatorname{span}\left(v_{1}, v_{2}\right)$. In other words, $v_{3}$ must not be a linear combination of $v_{1}$ and $v_{2}$. That is, $v_{3}$ must not be of the form $a_{1} v_{1}+a_{2} v_{2}$ where $a_{1}, a_{2}$ are in $\mathbb{F}_{q}$. There are $q$ possibilities for the scalar $a_{1}$ and $q$ possibilities for the scalar $a_{2}$. So there are $q^{2}$ vectors in $\operatorname{span}\left(v_{1}, v_{2}\right)$. So there are $q^{n}-q^{2}$ choices for $v_{3}$. Continuing in this manner, noting that each of the subsequent vectors in our $k$-tuple must avoid the span of all previously chosen vectors, we see that there are $\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)$ ways to form such a k-tuple of vectors.

Theorem 3.2 ([8]). The number $\left((n)_{k}\right)_{q}$ of length $k$ linearly independent lists of vectors in $\mathbb{F}_{q}^{n}$ is equal to $\prod_{i=0}^{k-1}\left(q^{n}-q^{i}\right)$.

Proof. To form such a list $\left(v_{1}, v_{2}, \ldots, v_{k}\right)$ we make $k$ independent choices of vectors in $\mathbb{F}_{q}^{n}$ so that $v_{j} \notin \operatorname{span}\left(v_{1}, \ldots, v_{j-1}\right)$ for all $j \in\{1, \ldots, k\}$. By theorem 2.1, there are $q^{j-1}$ vectors in $\operatorname{span}\left(v_{1}, \ldots, v_{j-1}\right)$. So there are $\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)=\prod_{i=0}^{k-1}\left(q^{n}-q^{i}\right)$ $k$-tuples of vectors that may serve as a basis of a $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$.

The number $\left((n)_{k}\right)_{q}$ of linearly independent $k$-tuples of vectors in $\mathbb{F}_{q}^{n}$ for the case $q=2$ is shown in Table 1. This table is indexed for $n \geq 1,0 \leq k \leq n$. It is given in OEIS as sequence A288853.
$\overline{\left((n)_{k}\right)_{q}}$ is neither a falling factorial of a falling factorial nor is it technically a $q$-analog of $(n)_{k}$. [4]


Table 1: $\left((n)_{k}\right)_{2}$, Number of $k$-Tuples of Linearly Independent Vectors in $\mathbb{F}_{2}^{n}$ for $n \geq 0$ and $0 \leq k \leq n$. A288253

These numbers may be thought of as being analogous to the falling factorials (A008279). The falling factorial $(n)_{k}=\frac{n!}{(n-k)!}$ counts the number of ways to order (list) $k$ elements contained in an $n$-set. In other words, $(n)_{k}=\frac{n!}{(n-k)!}$ is the number of injective functions from a $k$-set into an $n$-set. In section 4 we will show that $\left((n)_{k}\right)_{q}$ is also the number of injective linear maps from $\mathbb{F}_{q}^{k}$ into $\mathbb{F}_{q}^{n}$ which further illustrates the analogy with the falling factorials. We will also show in section 4 that this is the number of surjective linear maps from $\mathbb{F}_{q}^{n}$ onto $\mathbb{F}_{q}^{k}$.

From our derivation above we have that

$$
\left((n)_{k}\right)_{q}=\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right) .
$$

It is sometimes convenient to represent this quantity as

$$
\left((n)_{k}\right)_{q}=q^{\binom{k}{2}}\left(q^{n}-1\right)\left(q^{n-1}-1\right) \cdots\left(q^{n-k+1}-1\right)
$$

where we have factored a $q$ from the second factor, two $q$ 's from the third factor, and $\ldots$, and
$(k-1) q$ 's from the last factor. Also we define for natural numbers $n \geq 1$, the $q$-number,

$$
[n]_{q}=1+q+\cdots+q^{n-1}=\frac{1-q^{n}}{1-q}
$$

and the $q$-factorial

$$
[n]_{q}!=[n]_{q}[n-1]_{q} \cdots[1]_{q}[0]_{q}=\prod_{i=1}^{n} \frac{1-q^{i}}{1-q}
$$

where $[0]_{q}:=1$. So that

$$
\left((n)_{k}\right)_{q}=\frac{(q-1)^{k} q^{\binom{k}{2}}[n]_{q}!}{[n-k]_{q}!},
$$

where we may note the similarity to the expression for the falling factorial numbers.
Now we want to view the aforementioned $q$-factorial as a polynomial generating function. Let us denote the coefficient of $q^{r}$ in $[n]_{q}!$ by $\left[\left[q^{r}\right]\right][n]_{q}$ !.

Definition 3.3. The symmetric group on $n$ letters denoted by $S_{n}$ is the group of bijective functions on $\{1,2, \ldots, n\}$. An $n$-permutation is an ordered list of length $n$ containing each of the elements in $\{1,2, \ldots, n\}$ exactly once and hence represents an element of $S_{n}$.

Definition 3.4. Let $\pi=\left(a_{1}, a_{2}, \ldots, a_{n}\right)$ be an $n$-permutation. An inversion in $\pi$ is an ordered pair $\left(a_{i}, a_{j}\right)$ such that $i<j$ but $a_{i}>a_{j}$.

We claim that the number of $n$-permutations having exactly $r$ inversions is equal to $\left[\left[q^{r}\right]\right][n] q!$. The proof below is adapted from Theorem 1 in [14]. First we first give a specific example of the natural correspondence between the contributions to the coefficient of $q^{r}$ in $\prod_{i=1}^{n} \frac{1-q^{i}}{1-q}$ and the permutations of $\{1,2, \ldots, n\}$ having $r$ inversions.

Say $n=5$ and $r=7$. Consider the permutation (3,5,4,1,2) having 7 inversions and the
monomial $1 \cdot 1 \cdot q^{2} \cdot q^{2} \cdot q^{3}$ contributing to the coefficient of $q^{7}$ in the expansion of

$$
(\mathbf{1})(\mathbf{1}+q)\left(1+q+\mathbf{q}^{2}\right)\left(1+q+\mathbf{q}^{2}+q^{3}\right)\left(1+q+q^{2}+\mathbf{q}^{3}+q^{4}\right)
$$

The exponent of the boldfaced term in each of the five polynomial factors corresponds to the number of inversions in the permutation $(3,5,4,1,2)$ resulting from the five integers $1,2,3,4,5$ respectively. For example, $\mathbf{q}^{3}$ in the fifth polynomial factor signifies that there are exactly 3 entries in our permutation to the right of 5 that are less than 5 .

Theorem 3.5 ([14]). The generating function counting the number of n-permutations having exactly $r$ inversions is the $q$-factorial, $[n] q!$. More precisely, if $\operatorname{inv}(\pi)$ is the number of inversions of the permutation $\pi \in S_{n}$ then $\sum_{\pi \in S_{n}} q^{i n v(\pi)}=\prod_{i=1}^{n} \frac{1-q^{i}}{1-q}$.

Proof. The proof is by induction on $n$.
Basis step: If $n=1$, then both sides give the constant polynomial 1 .
Induction step: Let $n \geq 1$. Assume that $\sum_{\pi \in S_{n-1}} q^{i n v(\pi)}=\prod_{i=1}^{n-1} \frac{1-q^{i}}{1-q}$. An $n$-permutation can be formed from an $(n-1)$-permutation by inserting the integer $n$ into any of the $n$ insertion positions (between, before, or after the entries of the $(n-1)$-permutation). For each $j \in\{1,2, \ldots, n\}$, inserting the integer $n$ into the $j$ th such position increases the number of inversions by $n-j$. The generating function for the number of additional inversions is then $1+q+q^{2}+\cdots+q^{n-1}$. Then by the multiplication rule of ordinary generating functions (C.f. [7]),

$$
\begin{aligned}
\sum_{\pi \in S_{n}} q^{i n v(\pi)} & =\left(1+q+q^{2}+\cdots+q^{n-1}\right) \prod_{i=1}^{n-1} \frac{1-q^{i}}{1-q} \\
& =\prod_{i=1}^{n} \frac{1-q^{i}}{1-q}
\end{aligned}
$$

The triangular array of numbers enumerated by the $q$-factorials is given in A 008302 . These number are known as the Mahonian numbers in honor of Percy McMahon.


Table 2: Number of $n$-permutations having $k$ inversions for $n \geq 0,0 \leq k \leq\binom{ n}{2}$. A008302

If we differentiate $[n]_{q}$ ! and then evaluate at $q=1$, we get the total number of inversions over all permutations in $S_{n}$. This is sequence A001809. The sequence is indexed for $n \geq 0$. $0,0,1,9,72,600,5400,52920,564480,6531840,81648000,1097712000, \ldots$

Table 3: Total number of inversions over all $n$-permutations for $n \geq 0$. A001809

## 4. The Number of Subspaces of $\mathbb{F}_{q}^{n}$.

In this section we will count the total number of subspaces of $\mathbb{F}_{q}^{n}$. We will classify these subspaces according to their dimension $k$, for $0 \leq k \leq n$.

Since all finite-dimensional vector spaces with the same dimension are isomorphic, then each $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$ has the same number of bases as the vector space $\mathbb{F}_{q}^{k}$. So the number of $k$-tuples of vectors in $\mathbb{F}_{q}^{n}$ that are a basis for the same $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$ is exactly the number of $k$-tuples of linearly independent vectors in $\mathbb{F}_{q}^{k}$ (where we are assuming $k \leq n)$. By Theorem 3.1 there are $\left(q^{k}-1\right)\left(q^{k}-q\right) \cdots\left(q^{k}-q^{k-1}\right)$ linearly
independent $k$-tuples of vectors that may serve as a basis for any given $k$-dimensional vector space.

Following the notation in [16] we denote the quantity $\prod_{i=0}^{n-1}\left(q^{n}-q^{i}\right)$ by $\gamma_{n}(q)$ or just by $\gamma_{n}$ if the value of $q$ is clear from the context. Later we will show that $\gamma_{n}(q)$ is the order of the general linear group $\mathrm{GL}_{n}\left(\mathbb{F}_{q}\right)$ of $n \times n$ invertible matrices over $\mathbb{F}_{q}$. We note that

$$
\begin{aligned}
\gamma_{n}(q) & =\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{n-1}\right) \\
& =(q-1)^{n} q^{\binom{n}{2}}[n]_{q}! \\
& =\left((n)_{n}\right)_{q} .
\end{aligned}
$$

The first few terms of the sequence A002884, $\gamma_{n}(q)$ for $n \geq 0$ where $q=2$ are given in Table 4. Note that this is the main diagonal in Table 1.

$$
1,1,6,168,20160,9999360,20158709760,163849992929280, \ldots
$$

Table 4: $\gamma_{n}(2)$ for $n \geq 0$. (The order of $\left.\mathrm{GL}_{n}\left(\mathbb{F}_{2}\right)\right) . A 002884$

The number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ is the number of linearly independent k-tuples of vectors in $\mathbb{F}_{q}^{n}$ divided by the number of such $k$-tuples that generate the same subspace.

Definition 4.1. The number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ is called the $q$-binomial coefficient and is denoted $\binom{n}{k}_{q}$.

The $q$-binomial coefficient is also sometimes referred to as the Gaussian binomial coefficient. In a certain sense it is not a coefficient at all but a polynomial in $q$, and in fact it is also sometimes called the Gaussian polynomial. The following theorem quantifies the $q$-binomial as a number. The first equation gives an expression for (what turns out to be) the Gaussian polynomial in $q$. The last equation shows the analogy with the binomial coefficients.

Proof. The number $\binom{n}{k}_{q}$ of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ is the number $\left((n)_{k}\right)_{q}$ of linearly independent $k$-tuples of vectors in $\mathbb{F}_{q}^{n}$ divided by the number $\left((k)_{k}\right)_{q}$ of such $k$-tuples that generate the same subspace. So

$$
\binom{n}{k}_{q}=\frac{\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)}{\left(q^{k}-1\right)\left(q^{k}-q\right) \cdots\left(q^{k}-q^{k-1}\right)}
$$

The equality of the other two expressions follows from algebraic simplification and the definition of the $q$-factorial number.

These coefficients are shown in Table 5 for the case $q=2$. We can say that this table is a $q$-analog of Pascal's triangle. The table is indexed from $n \geq 0, k \geq 0$. For example, the number of 2-dimensional subspaces of a vector space of dimension 4 over $\mathbb{F}_{2}$ is 35 . This table is A022166.

| 1 |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 1 |  |  |  |  |  |  |  |
| 1 | 3 | 1 |  |  |  |  |  |  |
| 1 | 7 | 7 | 1 |  |  |  |  |  |
| 1 | 15 | 35 | 15 | 1 |  |  |  |  |
| 1 | 31 | 155 | 155 | 31 | 1 |  |  |  |
| 1 | 63 | 651 | 1395 | 651 | 63 | 1 |  |  |
| 1 | 127 | 2667 | 11811 | 11811 | 2667 | 127 | 1 |  |
| 1 | 255 | 10795 | 97155 | 200787 | 97155 | 10795 | 255 | 1 |

Table 5: Number of $k$-dimensional subspaces of $\mathbb{F}_{2}^{n}$ for $n \geq 0,0 \leq k \leq n$. A022166

## 5. The Number of $m \times n$ Matrices of a Given Rank with Entries in $\mathbb{F}_{q}$

To construct an $m \times n$ matrix with entries in $\mathbb{F}_{q}$ we make $m \cdot n$ independent choices of a field element. So there are $q^{m n}$ such matrices. In this section we elaborate on some results given in [16] to classify these matrices according to their rank, $k$, for $0 \leq k \leq \min \{m, n\}$. To that end, we first demonstrate that the number of bases over all $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ (i.e. the quantity, $\left((n)_{k}\right)_{q}=\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)$ determined in section 3 ) is also the number of surjective linear mappings from $\mathbb{F}_{q}^{n}$ onto a given k-dimensional subspace of $\mathbb{F}_{q}^{m}$ where $m, n \geq k$. In order to do so we will introduce the notion of a dual vector space and a dual mapping, following the ideas and proofs given in [5]. This will allow us to use the same simple counting argument that was used to count linearly independent tuples to count surjective mappings. We also give two alternate characterizations of the data in Tables 1, 5, and 6 (below) . Along the way, we state some basic theorems and definitions from linear algebra and group theory along with their proofs which are essentially those in [5] and [10]. We conclude the section with a look at the probability distribution of the rank of a random matrix.

The lemma below shows that every linear map from a vector space $V$ to a vector space $W$ is uniquely determined by the choice of vectors in $W$ to which we assign the vectors of a basis of $V$. We are free to map the basis vectors of $V$ to any tuple of vectors in $W$, but once this choice is made the mapping is established. Note how this implies that $\left|\mathcal{L}\left(\mathbb{F}_{q}^{n}, \mathbb{F}_{q}^{m}\right)\right|=\left|\mathcal{L}\left(\mathbb{F}_{q}^{m}, \mathbb{F}_{q}^{n}\right)\right|=q^{m n}$.

Lemma 5.1 ([5]). Suppose $V$ and $W$ are finite-dimensional vector spaces over a field $\mathbb{F}$ and that $v_{1}, \ldots, v_{n}$ is a basis of $V$, and that $w_{1}, \ldots, w_{n}$ are any vectors in $W$. Then there is a unique linear map $T$ from $V$ to $W$ such that $T v_{j}=w_{j}$ for all $j=1, \ldots, n$.

Proof. Fix a basis $v_{1}, \ldots, v_{n}$ of $V$. Let $w_{1}, \ldots, w_{n}$ be any list of vectors in $W$. Define
$T: V \rightarrow W$ by

$$
\begin{equation*}
T\left(a_{1} v_{1}+\cdots a_{n} v_{n}\right)=a_{1} w_{1}+\cdots+a_{n} w_{n} \text { for } a_{1}, \ldots, a_{n} \in \mathbb{F} \tag{5.1}
\end{equation*}
$$

Since $v_{1}, \ldots, v_{n}$ is a basis of $V$, the mapping is well-defined. For each $j \in\{1, \ldots, n\}$ taking $a_{j}=1$ and each of the other scalars equal to 0 , gives $T v_{j}=w_{j}$. It is routine to show that the mapping is linear. This establishes existence.

Suppose S is also a linear map from $V$ to $W$ such that $S v_{i}=T v_{i}$ for all $i \in\{1, \ldots, n\}$. Let $v$ be arbitrary in $V$. Then $v=a_{1} v_{1}+\ldots+a_{n} v_{n}$ for some scalars $a_{1}, \ldots, a_{n} \in \mathbb{F}$. Then

$$
\begin{aligned}
S v & =S\left(a_{1} v_{1}+\ldots+a_{n} v_{n}\right) \\
& =a_{1} S v_{1}+\ldots+a_{n} S v_{n} \\
& =a_{1} T v_{1}+\ldots+a_{n} T v_{n} \\
& =T\left(a_{1} v_{1}+\ldots+a_{n} v_{n}\right) \\
& =T v .
\end{aligned}
$$

The next two lemmas characterize injectivity and surjectivity of linear maps. The two lemmas taken together imply that a linear operator on a finite dimensional vector space is injective if and only it is surjective.

Lemma 5.2 ([5]). Let $V, W$ be vector spaces over field $\mathbb{F}$. Let $v_{1}, \ldots, v_{n}$ be a basis of $V$. Let $T$ be a linear map from $V$ to $W$. Then $T$ is injective if and only if $T v_{1}, \ldots, T v_{n}$ is linearly independent.

Proof. $\Rightarrow$ : Assume $T$ is injective and that $a_{1} T v_{1}+\ldots+a_{n} T v_{n}=0$ for some scalars $a_{1}, \ldots, a_{n} \in \mathbb{F}$. The equation implies that $T\left(a_{1} v_{1}+\ldots+a_{n} v_{n}\right)=0$. Since $T$ is injective
then null $T=0$. So $a_{1} v_{1}+\ldots+a_{n} v_{n}=0$. Since $v_{1}, \ldots, v_{n}$ is linearly independent $0=a_{1}=\cdots=a_{n}$.
$\Leftarrow$ : Assume $T v_{1}, \ldots, T v_{n}$ is linearly independent. Let $v \in V$ such that $T v=0$. Now $v=a_{1} v_{1}+\ldots+a_{n} v_{n}$ for some scalars $a_{1}, \ldots, a_{n} \in \mathbb{F}$. So

$$
0=T v=T\left(a_{1} v_{1}+\ldots+a_{n} v_{n}\right)=a_{1} T v_{1}+\ldots+a_{n} T v_{n}
$$

Since $T v_{1}, \ldots, T v_{n}$ is linearly independent $a_{1}=\cdots=a_{n}=0$. So $v=0$. So null $(T)=$ $\{0\}$. So $T$ is injective.

Lemma 5.3 ([5]). Let $V$, $W$ be vector spaces over field $\mathbb{F}$. Let $v_{1}, \ldots, v_{n}$ be a basis of $V$. Let $T$ be a linear map from $V$ to $W$. Then $T$ is surjective if and only if $\operatorname{span}\left(T v_{1}, \ldots, T v_{n}\right)=$ $W$.

Proof. $\Rightarrow$ : Assume $T$ is surjective. Then

$$
\begin{aligned}
W & =\operatorname{range} T \\
& =\{T v: v \in V\} \\
& =\left\{T\left(a_{1} v_{1},+\cdots+a_{n} v_{n}\right): a_{1}, \ldots, a_{n} \in \mathbb{F}\right\} \\
& =\left\{a_{1} T v_{1}+\cdots+a_{n} T v_{n}: a_{1}, \ldots, a_{n} \in \mathbb{F}\right\} \\
& =\operatorname{span}\left(T v_{1}, \ldots, T v_{n}\right)
\end{aligned}
$$

$\Leftarrow$ : Assume $W=\operatorname{span}\left(T v_{1}, \ldots, T v_{n}\right)$. Then from the above equations, $W=\operatorname{range} T$. So $T$ is surjective.

Definition 5.4. For positive integers $m$ and $n$, let $\mathbb{F}_{q}^{m, n}$ denote the set of all $m \times n$ matrices with entries in $\mathbb{F}_{q}$. The general linear group, denoted by $\mathrm{GL}_{n}\left(\mathbb{F}_{q}\right)$, is the set of all invertible matrices in $\mathbb{F}_{q}^{n, n}$ along with the operation of matrix multiplication.

A linear map is invertible if and only if it is both injective and surjective. An isomorphism between two vector spaces is an invertible linear map. An invertible linear map from an $n$-dimensional vector space $V$ onto itself is called a vector space automorphism. It is a bijective homomorphism that preserves both the vector addition and the scalar multiplication of $V$. The set of all such automorphisms with the operation of function composition forms a group which we will denote $\operatorname{Aut}(V)$. This group is isomorphic to $\mathrm{GL}_{n}\left(\mathbb{F}_{q}\right)$. A canonical isomorphism between these two groups is given in the definition below.

Definition 5.5. Suppose $T \in \mathcal{L}(V)$ and $v_{1}, \ldots, v_{n}$ is a basis of $V$. The matrix of $T$ with respect to this basis is the $n \times n$ matrix $\mathcal{M}(T)$ whose entries $a_{j, k}$ are defined by

$$
T v_{k}=a_{1, k} v_{1}+\cdots+a_{n, k} v_{n}
$$

The mapping given in the following theorem shows that $|\operatorname{Aut}(V)|=\mid$ is precisely the number of ways to choose a basis of $V$, that is, the number of linearly independent $n$-tuples of vectors in $V$.

Theorem 5.6 ([5]). Two finite dimensional vector spaces are isomorphic if and only if they have the same dimension.

Proof. $\Rightarrow$ : Suppose $T: V \rightarrow W$ is an invertible map (i.e. an isomorphism between $V$ and $W)$. Then $T$ is injective and surjective. So null $T=0$ and range $T=W$. Since $\operatorname{dim} V=$ $\operatorname{dim}$ null $T+\operatorname{dim}$ range $T$, we have $\operatorname{dim} V=\operatorname{dim} W$.
$\Leftarrow$ : Suppose $V$ and $W$ both have dimension $n$. Let $v_{1}, \ldots, v_{n}$ be a basis of $V$ and $w_{1}, \ldots, w_{n}$ be a basis of $W$. Define $T: V \rightarrow W$ by $T\left(a_{1} v_{1}+\cdots+a_{n} v_{n}\right)=a_{1} w_{1}+$ $\cdots+a_{n} w_{n}$. Then $T$ is well defined since $v_{1}, \ldots, v_{n}$ is a basis of $V$. Note that $T v_{1}=$ $w_{1}, \ldots, T v_{n}=w_{n}$. So $T$ is injective since $w_{1}, \ldots, w_{n}$ is linearly independent. Also $T$ is $\operatorname{surjective} \operatorname{since} \operatorname{span}\left(w_{1}, \ldots, w_{n}\right)=W$. Therefore, $T$ is an isomorphism.

Definition 5.7. A linear functional on $V$ is a linear map from $V$ to $\mathbb{F}$. The dual space of $V$, denoted $V^{*}$, is the vector space of all linear functionals on $V$. In other words, $V^{*}=\mathcal{L}(V, \mathbb{F})$ where $\mathbb{F}$ is the underlying field of $V$.

Definition 5.8. Let $v_{1}, \ldots, v_{n}$ be a basis of V. The dual basis of $v_{1}, \ldots, v_{n}$ is the list $\phi_{1}, \ldots, \phi_{n}$ of linear functionals in $V^{*}$ such that

$$
\phi_{j}\left(v_{k}\right)= \begin{cases}1, & k=j \\ 0, & k \neq j\end{cases}
$$

From the definitions above we should note that $V$ is isomorphic to its dual, $V^{*}$ because it has the same dimension as $V$. Also the dual basis $\phi_{1}, \ldots, \phi_{n}$ is indeed a basis of $V^{*}$. To see this note that for scalars $a_{1}, \ldots, a_{n} \in \mathbb{F}$ we have $a_{1} \phi_{1}+\cdots+a_{n} \phi_{n}=0$, then for each $j \in\{1, \ldots, n\},\left(a_{1} \phi_{1}+\cdots+a_{n} \phi_{n}\right) v_{j}=a_{j}$, so that $a_{1}=\cdots=a_{n}=0$.

Definition 5.9. Let $T$ be a linear map from $V \rightarrow W$. The dual map of $T$ is the linear map $T^{*}: W^{*} \rightarrow V^{*}$ defined by $T^{*}(\phi)=\phi \circ T$ for all $\phi \in W^{*}$.

Definition 5.10. Let $U$ be a subspace of V . The annihilator of $U$, denoted by $U^{\circ}$, is the subspace of $V^{*}$ defined by $U^{\circ}=\left\{\phi \in V^{*}: \phi(u)=0 \quad \forall u \in U\right\}$.

Lemma 5.11 ([5]). Let $U$ be a subspace of $V$. Then $\operatorname{dim} U+\operatorname{dim} U^{\circ}=\operatorname{dim} V$.

Proof. Let $u_{1}, \ldots, u_{m}$ be a basis of $U$. Extend it to a basis $u_{1}, \ldots, u_{m}, u_{m+1}, \ldots, u_{n}$ of $V$. Let $\phi_{1}, \ldots, \phi_{m}, \phi_{m+1}, \ldots, \phi_{n}$ be the corresponding dual basis of $V^{*}$. We will show $\phi_{m+1}, \ldots, \phi_{n}$ is a basis of $U^{\circ}$. Since $\phi_{m+1}, \ldots, \phi_{n}$ is linearly independent, we just need to show that $\operatorname{span}\left(\phi_{m+1}, \ldots, \phi_{n}\right)=U^{\circ}$.

Let $\phi \in \operatorname{span}\left(\phi_{m+1}, \ldots, \phi_{n}\right)$. Then $\phi=a_{m+1} \phi_{m+1}+\cdots+a_{n} \phi_{n}$ for some scalars $a_{m+1}, \ldots, a_{n} \in \mathbb{F}$. Let $u \in U$. Then $u=b_{1} u_{1}+\cdots+b_{m} u_{m}$ for some scalars $b_{1}, \ldots, b_{m} \in \mathbb{F}$.

Note that for all $j \in\{m+1, \ldots, n\}, \phi_{j}(u)=b_{1} \phi_{j}\left(u_{1}\right)+\cdots+b_{m} \phi_{j}\left(u_{m}\right)=0$ so that $\phi(u)=0$. So $\phi \in U^{\circ}$. So $\operatorname{span}\left(\phi_{m+1}, \ldots, \phi_{n}\right) \subseteq U^{\circ}$.

Now let $\phi \in U^{\circ}$. Since $\phi \in V^{*}$,

$$
\phi=c_{1} \phi_{1}+\ldots+c_{m} \phi_{m}+c_{m+1} \phi_{m+1}+\ldots+c_{n} \phi_{n}
$$

for some scalars $c_{1}, \ldots c_{n} \in \mathbb{F}$. Now $\phi(u)=0$ for all $u \in U$. In particular

$$
0=\phi\left(u_{1}\right)=c_{1} \phi_{1}\left(u_{1}\right)+\ldots+c_{m} \phi_{m}\left(u_{1}\right)+c_{m+1} \phi_{m+1}\left(u_{1}\right)+\ldots+c_{n} \phi_{n}\left(u_{1}\right)=c_{1} .
$$

So $c_{1}=0$. Likewise $c_{j}=0$ for all $j \in\{1, \ldots, m\}$. So $\phi \in \operatorname{span}\left(\phi_{m+1}, \ldots, \phi_{n}\right)$. So $U^{\circ} \subseteq \operatorname{span}\left(\phi_{m+1}, \ldots, \phi_{n}\right)$.

We note that the above lemma implies that $V^{*}=U^{\circ}$ if and only if $U=\{0\}$. Likewise, $U^{\circ}=\{0\}$ if and only if $U=V$.

Lemma 5.12 ([5]). Two linear maps $S: V \rightarrow W$ and $T: V \rightarrow W$ are equal if and only if their dual maps $S^{*}: W^{*} \rightarrow V^{*}$ and $T^{*}: W^{*} \rightarrow V^{*}$ are equal.

Proof. $\Rightarrow$ : Assume $S$ and $T$ are equal. Let $\phi$ be arbitrary in $W^{*}$. Then $S^{*}(\phi)=\phi \circ S=$ $\phi \circ T=T^{*}(\phi)$.
$\Leftarrow$ : Assume $S^{*}$ and $T^{*}$ are equal. Let $v \in V$. Then for all $\phi \in W^{*}, S^{*}(\phi)=T^{*}(\phi)$ . So that $\phi \circ S=\phi \circ T$. So that $\phi(S v)=\phi(T v) \Rightarrow \phi(S v)-\phi(T v)=0$. So that $\phi(S v-T v)=0$. Since this equation holds for every $\phi \in W^{*}$ then $(\operatorname{span}(S v-T v))^{\circ}=$ $W^{*}$ hence $\operatorname{span}(S v-T v)=\{0\}$. So that $S v=T v$.

Lemma 5.13 ([5]). Let $T$ be a linear map from $V$ to $W$. Then null $T^{*}=(\text { range } T)^{\circ}$.

Proof.

$$
\begin{aligned}
\phi \in \operatorname{null}\left(T^{*}\right) & \Leftrightarrow T^{*}(\phi)=0 \\
& \Leftrightarrow(\phi \circ T)(v)=0 \quad \text { for all } v \in V \\
& \Leftrightarrow \phi(T v)=0 \quad \text { for all } v \in V \\
& \Leftrightarrow \phi \in(\text { range } T)^{\circ} .
\end{aligned}
$$

Lemma 5.14 ([5]). Let $T$ be a linear map from $V$ to $W$. Then $T$ is surjective if and only if $T^{*}$ is injective.

Proof.

$$
\begin{aligned}
\text { The map } T \text { is surjective } & \Leftrightarrow \text { range } T=W, \\
& \Leftrightarrow(\text { range } T)^{\circ}=\{0\}, \\
& \Leftrightarrow \operatorname{null} T^{*}=\{0\}, \\
& \Leftrightarrow T^{*} \text { is injective. }
\end{aligned}
$$

Lemma 5.15. There is a 1-1 correspondence between the linear maps $T \in \mathcal{L}(V, W)$ and the dual maps $T^{*} \in \mathcal{L}\left(W^{*}, V^{*}\right)$. More precisely, $\Phi: \mathcal{L}(V, W) \rightarrow \mathcal{L}\left(V^{*}, W^{*}\right)$ by $\Phi(T)=$ $T^{*}$ for all $T \in \mathcal{L}(V, W)$ is a linear isomorphism (and hence is a bijective function).

Proof. It is straightforward to show that $\Phi$ is a linear map. Now observe that the $\operatorname{dim}(\mathcal{L}(V, W))=$ $\operatorname{dim}\left(\mathcal{L}\left(V^{*}, W^{*}\right)\right.$. So it suffices to show that $\Phi$ is an injection. For each $T \in \mathcal{L}(V, W)$

$$
\begin{aligned}
T \in \operatorname{null}(\Phi) & \Leftrightarrow \Phi(T)=0 \\
& \Leftrightarrow T^{*}=0 \\
& \Leftrightarrow \phi \circ T=0 \quad \forall \phi \in W^{*} \\
& \Leftrightarrow(\operatorname{span}(T))^{\circ}=W^{*} \\
& \Leftrightarrow \operatorname{span}(T)=0 \\
& \Leftrightarrow T=0 \\
& \Leftrightarrow \operatorname{null}(\Phi)=\{0\} \\
& \Leftrightarrow \Phi \text { is injective }
\end{aligned}
$$

Theorem 5.16. Let $V, W$ be vector spaces over $\mathbb{F}_{q}$. Let $\operatorname{dim} V=n$ and let $\operatorname{dim} W=m$. Then
(a) the number of injective linear maps from $V$ to $W$ is $\left(q^{m}-1\right)\left(q^{m}-q\right) \cdots\left(q^{m}-q^{n-1}\right)=$ $\left((m)_{n}\right)_{q} ;$
(b) the number of surjective linear maps from $V$ to $W$ is $\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{m-1}\right)=$ $\left((n)_{m}\right)_{q}$.

Proof. Fix a basis $v_{1}, \ldots, v_{n}$ of $V$. Let T be a linear map from $V$ to $W$. Then T is completely determined by the values $T v_{1}, \ldots, T v_{n}$. Also, $T$ is injective if and only if $T v_{1}, \ldots, T v_{n}$ is linearly independent. Then (a) follows from Theorem 3.2, i.e., ( $q^{m}-$ 1) $\left(q^{m}-q\right) \cdots\left(q^{m}-q^{n-1}\right)$ is the number of linearly independent length $n$ lists of vectors in $W$.

By lemma 5.12 the linear maps $T \in \mathcal{L}(V, W)$ and the dual maps $T^{*} \in \mathcal{L}\left(W^{*}, V^{*}\right)$ are in 1-1 correspondence. Also by Lemma $5.14 T$ is surjective if and only if $T^{*}$ is injective. Then (b) follows by applying statement (a) to $T^{*} \in \mathcal{L}\left(W^{*}, V^{*}\right)$.

Theorem 5.17 ([16]). The number of $m \times n$ matrices of rank $k$ (for $0 \leq k \leq \min \{m, n\}$ ) is equal to $\binom{m}{k}_{q} \cdot\left((n)_{k}\right)_{q}$.

Each surjection from $\mathbb{F}_{q}^{n}$ onto a given $k$-dimensional subspace of $\mathbb{F}_{q}^{m}$ corresponds in a 1-1 fashion to a linearly independent $k$-tuple of vectors in $\mathbb{F}_{q}^{n}$. The number of $m \times n$ matrices having rank $k$ is equal to the number of linear maps from $\mathbb{F}_{q}^{n}$ onto a given $k$ dimensional subspace of $\mathbb{F}_{q}^{m}$. There are $\binom{m}{k}_{q}$ subspaces of $\mathbb{F}_{q}^{m}$ that have dimension $k$ . These subspaces will serve as the range of our mapping. By Theorem 5.16, there are $\left(q^{n}-1\right)\left(q^{n}-q\right) \ldots\left(q^{n}-q^{k-1}\right)$ surjections onto each k-dimensional subspace. So there are $\binom{m}{k}_{q}\left(q^{n}-1\right)\left(q^{n}-q\right) \ldots\left(q^{n}-q^{k-1}\right)=\binom{m}{k}_{q} \cdot\left((n)_{k}\right)_{q}$ surjective linear maps from $\mathbb{F}_{q}^{n}$ onto a given k -dimensional subspace of $\mathbb{F}_{q}^{m}$.

Considering the case when $m=n$, we have that the number of linear operators $T$ on $\mathbb{F}_{q}^{n}$ such that $\operatorname{dim}($ range $T)=k$ is

$$
\binom{n}{k}_{q}\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)=\frac{\left(\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)\right)^{2}}{\left(q^{k}-1\right)\left(q^{k}-q\right) \cdots\left(q^{k}-q^{k-1}\right)}
$$

Table 6 (A286331) gives these numbers for $q=2$ and $n \geq 0,0 \leq k \leq n$.

```
1
11
\(1 \quad 9 \quad 6\)
\(1 \begin{array}{llll}1 & 49 & 294 & 168\end{array}\)
\(\begin{array}{lllll}1 & 225 & 7350 & 37800 & 20160\end{array}\)
\(\begin{array}{llllll}1 & 961 & 144150 & 4036200 & 19373760 & 9999360\end{array}\)
\(139692542806326932200 \quad 8543828160 \quad 39687459840 \quad 20158709760\)
```

Table 6: Number of $n \times n$ matrices with rank $k$ for $n \geq 0,0 \leq k \leq n$. A286331

## Some equivalent characterizations of the data in Tables 1,5 , and 6.

We can characterize the enumeration results given in Tables 1, 5, and 6 in terms of an equivalence relation. Let $\mathcal{L}\left(\mathbb{F}_{2}^{n}\right)$ denote the set of all linear operators on $\mathbb{F}_{2}^{n}$. Define an equivalence relation $\sim_{R}$ on $\mathcal{L}\left(\mathbb{F}_{2}^{n}\right)$ by $S \sim_{R} T$ if and only if range $S=$ range $T$ for all $S, T \in \mathcal{L}\left(\mathbb{F}_{2}^{n}\right)$. By associating each operator to the subspace of its range we make the following observations.
(i) The entries in Table 5 are the number, $\binom{n}{k}_{2}$ of equivalence classes containing elements (operators) that have a range of a particular dimension $k$.
(ii) The entries in Table 1 give the number, $\left((n)_{k}\right)_{2}$ of equivalent operators that are in each of the classes. That is, the number of operators in $\mathcal{L}\left(\mathbb{F}_{2}^{n}\right)$ that have exactly the same range with dimension $k$.
(iii) The row sums of Table 5 give the number of equivalence classes.
(iv) Table 6 is the product $\left((n)_{k}\right)_{2} \cdot\binom{n}{k}_{2}$ of corresponding entries in Table 1 and Table 5.
(v) Each operator is accounted for exactly once in Table 6 so that the row sums are $2^{n^{2}}$.

Now let $\mathbb{F}_{q}^{n, n}$ be the set of all $n \times n$ matrices over $\mathbb{F}_{q}$. Each operator in $\mathcal{L}\left(\mathbb{F}_{q}^{n}\right)$ corresponds to exactly one matrix in $\mathbb{F}_{q}^{n, n}$. Also if two matrices are row equivalent then their row space is the same and that for any $M \in \mathbb{F}_{q}^{n, n}$ the row space of $M^{T}$ is the column space of $M$. Then we can make the following equivalent characterizations of Tables 1,5 , and 6 .
(i) The row sums of Table $5, \sum_{k=0}^{n}\binom{n}{k}$ are the number of classes of row equivalent matrices in $\mathbb{F}_{2}^{n, n}$.
(ii) The entries in Table 1 are the number, $\left((n)_{k}\right)_{2}$ of matrices in $\mathbb{F}_{2}^{n, n}$ that row reduce to a given matrix $M$ in reduced row echelon form with $\operatorname{rank} k$ (or equivalently $\operatorname{dim} \operatorname{Row}(M)=$ $k)$.
(iii) Table 6 is the number, $\left((n)_{k}\right)_{2} \cdot\binom{n}{k}_{2}$ of matrices $M$ in $\mathbb{F}_{2}^{n, n}$ with rank $k$ (or equivalently $\operatorname{dim} \operatorname{Row}(M)=k)$.

## The probability distribution for the rank of an $n \times n$ matrix over $\mathbb{F}_{q}$

If we construct a random $n \times n$ matrix with entries in $\mathbb{F}_{q}$ or equivalently select a random operator $T$ on $\mathbb{F}_{q}^{n}$, what is the likelihood that the matrix has rank $k$ (or equivalently $\operatorname{dim}(\operatorname{range} T)=k$. Let us denote this likelihood as $\mathrm{P}(\operatorname{dim}(\operatorname{range} T)=k)$. Since there are
$q^{n^{2}}$ operators on $\mathbb{F}_{q}^{n}$ we have

$$
\begin{aligned}
\mathrm{P} & (\operatorname{dim}(\operatorname{range} T)=k) \\
& =\frac{\left(\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)\right)^{2}}{q^{n^{2}}\left(q^{k}-1\right)\left(q^{k}-q\right) \cdots\left(q^{k}-q^{k-1}\right)} \\
& =\frac{\left(1-\frac{1}{q^{n}}\right)\left(1-\frac{1}{q^{n-1}}\right) \cdots\left(1-\frac{1}{q^{n-k+1}}\right) \cdot\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)}{q^{n(n-k)}\left(q^{k}-1\right)\left(q^{k}-q\right) \cdots\left(q^{k}-q^{k-1}\right)} \\
& =\frac{\left(1-\frac{1}{q^{n}}\right)\left(1-\frac{1}{q^{n-1}}\right) \cdots\left(1-\frac{1}{q^{n-k+1}}\right) \cdot\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)}{q^{(n-k)^{2}}\left(q^{n}-q^{n-k}\right)\left(q^{n}-q^{n-k+1}\right) \cdots\left(q^{n}-q^{n-1}\right)} \\
& =\frac{1}{q^{(n-k)^{2}}} \prod_{i=n-k+1}^{n}\left(1-\frac{1}{q^{i}}\right) \cdot \prod_{i=0}^{k-1} \frac{q^{n}-q^{i}}{q^{n}-q^{n-k+i}} .
\end{aligned}
$$

Now we would like to know the probability in the limit as $n$ approaches infinity that the range of a random operator on $\mathbb{F}_{q}^{n}$ has dimension $n-j$, for $0 \leq j \leq n$. We substitute $j=n-k$ into the above expression. We claim that $\prod_{i=0}^{k-1} \frac{q^{n}-q^{i}}{q^{n}-q^{n-k+i}}=\prod_{i=1}^{j=n-k} \frac{q^{n}-q^{i-1}}{q^{n}-q^{n-i}}$. To see this, observe that the numerator in the expression on the left multiplied by the denominator in the expression on the right is equal to the numerator in the expression on the right multiplied by the denominator of the expression on the left. So we have

$$
\begin{aligned}
\mathrm{P}(\operatorname{dim}(\operatorname{range} T)=(n-j)) & =\frac{1}{q^{j^{2}}} \prod_{i=j+1}^{n}\left(1-\frac{1}{q^{i}}\right) \cdot \prod_{i=1}^{j} \frac{q^{n}-q^{i-1}}{q^{n}-q^{n-i}} \\
& =\prod_{i=j+1}^{n}\left(1-\frac{1}{q^{i}}\right) \cdot \prod_{i=1}^{j} \frac{q^{n}-q^{i-1}}{q^{n+j}-q^{n+j-i}} \\
& =\prod_{i=j+1}^{n}\left(1-\frac{1}{q^{i}}\right) \cdot \prod_{i=1}^{j} \frac{1-\frac{q^{i}-1}{q^{n}}}{q^{j}-q^{j-i}} .
\end{aligned}
$$

Taking the limit as $n \rightarrow \infty$, the expression becomes

$$
\prod_{i=j+1}^{\infty}\left(1-\frac{1}{q^{i}}\right) \cdot \prod_{i=1}^{j} \frac{1}{q^{j}-q^{j-i}}=\frac{1}{\gamma_{j}(q)} \cdot \prod_{i=j+1}^{\infty}\left(1-\frac{1}{q^{i}}\right)
$$

## 6. A Closer Look at the $q$-Binomial Coefficients.

In this section we prove a two term recurrence relation for the Galois numbers. We also give a well known derivation of the $q$-analog of Pascal's Identity.

Let $\mathcal{G}_{n}(q)$ be the collection of all subspaces of $\mathbb{F}_{q}^{n}$. We can think of this collection as a $q$-analog of the power set of an $n$-set. Let $G_{n}(q)$ denote the total number of subspaces of $\mathbb{F}_{q}^{n}$. In other words, $G_{n}(q)=\left|\mathcal{G}_{n}(q)\right|$. The numbers $G_{n}(q)$ are called the Galois numbers. The numbers $G_{n}(2)$ are the row sums of Table 5 . The first few terms of this sequence (A006116), for $n \geq 0$, are given in Table 7 . $1,2,5,16,67,374,2825,29212,417199,8283458,229755605 \ldots$

Table 7: Galois numbers, $G_{n}(2)$, for $n \geq 0$. A006116

Let $v$ be a nonzero vector in $\mathbb{F}_{q}^{n}$. We claim that the number of appearances of the vector $v$ over the collection $\mathcal{G}_{n}(q)$ is $G_{n-1}(q)$. In other words, the multiplicity of the vector $v$ in the multiset $\sqcup_{U \in \mathcal{G}_{n}(q)} U$ is equal to $G_{n-1}(q)$, where $\sqcup_{U \in \mathcal{G}_{n}(q)} U$ is the disjoint union of $\mathcal{G}_{n}(q)$. For example, if $q=2$ and $n=2$ and

$$
v=\binom{0}{1}
$$

then $G_{n-1}(q)=2$ and $\mathcal{G}_{n}(q)$ is the collection

$$
\begin{aligned}
& \left\{\left\{\binom{0}{0}\right\},\left\{\binom{0}{0},\binom{0}{1}\right\},\left\{\binom{0}{0},\binom{1}{0}\right\},\left\{\binom{0}{0},\binom{1}{1}\right\},\right. \\
& \left.\left\{\binom{0}{0},\binom{0}{1},\binom{1}{0},\binom{1}{1}\right\}\right\}
\end{aligned}
$$

We see that the vector $v$ appears exactly two times in this collection. Note that the
claim is analogous with the number of times a given element occurs in the power set of $\{1,2, \ldots, n\}$ which is indeed the total number of subsets in the collection of all subsets of $\{1,2, \ldots, n-1\}$. The claim follows from the proof of Theorem 6.3 , below, but first we give another result that also has an analogy in enumeration of subsets.

We want to count the number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ that contain any $j$ linearly independent vectors for $j=1, \ldots, k$. Equivalently, we will count the number of $k$-dimensional subspaces that contain the subspace $W=\operatorname{span}\left(v_{1}, \ldots, v_{j}\right)$, where $v_{1}, \ldots, v_{j}$ is a linearly independent list of vectors in $\mathbb{F}_{q}^{n}$.

Definition 6.1. Suppose $U$ is a subspace of $V$. Then the quotient space $V / U$ is the set $\{v+U: v \in V\}$ where $v+U=\{v+u: u \in U\}$.

It is straightforward to show that $V / U$ is a vector space where addition and scalar multiplication are defined by

$$
\begin{aligned}
(v+U)+(w+U) & =((v+w)+U) \\
\lambda(v+U) & =(\lambda v+U)
\end{aligned}
$$

for all $v, w \in V$ and $\lambda \in \mathbb{F}$. Also note that $\operatorname{dim} V / U=\operatorname{dim} V-\operatorname{dim} U$.

Let $W$ be a subspace of $\mathbb{F}_{q}^{n}$. Consider the quotient space $\mathbb{F}_{q}^{n} / W$. We can view this space as a condensed version of the vector space $\mathbb{F}_{q}^{n}$ where each subspace has decreased in dimension by $j=\operatorname{dim} W$. In $\mathbb{F}_{q}^{n} / W$, the subspace $W$ is playing the role of the zero vector. So in a certain sense, $W$ is in every subspace of $\mathbb{F}_{q}^{n} / W$. So our desired number is the number of $(k-j)$-dimensional subspaces of $\mathbb{F}_{q}^{n} / W$ which $\left(\right.$ since $\operatorname{dim} \mathbb{F}_{q}^{n} / W=(n-j)$ ) is $\binom{n-j}{k-j}_{q}$.

We make these notions mathematically precise in the following theorem which is the Correspondence Theorem applied to vector spaces C.f. [10] and [17]. This proof is essentially that given in [17] and [1].

Theorem 6.2 ([1]). Let $V$ be a finite dimensional vector space over a field $\mathbb{F}$. Let $W$ be a subspace of $V$. Then there is a 1-1 correspondence between the subspaces of $V$ containing $W$ and the subspaces of $V / W$.

Proof. Let $U$ be a subspace of $V$ that contains $W$. Let $\pi: V \rightarrow V / W$ by $\pi(v)=v+U$ . be the quotient map. Since $0 \in U, 0+W \in \pi(U)$. Assume $x+W, y+W \in \pi(U)$. Then $x, y \in U$. So $x+y \in U$. So $(x+y)+W \in \pi(U)$. Let $\lambda \in \mathbb{F}$. Then $\lambda x \in U$. Now $\lambda x+W:=\lambda(x+W)$. So $\lambda(x+W) \in \pi(U)$. Hence, $\pi(U)$ is a subspace of $V / W$.

So we may define the function $f:\{$ subspaces of $V$ that contain $W\} \rightarrow\{$ subspaces of $V / W\}$ by $f(U)=\pi(U)$ for all $U \in\{$ subspaces of $V$ that contain $W\}$.

Now consider $g:\{$ subspaces of $V / W\} \rightarrow\{$ subspaces of $V$ that contain $W\}$ by $g(\bar{U})=$ $\pi^{-1}(\bar{U})$, where $\bar{U} \in V / W$ and $\pi^{-1}(\bar{U})$ is the preimage of $\bar{U}$ under the quotient map $\pi$. In other words, $\pi^{-1}(\bar{U})=\{v \in V: \pi(v) \in \bar{U}\}$. We will show that $f$ and $g$ are inverses, but first we need to show that $g$ is a well defined function.

Let $a+W=b+W \in \bar{U}$. Then

$$
\begin{aligned}
\pi^{-1}(a+W) & =\{v \in V: v-a \in W\} \\
& =\{v \in V: v+W=a+W\} \\
& =\{v \in V: v+W=b+W\} \\
& =\{v \in V: v-b \in W\} \\
& =\pi^{-1}(b+W) .
\end{aligned}
$$

Now, it is straightforward to show that $\pi^{-1}(\bar{U})$ is a subspace of V . To see that $\pi^{-1}(\bar{U})$
contains $W$ we realize that $0+W \in \bar{U}$. Then $\pi^{-1}(0+W)=\{v \in V: v-0 \in W\}=W$.
Now we will show that $f$ and $g$ are inverses. First we show $f \circ g(\bar{U})=\bar{U}$. Let $a+W$ be arbitrary in $\bar{U}$. Now $g(a+W)=\{v \in V: v-a \in W\}$. Let $v \in V$ be such that $v-a \in W$. Then $\pi(v)=v+W=a+W$. So $f$ maps the subspace $\{v \in V: v-a \in W\}$ to $a+W$. So $f \circ g(\bar{U})=\bar{U}$.
Also, $g \circ f(U)=g(\pi(U))=\pi^{-1}(\pi(U)) \subseteq U$. Now let $v \in \pi^{-1}(\pi(U)):=\{v \in V$ : $\pi(v) \in \pi(U)\}$. So $\pi(v)=v+W \in \pi(U)$ implies that $v \in U$. So $g \circ f(U)=U$.

Theorem 6.3 ([6]). The $q$-binomial coefficients obey the following recurrence: $\binom{n}{k}_{q}=$ $q^{k}\binom{n-1}{k}_{q}+\binom{n-1}{k-1}$.

Proof. Let $v$ be some fixed nonzero vector in $\mathbb{F}_{q}^{n}$. We will show that the first term on the right-hand side is the number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ that do not contain $v$ then we will show that the second term on right-hand side is the number of subspaces that do contain $v$. Following a counting argument very similar to that made in section 3 , the number of $k$-tuples of vectors in $\mathbb{F}_{q}^{n}$ that avoid the span of $v$ is $\left(q^{n}-q\right)\left(q^{n}-q^{2}\right) \ldots\left(q^{n}-q^{k}\right)$. So the number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ that do not contain $v$ is

$$
\begin{aligned}
\frac{\left(q^{n}-q\right)\left(q^{n}-q^{2}\right) \ldots\left(q^{n}-q^{k}\right)}{\left(q^{k}-1\right)\left(q^{k}-q\right) \ldots\left(q^{k}-q^{k-1}\right)} & =\frac{q^{k}\left(q^{n-1}-1\right)\left(q^{n-1}-q\right) \ldots\left(q^{n-1}-q^{k-1}\right)}{\left(q^{k}-1\right)\left(q^{k}-q\right) \ldots\left(q^{k}-q^{k-1}\right)} \\
& =q^{k}\binom{n-1}{k}_{q} .
\end{aligned}
$$

Also since $\operatorname{dim} \mathbb{F}_{q}^{n} / \operatorname{span}(v)=n-1=\operatorname{dim} \mathbb{F}_{q}^{n-1}$ (so that $\mathbb{F}_{q}^{n} / \operatorname{span}(v)$ is isomorphic to $\mathbb{F}_{q}^{n-1}$ ) we have by Theorem 6.2 that the number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ that contain $v$ is equal to the number of $(k-1)$-dimensional subspaces of $\mathbb{F}_{q}^{n-1}$, which is $\binom{n-1}{k-1}_{q}$.

Theorem 6.4. The $q$ binomial coefficient is a polynomial of degree $k(n-k)$.

Proof. The proof is by induction on $n$.

Basis step: If $n=0$ then $\binom{0}{0}_{q}$ is the constant polynomial 1 of degree $0=0(0-0)$. If $n=1$ then $\binom{1}{0}_{q}$ is the constant polynomial 1 of degree $0=0(1-0)$. Also, $\binom{1}{1}_{q}$ is the constant polynomial 1 of degree $0=1(1-1)$. Also, for any $n \geq 0$, if $k=0$ then $\binom{n}{0}_{q}$ is the constant polynomial 1 of degree $0=0(n-0)$. Also, for any $n \geq 0$, if $k=n$ then $\binom{n}{k}_{q}$ is the constant polynomial 1 of degree $0=n(n-n)$.

Induction step: Let $n \geq 1$ and let $1 \leq k \leq n$ Assume that $\binom{n}{k}_{q}$ is a polynomial of degree $k(n-k)$ and that $\binom{n}{k-1}_{q}$ is a polynomial of degree $(k-1)(n-(k-1))$. Then by our recurrence in Theorem 6.3, $\binom{n+1}{k}_{q}$ is the sum of the two polynomials $\binom{n}{k-1}_{q}$ and $q^{k}\binom{n}{k}_{q}$. By our induction hypothesis the former has degree $(k-1)(n-(k-1))=(k-1)(n+1-k)$ while the latter has degree $k+k(n-k)=k(n+1-k)$. So the degree of $\binom{n+1}{k}_{q}$ is $k(n+1-k)$ as was to be shown.

The above theorem gives a recurrence to generate the $q$-binomial coefficients. There is also a recurrence for the Galois numbers, i.e., a recurrence for the total number of subspaces of $\mathbb{F}_{q}^{n}$.

Theorem 6.5. Let $G_{n}(q)$ be the number of subspaces of $\mathbb{F}_{q}^{n}$. Then

$$
G_{n+1}(q)=2 G_{n}(q)+\left(q^{n}-1\right) G_{n-1}(q) .
$$

Proof. Let $v$ be a fixed but arbitrary nonzero vector in $\mathbb{F}_{q}^{n+1}$. We will show that the number of subspaces of $\mathbb{F}_{q}^{n+1}$ that contain $v$ is $G_{n}(q)$ while the number of subspaces that do not contain $v$ is $G_{n}(q)+\left(q^{n}-1\right) G_{n-1}(q)$.

By Theorem 6.3 we have that the number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n+1}$ that contain $v$ is $\binom{n}{k-1}_{q}$. So the total number of subspaces of $\mathbb{F}_{q}^{n+1}$ that contain $v$ is

$$
\sum_{k=0}^{n+1}\binom{n}{k-1}_{q}=\sum_{k=1}^{n+1}\binom{n}{k-1}_{q}=\sum_{j=0}^{n}\binom{n}{j}_{q}=G_{n}(q)
$$

Also from Theorem 6.3, we have that the number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n+1}$ that do not contain $v$ is $q^{k}\binom{n}{k}_{q}$. So the total number of subspaces of $\mathbb{F}_{q}^{n+1}$ that do not contain $v$ is $\sum_{k=0}^{n} q^{k}\binom{n}{k}_{q}$. Since each $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$ contains $q^{k}$ vectors then $\sum_{k=0}^{n} q^{k}\binom{n}{k}$ is also the total number of vectors counted with multiplicity over each subspace in the collection $\mathcal{G}_{n}(q)$. In other words, $\sum_{k=0}^{n} q^{k}\binom{n}{k}_{q}=\left|\sqcup_{U \in \mathcal{G}_{n}(q)} U\right|$ where $\sqcup_{U \in \mathcal{G}_{n}(q)} U$ is the disjoint union of the collection $\mathcal{G}_{n}(q)$.

Claim: $\left|\sqcup_{U \in \mathcal{G}_{n}(q)} U\right|=G_{n}(q)+\left(q^{n}-1\right) G_{n-1}(q)$.
The number of subspaces of $\mathbb{F}_{q}^{n}$ that contain a given nonzero vector is $G_{n-1}(q)$. There are $q^{n}-1$ nonzero vectors in $\mathbb{F}_{q}$. So the number of nonzero vectors, counted with multiplicity over each subspace in $\mathcal{G}_{n}(q)$, is $\left(q^{n}-1\right) G_{n-1}(q)$. Now each subspace of $\mathbb{F}_{q}^{n}$ contains the zero vector exactly once. So the zero vector appears $G_{n}(q)$ times in the collection $\mathcal{G}_{n}(q)$. Then we have that the total number of vectors over $\mathcal{G}_{n}(q)$, counted with multiplicity over each subspace is, $G_{n}(q)+\left(q^{n}-1\right) G_{n-1}(q)$.

By our claim we have

$$
\sum_{k=0}^{n} q^{k}\binom{n}{k}_{q}=G_{n}(q)+\left(q^{n}-1\right) G_{n-1}(q)
$$

So $\sum_{k=0}^{n} q^{k}\binom{n}{k}_{q}$ is the number of subspaces of $\mathbb{F}_{q}^{n+1}$ that do not contain $v$ and $G_{n}(q)$ is the number of subspaces of $\mathbb{F}_{q}^{n+1}$ that contain $v$. Therefore,

$$
G_{n+1}(q)=2 G_{n}(q)+\left(q^{n}-1\right) G_{n-1}(q) .
$$

## 7. A Group Theoretical Derivation of the $q$-Binomial Coefficients

Now we want to count the number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ in an entirely different manner. In this section we will show how some general results from group theory may be applied to this particular counting problem. The group theoretical theorems and proofs in this section are modeled from those given in [10],[17],[11].

Let $\operatorname{Aut}(V)$ denote the subset of $\mathcal{L}(V)$ containing all of the invertible linear operators on vector space $V$. In other words, $\operatorname{Aut}(V)$ is the set of linear maps from $V$ to $V$ that have an inverse. We can think of $\operatorname{Aut}(V)$ as being the group of units in the ring of $\mathcal{L}(V)$ equipped with the operations of vector addition and function composition.

Let $G=\operatorname{Aut}(V)$ act on the set $X$ of $k$-dimensional subspaces of $V$. Let $x$ be some fixed but arbitrary subspace in $X$. Let $G . x$ be the image of $x$ under this action. In other words, $G . x=\{g \cdot x: g \in G\}$. The set $G . x$ is called the orbit of $x$ under the action of $G$. The stabilizer of $x$, denoted by $G_{x}$, is the subgroup of $G$ defined by $G_{x}=\{g \in G: g \cdot x=x\}$. Let $G / G_{x}$ denote the collection of all left cosets of the subgroup $G_{x}$ of $G$. In the following theorem (which is essentially the orbit stabilizer theorem) we show that the number of left cosets in $G / G_{x}$ is equal to the image size of $G$.x.

Theorem 7.1 ([10]). Let $\phi: G / G_{x} \rightarrow G . x$ by $g G_{x} \mapsto g . x$. Then $\phi$ is a bijection.

Proof. Certainly $\phi$ is surjective since $\phi$ maps $g G_{x}$ to $g . x$ for all $g \in G$.
Let $g G_{x}, h G_{x} \in G / G_{x}$. Assume $g \cdot x=h . x$. Then left multiplying by $h^{-1}$ we have $\left(h^{-1} g\right) . x=x$. So $h^{-1} g \in G_{x}$. Left multiplying by $h$ we have $g \in h G_{x}$. Since $h \in h G_{x}$ we have $g G_{x}=h G_{x}$.

So we have $\left|G / G_{x}\right|=|G . x|$. In the next theorem (which is the crucial argument in

LaGrange's Theorem) we show that all the left cosets of $G_{x}$ have the same cardinality so that $\left|G / G_{x}\right|=\frac{|G|}{\left|G_{x}\right|}$.

Theorem 7.2 ([10]). Let $H$ be a subgroup of group G. Every left coset of $H$ in $G$ has the same cardinality.

Proof. Let $a H, b H$ be left cosets of $H$ in group $G$. Define $f: a H \rightarrow b H$ by $x \mapsto b a^{-1} x$. Then $f$ is injective: Let $x, y \in a H$. Assume $b a^{-1} x=b a^{-1} y$. Then successively left multiplying by $b^{-1}$ and then $a$ we have $x=y$. Also $f$ is surjective: Let $z \in b H$. Then there is an $h$ in $H$ such that $b h=z$. So $f(a h)=b a^{-1} a h=b h=z$.

The following theorem will show that $|G \cdot x|$ is the number of $k$-dimensional subspaces of $V$ by showing that that the action of $G=\operatorname{Aut}(V)$ on $X$, the set of $k$-dimensional subspaces of $V$, is transitive. In other words, for all $x_{1}, x_{2} \in X$, there is an invertible linear operator $g \in G$ such that $g\left(x_{1}\right)=x_{2}$. So that every subspace in $X$ is in $G \cdot x=\{g . x: g \in$ $G\}$.

Theorem 7.3. Let $V$ be an n-dimensional vector space over $\mathbb{F}_{q}$. Let $U, W$ be $k$-dimensional subspaces of $V$. Then there exists an invertible operator $T$ in $\operatorname{Aut}(V)$ such that $T(U)=W$.

Proof. Fix a basis $u_{1}, \ldots, u_{k}$ of $U$. Extend it to a basis $u_{1}, \ldots u_{k}, \ldots u_{n}$ of $V$. Fix a basis $w_{1}, \ldots, w_{k}$ of $W$. Extend it to a basis $w_{1}, \ldots w_{k}, \ldots w_{n}$ of $V$. Define $T: V \rightarrow V$ by $T u_{j}=w_{j}$ for all $j=1, \ldots, n$. By Lemma $5.2, T$ is injective. Also, $T$ is surjective since $w_{1}, \ldots w_{n}$ spans $V$. So $T$ is an invertible linear operator in $\operatorname{Aut}(V)$.

Now consider $\left.T\right|_{U}$. By the same argument given above $T(U)=W$.

So we have $\frac{|G|}{\left|G_{x}\right|}=|G \cdot x|=\binom{n}{k}_{q}$ where $x$ is any given $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$.

We will show

$$
\frac{|G|}{\left|G_{x}\right|}=\frac{\gamma_{n}}{\gamma_{k} \gamma_{n-k} q^{k(n-k)}} .
$$

The numerator, $|G|=\gamma_{n}$.
To find $\left|G_{x}\right|$ we will count the number of of invertible operators $T$ on $\mathbb{F}_{q}^{n}$ such that $T(U)=U$ where $U$ is a $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$. Fix a basis $u_{1}, \ldots, u_{k}$ of $U$ and extend it to $u_{1}, \ldots, u_{k}, v_{k+1}, \ldots, v_{n}$ a basis of $\mathbb{F}_{q}^{n}$. Now $T(U)=U$ if and only if $\left.T\right|_{U}$ is an automorphism of $U$. There are $\gamma_{k}$ ways to map $U$ bijectively to itself. The basis vectors, $v_{k+1}, \ldots, v_{n}$ must be mapped to a linearly independent list of vectors in $V-U$. There are

$$
\begin{aligned}
\left(q^{n}\right. & \left.-q^{k}\right)\left(q^{n}-q^{k+1}\right) \cdots\left(q^{n}-q^{n-1}\right) \\
& =q^{k(n-k)}\left(q^{n-k}-1\right)\left(q^{n-k}-q\right) \cdots\left(q^{n-k}-q^{n-k-1}\right) \\
& =\gamma_{n-k} q^{k(n-k)}
\end{aligned}
$$

such lists of vectors. So $\left|G_{x}\right|=\gamma_{k} \gamma_{n-k} q^{k(n-k)}$. So we have

$$
\binom{n}{k}_{q}=\frac{\gamma_{n}}{\gamma_{k} \gamma_{n-k} q^{k(n-k)}}
$$

## 8. A Derivaton of the $q$-Binomial Coefficients via Generating Functions

In this section we use some ideas given in [9] ,[22],[23],[13] in deriving the $q$-binomial coefficients by considering them as ordinary generating functions. We show that the coefficient of $q^{r}$ in the expansion of $\binom{n}{k}_{q}$, denoted $\left[\left[q^{r}\right]\right]\binom{n}{k}_{q}$, upon multiplication by $q^{r}$, is the number of classes of row equivalent $n \times n$ matrices over $\mathbb{F}_{q}$ of rank $k$ that have exactly $r$ entries not constrained to be 0 or 1 . Our argument proceeds as follows: To each
$k$-dimensional subspace of $\mathbb{F}_{q}^{n}$ we associate exactly one matrix $A$ in $\mathbb{F}^{n, n}$ in ref of rank $k$. Taking $A$ to be a representative of its equivalence class in the row equivalence relation on $\mathbb{F}^{n, n}$ we associate $A$ to exactly one integer partition into at most $k$ parts with each part at most $n-k$. We then show that the o.g.f. counting such partitions is precisely $\binom{n}{k}_{q}$.

Theorem 8.1. Let $\mathcal{G}_{n}(q)$ be the set of all subspaces of $\mathbb{F}_{q}^{n}$. Let $\sim_{R^{*}}$ be the equivalence relation on $\mathbb{F}^{n, n}$ defined by $A \sim_{R^{*}} B$ if and only if $\operatorname{rref}(A)=\operatorname{rref}(B)$ for all $A, B \in \mathbb{F}^{n, n}$. Let $\mathcal{C}$ be the collection of all equivalence classes of $\sim_{R^{*}}$ on $\mathbb{F}_{q}^{n}$. That is, let $\mathcal{C}=\{[A]: A \in$ $\left.\mathbb{F}^{n, n}\right\}$ where $[A]=\left\{B \in \mathbb{F}^{n, n}: A \sim_{R^{*}} B\right\}$. Then there is a 1-1 correspondence between $\mathcal{G}_{n}(q)$ and $\mathcal{C}$.

Proof. Define $\phi: \mathcal{G}_{n}(q) \rightarrow \mathcal{C}$ in the following manner. Let $U \in \mathcal{G}_{n}(q)$ be a $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$ for some $k=0,1, \ldots, n$. Fix a basis $u_{1}, \ldots, u_{k}$ of $U$. Form a matrix $A$ in $\mathbb{F}^{n, n}$ in which the first $k$ rows of $A$ are the $n$-tuples $u_{1}, \ldots, u_{k}$. Complete the matrix by letting the remaining $n-k$ rows be all zeros. Let $\phi(U)=[A]$. Then $\phi$ is a well defined bijection from $\mathcal{G}_{n}(q) \rightarrow \mathcal{C}$.

To show that $\phi$ is well-defined, suppose $\phi(U)=[A]$ and $\phi(U)=[B]$ for some subspace $U \in \mathcal{G}_{n}(q)$ and $[A],[B] \in \mathcal{C}$. Since every matrix is row equivalent to one and only one reduced echelon matrix then $[\mathrm{A}]=[\mathrm{B}]$.

To show that $\phi$ is injective, let $U, V \in \mathcal{G}_{n}(q)$. Assume $\phi(U)=\phi(V)$. Since row reduction does not change the row space of a matrix then the equation $\phi(U)=\phi(V)$ implies that the span of a basis of $U$ is equal to the span of a basis of $V$. So $U=V$.

To show that $\phi$ is surjective, let $[A] \in \mathcal{C}$. Let $U \in \mathcal{G}(q)$ be such that $U$ is equal to the row span of $A$. Then $\phi(U)=[A]$.

The theorem above establishes that there is exactly one matrix of rank $k$ in rref for each $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$. Now we proceed to show that each class of row equivalent
matrices in the collection $\mathcal{C}$ corresponds to an integer partition of $n$ into at most $k$ parts with each part at most $n-k$.

Theorem 8.2. The number of integer partitions of $r$ into at most $k$ parts with each part at most $(n-k)$ is equal to the number of binary words of length $n$ with exactly $k$ l's having exactly $r$ inversions.

Proof. Let $\lambda_{1}+\lambda_{2}+\cdots+\lambda_{j}$ be a partition of $r$ into at most $k$ parts with each part at most $(n-k)$. In other words, choose $j \in\{0, \ldots, k\}$ and $\lambda_{1}, \ldots, \lambda_{j} \in\{1, \ldots, n-k\}$ to satisfy $\sum_{i=1}^{j} \lambda_{i}=r$. Form a binary word $w$ on alphabet $\{0,1\}$ by starting with a string of 0 's having length $(n-k)$. For each $i=1,2, \ldots, j$ counting from the rightmost 0 , insert a 1 to the left of the $\lambda_{i}$ th 0 . Then, in the case that $k>j$ append $(k-j) 1$ 's to the word. Then $w$ is a binary word with exactly $k$ 1's having exactly $r$ inversions. More precisely, for each $i \in\{1,2, \ldots, j\}$ there are exactly $\lambda_{i} 0$ 's appearing to the right of the $i$ 'th 1 in $w$.

The process is reversible. Form an integer partition $\pi$ from a binary word with exactly $k$ 1's and $r$ inversions so that the $i$ th part is equal to the (positive) number of 0 's to the right of the $i$ th 1 for each of the $k 1$ 's in the word. If a 1 has no 0 's to the right of it then it is ignored. In this way $\pi$ will have at most $k$ parts and each part will be at most $n-k$.

In the procedure given in the proof above, we may replace each 0 with a column vector of $n 0$ 's. We may replace each 1 (proceeding in order from left to right) with $e_{1}, e_{2}, \ldots, e_{k}$, the vectors in the standard basis of $\mathbb{F}_{q}^{n}$. We may then replace each 0 appearing to the right of a 1 in any row but not in a column containing a 1 (pivot column) with an X . The resulting array corresponds to an $n \times n$ matrix over $\mathbb{F}$ in rref where the X 's are the field elements in the matrix not constrained to be 0 or 1 .

So we have that each partition of an integer $n$ into at most $k$ parts with each part at most $n-k$ corresponds to exactly one class of row equivalent matrices in $\mathcal{C}$. The following
theorem establishes the generating function counting such partitions, hence such matrices, hence the number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$.

Theorem 8.3. The number of integer partitions into at most $k$ parts with each part at most $l$ is counted by the generating function

$$
\frac{\prod_{i=1}^{k+l}\left(1-q^{i}\right)}{\prod_{i=1}^{k}\left(1-q^{i}\right) \cdot \prod_{i=1}^{l}\left(1-q^{i}\right)}
$$

Proof. The proof is by induction on $k+l$.
Basis step: When $k=0$ or $l=0$ then the generating function is the constant 1 . We will also give here as a basis case the slightly less trivial case when $k=1$ or $l=1$. Then the generating function that counts integer partitions into at most 1 part with each part at most $l$ is

$$
1+q+q^{2}+\cdots+q^{l}=\frac{1-q^{l+1}}{1-q}=\frac{\prod_{i=1}^{1+l}\left(1-q^{i}\right)}{\prod_{i=1}^{1}\left(1-q^{i}\right) \cdot \prod_{i=1}^{l}\left(1-q^{i}\right)}
$$

The same generating function also counts the number of partitions into at most k parts with each part at most 1.

Induction step: Let $k, l \geq 1$. Assume that the statement holds with $\left(k^{\prime}, l^{\prime}\right)$ in place of $(k, l)$ for all $k^{\prime}, l^{\prime}$ with $k^{\prime}+l^{\prime} \leq k+l$. We want to establish the o.g.f. that counts the number of partitions into at most $k+1$ parts with each part at most $l+1$. We may classify such partitions into two types, those that have strictly less that $k+1$ parts and those that have exactly $k+1$ parts. By our induction hypothesis, the former case is counted by

$$
\frac{\prod_{i=1}^{k+l+1}\left(1-q^{i}\right)}{\prod_{i=1}^{k}\left(1-q^{i}\right) \cdot \prod_{i=1}^{l+1}\left(1-q^{i}\right)}
$$

the o.g.f. for partitions into at most $k$ parts with each part at most $l+1$.
The partitions into exactly $k+1$ parts with parts at most $l+1$ are formed from a partition into at most $k+1$ parts with parts at most $l$ by adding 1 to each existing part and
then appending parts of size 1 as needed so that there are exactly $k+1$ parts. So by the multiplication rule for ordinary generating functions [7], the o.g.f. for these partitions is

$$
q^{k+1} \frac{\prod_{i=1}^{k+1+l}\left(1-q^{i}\right)}{\prod_{i=1}^{k+1}\left(1-q^{i}\right) \cdot \prod_{i=1}^{l}\left(1-q^{i}\right)}
$$

So we have that the o.g.f. for the number of partitions into at most $k+1$ parts with each part at most $l+1$ is

$$
\frac{\prod_{i=1}^{k+l+1}\left(1-q^{i}\right)}{\prod_{i=1}^{k}\left(1-q^{i}\right) \cdot \prod_{i=1}^{l+1}\left(1-q^{i}\right)}+q^{k+1} \frac{\prod_{i=1}^{k+1+l}\left(1-q^{i}\right)}{\prod_{i=1}^{k+1}\left(1-q^{i}\right) \cdot \prod_{i=1}^{l}\left(1-q^{i}\right)},
$$

which simplifies to

$$
\frac{\prod_{i=1}^{k+l+2}\left(1-q^{i}\right)}{\prod_{i=1}^{k+1}\left(1-q^{i}\right) \cdot \prod_{i=1}^{l+1}\left(1-q^{i}\right)} .
$$

Making the substitution $l=n-k$ into the expression we have

$$
\frac{\prod_{i=1}^{k+l}\left(1-q^{i}\right)}{\prod_{i=1}^{k}\left(1-q^{i}\right) \cdot \prod_{i=1}^{l}\left(1-q^{i}\right)},
$$

$$
\begin{aligned}
& \frac{\prod_{i=1}^{n}\left(1-q^{i}\right)}{\prod_{i=1}^{k}\left(1-q^{i}\right) \cdot \prod_{i=1}^{n-k}\left(1-q^{i}\right)} \\
& \quad=\frac{\left(q^{n}-1\right)\left(q^{n-1}-1\right) \cdots(q-1)}{\left(q^{k}-1\right)\left(q^{k-1}-1\right) \cdots(q-1) \cdot\left(q^{n-k}-1\right)\left(q^{n-k-1}-1\right) \cdots(q-1)} \\
& \quad=\frac{\left(q^{n}-1\right)\left(q^{n-1}-1\right) \cdots\left(q^{n-k+1}-1\right)}{\left(q^{k}-1\right)\left(q^{k-1}-1\right) \cdots(q-1)} \\
& \quad=\frac{\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)}{\left(q^{k}-1\right)\left(q^{k}-q\right) \cdots\left(q^{k}-q^{k-1}\right)} \\
& \quad=\binom{n}{k}_{q}
\end{aligned}
$$

So we have that $\binom{n}{k}_{q}$ is the o.g.f. for the number of partitions into at most $k$ parts with each part at most $n-k$. We will use this fact to prove the next two theorems sometimes called the $q$-Binomial Theorem and the $q$-Binomial Series. These proofs are based off ideas expressed in [15] and [6]

Theorem 8.4 ([6][15]). For all $n \geq 0$,

$$
\prod_{j=1}^{n}\left(1+t q^{j}\right)=\sum_{k=0}^{n} t^{k} q^{\frac{k(k+1)}{2}}\binom{n}{k}_{q}
$$

Proof. The left-hand side is the bivariate generating function counting the number of integer partitions into distinct parts with each part at most $n$. From each such partition having $k$ parts we may subtract 1 from the smallest part, subtract 2 from the second smallest part, and in general subtract $i$ from the $i$-th smallest part. In this way we obtain a partition into at most $k$ parts with each part at most $n-k$. These are precisely the partitions counted on the left-hand side.

Theorem 8.5 ([6][15]). For all $n \geq 1$,

$$
\prod_{j=1}^{n} \frac{1}{1-t q^{j}}=\sum_{k=0}^{\infty} t^{k} q^{k}\binom{n+k-1}{k}_{q} .
$$

Proof. The left-hand side is the bivariate generating function counting the integer partitions into parts at most $n$. From each such partition having $k$ parts we may subtract 1 from each part to obtain a partition into at most $k$ parts with each part at most $n-1$. These are precisely the partitions counted on the right-hand side.

We have shown that $\left[\left[q^{r}\right]\right]\binom{n}{k}_{q}$ is the number of binary words on alphabet $\{0,1\}$ with exactly $k$ 's and exactly $r$ inversions. We use this interpretation to prove yet another $q$-binomial identity.

Theorem 8.6 ([6][15]). For all $n \geq 0$,

$$
\binom{2 n}{n}_{q}=\sum_{j=0}^{n} q^{j^{2}}\binom{n}{j}_{q}^{2}
$$

Proof. The coefficients of $q^{r}$ in the expansion of the left-hand side give the number of binary words on $\{0,1\}$ with exactly $n 1$ 's and exactly $r$ inversions. We will show that the right-hand side counts the same words. Suppose there are $j$ 1's appearing amongst the first $n$ letters of the word. Then $\binom{n}{j}_{q}$ counts the number of inversions amongst the first n letters. Since there are $j$ 1's amongst the first $n$ letters then there are $(n-j) 1$ 's in the second $n$ letters of the word. So $\binom{n}{n-j}_{q}$ counts the inversions amongst the second half of the word. But we have ignored the inversion pairs with an element in both the first and second half of the word. Since there are $j 1$ 's in the first half there must be $j 0$ 's in the second half of the word. So there are $j^{2}$ such inversions. Summing over all possible $j$ we have $\sum_{j=0}^{n} q^{j^{2}}\binom{n}{j}_{q}\binom{n}{n-j}_{q}=\sum_{j=0}^{n} q^{j^{2}}\binom{n}{j}_{q}^{2}$.

If we sum the Gaussian polynomials $\binom{n}{k}_{q}$ over all possible values $0 \leq k \leq n$, then the coefficient of $q^{r}$ is the total number of binary words having exactly $k$ inversions. These coefficients are given below. A083906.

| 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | 2 |  | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | 3 |  | 4 | 3 | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | 4 |  | 6 | 6 | 6 | 2 | 2 |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | 5 |  | 8 | 9 | 11 | 9 | 7 | 4 |  | 3 | 1 |  |  |  |  |  |  |  |  |
| 8 | 6 | 1 | 0 | 12 | 16 | 16 | 18 | 12 | 21 | 12 | 8 | 6 | 2 |  | 2 |  |  |  |  |
| 9 | 7 |  |  | 15 | 21 | 23 | 29 | 27 |  |  | 23 |  | 15 |  |  | 7 | 4 | 3 | 1 |

Table 8: Coefficients of $\sum_{k=0}^{n}\binom{n}{k}_{q}$, Number of Binary Words Having $k$ Inversions, $n \geq$ $0,0 \leq k \leq \max \{k(n-k): 0 \leq k \leq n\}$. A083906

If we take the derivative of $\sum_{k=0}^{n}\binom{n}{k}_{q}$ and evaluate at $q=1$, then we have the total number of inversions over all binary words of length $n$. A001788
$0,0,1,6,24,80,240,672,1792,4608,11520,28160,67584, \ldots$
Table 9: The total number of inversions over all binary words of length $n$. A001788

## 9. The Rogers-Szego polynomials

In this section we exposit some of the ideas given in [21] regarding the Rogers-Szego polynomials.

For $n \geq 0$, let $H_{n}(z)=\sum_{k=0}^{n}\binom{n}{k}_{q} z^{k}$. The functions in this sequence are called Rogers-Szego polynomials. We can think of the polynomials $H_{n}(z)$ as being $q$-analogs of the polynomial generating functions $B_{n}(z)=(1+z)^{n}$ that count the number of subsets of an $n$-set. Just as the polynomials $B_{n}(z)$ obey the recurrence $B_{n}(z)=(1+z) B_{n-1}(z)$, we
will see that the Rogers-Szego polynomials are such that

$$
H_{n+1}(z)=(1+z) H_{n}(z)+z\left(q^{n}-1\right) H_{n-1}(z)
$$

The equality follows directly from Theorem 9.2 (yet another recurrence relation on the $q$-binomial coefficients). We first give a lemma which is essentially that given in [21].

Lemma 9.1 ([21]). Let $V$ be an $(n+1)$-dimensional vector space over $\mathbb{F}_{q}$ with basis $v_{1}, \ldots, v_{n+1}$. Let $1 \leq k \leq n+1$. Every $k$-dimensional subspace $W$ of $V$ is such that $W=W^{\prime} \oplus \operatorname{span}(v)$, for some $(k-1)$-dimensional subspace $W^{\prime}$ of $V^{\prime}=\operatorname{span}\left(v_{1}, \ldots, v_{n}\right)$ and some $v \in V$.

Proof. Let $W$ be an arbitrary $k$-dimensional subspace of $V$. Suppose first that $W$ is a subspace of $V^{\prime}$. Let $w_{1}, \ldots, w_{k}$ be a basis of $W$. Let $v=w_{1}$ and let $W^{\prime}=\operatorname{span}\left(w_{2}, \ldots, w_{k}\right)$. Then $W=W^{\prime} \oplus \operatorname{span}(v)$.

Now suppose that $W$ is not a subspace of $V^{\prime}$. Then there is some $v \in W$ such that $v \notin V^{\prime}$. Also $\operatorname{dim}\left(W+V^{\prime}\right) \geq \operatorname{dim} V^{\prime}+1=n+1$, and since $\operatorname{dim}\left(W+V^{\prime}\right)$ is not greater than $n+1, \operatorname{dim}\left(W+V^{\prime}\right)=n+1$. Now $\operatorname{dim}\left(W+V^{\prime}\right)=\operatorname{dim} W+\operatorname{dim} V^{\prime}-\operatorname{dim}\left(W \cap V^{\prime}\right)$. So $\operatorname{dim}\left(W \cap V^{\prime}\right)=k-1$. Extend $v$ to a basis $v, w_{1}, \ldots, w_{k-1}$ of $\operatorname{span}(v) \oplus\left(W \cap V^{\prime}\right)$. Then $v, w_{1}, \ldots, w_{k-1}$ is a length $k$ list of linearly independent vectors in $W$. So $W=$ $\operatorname{span}(v) \oplus\left(W \cap V^{\prime}\right)$.

Theorem 9.2. The $q$-binomial coefficients obey the recurrence

$$
\binom{n+1}{k}_{q}=\binom{n}{k}_{q}+\binom{n}{k-1}_{q}+\left(q^{n}-1\right)\binom{n-1}{k-1}_{q}
$$

Proof. By Theorem 6.3, we have

$$
\begin{aligned}
\binom{n+1}{k}_{q}-\binom{n}{k-1}_{q}-\binom{n}{k}_{q} & =q^{k}\binom{n}{k}_{q}-\binom{n}{k}_{q}=\left(q^{k}-1\right)\binom{n}{k}_{q} \\
& =\left(q^{k}-1\right) \frac{\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)}{\left(q^{k}-1\right)\left(q^{k}-q\right) \cdots\left(q^{k}-q^{k-1}\right)} \\
& =\left(q^{n}-1\right) \frac{\left(q^{n}-q\right) \cdots\left(q^{n}-q^{k-1}\right)}{\left(q^{k}-q\right) \cdots\left(q^{k}-q^{k-1}\right)} \\
& =\left(q^{n}-1\right)\binom{n-1}{k-1}_{q}
\end{aligned}
$$

Let $V$ and $V^{\prime}$ be as above in our lemma. By Theorem 6.3, the first term $\binom{n}{k}_{q}$ on the right-hand side of the recurrence $\binom{n+1}{k}_{q}=\binom{n}{k}_{q}+\binom{n}{k-1}_{q}+\left(q^{n}-1\right)\binom{n-1}{k-1}_{q}$ is the number of $k$-dimensional subspaces $W$ of $V$ such that $W$ is a subspace of $V^{\prime}$. Likewise, the second term $\binom{n}{k-1}_{q}$ is the number of $k$-dimensional subspaces $W$ of $V$ such that $W$ is not a subspace of $V^{\prime}$ and $v_{n+1} \in W$. The third term is then the number of $k$-dimensional subspaces $W$ of $V$ such that $W$ is not a subspace of $V^{\prime}$ and $v_{n+1} \notin W$.

By the recurrence in Theorem 9.2 we have

$$
\begin{aligned}
H_{n+1}(z) \sum_{k=0}^{n+1} z^{k} & =\sum_{k=0}^{n+1}\binom{n}{k} z^{k}+\sum_{k=0}^{n+1}\binom{n}{k-1} z^{k}+\left(q^{n}-1\right) \sum_{k=0}^{n+1}\binom{n-1}{k-1} z^{k} \\
& =H_{n}(z)+z H_{n}(z)+\left(q^{n}-1\right) z H_{n-1}(z) \\
& =(1+z) H_{n}(z)+z\left(q^{n}-1\right) H_{n-1}(z)
\end{aligned}
$$

Upon substituting $z=1$ into these polynomials we have $H_{n}(1)=\sum_{k=0}^{n}\binom{n}{k}_{q}$, which gives the Galois numbers. Since the number of vectors in a $k$-dimensional subspace of $\mathbb{F}_{q}^{n}$
is $q^{k}$, then substituting $z=q$ we have $H_{n}(q)=\sum_{k=0}^{n}\binom{n}{k}_{q} q^{k}$, which gives the total number of vectors counted with multiplicity over all subspaces of $\mathbb{F}_{q}^{n}$. The first few terms of the sequence (A182176) for the case $q=2$ and $n \geq 0$ are given in Table 10
$1,3,11,51,307,2451,26387,387987,7866259,221472147,8703733139 \ldots$.

Table 10: The size of the disjoint union, $\sqcup_{U \in \mathcal{G}_{n}(2)} U$. A182176

Substituting $z=-1$ into the functional recurrence,

$$
H_{n+1}(z)=(1+z) H_{n}(z)+z\left(q^{n}-1\right) H_{n-1}(z),
$$

gives $H_{n}(-1)=\left(1-q^{n}\right) H_{n-1}(-1)$. Since $H_{0}(-1)=1$ and $H_{1}(-1)=0$, we have $H_{n}(-1)=\left(1-q^{n-1}\right)\left(1-q^{n-3}\right) \cdots(1-q)$ for even $n$ and $H_{n}(-1)=0$ for odd $n$. In particular for the case $q=2$ we have the alternating sums of the Gaussian coefficients, that is, we have sequence A290974 defined by $a_{n}=\sum_{k=0}^{n}(-1)^{k}\binom{n}{k}$. Note that the analogous alternating sums in Pascal's triangle are always 0 .
$1,0,-1,0,7,0,-217,0,27559,0,-14082649,0,28827182503,0,-236123451882073, \ldots$
Table 11: $H_{n}(-1)=\sum_{k=0}^{n}\binom{n}{k}_{2}(-1)^{k}$ for $n \geq 0$. A290974

## 10. Flags in Finite Vector Spaces

In this section we count the number of complete flags by two different methods. We loosely follow similar arguments given in [16] and [21].

Definition 10.1. A flag of length $m$ is a sequence of subspaces

$$
V=V_{0} \supset V_{1} \supset V_{2} \supset \cdots \supset V_{m-1} \supset V_{m}=\{0\}
$$

of a vector space $V$, where each subspace in the sequence properly contains the subsequent subspace.

Let $\operatorname{dim} V=n$. Let $n_{k}=\operatorname{dim} V_{k}-\operatorname{dim} V_{k+1}$ for $k=0,1, \ldots m-1$. Then $n=$ $n_{0}+n_{1}+\cdots+n_{m-1}$. We will call $\left(n_{0}, n_{1}, \ldots, n_{m}-1\right)$ the signature of our flag. The dimension of $V_{1}$ is $n-n_{0}$ so there are $\binom{n}{n-n_{0}}_{q}$ choices for $V_{1}$. Likewise there are $\binom{n-n_{0}}{n-n_{0}-n_{1}}$. choices for $V_{2}$. Continuing in this fashion we have that the number of flags of length $m$ with signature $\left(n_{0}, n_{1}, \ldots, n_{m}-1\right)$ is

$$
\binom{n}{n-n_{0}}_{q}\binom{n-n_{0}}{n-n_{0}-n_{1}}_{q} \cdots\binom{n-n_{0}-\cdots n_{m-3}}{n-n_{0}-n_{1}-\cdots n_{m-2}}_{q}\binom{n-n_{0}-\cdots n_{m-2}}{n-n_{0}-n_{1}-n_{m-1}}_{q}
$$

We note that the last factor is equal to 1 and represents the number of ways to choose a 0 dimensional subspace of $V_{m-1}$. Since the $q$-binomial coefficients are such that $\binom{n}{j}_{q}=$ $\binom{n}{n-j}_{q}$ for $j \in\{1, \ldots, n\}$, the above expression can be simplified to

$$
\binom{n}{n_{0}}_{q}\binom{n-n_{0}}{n_{1}}_{q} \cdots\binom{n-n_{0}-\cdots n_{m-3}}{n_{m-2}}_{q}\binom{n-n_{0}-\cdots n_{m-2}}{n_{m-1}}_{q} .
$$

Then since $\binom{n}{k}_{q}=\frac{[n]_{q}!}{[n-k]_{q}![k]_{q}!}$ we have that the number of flags of an $n$-dimensional vector space over $\mathbb{F}_{q}$ with signature $\left(n_{0}, n_{1}, \ldots, n_{m}-1\right)$ is $\frac{[n]_{q}!}{\left.\left[n_{0}\right]\right]_{q}!,\left[n_{1}\right] q^{!}, \ldots,\left[n_{m}-1\right]_{q}!}$. This quantity is called the $q$-multinomial coefficient.

A complete flag of an $n$ dimensional vector space is a flag of length $n$. From the above, we see that the number of complete flags is $[n]_{q}!$. For $n \geq 0, q=2$ we have A005329, as given in Table 12.
$1,1,3,21,315,9765,615195,78129765,19923090075, \ldots$
Table 12: Number of complete flags in $\mathbb{F}_{2}^{n}$, for $n \geq 0$. A005329

Alternatively, we can arrive at the same result by considering the group action on a set where the group is the group $\operatorname{Aut}\left(\mathbb{F}_{q}\right)$ of vector space automorphisms and the set is the set
$\mathcal{F}$ of all complete flags of $\mathbb{F}_{q}^{n}$. Each operator $T$ in $\operatorname{Aut}\left(\mathbb{F}_{q}\right)$ will act on a flag in $\mathcal{F}$ in the expected way, that is, by mapping its subspaces to $T(U)$ for each $U$ in the flag. The next two theorems will allow us to determine the order of the stabilizer subgroup of an arbitrary flag in $X$. The second proof is essentially that given in [5].

Theorem 10.2. The group $\operatorname{Aut}\left(\mathbb{F}_{q}\right)$ acts transitively on the set $\mathcal{F}$ of all complete flags of $\mathbb{F}_{q}^{n}$.

Proof. Let $A$ be an arbitrary complete flag $\{0\}=U_{0} \subset U_{1} \subset U_{2} \subset \cdots \subset U_{n}=\mathbb{F}_{q}^{n}$ in $\mathcal{F}$. Let $B$ be an arbitrary complete flag $\{0\}=W_{0} \subset W_{1} \subset W_{2} \subset \cdots \subset W_{n}=\mathbb{F}_{q}^{n}$ in $\mathcal{F}$. Fix basis $u_{1}, \ldots u_{n}$ and $w_{1}, \ldots w_{n}$ of $\mathbb{F}_{q}^{n}$ such that for each $j \in\{1, \ldots, n\}, u_{1}, \ldots u_{j}$ is a basis of $U_{j}$ and $w_{1}, \ldots w_{j}$ is a basis of $W_{j}$. Let $T \in \operatorname{Aut}\left(\mathbb{F}_{q}\right)$ be such that $T u_{j}=w_{j}$. for each $j \in\{1, \ldots, n\}$ Then $T\left(U_{j}\right)=W_{j}$ for each $j \in\{1, \ldots, n\}$. So $T . A=B$. So that $\operatorname{Aut}\left(\mathbb{F}_{q}\right)$ acts transitively on the set $\mathcal{F}$.

Theorem 10.3 ([5]). Let $T \in \mathcal{L}\left(\mathbb{F}_{q}^{n}\right)$ and let $v_{1}, \ldots, v_{n}$ be a basis of $\mathbb{F}_{q}^{n}$. Then the following are equivalent.
(a) The matrix of $T$ with respect to $v_{1}, \ldots, v_{n}$ is upper triangular.
(b) $T v_{j} \in \operatorname{span}\left(v_{1}, \ldots, v_{j}\right)$ for each $j=1, \ldots, n$.
(c) $\operatorname{span}\left(v_{1}, \ldots, v_{n}\right)$ is invariant under $T$ for each $j=1, \ldots, n$.

Proof. The equivalence of (a) and (b) are obvious from the definition of an upper triangular matrix and its associated linear operator. Also (c) clearly implies (b). We will show that (b) implies (c).

Assume $T v_{j} \in \operatorname{span}\left(v_{1}, \ldots, v_{j}\right)$ for each $j \in\{1, \ldots, n\}$. Let $j$ be fixed but arbitrary. Let $v \in \operatorname{span}\left(v_{1}, \ldots, v_{j}\right)$. Then $v=a_{1} v_{1}+\cdots+a_{j} v_{j}$ for some scalars $a_{1}, \ldots, a_{j} \in \mathbb{F}$. Then $T v=a_{1} T v_{1}+\cdots+a_{j} T v_{j}$. Since $T v_{j} \in \operatorname{span}\left(v_{1}, \ldots, v_{j}\right)$ for each $j$ then each term is in $\operatorname{span}\left(v_{1}, \ldots, v_{j}\right)$. So $T v \in \operatorname{span}\left(v_{1}, \ldots, v_{j}\right)$. So $\operatorname{span}\left(v_{1}, \ldots, v_{j}\right)$ is invariant under $T$.

From the above proof we see that the matrices in $\mathrm{GL}_{n}\left(\mathbb{F}_{q}\right)$ that act trivially on a complete flag are precisely the upper triangular matrices. So the order of the stabilizer subgroup of a particular flag is the number of $n \times n$ invertible upper triangular matrices with respect to an appropriate choice of basis. For each of the $n$ entries along the main diagonal we may choose any of the $(q-1)$ nonzero field elements. For each of the $\binom{n}{2}$ entries above the diagonal we have $q$ choices. So there are $(q-1)^{n} q^{\binom{n}{2}}$ upper triangular matrices over $\mathbb{F}_{q}^{n}$. So the number of complete flags is

$$
\frac{\gamma_{n}}{(q-1)^{n} q^{\binom{n}{2}}}
$$

## 11. The $q$-analog of the Exponential Function

In this section we define the $q$-exponential function $e_{q}(z)$. We view $e_{q}(z)$ as a generating function suceptible to the various operations (e.g. multiplication, taking derivatives, functional compositions ) that we would apply to other functions to obtain counting results via exponential generating functions. We give some examples where operations applied to $e_{q}(z)$ give enumeration results concerning subspaces analogous to the results concerning subsets obtained by applying the same operations on the exponential function $\exp (z)$.

Definition 11.1. The $q$-exponential function is defined $e_{q}(z)=\sum_{n=0}^{\infty} \frac{z^{n}}{[n]_{q}!}$ where $[n]_{q}$ is called the $q$-number and is defined $[n]_{q}=1+q+q^{2}+\cdots+q^{n-1}=\frac{1-q^{n}}{1-q}$ for $n \geq 1$ and $[0]_{q}=1$.

Definition 11.2. Let $\left(a_{n}\right)_{n=0}^{\infty}$ be a sequence. The $q$-exponential generating function ( $q$ e.g.f.) of the sequence $\left(a_{n}\right)_{n=0}^{\infty}$ is the formal power series $A(z)=\sum_{n=0}^{\infty} \frac{a_{n}}{[n] q!} z^{n}$.

Definition 11.3. Let $\left(f_{n, k}\right)$ be an array of numbers. The bivariate $q$-exponential generating function of the array $\left(f_{n, k}\right)$ is the formal power series $F(z, u)=\sum_{n, k} f_{n, k} u^{k} \frac{z^{n}}{[n]!!}$.

Since we have $\binom{n}{k}_{q}=\frac{[n]_{q}!}{\left.[n-k]_{q}!k\right]_{q}!}$

$$
\begin{aligned}
& e_{q}(z) \cdot e_{q}(z) \\
& \quad=\sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{z^{n}}{[k]_{q}![n-k]_{q}!} \\
& \quad=\sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{\binom{n}{k}_{q} z^{n}}{[n]_{q}!} \\
& \\
& =\sum_{n=0}^{\infty} \frac{1}{[n]_{q}!} G_{n}(q) z^{n}
\end{aligned}
$$

So the coefficient of $z^{n}$ in the expansion of $e_{q}(z)^{2}$ upon multiplication by $[n]_{q}!$ is $G_{n}(q)$, the total number of subspaces of $\mathbb{F}_{q}^{n}$. So $e_{q}(z)^{2}$ is the $q$-exponential generating function for the sequence of Galois numbers. We note that in particular $\frac{z^{k}}{[k]_{q}!} e_{q}(z)$ is the $q$-e.g.f. for the number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$. Also, the bivariate $q$-exponential generating function for the number of $k$-dimensional subspaces of $\mathbb{F}_{q}^{n}$ is $e_{q}(u z) \cdot e_{q}(z)$. So that $e_{q}(u z)$. $e_{q}(z)$ generates Table 5 in section 3.

Let $\cosh _{q}(z)=\sum_{n=0}^{\infty} \frac{z^{2 n}}{[2 n] q!}$. Then the $q$-e.g.f. for the sequence counting the number of subspaces of even dimension over $\mathbb{F}_{q}^{n}$ is $\cosh _{q}(z) \cdot e_{q}(z)$. For $q=2$ and $n \geq 0$ the sequence

## $1,1,2,8,37,187,1304,14606,222379,4141729,107836478 \ldots$

Table 13: Number of subspaces in $\mathbb{F}_{2}^{n}$ that have even dimension, for $n \geq 0$. A289540

We may similarly define $\sinh _{q}(z)=\sum_{n=0}^{\infty} \frac{z^{2 n+1}}{[2 n+1]_{q}!}$. Then the $q$-e.g.f. counting the subspaces of odd dimension is $\sinh _{q}(z) \cdot e_{q}(z)$. So we have the identity $e_{q}(z)=\sinh _{q}(z)+$ $\cosh _{q}(z)$.

The $q$-e.g.f. for the sequence of alternating sums of the Gaussian coefficients is $e_{q}(-z)$. $e_{q}(z)$. So that $e_{q}(-z) \cdot e_{q}(z)$ generates Table 11 in section 9 . We note that $e_{q}(-z) \cdot e_{q}(z) \neq 1$.

Choose a subspace $U$ of $\mathbb{F}_{q}^{n}$ then choose a subspace $W$ of $U$. The $q$-e.g.f. for the number of ways to perform this task is $e_{q}(z)^{3}$. The number of choices in which $W$ has dimension $m=0,1, \ldots, n$ is $\sum_{k=0}^{n}\binom{n}{k}_{q}\binom{k}{m}_{q}$ and is given by $e_{q}(u z) e_{q}(z)^{2}$. These numbers for the case $q=2$ are given in the table below.

| 1 |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 2 | 1 |  |  |  |  |
| 5 | 6 | 1 |  |  |  |
| 16 | 35 | 14 | 1 |  |  |
| 67 | 240 | 175 | 30 | 1 |  |
| 374 | 2077 | 2480 | 775 | 62 | 1 |

Table 14: Number of ways to choose a $k$-dimensional subspace of a subspace of $\mathbb{F}_{2}^{n}$, for $0 \leq k \leq n, n \geq 0$

We note that the column corresponding to $m=0$ is $G_{n}(2)$ and the column $m=1$ is the number of nonzero vectors over $\mathcal{G}_{n}(2)$ and is equal to $\left(2^{n}-1\right) G_{n-1}(2)$ per our results from

Theorem 4.2 . It is also important to realize that the number of nonzero vectors corresponds to the number of 1-dimensional subspaces only for the case when $q=2$. For example the table below gives the number of ways to choose a subspace $U$ of $\mathbb{F}_{3}^{n}$ and then choose a subspace $W$ of $U$ having dimension $m$ for $0 \leq m \leq n$. The column corresponding to $m=1$ is NOT the number of nonzero vectors over $\mathcal{G}_{n}(3)$.

| 1 |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 2 | 1 |  |  |  |  |
| 6 | 8 | 1 |  |  |  |
| 28 | 78 | 26 | 1 |  |  |
| 212 | 1120 | 780 | 80 | 1 |  |
| 2664 | 25652 | 33880 | 7260 | 242 | 1 |

Table 15: Number of ways to choose a $k$-dimensional subspace of a subspace of $\mathbb{F}_{3}^{n}$, for $0 \leq k \leq n, n \geq 0$

The $q$-multinomial coefficient was shown in Section 8 to be the number of flags of an $n$ dimensional vector space over $\mathbb{F}_{q}$. So the $q$-e.g.f. for the number of complete flags is $\frac{1}{1-z}$. The $q$-exponential generating function counting the number of flags in $\mathbb{F}_{q}^{n}$ of all lengths is then $\frac{1}{\left.1-\left(e_{q}(z)-1\right)\right)}$. The analogy with ordered set partitions is clear. This is sequence A289545.

$$
1,1,4,36,696,27808,2257888,369572160,121459776768,79991977040128, \ldots
$$

Table 16: Number of flags in $\mathbb{F}_{q}^{n}$ for $n \geq 0$. A289545

We classify these flags by their length in the following table given by $\frac{1}{\left.1-u\left(e_{q}(z)-1\right)\right)}$. This is sequence A289946.


Table 17: Number of flags of length m in $\mathbb{F}_{q}^{n}$ for $0 \leq m \leq n, n \geq 0$. A289946

We note that the main diagonal is the $q$-factorial numbers counting complete flags and that the column for flags of length two is $G_{n}(q)-2$.

We may neglect the restrictions in our definition of a flag that the initial subspace of the sequence be the zero subspace and that the final subspace of the sequence be the entire space. We will call such sequences, chains of subspaces. A chain is then a path in the graph of the partial order (by subspace inclusion) of the subspaces of a finite dimensional vector space. The path may have length from 0ton, the dimension of the vector space. Note that there are $G_{n}(q)$ chains of length zero in $\mathbb{F}_{q}^{n}$. The total number of chains of subspaces is counted by $\frac{e_{q}(z)^{2}}{\left.1-\left(e_{q}(z)-1\right)\right)}$. This is sequence A293844.
$1,3,15,143,2783,111231,9031551,1478288639,485839107071$

Table 18: Number of chains in $\mathbb{F}_{q}^{n}$ for $n \geq 0$. A293844

The number of chains in $\mathbb{F}_{q}^{n}$ of length $k, 0 \leq k \leq n$ is counted by the bivariate function $\frac{e_{q}(z)^{2}}{\left.1-u\left(e_{q}(z)-1\right)\right)}$. This is sequence A293845.

| 1 |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 2 | 1 |  |  |  |  |
| 5 | 7 | 3 |  |  |  |
| 16 | 50 | 56 | 21 |  |  |
| 67 | 446 | 1010 | 945 | 315 |  |
| 374 | 5395 | 22692 | 40455 | 32550 | 9765 |

Table 19: Number of chains of length k in $\mathbb{F}_{q}^{n}$ for $0 \leq k \leq n, n \geq 0$. A293845

## 12. Direct Sum Decompositions

In this section we follow [16] and [8] to develop the $q$-analog of the Bell and Stirling set partition numbers. We will count the number of direct sum decompositions (DSD's) of $\mathbb{F}_{q}^{n}$ and classify them in various manners.

Definition 12.1. A direct sum decomposition (splitting) of $\mathbb{F}_{q}^{n}$ into $m$ subspaces is a set of nonzero subspaces $\left\{U_{i}\right\}_{i=1, \ldots, m}$ such that each vector $v$ in $\mathbb{F}_{q}^{n}$ has a unique representation $v=u_{1}+\ldots+u_{m}$ where $u_{i} \in U_{i}, \forall i \in\{1, \ldots, m\}$.

We let $\left\{\begin{array}{l}n \\ k\end{array}\right\}_{q}$ denote the number of DSD's of an $n$ dimensional vector space over $\mathbb{F}_{q}$ into exactly $k$ subspaces. We will call two subspaces of $\mathbb{F}_{q}^{n}$ disjoint if their intersection is the zero subspace.

Let $n_{1}+n_{2}+\cdots+n_{m}=n$ (where $n_{i}$ is a positive integer $\forall i \in\{1, \ldots, m\}$ ) be a composition of $n$ into exactly $m$ parts. We want to first count the number of direct sum decompositions $U_{1} \oplus \cdots \oplus U_{m}$ of $\mathbb{F}_{q}^{n}$ such that $\operatorname{dim} U_{i}=n_{i}$ for all $i \in\{1, \ldots, m\}$.

There are $\binom{n}{n_{1}}_{q}=\frac{\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{n_{1}-1}\right)}{\left(q^{n_{1}}-1\right)\left(q^{n_{1}}-q\right) \cdots\left(q^{n_{1}}-q^{n_{1}-1}\right)}=\frac{\left(q^{n}-1\right)\left(q^{n}-q\right) \cdots\left(q^{n}-q^{n_{1}-1}\right)}{\gamma_{n_{1}}}$ subspaces of $\mathbb{F}_{q}^{n}$
with dimension $n_{1}$. The number of dimension $n_{2}$ subspaces that are disjoint from such a subspace (equivalently the number of dimension $n_{2}$ subspaces that avoid the span of such a subspace) is $\frac{\left(q^{n}-q^{n_{1}}\right)\left(q^{n}-q^{n_{1}+1}\right) \cdots\left(q^{n}-q^{n_{1}+n_{2}-1}\right)}{\left(q^{n_{2}}-1\right)\left(q^{n_{2}}-q\right) \cdots\left(q^{n_{2}}-q^{n_{2}-1}\right)}=\frac{\left(q^{n}-q^{n_{1}}\right)\left(q^{n}-q^{n_{1}+1}\right) \cdots\left(q^{n}-q^{n_{1}+n_{2}-1}\right)}{\gamma_{n_{2}}}$. Continuing in this fashion we have:

$$
\begin{gathered}
\frac{\left(q^{n}-1\right) \cdots\left(q^{n}-q^{n_{1}-1}\right)}{\gamma_{n_{1}}} \cdot \frac{\left(q^{n}-q^{n_{1}}\right) \cdots\left(q^{n}-q^{n_{1}+n_{2}-1}\right)}{\gamma_{n_{2}}} \cdots \frac{\left(q^{n}-q^{\left.n_{1}+n_{2}+\cdots+n_{m-1}\right) \cdots\left(q^{n}-q^{n-1}\right)}\right.}{\gamma_{n_{m}}}= \\
\frac{\gamma_{n}}{\gamma_{n_{1} \gamma_{n_{2}} \cdots \gamma_{n}}} .
\end{gathered}
$$

What we have counted here could be called ordered decompositions having a particular signature, i.e., $n_{1}, n_{2}, \ldots n_{m}$. To count the number of decompositions of $\mathbb{F}_{q}^{n}$ into exactly $m$ subspaces we need to sum over all possible compositions of $n$ into exactly $m$ parts and then divide by $m$ !. So we have that there are $\frac{1}{m!} \sum_{n_{1}+\cdots+n_{m}=n, n_{i} \geq 1} \frac{\gamma_{n}}{\gamma_{n_{1}} \cdots \gamma_{n_{m}}}$ direct sum decompositions of $\mathbb{F}_{q}^{n}$ into exactly $m$ subspaces.

Define $\gamma(z)=\sum_{r=0}^{\infty} \frac{z^{r}}{\gamma_{r}}$. Then $\exp (\gamma(z)-1)$ does the work of summing over every possible integer composition into an arbitrary number (say $m$ ) of parts and then dividing by $m!$. In other words, $\gamma_{n}\left[\left[z^{n}\right]\right] \exp (\gamma(z)-1)$ is the total number of DSD's of $\mathbb{F}_{q}^{n}$ into any number of subspaces. For the case $q=2, n \geq 0$ this is sequence A270881. We can think of this sequence as a $q$-analog of the Bell numbers. The terms for $n=1, \ldots 9$ are:
$1,1,4,57,2921,540145,364558049,906918346689,8394259686375297 \ldots$
Table 20: Number of direct sum decompositions of $\mathbb{F}_{2}^{n}$, for $n \geq 0$. A270881

The number of DSD's of $\mathbb{F}_{q}^{n}$ into exactly $k$ subspaces is given by the bivariate generating function, $\exp (u(\gamma(z)-1))$. For the case $q=2, n \geq 1,1 \leq k \leq n$, this is sequence A270880.

| 1 |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: |
| 1 | 3 |  |  |  |
| 1 | 28 | 28 |  |  |
| 1 | 400 | 1680 | 840 | 83328 |
| 1 | 10416 | 168640 | 277760 |  |
| 1 | 525792 | 36053248 | 159989760 | 139991040 |
| 27998208 |  |  |  |  |

Table 21: Number of direct sum decompositions of $\mathbb{F}_{2}^{n}$ into exactly $k$ subspaces, for $0 \leq$ $k \leq n, n \geq 0 . \mathrm{A} 270880$

The number of DSD's of $\mathbb{F}_{q}^{n}$ containing exactly $k, 0 \leq k \leq n$ subspaces of dimension 1 is given by $\exp (\gamma(z)-1-z+u z)$. For $q=2, n \geq 1,1 \leq k \leq n$, this is sequence A289544.

| 1 |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 0 | 1 |  |  |  |  |  |
| 1 | 0 | 3 | 28 |  |  |  |
| 1 | 28 | 0 | 0 | 840 |  |  |
| 281 | 120 | 1680 | 0338 |  |  |  |
| 9921 | 139376 | 29760 | 277760 | 0 | 8339 | 0 |
| 16078337 | 20000736 | 140491008 | 19998720 | 139991040 | 0 | 27998208 |

Table 22: Number of direct sum decompositions of $\mathbb{F}_{2}^{n}$, having exactly $k$ subspaces of dimension 1 for $0 \leq k \leq n, n \geq 0$. A289544

The number of DSD's of $\mathbb{F}_{q}^{n}$ into subspaces of dimension at most $k, 1 \leq k \leq n$ is sequence A298561. The generating function for column $k$ is $\exp \left(\sum_{r=0}^{\infty} \frac{z^{r}}{\gamma_{r}}\right)$.

| 1 |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :--- |
| 3 | 4 |  |  |  |  |
| 28 | 56 | 57 |  |  |  |
| 840 | 2800 | 2920 | 2921 |  |  |
| 83328 | 499968 | 539648 | 540144 | 540145 |  |
| 27998208 | 323534848 | 363889408 | 364556032 | 364558048 | 364558049 |

Table 23: number of direct sum decompositions of $\mathbb{F}_{q}^{n}$ into subspaces of dimension at most $k, 1 \leq k \leq n$. A298561

We note that the first column (A053601) is the number of unordered basis of $\mathbb{F}_{2}^{n}$, that is $\frac{\gamma_{n}}{n!}$. The main diagonal is Table 20.

The number of DSD's of $\mathbb{F}_{2}^{n}$ with maximal subspace of dimension $k, 1 \leq k \leq n$ is the differences in adjacent columns of the table above. This is sequence A298399.

| 1 |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 3 | 1 |  |  |  |  |
| 28 | 28 | 1 |  |  |  |
| 840 | 1960 | 120 | 1 |  |  |
| 83328 | 416640 | 39680 | 496 | 1 |  |
| 27998208 | 295536640 | 40354560 | 666624 | 2016 | 1 |

Table 24: number of direct sum decompositions of $\mathbb{F}_{2}^{n}$ with maximal subspace of dimen$\operatorname{sion} k, 1 \leq k \leq n$. A298399

The number of ordered DSD's of $\mathbb{F}_{q}^{n}$ is given by $\frac{1}{1-(\gamma(z)-1)}$. For $q=2, n \geq 0$ this is sequence A000000.

```
\(1,1,7,225,31041,17698273,41014759873,383214694567809,14378402336340492033 \ldots\).
```

Table 25: Number of ordered direct sum decompositions of $\mathbb{F}_{2}^{n}$ for $n \geq 0$

The number of ordered DSD's of $\mathbb{F}_{q}^{n}$ containing exactly $k$ subspaces is given by $\frac{1}{1-u(\gamma(z)-1)}$. For $q=2$, this is sequence A 000000 for $n \geq 1,1 \leq k \leq n$. Note that the main diagonal is $\gamma_{n}(2)$

| 1 |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 6 |  |  |  |  |
| 1 | 56 | 168 |  |  |  |
| 1 | 800 | 10080 | 20160 |  |  |
| 1 | 20832 | 1011840 | 6666240 | 999360 |  |
| 1 | 1051584 | 216319488 | 3839754240 | 16798924800 | 20158709760 |

Table 26: Number of ordered direct sum decompositions of $\mathbb{F}_{2}^{n}$ containing exactly $k$ subspaces for $1 \leq k \leq n, n \geq 0$.

Suppose $U$ is an $(n-k)$-dimensional subspace of $\mathbb{F}_{q}^{n}$. How many subspaces $W$ are there such that $U \oplus W=\mathbb{F}_{q}^{n}$ ? Now $W$ must be of dimension $k$ and must be disjoint from $U$, so we will choose an ordered basis that avoids the span of $U$. There are $\left(q^{n}-q^{n-k}\right)\left(q^{n}-\right.$ $\left.q^{n-k+1}\right) \cdots\left(q^{n}-q^{n-1}\right)$ ways to do this. We divide this product by $\gamma_{k}$ and do some creative simplification.

$$
\begin{gathered}
\frac{\left(q^{n}-q^{n-k}\right)\left(q^{n}-q^{n-k+1}\right) \cdots\left(q^{n}-q^{n-1}\right)}{\left(q^{k}-1\right)\left(q^{k}-q\right) \cdots\left(q^{k}-q^{k-1}\right)}= \\
\frac{\left(q^{k}-1\right)\left(q^{k-1}-1\right) \cdots(q-1) q^{(n-k)+(n-k+1)+\cdots(n-1)}}{\left(q^{k}-1\right)\left(q^{k-1}-1\right) \cdots(q-1) q^{1+2+\cdots+(k-1)}}= \\
\frac{\left(q^{k}-1\right)\left(q^{k-1}-1\right) \cdots(q-1) q^{k(n-k)} q^{1+2+\cdots(k-1)}}{\left(q^{k}-1\right)\left(q^{k-1}-1\right) \cdots(q-1) q^{1+2+\cdots+(k-1)}}= \\
q^{k(n-k)}
\end{gathered}
$$

Unlike a set partition, not every vector in $\mathbb{F}_{q}^{n}$ appears in a DSD of $\mathbb{F}_{q}^{n}$. More precisely, given any nonzero vector $v \in \mathbb{F}_{q}^{n}$, it is not the case that $v \in \bigcup_{i=1}^{m} U_{i}$ for every DSD $\left\{U_{1}, \ldots U_{m}\right\}$. For example, in the extreme case of a DSD that is composed entirely of 1dimensional subspaces, only $n$ of the $q^{n}-1$ nonzero vectors appear in the splitting. We are led to ask what is the number of DSD's in which a given nonzero vector appears. Adopting the notation and following the arguments given in [8] we let $D_{q}(n, m)$ notate the number of DSD's of $\mathbb{F}_{q}^{n}$ into exactly $m$ subspaces in which a given nonzero vector appears. We will follow closely the argument in [8] to derive a recurrence formula that provides the answer.

Let $v$ be a given nonzero vector in $\mathbb{F}_{q}^{n}$. Let $U$ be an $(n-k)$-dimensional subspace of $\mathbb{F}_{q}^{n}$ that contains $v$ where $k$ ranges from 0 to $(n-1)$. Then $U$ contains $\operatorname{span}(v)$ so there are $\binom{n-1}{n-k-1}_{q}$ choices for such a subspace $U$. From above, there are $q^{k(n-k)}$ choices for a subspace $W$ that is disjoint from $U$ such that $U \oplus W=V$. Then there are $D_{q}(k, m-1)$ ways to form a DSD of $W$ into $m-1$ subspaces. Summing over all possible values of $k$ we have: $D_{q}(n, m)=\sum_{k=0}^{n-1}\binom{n-1}{n-k-1} q^{k(n-k)} D_{q}(k, m-1)$. The number of DSD's of $\mathbb{F}_{2}^{n}$ in which a given nonzero vector appears for $n \geq 1$ is sequence A270883.
$1,3,29,961,110657,45148929,66294748161,355213310611457 \ldots$

Table 27: Number of direct sum decompositions of $\mathbb{F}_{2}^{n}$ containing a given nonzero vector for $n \geq 1$. A270883

The number of such DSD's of $\mathbb{F}_{2}^{n}$ into exactly $k$ subspaces $n \geq 1,1 \leq k \leq n$ is sequence A270882

| 1 |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 2 |  |  |  |  |  |
| 1 | 16 | 12 |  |  |  |  |
| 1 | 176 | 560 | 224 | 13440 |  |  |
| 1 | 3456 | 40000 | 53760 | 15554560 | 2666496 |  |
| 1 | 128000 | 5848832 | 20951040 |  |  |  |
| 1 | 9115648 | 1934195712 | 17826414592 | 30398054400 | 14335082496 | 1791885312 |

Table 28: Number of direct sum decompositions of $\mathbb{F}_{2}^{n}$ that contain a given nonzero vector and that contain exactly $k$ subspaces for $1 \leq k \leq n, n \geq 1$. A270882

## 13. The Number of $n \times n$ Diagonalizable Matrices

In this section we follow the arguments in [16] to determine the number of diagonalizable $n \times n$ matrices with entries in $\mathbb{F}_{q}$. We will see that each such matrix corresponds to a sequence of eigenspaces. As in the previous section we will follow [16] by employing the function, $\gamma(z)=\sum_{r \geq 0} \frac{z^{r}}{\gamma_{r}}$ to obtain various statistics concerning diagonalizable matrices. We exposit the ideas in [16] to derive generating function formulas for sequences of integers related to projections.

Definition 13.1 ([5]). Let $A$ be an $n \times n$ matrix over a field $\mathbb{F}$ and let $\lambda \in \mathbb{F}$. The eigenspace of $A$ corresponding to $\lambda$ is denoted $E(\lambda, A)$ and is equal to null $(A-\lambda I)$. In other words, $E(\lambda, A)$ is the vector space consisting of all eigenvectors corresponding to $\lambda$ along with the zero vector. Note that if $\lambda$ is not an eigenvalue of $A$ then $E(\lambda, A)=\{0\}$.

An $n \times n$ matrix A with entries in $\mathbb{F}_{q}$ is diagonalizable if and only if there is a basis of $\mathbb{F}_{q}^{n}$ consisting precisely of eigenvectors of A if and only if the sum of its eigenspaces is a direct sum equaling $\mathbb{F}_{q}^{n}$.

We define a weak decomposition of a vector space $V$ as a sequence of subspaces of $V$ in which the nonzero subspaces form a direct sum decomposition of $V$. In other words, a weak decomposition of $V$ is a sequence $U_{1}, U_{2}, \ldots, U_{k}$ of subspaces of $V$ in which some of the subspaces are allowed to be the zero subspace and $U_{1} \oplus U_{2} \oplus \cdots \oplus U_{k}=V$.

Theorem 13.2. There is a 1-1 correspondence between the number of diagonalizable $n \times n$ matrices $A$ with entries in $\mathbb{F}_{q}$ and the number of weak decompositions of $\mathbb{F}_{q}^{n}$ into exactly $q$ subspaces, $U_{0}, U_{1}, \ldots, U_{q-1}$.

Proof. Let A be a diagonalizable $n \times n$ matrix with entries in $\mathbb{F}_{q}$. Let $0,1, \ldots, q-1$ be the field elements of $\mathbb{F}_{q}$. Form the sequence of subspaces $E(0, A), E(1, A), \ldots, E(q-1, A)$. Since $A$ is diagonalizable then $\mathbb{F}_{q}^{n}$ is the direct sum of the eigenspaces corresponding to the distinct eigenvalues of $A$. The eigenspace of a field element that is not an eigenvalue is $\{0\}$. So $E(0, A), E(1, A), \ldots, E(q-1, A)$ is a weak decomposition of $\mathbb{F}_{q}^{n}$.

Let $S=U_{0}, U_{1}, \ldots, U_{q-1}$ be a weak decomposition of $\mathbb{F}_{q}^{n}$. Let $S_{n}=U_{i_{1}}, \ldots, U_{i_{m}}$ be the subsequence of $S$ containing all of the nonzero subspaces of $S$. Then $S_{n}$ forms a direct sum decomposition of $\mathbb{F}_{q}^{n}$ and determines a basis of eigenvectors of $\mathbb{F}_{q}^{n}$. So $A$ is diagonalizable.

Let $d_{n}$ be the number of $n \times n$ diagonalizable matrices. By the above theorem and our work in the previous section, $d_{n}=\sum_{n_{1}+\cdots+n_{q}=n, n_{i} \geq 0} \frac{\gamma_{n}}{\gamma_{n_{1}} \cdots \gamma_{n_{q}}}$. Then with $\gamma(z)=\sum_{r \geq 0} \frac{z^{r}}{\gamma_{r}}$, the generating function for the sequence $d_{n}$ is $\gamma(z)^{q}$. For $q=2$ and $n \geq 0$ the sequence is A132186.
$1,2,8,58,802,20834,1051586,102233986,19614424834 \ldots$

Table 29: Number of $n \times n$ diagonalizable matrices over $\mathbb{F}_{q}$ for $n \geq 0$. A132186

For $q=3$ and $n \geq 0$ we have A290516.

```
\(1,3,39,2109,417153,346720179,1233891662727,17484682043488557 \ldots\)
```

Table 30: Number of $n \times n$ diagonalizable matrices over $\mathbb{F}_{3}$ for $n \geq 0$. A290516

We can classify the number of diagonalizable operators $T$ on $\mathbb{F}_{q}^{n}$ according to the dimension of the range. Since $T$ is diagonalizable then $\mathbb{F}_{q}^{n}=E\left(\lambda_{1}, T\right) \oplus \cdots \oplus E\left(\lambda_{m}, T\right)$. The dimension of the range of $T$ is the sum of the dimensions of the nonzero eigenspaces. The triangular array $T(n, k)$ below is then given by the bivariate generating function $\gamma(z) \gamma(u z)^{q-1}$. For $q=2, n \geq 0,0 \leq k \leq n$ we have A296548:

```
1
1 1
1 6 1
1
1
1 496 9920
```

Table 31: Number of $n \times n$ diagonalizable operators $T$ over $\mathbb{F}_{2}$ such that range $(T)=k$ for $0 \leq k \leq n, n \geq 0$. A296548

We note the main diagonal is all 1 's as the only diagonalizable operator on $\mathbb{F}_{2}^{n}$ that is also invertible is the identity operator.

For $q=3, n \geq 0,0 \leq k \leq n$ we have A297892:

| 1 |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: |
| 1 | 2 |  |  |  |
| 1 | 24 | 14 |  |  |
| 1 | 234 | 1638 | 236 | 12692 |
| 1 | 2160 | 147420 | 254880 |  |
| 1 | 19602 | 12349260 | 208173240 | 124394292 |
| 1783784 |  |  |  |  |

Table 32: Number of $n \times n$ diagonalizable operators $T$ over $\mathbb{F}_{3}$ such that range $(T)=k$ for $0 \leq k \leq n, n \geq 0$. A297892

A projection is a linear operator $P$ such that $P^{2}=P$ [16]. The following theorem
shows that projections are also characterized as diagonalizable matrices having only eigenvalues of 0 or 1 .

Theorem 13.3 ([16]). Let $P$ be a linear map on vector space $V$ over a field $\mathbb{F}$. Then $P$ is a projection if and only if $P$ is diagonalizable and has only 0 or 1 as eigenvalues.

Proof. $\Rightarrow$ Let $P$ be a linear map on vector space $V$ over a field $\mathbb{F}$. Assume $P^{2}=P$. Let $\lambda$ be an eigenvalue of $P$ with corresponding eigenvector $v$. Then $\lambda v=P v=P^{2} v=$ $P(P v)=P(\lambda v)=\lambda P v=\lambda^{2} v$. Since $v$ is an eigenvector, $v \neq 0$. So $\lambda=\lambda^{2}$. So $\lambda=0$ or 1.
$\Leftarrow$ Assume that $P$ is diagonalizable and that 0 or 1 are the only eigenvalues of $P$. Let $v \in V$. Since $P$ is diagonalizable then $V$ has a basis $v_{1}, \ldots v_{n}$ consisting of eigenvectors of $P$. By reordering the basis vectors we may assume that there is an $m \in\{0, \ldots, n\}$ such that $v_{1}, \ldots v_{m}$ are eigenvectors corresponding to eigenvalue 0 and that $v_{m+1}, \ldots, v_{n}$ are eigenvectors corresponding to eigenvalue 1 . Now $v=a_{1} v_{1}+\ldots+a_{n} v_{n}$ for some scalars $a_{1}, \ldots a_{n}$ in $\mathbb{F}$. So $P v=a_{1} P v_{1}+\ldots a_{m} P v_{m}+a_{m+1} P v_{m+1}+\ldots a_{n} P v_{n}=a_{m+1} v_{m+1}+$ $\ldots a_{n} v_{n}$. So $P^{2} v=P(P v)=P\left(a_{m+1} v_{m+1}+\ldots a_{n} v_{n}\right)=a_{m+1} P v_{m+1}+\ldots a_{n} P v_{n}=$ $a_{m+1} v_{m+1}+\ldots a_{n} v_{n}=P v$.

So the number of $n \times n$ projections over $\mathbb{F}_{q}$ is the same as the number of $n \times n$ diagonalizable matrices over $\mathbb{F}_{q}$ that have only 0 or 1 as eigenvalues. These numbers are thus given by the generating function $\gamma(z)^{2}$. So for $q=2$ the number of projections is the same as the number of diagonalizable matrices (Table 29). For $q=3$ we have A053846.
$1,2,14,236,12692,1783784,811523288,995733306992,3988947598331024 \ldots$

Table 33: Number of $n \times n$ projections over $\mathbb{F}_{3}$ for $n \geq 0$. A053846

Theorem 13.4 ([16]). There is a 1-1 correspondence between the set of projections on $\mathbb{F}_{q}^{n}$ and the set of weak direct sum decompositions of $\mathbb{F}_{q}^{n}$ into exactly 2 subspaces.

Proof. Let $P$ be a projection on $\mathbb{F}_{q}$. Then Range $(P) \oplus \operatorname{Null}(P)=\mathbb{F}_{q}^{n}$.

We have the number of weak decompositions $d_{n}=\sum_{n_{1}+\cdots+n_{q}=n, n_{i} \geq 0} \frac{\gamma_{n}}{\gamma_{n_{1}} \cdots \gamma_{n_{q}}}$. Since each $n \times n$ projection matrix corresponds with a weak decomposition of $\mathbb{F}_{q}^{n}$ into exactly two subspaces then the number of projections of rank $k, 0 \leq k \leq n$, is $\frac{\gamma_{n}}{\gamma_{k} \gamma_{n-k}}$. So we have the following equality which agrees with our result in Section 5:

$$
\binom{n}{k}_{q} \cdot q^{k(n-k)}=\frac{\gamma_{n}}{\gamma_{k} \gamma_{n-k}}
$$

A square matrix is invertible if and only if it does not have 0 as an eigenvalue. So the number of $n \times n$ matrices that are invertible and diagonalizable is given by $\gamma(z)^{q-1}$. For $q=2$ there is only one such matrix, the identity matrix. For $q=3$ and $n \geq 0$ we have sequence A053846.
$1,2,14,236,12692,1783784,811523288,995733306992, \ldots$

Table 34: Number of $n \times n$ matrices over $\mathbb{F}_{3}$ that are invertible and diagonalizable for $n \geq 0$. A053846

We note that this is the same sequence given above counting the number of $n \times n$ projections and is the main diagonal of the triangular array given above classifying the diagonalizable matrices by rank.

We can classify the diagonalizable matrices according to their number of distinct eigenvalues. We count the occurrences of the subspace $\{0\}$ in the corresponding sequence of subspaces (weak decomposition) with the bivariate generating function: $(\gamma(z)-1+u)^{q}$. For $n \geq 1$, there are $q$ diagonalizable matrices that have exactly one eigenvalue. For $q=2$, every diagonalizable matrix except the identity and the zero matrix has exactly two distinct eigenvalues. For $q=3, n \geq 0,0 \leq k \leq 3$, the number of $n \times n$ diagonalizable matrices with exactly $k$ distinct eigenvalues is given in the table below. This is sequence A296605. The row sums are A290516 given above :

| 1 | 0 | 0 | 0 |
| :--- | :---: | :---: | :---: |
| 0 | 3 | 0 | 0 |
| 0 | 3 | 36 | 0 |
| 0 | 3 | 702 | 1404 |
| 0 | 3 | 38070 | 379080 |
| 0 | 3 | 5351346 | 341368830 |
| 0 | 3 | 2434569858 | 1231457092866 |
| 0 | 3 | 2987199920970 | 17481694843567584 |
| 0 | 3 | 11966842794993066 | 1077553466091961763220 |

Table 35: Number of $n \times n$ diagonalizable matrices over $\mathbb{F}_{3}$ having $k$ distinct eigenvalues $0 \leq k \leq 3, n \geq 0$. A296605

Theorem 13.5. Let $V$ be a finite dimensional vector space over a field with characteristic other than 2. Let $T \in \mathcal{L}(V)$. Then $T^{2}=I$ if and only if $T$ is diagonalizable and the only eigenvalues of $T$ are 1 or -1 .

Proof. $\Rightarrow$ Assume $T \in \mathcal{L}(V)$ is diagonalizable and has only 1 or -1 as eigenvalues. Let $v \in V$. By our assumptions $V=E(1, T) \oplus E(-1, T)$. So $v=u+w$ where $u \in E(1, T)$ and $w \in E(-1, T)$. So $T^{2} v=T(T v)=T(T(u+w)=T(T u+T w)=T(u+-w)=$ $T u-T w=u--w=u+w=v$.
$\Leftarrow$ Assume that $T^{2}=I$. Suppose $\lambda$ is an eigenvalue of $T$ and $v$ is a corresponding eigenvector. Then $\mathrm{v}=T^{2} v=T(T v)=T(\lambda v)=\lambda^{2} v$. Since $v \neq 0$ then $\lambda^{2}=1$. So $\lambda=1$ or -1 .

Since the only eigenvalues of $T$ are 1 or -1 , and both of these eigenvalues are contained in the underlying field of our vector space $V$, then there is a basis $\beta$ of $V$ such that the matrix $M(T, \beta)$ has the Jordan normal form. That is, $M(T, \beta)$ is a block diagonal matrix where each block $B$ has an eigenvalue of $T$ along its main diagonal and 1's on its superdiagonal and 0 's everywhere else. Since $M(T, \beta)^{2}=I$ then $B^{2}$ must be a diagonal matrix with all 1's along its diagonal. Notice that the entry in the first row, second column of $B^{2}$ is $2 \lambda$. For example if the Jordan block is of size 4 then:

$$
\left(\begin{array}{cccc}
\lambda & 1 & 0 & 0 \\
0 & \lambda & 1 & 0 \\
0 & 0 & \lambda & 1 \\
0 & 0 & 0 & \lambda
\end{array}\right)^{2}=\left(\begin{array}{cccc}
\lambda^{2} & 2 \lambda & 1 & 0 \\
0 & \lambda^{2} & 2 \lambda & 1 \\
0 & 0 & \lambda^{2} & 2 \lambda \\
0 & 0 & 0 & \lambda^{2}
\end{array}\right)
$$

Since the underlying field is of characteristic other than 2 then $2 \lambda=2$ or -2 which is not the zero element of the field. So each Jordan block must be of size 1. Since each Jordan block is of size 1 then $M(T, \beta)$ is a diagonal matrix, hence $T$ is diagonalizable.

We note that if $T$ is an operator on a vector space over a field of characteristic 2 then $T^{2}=I$ does not imply that $T$ is diagonalizable. For example, If $T \in \mathcal{L}\left(\mathbb{F}_{2}\right)$ such that $M(T)=\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$ then $T^{2}=I$ but $T$ is not diagonalizable since its only eigenvalue is 1 and $E(1, T)$ has dimension 1 .

Let $T$ be an operator on $\mathbb{F}_{q}^{n}$ where $q$ is a power of an odd prime and $T^{2}=I$. By the above theorem in order to count the number of such operators $T$ it suffices to count the number of diagonalizable matrices with at most 2 eigenvalues. The generating function is then $(\gamma(z))^{2}$. We see that the number of such matrices is the same as the number of projections.

## 14. Subgroups of $G L_{n}\left(\mathbb{F}_{q}\right)$

In this section we view the vector space $G L_{n}\left(\mathbb{F}_{q}\right)$ as a group. We expound on the ideas in [2] to show that when $p$ is a prime $G L_{n}\left(\mathbb{F}_{p}\right)$ is precisely the automorphism group of the finite abelian group:

$$
\left(\mathbb{F}_{p}^{n}=\left\{\left(a_{1}, \ldots, a_{n}\right): a_{i} \in \mathbb{F}_{p} \forall i=1, \ldots, n\right\},+\right)
$$

where the group operation + is componentwise addition of the $n$-tuples. We use the arguments given in [2] to characterize the elementary abelian $p$-group, which is the group underlying every vector space over a finite field. We determine the orders (as given in [12]) of some important subgroups of $G L_{n}\left(\mathbb{F}_{q}\right)$ and point out some well known facts about them.

Definition 14.1 ([10]). Let $p$ be a prime and let $n$ be a positive integer. The elementary abelian group of order $p^{n}$, denoted $E_{p^{n}}$ is an abelian group of order $p^{n}$ with the property that for all $x \in E_{p^{n}}, p x=0$.

We note that in the definition above, the equation $p x=0$ is written additively. That is, the group operation is addition and $p x:=x+x+\cdots+x(\mathrm{p}$ summands of $x)$.

Let $q=p^{\alpha}$ where $p$ is a prime number. An $n$-dimensional vector space $V$ over a field containing $q$ elements is, in particular, an abelian group of order $q^{n}$. The vectors in such a vector space along with the operation of vector addition form an additive group. The identity element is the zero vector. We can consider the vectors in $V$ as $n$-tuples of field elements, so it is clear that every nonidentity vector has the same order (namely the least
common multiple of the orders of each component, which is $p$ ). So for all $v \in V, p v=0$ and $V$ is the elementary abelian group, $\left(\mathbb{Z}_{p}\right)^{\alpha n}$.

Definition 14.2. The general linear group of a vector space $V$ is denoted by $G L(V)$ and is the group comprised of the set (along with function composition) of all bijective mappings from $V$ into $V$ that preserve both the underlying abelian group structure of $V$ as well as the scalar multiplication of $V$.

The following theorem shows that the group of automorphisms on any finite dimensional vector space acts transitively on the set of nonzero vectors.

Theorem 14.3. If $V$ is a finite dimensional vector space, then the $\operatorname{group} \operatorname{Aut}(V)$ acts transitively on the set $V-\{0\}$.

Proof. Let $V$ be a finite dimensional vector space. Say $\operatorname{dim} V=n$. Let the automorphisms of $V$ act on the set $V-\{0\}$. Let $u, v \in V-\{0\}$. Since $u \neq 0$ then we may fix a basis $u=u_{1}, u_{2}, \ldots, u_{n}$ of $V$. Likewise, fix a basis $v=v_{1}, v_{2}, \ldots, v_{n}$ of $V$. Define $T: V \rightarrow V$ by $T u_{i}=v_{i}$ for all $i=1, \ldots, n$. Then $T u=v$ and $T$ maps a basis of $V$ into a list of linearly independent vectors in $V$ so $T$ is a bijective linear map.

Elementary abelian groups are characterized in the following Theorem. We first give as a lemma a well known result from group theory.

Lemma 14.4 ([10]). If $G$ is a group of order $p^{\alpha}$ for some $\alpha \geq 0$, then $Z(G)$, the center of $G$ is nontrivial.

Proof. Let $G$ act on itself by conjugation. Let $g_{1}, g_{2}, \ldots, g_{r}$ be a set of representatives of all the distinct noncentral conjugacy classes of $G$. Then

$$
|G|=|Z(G)|+\sum_{i=1}^{r}\left[G: G_{g_{i}}\right] .
$$

Now $G_{g_{i}} \neq G$ (because otherwise $g_{i}$ would be in the center of $G$ ). So $p \mid\left[G: G_{g_{i}}\right]$ for all $i=1, \ldots, r$. Since $p$ divides the LHS of our equation and $p$ divides every term in the summation on the RHS, $p$ divides $|Z(G)|$. So $Z(G)$ is nontrivial.

Theorem 14.5 ([2]). Let $G$ be a nontrivial finite group with identity 0 . Then Aut $G$ acts transitively on $G /\{0\}$ if and only if $G$ is elementary abelian.

Proof. $\Leftarrow$ If $G$ is elementary abelian, then it is a vector space over a field with a prime number of elements. So by Theorem 14.5, Aut $G$ acts transitively on $G$.
$\Rightarrow$ Assume that Aut $G$ acts transitively on $G /\{0\}$. Suppose $\phi \in \operatorname{Aut} G$ and $x \in G /\{0\}$ and that $|x|=j$ for some integer $j$. Then $(\phi(x))^{j}=\phi\left(x^{j}\right)=\phi(0)=0$. Also if $(\phi(x))^{k}=0$ for some $k<j$ then $\phi\left(x^{k}\right)=0$ so $x^{k}=(\phi(0))^{-1}=0$ which is a contradiction. So $|\phi(x)|=j$. So every element in the orbit of $x$ has the same order. Since the action is transitive then every element in $G$ has the same order. Since $G$ is nontrivial, there is some prime $p$ that divides $|G|$. By Cauchy's Theorem, $G$ contains at least one element of order $p$. So every nonzero element of $G$ has order $p$. So $|G|$ is a power of $p$, that is, $G$ is a $p$-group. So $G$ has a nontrivial center, that is, $Z(G) \neq 0$.

Claim: If $x \in Z(G)$ then $\phi(x) \in Z(G)$. Let $x \in Z(G)$ and let $g \in G$. Then $x g=g x$ so we have: $\phi(x g)=\phi(x) \phi(g)=\phi(g x)=\phi(g) \phi(x)$. So $\phi(x)$ commutes with our arbitrary element $\phi(g)$. So $\phi(x) \in Z(G)$.

By our claim every element in the orbit of $x$ is in $Z(G)$. So $Z(G)=G$. So $G$ is abelian. Therefore, $G$ is an elementary abelian group.

Let $V$ be an $n$-dimensional vector space over any finite field $\mathbb{F}_{q}^{n}$. By the definition of a linear map $T$ on $V, T\left(v_{1}+v_{2}\right)=T\left(v_{1}\right)+T\left(v_{2}\right) \forall v_{1}, v_{2} \in V$, then each $T \in \mathcal{L}(V)$
is a group homomorphism from $V$ into $V$. If $T$ is such that the kernel of $T$ is the zero vector, then by the first isomorphism theorem $V \cong V / \operatorname{ker} T \cong T(V)=V$. So that $T$ is an automorphism on $V$. So the group $G L_{n}\left(\mathbb{F}_{q}\right)$ is a subgroup of $\operatorname{Aut}(V)$. Only in the special case when $q=p$ for a prime $p$, is the group of automorphisms on $V$ precisely the group of invertible linear transformations. Viz., $\operatorname{Aut}(V) \cong G L_{n}\left(\mathbb{F}_{q}\right)$ if and only if $q$ is a prime.

Before we give a proof we look at two examples that illustrate the idea. Let $V$ be the 2dimensional vector space over the field $\mathbb{F}_{5}$. (Note the articles "the" in the previous sentence are somewhat justified in the sense that any two vector spaces of the same dimension are isomorphic and likewise all fields of the same order are isomorphic). Notice that each vector $v$ in $\mathbb{F}_{5}^{2}$ can be added to itself some number of times to arrive at any scalar multiple of $v$. For example:

$$
\binom{3}{2}+\binom{3}{2}+\binom{3}{2}=\binom{4}{1}=3\binom{3}{2}
$$

But this is not the case if the characteristic of the field is not equal to the order of the field. That is, if the order of the field is not prime. For example, the field elements in $\mathbb{F}_{4} \cong \mathbb{F}_{2}[x] /\left\langle x^{2}+x+1\right\rangle$ can be represented as $\overline{0}, \overline{1}, \bar{x}, \overline{x+1}$. Now

$$
\overline{x+1}\binom{\bar{x}}{\overline{x+1}}=\binom{\overline{1}}{\bar{x}}
$$

But

$$
\binom{\bar{x}}{\overline{x+1}}+\binom{\bar{x}}{\overline{x+1}}=\binom{\overline{0}}{\overline{0}}
$$

So adding the vector $\left(\frac{\bar{x}}{\overline{x+1}}\right)$ to itself any number of times will never yield its multiple with the scalar $\overline{x+1}$.

Theorem 14.6. Let $V$ be an n-dimensional vector space over $\mathbb{F}_{p}$. In particular, $V$ is an abelian group. If p is a prime then $\operatorname{Aut}(V) \cong G L_{n}\left(\mathbb{F}_{p}\right)$.

Proof. Assume $p$ is a prime. We have already shown in the first paragraph of this section that $G L_{n}\left(\mathbb{F}_{q}\right) \leq \operatorname{Aut}(V)$ where $q$ is a prime power.

Let $\phi \in \operatorname{Aut}(V)$. Let $u, v \in V$. Let $a \in \mathbb{F}_{p}$. Now $\phi(u+v)=\phi(u)+\phi(v)$. So $\phi$ respects additivity. Also, since $p$ is prime, $a v=v+v+\cdots+v$ ( $a$ summands of $v$ ). So $\phi(a v)=\phi(v+v+\cdots+v)=\phi(v)+\cdots+\phi(v)=a \phi(v)$. So $\phi$ respects homogeneity. So, $\phi \in G L_{n}\left(\mathbb{F}_{p}\right)$. So $\operatorname{Aut}(V) \leq G L_{n}\left(\mathbb{F}_{p}\right)$.

In the next section we will derive an explicit formula for the number of automorphisms on $V$. The formula shows that when $q$ is not a prime, there are many automorphisms on $V$ which are not linear maps. For now we give an example again using the field $\mathbb{F}=\mathbb{F}_{2}[x] /\left\langle x^{2}+x+1\right\rangle$. Consider the 1-dimensional vector space $V$ over $\mathbb{F}$. Then $V$ is isomorphic to $C_{2} \times C_{2}$. It is well known that the group of automorphisms on $V$ is isomorphic to $S_{3}$. Let $\phi$ be the automorphism that swaps $\bar{x}$ with $\overline{x+1}$. But $\phi$ is not a linear map because (in particular)

$$
\begin{gathered}
\overline{x+1} \phi(\bar{x})=\overline{x+1} \overline{x+1}=\bar{x} \quad \text { but } \\
\phi(\overline{x+1} \bar{x})=\phi(\overline{1})=\overline{1}
\end{gathered}
$$

## The Special Linear Group

The special linear group, denoted $S L_{n}\left(\mathbb{F}_{q}\right)$, is the subgroup of $G L_{n}\left(\mathbb{F}_{q}\right)$ consisting of the $n \times n$ matrices with determinant 1 . Equivalently, $S L_{n}\left(\mathbb{F}_{q}\right)$ is the kernel of the group homomorphism $\phi: G L_{n}\left(\mathbb{F}_{q}\right) \rightarrow \mathbb{F}_{q}^{\times}$by $\phi(A)=\operatorname{det} A$ for all $A \in G L_{n}\left(\mathbb{F}_{q}\right)$. Now $\phi$ is a homomorphism because for any $A, B \in G L_{n}(\mathbb{F})_{q}$, $\operatorname{det} A \operatorname{det} B=\operatorname{det} A B$. Also $\phi$ is surjective since for any $x \in \mathbb{F}_{q}$, we can construct the $n \times n$ diagonal matrix $A=\left[a_{i, j}\right]$ with $a_{1,1}=x$ and all other diagonal entries equal to 1 . Then $\phi(A)=x$. Since $\phi$ is surjective, by First Isomorphism Theorem, the quotient group $G L_{n}\left(\mathbb{F}_{q}\right) / S L_{n}\left(\mathbb{F}_{q}\right)$ is isomorphic to $\mathbb{F}_{q}^{\times}$. Since $\left|\mathbb{F}_{q}^{\times}\right|=q-1$ then we have:

$$
\begin{gathered}
\left|G L_{n}\left(\mathbb{F}_{q}\right) / S L_{n}\left(\mathbb{F}_{q}\right)\right|=\left|\mathbb{F}_{q}^{\times}\right| \\
\frac{\prod_{i=0}^{n-1} q^{n}-q^{i}}{\left|S L_{n}\left(\mathbb{F}_{q}\right)\right|}=q-1 \\
\left|S L_{n}\left(\mathbb{F}_{q}\right)\right|=\frac{\prod_{i=0}^{n-1} p^{n}-p^{i}}{q-1}
\end{gathered}
$$

The order of $S L_{n}\left(\mathbb{F}_{q}\right)$ turns out to be the same as the order of another subgroup of $G L_{n}\left(\mathbb{F}_{q}\right)$ called the projective linear group.

## The Projective General Linear Group

The projective general linear group over $\mathbb{F}_{q}$ is the quotient group $G L_{n}\left(\mathbb{F}_{q}\right) / Z\left(G L_{n}\left(\mathbb{F}_{q}\right)\right.$. That is, the projective general linear group is the quotient group of the general linear group with its center. It is the group of inner automorphisms of the general linear group. It is also called simply the projective linear group and is denoted $P G L_{n}\left(\mathbb{F}_{q}\right)$. Let $G L_{n}\left(\mathbb{F}_{q}\right)$ act on itself by conjugation. To this group action we can associate a homomorphism $\phi: G L_{n}\left(\mathbb{F}_{q}\right) \rightarrow S_{G L_{n}\left(\mathbb{F}_{q}\right)}$ called the permutation representation of the action. Then $P G L_{n}\left(\mathbb{F}_{\|}\right)$is isomorphic to the image of $\phi$ in $S_{G L_{n}\left(\mathbb{F}_{q}\right)}$. We can view the projective general linear group as equivalence classes of $n \times n$ matrices where two matrices $A, B$ are related if there is a scalar matrix $C$ such that $A=B C$. The following theorem shows that the center of $G L_{n}\left(\mathbb{F}_{q}\right)$ consists of all the scalar matrices in $G L_{n}\left(\mathbb{F}_{q}\right)$, i.e., the nonzero scalar multiples of $I_{n}$.

Theorem 14.7. Suppose that $V$ is a finite dimensional vector space over a field $\mathbb{F}$ and $T \in \mathcal{L}(V)$. Then $T$ is a scalar multiple of the identity if and only if $S T=T S$ for all $S \in \mathcal{L}(V)$.

Proof. $\Rightarrow$ Assume $T$ is a scalar multiple of the identity. Let $S \in \mathcal{L}(V)$. Let $v \in V$. Since $T$ is a scalar multiple of the identity then there is some $a \in \mathbb{F}$ such that $T v=a v$. Then $S T v=S(a v)=a S v=T S v$.
$\Leftarrow$ Assume $S T=T S$ for all $S \in \mathcal{L}(V)$. If $n=1$, then we are done so assume $n \geq 2$. Fix a basis $v_{1}, \ldots, v_{n}$ of $V$. For each $i \in\{1, \ldots, n\}$ define $S_{i} \in \mathcal{L}(V)$ by

$$
S_{i}\left(v_{k}\right)= \begin{cases}v_{i} & \text { if } k=i \\ 0, & \text { otherwise }\end{cases}
$$

For each $i, j \in\{1,2, \ldots, n\}$ with $i<j$ define $S_{i, j} \in \mathcal{L}(V)$ by

$$
S_{i, j}\left(v_{k}\right)= \begin{cases}v_{i} & \text { if } k=j \\ v_{j} & \text { if } k=i \\ 0, & \text { otherwise }\end{cases}
$$

For any fixed $i \in\{1, \ldots, n\}$ we have: $T\left(v_{i}\right)=c_{1} v_{1}+\cdots c_{n} v_{n}$ for some unique scalars $c_{1}, \ldots, c_{n} \in \mathbb{F}$. So that

$$
\begin{gathered}
S_{i} T\left(v_{i}\right)=S_{i}\left(\sum_{k=1}^{n} c_{k} v_{k}\right)=\sum_{k=1}^{n} c_{k} S_{i}\left(v_{k}\right)=c_{i} v_{i} . \\
\text { and } \\
T S_{i}\left(v_{i}\right)=T\left(v_{i}\right)=c_{1} v_{1}+\cdots+c_{n} v_{n}
\end{gathered}
$$

So $c_{1} v_{1}+\cdots+c_{n} v_{n}=c_{i} v_{i}$. Since $v_{1}, \ldots, v_{n}$ is linearly independent then $c_{k}=0$ for all $k \neq i$. Since $i$ is arbitrary in $\{1, \ldots, n\}$ then for each $i$ there is a scalar $a_{i} \in \mathbb{F}$ such that $T\left(v_{i}\right)=a_{i} v_{i}$. This shows that $M\left(T, v_{1}, \ldots, v_{n}\right)$ is a diagonal matrix. Now we will show that $M\left(T, v_{1}, \ldots, v_{n}\right)$ is a scalar multiple of $I_{n}$ by showing that $a_{1}=\cdots=a_{n}$.

Let $i, j$ be fixed in $\{1, \ldots, n\}$ with $i \neq j$. Then

$$
\begin{gathered}
S_{i, j} T\left(v_{i}\right)=S_{i, j}\left(a_{i} v_{i}\right)=a_{i} S_{i, j}\left(v_{i}\right)=a_{i} v_{j} \\
\text { and } \\
T S_{i, j}\left(v_{i}\right)=T\left(v_{j}\right)=a_{j} v_{j}
\end{gathered}
$$

So $a_{i}=a_{j}$. Since our $i$ and $j$ are arbitrary in $\{1, \ldots, n\}$ then $a_{1}=\cdots=a_{n}$.

So there is a unique scalar $a \in \mathbb{F}$ such that $T\left(v_{i}\right)=a v_{i}$ for each $i \in\{1, \ldots, n\}$. Let $v \in V$. Then $v=\sum_{k=1}^{n} b_{k} v_{k}$ for some scalars $b_{1}, \ldots, b_{n} \in \mathbb{F}$. So $T(v)=T\left(\sum_{k=1}^{n} b_{k} v_{k}\right)=$ $\sum_{k=1}^{n} b_{k} T\left(v_{k}\right)=\sum_{k=1}^{n} b_{k} a v_{k}=a \sum_{k=1}^{n} b_{k} v_{k}=a v$. So $T=a I$.

From the above theorem we see that $\left|Z\left(G L_{n} \mathbb{F}_{\|}\right)\right|=q-1$. So we have:

$$
\left|P G L_{n}\left(\mathbb{F}_{q}\right)\right|=\left\lvert\, G L_{n}\left(\mathbb{F}_{q}\right) / Z\left(G L_{n}\left(\mathbb{F}_{q}\right) \left\lvert\,=\frac{\left|G L_{n}\left(\mathbb{F}_{q}\right)\right|}{\mid Z\left(G L_{n}\left(\mathbb{F}_{q}\right)\right.}=\frac{\prod_{i=0}^{n-1} q^{n}-q^{i}}{q-1}\right.\right.\right.
$$

The orders of $P G L_{n}\left(\mathbb{F}_{3}\right)$ for $n \geq 1$ are given in sequence A003787

```
\(1,24,5616,12130560,237783237120,42064805779476480 \ldots\)
```

Table 36: Order of $P G L_{n}\left(\mathbb{F}_{3}\right)$ for $n \geq 1$. A003787

The orders of $P G L_{n}\left(\mathbb{F}_{4}\right)$ for $n \geq 1$ are given in sequence A003788.

1, 60, 60480, $987033600,258492255436800,1083930404878024704000 \ldots$
Table 37: Order of $P G L_{n}\left(\mathbb{F}_{4}\right)$ for $n \geq 1$. A003788

## The Projective Special Linear Group

The projective special linear group over $\mathbb{F}_{q}$ is denoted $P S L_{n}\left(\mathbb{F}_{q}\right)$. It is the subgroup of $P G L_{n}\left(\mathbb{F}_{q}\right)$ that contains all the matrices in $P G L_{n}\left(\mathbb{F}_{q}\right)$ whose determinant is equal to 1 . The order of $P S L_{n}\left(\mathbb{F}_{q}\right)$ is equal to the order of $S L_{n}\left(\mathbb{F}_{q}\right)$ divided by the number of $n \times n$ scalar matrices with determinant of 1 . The number of such scalar matrices is the number of $n^{\text {th }}$ roots of unity in $\mathbb{F}_{q}$. In other words, the number elements $a \in \mathbb{F}_{q}$ such that $a^{n}=1$. In order to count the number of such elements we first show that the group $\mathbb{F}_{q}^{\times}$is cyclic. The following lemma is proved in [20] and is stated here without proof. Theorem 14.9 is essentially that given in [20].

Lemma 14.8 ([20]). Suppose $G$ is an abelian group. If $x, y \in G$ and $|x|=r<\infty,|y|=$ $s<\infty$ then there is an element of $G$ with order lcm $(r, s)$.

Theorem 14.9 ([20]). Suppose $\mathbb{F}$ is a finite field. Then $\mathbb{F}^{\times}$is a cyclic group.

Proof. Let $\left|\mathbb{F}^{\times}\right|=m$. Suppose $\alpha \in \mathbb{F}^{\times}$has maximal order of all elements in $\mathbb{F}^{\times}$. Say $|\alpha|=k$. We will show that $k=m$ so that $\langle\alpha\rangle=\mathbb{F}^{\times}$.

By LaGrange's theorem $k \mid m$ so $k \leq m$.
Let $\beta$ be an arbitrary element in $\mathbb{F}^{\times}$. Say $|\beta|=r$. Then by the above lemma, $\mathbb{F}^{\times}$has an element of order $\operatorname{lcm}(r, k)$. Now $k$ is maximal of all the orders in the group and $\operatorname{lcm}(r, k) \geq$ $k$ so it must be that $r \mid k$. Since $|\beta|=r$ and $r \mid k$ then $\beta^{k}=1$. Since $\beta$ is arbitrary in $\mathbb{F}^{\times}$then every element in $\mathbb{F}^{\times}$satisfies the polynomial equation $x^{k}-1=0$. So $x^{k}-1$ has $m$ roots in $\mathbb{F}^{\times}$. By the Fundamental Theorem of Algebra there are at most $k$ distinct roots of the polynomial. So $m \leq k$.

Lemma 14.10 ([10]). If $G$ is any group and $x \in G,|x|=n, a \in \mathbb{Z}, a \neq 0$ then $\left|x^{a}\right|=\frac{n}{\operatorname{gcd}(n, a)}$.

Proof. Let $d=\operatorname{gcd}(n, a)$. Then $n=d b, a=d c$ for some $d, c \in \mathbb{Z}, b \geq 1$ where $\operatorname{gcd}(b, c)=1$ (otherwise $d$ is not a greatest common divisor). Let $y=x^{a}$. We will show that $|y| \leq b$ and $|y| \geq b$, hence $|y|=b=\frac{n}{\operatorname{gcd}(n, a)}$.
Now $y^{b}=\left(x^{a}\right)^{b}=\left(x^{d c}\right)^{b}=\left(x^{b d}\right)^{c}=\left(x^{n}\right)^{c}=1^{c}=1$. So $|y|$ divides $b$. So $|y| \leq b$.
Let $k=|y|$. Then $y^{k}=1=\left(x^{a}\right)^{k}$. So $|x| \mid a k$. So $n \mid a k$ So $d b \mid d c k$. So $b \mid c k$. Since $\operatorname{gcd}(b, c)=1$ then $b \mid k$. So $b||y|$. So $b \leq|y|$.

Theorem 14.11 ([10]). In any cyclic group, the number of elements that have order $d$ is $\phi(d)$.

Proof. Let $G$ be a cyclic group of order $n$. Then there is a generator $a \in G$ such that $G=\langle a\rangle=\left\{a, a^{2}, \ldots, a^{n}=1\right\}$. By LaGrange's theorem for each $k \in\{1,2, \ldots, n\}$ the order of $a^{k}$ is a divisor of $n$. Now $|a|=n$, so by the previous lemma, $\left|a^{k}\right|=\frac{n}{\operatorname{gcd}(n, k)}$. So for any $i, j \in\{1,2, \ldots, n\},\left|a^{i}\right|=\left|a^{j}\right|$ if and only if $\operatorname{gcd}(i, n)=\operatorname{gcd}(j, n)$.

Let $d$ be a divisor of $n$. Then $d h=n$ for some $h \in \mathbb{Z}^{+}$. Now $\phi(d)$ is the number of positive integers less than or equal to $d$ that have no common factors with $d$. In other words, $\phi(d)=|A|=\left|\left\{m \in \mathbb{Z}^{+}: m \leq d, \operatorname{gcd}(m, d)=1\right\}\right|$. Let $B=\{h m: m \in A\}$. Consider the map $\psi: A \rightarrow B$ by $\psi(m)=m h$ for all $m \in A$. It is clear that $\psi$ is a bijection. Also, since for all $m \in A, \operatorname{gcd}(d, m)=1$ and $d h=n$ then $\operatorname{gcd}(\psi(m), n)=h$. So each element
$b \in B$ is such that $\operatorname{gcd}(b, n)=h$. So $\phi(d)=|B|$. That is, $\phi(d)$ is the number of positive integers less than or equal to $n$ whose greatest common divisor with $n$ is equal to $h$. So $\phi(d)$ is the number of elements in $G$ that have order $d$.

Theorem 14.12 ([10]). For any positive integer $n, \sum_{d \mid n} \phi(d)=n$.

Proof. Let $G$ be a cyclic group of order $n$. Let $R$ be the relation on the elements of $G$ defined by $x R y$ if and only if $|x|=|y|$ for all $x, y \in G$. By the above theorem, $R$ is an equivalence relation on $G$. The number of equivalence classes is equal to the number of divisors d of $n$. If $x \in G$ and $|x|=d$ then the cardinality of the class containing $x$ is $\phi(d)$. So $n=\sum_{d \mid n}|\{y \in G: x R y\}|=\sum_{d \mid n} \phi(d)$

Theorem 14.13. For any $n \geq 1$, the number of elements $a$ in $\mathbb{F}_{q}^{\times}$such that $a^{n}=1$ is $\operatorname{gcd}(n, q-1)$.

Proof. Since $\mathbb{F}_{q}^{\times}$is a cyclic group of order $q-1$ it suffices to count the number of elements in $\mathbb{F}_{q}^{\times}$whose order divides $n$. Since the order of every element divides $q-1$, the set of elements $a$ in $\mathbb{F}_{q}^{\times}$such that $a^{n}=1$ is precisely the set of elements whose order is a common divisor of $n$ and $q-1$. So by Theorem 12.9, the desired number is $\sum_{\{d: d|n, d| q-1\}} \phi(d)$. Notice that the set $\{d: d|n, d| q-1\}$ is the set of common divisors of $n$ and $q-1$ which is precisely the set of divisors of $\operatorname{gcd}(n, q-1)$. So by Theorem $12.10 \sum_{\{d: d|n, d| q-1\}} \phi(d)=$ $\operatorname{gcd}(n, q-1)$.

So we have:

$$
\left|P S L_{n}\left(\mathbb{F}_{q}\right)\right|=\frac{\left|S L_{n}\left(\mathbb{F}_{q}\right)\right|}{\operatorname{gcd}(n, q-1)}=\frac{\prod_{i=0}^{n-1} q^{n}-q^{i}}{(q-1) \operatorname{gcd}(n, q-1)}
$$

The orders of $P S L_{n}\left(\mathbb{F}_{3}\right)$ for $n \geq 1$ are given in sequence A003793.

$$
1,12,5616,6065280,237783237120,21032402889738240 \ldots
$$

Table 38: Order of $\operatorname{PSL} L_{n}\left(\mathbb{F}_{3}\right)$ for $n \geq 1$. A003793
$\left|P S L_{2}\left(\mathbb{F}_{3}\right)\right|=12$ because we have the following 12 classes of $2 \times 2$ matrices over $\mathbb{F}_{3}$. The two matrices listed in each row (cosets of the center) are scalar multiples of each other and have determinant equal to 1 . The identity element is in the 4 th row. This group is isomorphic to the alternating group $A_{4}$.

## 15. Subgroups of $G L_{n}\left(\mathbb{Z}_{m}\right)$

The set of $n \times n$ matrices with entries in the ring of integers modulo $m$, (here denoted $\mathbb{Z}_{m}$ ) is an $R$-module. It is itself a matrix ring and is denoted $\mathcal{M}_{n}\left(\mathbb{Z}_{m}\right)$. We call $\mathcal{M}_{n}\left(\mathbb{Z}_{m}\right)$ the full ring of $n \times n$ matrices. There are of course $m^{n^{2}}$ elements in $\mathcal{M}_{n}\left(\mathbb{Z}_{m}\right)$. In this section we will determine the number of these matrices which are invertible. In other words, we determine the order of the group of units in this matrix ring which we denote as $G L_{n}\left(\mathbb{Z}_{m}\right)$. We follow very closely the arguments presented in [19]. We use these arguments to derive formulas given in [12] for the order of some important subgroups of this group.

Theorem 15.1 ([19]). If $A \in M_{n}(R)$, then $A$ is invertible if and only if $\operatorname{det}(A)$ is a unit in $R$.

Proof. $\Rightarrow$ Assume $A$ is invertible. Then $1=\operatorname{det}(I)=\operatorname{det}\left(A A^{-1}\right)=\operatorname{det}(A) \operatorname{det}\left(A^{-1}\right)$.
$\Leftarrow$ Assume $\operatorname{det}(A)$ is a unit in $R$. Now $A \operatorname{adj}(A)=I_{n} \operatorname{det}(A)$. So $A \operatorname{adj}(A) \operatorname{det}(A)^{-1}=$ $I_{n}$.

Let $G L_{n}(R)$ be the group of units in $\mathcal{M}_{n}(R)$. In other words, $G L_{n}(R)$ is the group of invertible $n \times n$ matrices whose entries are in the ring $R$. We want to determine the order of these groups when $R=\mathbb{Z}_{m}$ is the ring of integers modulo $m$. We will first consider the case when $m$ is a prime number, then we consider the case when $m$ is a prime power and finally we consider the general case for any integer $m$.

When $m=p$ where $p$ is a prime then $\mathbb{Z}_{m}$ is a field so $\mathcal{M}_{n}\left(\mathbb{Z}_{m}\right)$ is the general linear group. So $\left|G L_{n}\left(\mathbb{Z}_{m}\right)\right|=\prod_{i=0}^{n-1} p^{n}-p^{i}=\gamma_{n, p}$.

Lemma 15.2 ([19]). If $A$ and $B$ are square matrices such that $A \equiv B \bmod m$ then det $A \equiv \operatorname{det} B \bmod m$.

Proof. Let $A=a_{i, j}$ and $B=b_{i, j}$ be $n \times n$ matrices with $A \equiv B \bmod m$. Now $\operatorname{det} A:=$ $\sum_{\sigma \in S_{n}} \operatorname{sign}(\sigma) a_{1, \sigma(1)} \cdots a_{n, \sigma(n)}$ so that:

$$
\begin{gathered}
\operatorname{det} A \bmod m:=\left(\sum_{\sigma \in S_{n}} \operatorname{sign}(\sigma) a_{1, \sigma(1)} \cdots a_{n, \sigma(n)}\right) \bmod m \equiv \\
\left(\sum_{\sigma \in S_{n}}\left(\operatorname{sign}(\sigma) a_{1, \sigma(1)} \cdots a_{n, \sigma(n)}\right) \bmod m\right) \bmod m \equiv \\
\left(\sum_{\sigma \in S_{n}}\left(\operatorname{sign}(\sigma) a_{1, \sigma(1)} \bmod m \cdots a_{n, \sigma(n)} \bmod m\right) \bmod m\right) \bmod m \equiv \\
\left(\sum_{\sigma \in S_{n}}\left(\operatorname{sign}(\sigma) b_{1, \sigma(1)} \bmod m \cdots b_{n, \sigma(n)} \bmod m\right) \bmod m\right) \bmod m \equiv \\
\left(\sum_{\sigma \in S_{n}}\left(\operatorname{sign}(\sigma) b_{1, \sigma(1)} \cdots b_{n, \sigma(n)}\right) \bmod m\right) \bmod m \equiv \\
\left(\sum_{\sigma \in S_{n}}\left(\operatorname{sign}(\sigma) b_{1, \sigma(1)} \cdots b_{n, \sigma(n)}\right)\right) \bmod m \equiv \\
\operatorname{det} B \bmod m .
\end{gathered}
$$

Now we give the arguments leading to Theorem 2.2.2 in [19]. Suppose $m=p^{\alpha}$ where $p$ is prime and $\alpha$ is a positive integer. Let $A \in \mathcal{M}_{n}\left(\mathbb{Z}_{m}\right)$. Then $A=p B+C$ where $B$ is the matrix of quotients of $A$ by $p$ and $C$ is the matrix of the remainders. For example:

$$
\text { If } p=5, \alpha=3 \text {, so that } m=5^{3}=125 \text { and } A=\left(\begin{array}{ccc}
111 & 61 & 8 \\
4 & 10 & 12 \\
22 & 13 & 14
\end{array}\right)
$$

then $B=\left(\begin{array}{ccc}22 & 12 & 1 \\ 0 & 2 & 2 \\ 4 & 2 & 2\end{array}\right)$ and $C=\left(\begin{array}{lll}1 & 1 & 3 \\ 4 & 0 & 2 \\ 2 & 3 & 4\end{array}\right)$ because $A=5 B+C$.
Notice that the entries in $B$, the matrix of quotients, must be in $\left\{0,1, \ldots, p^{\alpha-1}-1\right\}$ and the entries in $C$, the matrix of remainders, must be in $\{0,1, \ldots, p-1\}$. In other words, $B \in \mathcal{M}_{n}\left(\mathbb{Z}_{p^{\alpha-1}}\right)$ and $C \in \mathcal{M}_{n}\left(\mathbb{Z}_{p}\right)$. Also by our construction $A \equiv C(\bmod p)$. So by our lemma we have that $\operatorname{det} A \equiv \operatorname{det} C(\bmod p)$. So $\operatorname{gcd}(\operatorname{det} A, p)=\operatorname{gcd}(\operatorname{det} C, p)$. So we have:

$$
\begin{gathered}
A \text { is invertible modulo } p^{n} \Leftrightarrow \\
\operatorname{gcd}\left(\operatorname{det} A, p^{n}\right)=1 \Leftrightarrow \\
\operatorname{gcd}(\operatorname{det} A, p)=1 \Leftrightarrow \\
\operatorname{gcd}(\operatorname{det} C, p)=1 \Leftrightarrow \\
C \text { is invertible modulo } p .
\end{gathered}
$$

By our decomposition of $A$, in order to count the number of invertible matrices in $\mathcal{M}_{n}\left(\mathbb{Z}_{m}\right)$, we may choose any matrix in $\mathcal{M}_{n}\left(\mathbb{Z}_{p^{\alpha-1}}\right)$ and then choose an invertible matrix in $\mathcal{M}_{n}\left(\mathbb{Z}_{p}\right)$. The number of matrices in $\mathcal{M}_{n}\left(\mathbb{Z}_{p^{\alpha-1}}\right)$ is $\left(p^{\alpha-1}\right)^{\left(n^{2}\right)}$. The number of invertible matrices in $\mathcal{M}_{n}\left(\mathbb{Z}_{p}\right)$ is $\gamma_{n}$. So we have:

$$
\left|\mathcal{M}_{n}\left(\mathbb{Z}_{p^{\alpha}}\right)\right|=p^{(\alpha-1) n^{2}} \gamma_{n}=p^{(\alpha-1) n^{2}} \prod_{i=0}^{n-1} p^{n}-p^{i}
$$

Now we will consider the case where $m$ is any integer greater than 1 . Our arguments here are essentially Theorem 2.3.2 in [19]. Express $m$ in its unique prime factorization, i.e., write $m=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \cdots p_{k}^{\alpha_{k}}$. Define $\phi: \mathcal{M}_{n}(\mathbb{Z} m) \rightarrow \oplus_{j=1}^{k} \mathcal{M}_{n}\left(\mathbb{Z}_{p_{j}}^{\alpha_{j}}\right)$ by
$\phi(A)=\left(A\left(\bmod p_{1}^{\alpha_{1}}\right), A\left(\bmod p_{2}^{\alpha_{2}}\right), \ldots, A\left(\bmod p_{k}^{\alpha_{k}}\right)\right)$. In other words, $\phi$ maps the matrix ring $\mathcal{M}_{n}\left(\mathbb{Z}_{p}\right)$ into a $k$-tuple of matrix rings which is itself a ring. We will show that $\phi$ is a ring isomorphism.

Clearly $\phi$ is well defined. By the Chinese Remainder Theorem, $\phi$ is a bijection. To show that $\phi$ preserves matrix multiplication first note that by properties of modular arithmetic matrix multiplication preserves modular equivalence. That is, $A(\bmod m) \cdot B(\bmod m)=$ $A B(\bmod m)$.

Let $A, B \in \mathcal{M}_{n}(\mathbb{Z} m)$. For conciseness, let $C^{(i)}$ denote $C\left(\bmod p_{i}^{\alpha_{i}}\right)$ for any matrix $C$ where $m=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \cdots p_{k}^{\alpha_{k}}$. Then

$$
\begin{gathered}
\phi(A B)= \\
\left(A B^{(1)}, \ldots, A B^{(k)}\right)= \\
\left(A^{(1)} B^{(1)}, \ldots, A^{(k)} B^{(k)}=\right. \\
\left(A^{(1)}, \ldots, A^{(k)}\right)\left(B^{(1)}, \ldots, B^{(k)}\right)= \\
\phi(A) \phi(B) .
\end{gathered}
$$

Replacing matrix multiplication with addition in the argument above shows that $\phi$ also preserves the addition operation in the ring $\mathcal{M}_{n}\left(\mathbb{Z}_{m}\right)$. So we have shown that $\phi$ is a ring isomorphism.

Now if $A \in \mathcal{M}_{n}\left(\mathbb{Z}_{m}\right)$ is invertible then $\phi(A) \phi\left(A^{-1}\right)=\phi\left(A A^{-1}\right)=\phi(I)=\left(I \bmod p_{1}^{\alpha_{1}}, \ldots, I \bmod p_{k}^{\alpha_{k}}\right)$, which is the identity element in the codomain, $\oplus_{i=1}^{k} \mathcal{M}_{n}\left(\mathbb{Z}_{p_{i}^{\alpha_{i}}}\right)$. So $\phi(A)$ has an inverse. In other words, $\phi(A)$ is invertible. Conversely, if $\phi(A)$ has an inverse, $(\phi(A))^{-1}$, then by ho-
momorphism properties, $(\phi(A))^{-1}=\phi\left(A^{-1}\right)$. Hence, $A$ is invertible.

Then in order to count the number of invertible matrices in $\mathcal{M}_{n}\left(\mathbb{Z}_{m}\right)$ it suffices to count the number of invertible matrices in $\oplus_{j=1}^{k} \mathcal{M}_{n}\left(\mathbb{Z}_{p_{j}}^{\alpha_{j}}\right)$. A tuple in $\oplus_{i=1}^{k} \mathcal{M}_{n}\left(\mathbb{Z}_{p_{i}^{\alpha_{i}}}\right)$ is invertible if and only if each of its components is invertible. From our work above we know the number of invertible matrices in each $\mathcal{M}_{n}\left(\mathbb{Z}_{p_{j} \alpha_{j}}\right)$ is $p_{j}^{(\alpha-1) n^{2}} \prod_{i=0}^{n-1} p_{j}^{n}-p_{j}^{i}$. Each component of the tuple is independently chosen so we have for $m=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \cdots p_{k}^{\alpha_{k}}$ :

$$
\left|G L_{n}\left(\mathbb{Z}_{m}\right)\right|=\prod_{j=1}^{k}\left(p_{j}^{\left(\alpha_{j}-1\right) n^{2}} \prod_{i=0}^{n-1} p_{j}^{n}-p_{j}^{i}\right)=\prod_{j=1}^{k}\left(p_{j}^{\left(\alpha_{j}-1\right) n^{2}} \gamma_{n, p_{j}}\right)
$$

We note that in the case $n=1$ our formula reduces to $\prod_{j=1}^{k} p_{j}^{\alpha_{j}}-p_{j}$. This is the number of positive integers less than or equal to $n$ that are relatively prime to $n$ (Euler's Phi function).

Also, when $m$ is square free then the formula reduces to $\prod_{j=1}^{k} \gamma_{n, p_{j}}$ where $\gamma_{n, p_{j}}$ is the order of $G L_{n}\left(\mathbb{F}_{p_{j}}\right)$.

Finally, $\left|G L_{n}\left(\mathbb{Z}_{m}\right)\right|=\left|G L_{n}\left(\mathbb{F}_{q}\right)\right|$ if and only if $m=q=p$ for some prime $p$.

For $m=4$ and $n \geq 0$ we have sequence A065128.

$$
1,2,96,86016,1321205760,335522845163520,1385295986380096143360, \ldots
$$

Table 39: Order of $G L_{n}\left(\mathbb{Z}_{4}\right)$ for $n \geq 0$. A065128

For $m=6$ and $n \geq 0$ we have sequence A065498.
$1,2,288,1886976,489104179200,4755360379856486400, \ldots$

Table 40: Order of $G L_{n}\left(\mathbb{Z}_{6}\right)$ for $n \geq 0$. A065498

The number of $2 \times 2$ invertible matrices over $\mathbb{Z}_{m}$ for $m \geq 1$ is A000252.
$\square$
$1,6,48,96,480,288,2016,1536,3888,2880 \ldots$

Table 41: Order of $G L_{2}\left(\mathbb{Z}_{m}\right)$ for $m \geq 1$. A000252

The number of $3 \times 3$ invertible matrices over $\mathbb{Z}_{m}$ for $m \geq 1$ is A064767.

$$
\begin{array}{|r}
\hline 1,168,11232,86016,1488000,1886976,33784128, \ldots \\
\text { Table 42: Order of } G L_{3}\left(\mathbb{Z}_{m}\right) \text { for } m \geq 1 \text {. A064767 }
\end{array}
$$

It is important to understand that what is being counted in the last two sequences given above is the number of automorphisms on the finite abelian groups $C_{m} \times C_{m}$ and $C_{m} \times C_{m} \times C_{m}$ respectively where $C_{m}$ is the cyclic group of order $m$. We want to realize that $G L_{n}\left(\mathbb{Z}_{m}\right)$ is the group of automorphisms on $C_{m}^{n}$. It is insightful to observe that by the following well known theorem, the special case when $n=1$ again gives the expected result.

Theorem 15.3 ([10]). The automorphism group of the cyclic group $C_{m}$ is isomorphic to the abelian group $\mathbb{Z}_{m}^{\times}$of order $\phi(n)$.

Proof. Let $x$ be a generator of $C_{m}$. If $\sigma$ is an automorphism of $C_{m}$ then $\sigma(x)=x^{a}$ for some $a \in \mathbb{Z}$. Since $x$ is a generator, the integer $a$ uniquely determines the map $\sigma$. Denote this mapping as $\sigma_{a}$. Since $|x|=n$ then $a$ is only defined modulo $n$. Since $\sigma_{a}$ is an automorphism then $|x|=\left|x^{a}\right|$. So $\frac{n}{\operatorname{gcd}(n, a)}=n$. So $\operatorname{gcd}(n, a)=1$. So for every $a$ relatively prime to $n$ we have exactly one map $x \mapsto a$ that is an automorphism on $C_{m}$. Then we have the bijective map:

$$
\psi: \operatorname{Aut}\left(C_{m}\right) \rightarrow \mathbb{Z}_{m}^{\times}
$$

$$
\text { by } \psi\left(\sigma_{a}\right)=a(\bmod n)
$$

Now $\psi$ is a homomorphism because for all $\sigma_{a}, \sigma_{b} \in \operatorname{Aut}\left(C_{m}\right)$ we have:

$$
\begin{gathered}
\sigma_{a} \circ \sigma_{b}(x)=\sigma_{a}\left(\sigma_{b}(x)\right)=\sigma_{a}\left(x^{b}\right)=\left(x^{b}\right)^{a}=x^{a b}=\sigma_{a b}(x) \text { so that } \\
\psi\left(\sigma_{a} \circ \sigma_{b}\right)=\psi\left(\sigma_{a b}\right)=a b(\bmod n)=\psi\left(\sigma_{a}\right) \circ \psi\left(\sigma_{b}\right)
\end{gathered}
$$

## The special linear group of matrices over $Z_{m}$

The set of $n \times n$ matrices with entries in the ring $\mathbb{Z}_{m}$ that have determinant equal to 1 is denoted $S L_{n}\left(\mathbb{Z}_{m}\right)$. It is a subgroup of $G L_{n}\left(\mathbb{Z}_{m}\right)$. The matrices in $S L_{n}\left(\mathbb{Z}_{m}\right)$ are the kernel
of the group homomorphism $\psi: G L_{n}\left(\mathbb{Z}_{m}\right) \rightarrow \mathbb{Z}_{m}^{\times}$where $\psi$ is the determinant mapping and $\mathbb{Z}_{m}^{\times}$is the group of units in the ring $\mathbb{Z}_{m}$. Now $\psi$ is a surjective homomorphism, so by First Isomorphism Theorem, the quotient group $G L_{n}\left(\mathbb{Z}_{m}\right) / S L_{n}\left(\mathbb{Z}_{m}\right)$ is isomorphic to $\mathbb{Z}_{m}^{\times}$. By Theorem 13.3, $\left|\mathbb{Z}_{m}^{\times}\right|=\phi(m)$. So we have:

$$
\begin{aligned}
& \left|G L_{n}\left(\mathbb{Z}_{m}\right) / S L_{n}\left(\mathbb{Z}_{m}\right)\right|=\left|\mathbb{Z}_{q}^{\times}\right| \\
& \frac{\prod_{j=1}^{k}\left(p_{j}^{\left(\alpha_{j}-1\right) n^{2}}{ }_{\left.\gamma_{n, p_{j}}\right)}\right.}{\left|S L_{n}\left(\mathbb{Z}_{m}\right)\right|}=\phi(m) \\
& \left|S L_{n}\left(\mathbb{Z}_{m}\right)\right|=\frac{\prod_{j=1}^{k}\left(p_{j}^{\left(\alpha_{j}-1\right) n^{2}} \gamma_{n, p_{j}}\right)}{\phi(m)}
\end{aligned}
$$

The number of $2 \times 2$ invertible matrices over $\mathbb{Z}_{m}$ with determinant 1 for $m \geq 1$ is A00056.
$1,6,24,48,120,144,336,384,648,720,1320,1152,2184,2016,2880 \ldots$
Table 43: Order of $S L_{2}\left(\mathbb{Z}_{m}\right)$ for $m \geq 1$. A000056

The number of $3 \times 3$ invertible matrices over $\mathbb{Z}_{m}$ with determinant 1 for $m \geq 1$ is A011785.

$$
1,168,5616,43008,372000,943488,5630688,11010048,36846576, \ldots
$$

Table 44: Order of $S L_{3}\left(\mathbb{Z}_{m}\right)$ for $m \geq 1$. A011785

## The projective special linear group of matrices over $\mathbb{Z}_{m}$

The projective special linear group of matrices over $\mathbb{Z}_{m}$ is the quotient group of $S L_{n}\left(\mathbb{Z}_{m}\right)$ with its center. It is denoted $\operatorname{PS} L_{n}\left(\mathbb{Z}_{m}\right)$. The center of $S L_{n}\left(\mathbb{Z}_{m}\right)$ is the group of $n \times n$ scalar matrices whose diagonal contains the element $x \in \mathbb{Z}_{m}$ such that $x^{n}=1$. In other words, the center of $S L_{n}\left(\mathbb{Z}_{m}\right)$ is the set $\left\{x I_{n}: x \in \mathbb{Z}_{m}^{\times}, x^{n}=1\right\}$. The elements in $\left|P S L_{n}\left(\mathbb{Z}_{m}\right)\right|$ are equivalence classes, where two matrices are equivalent if all the entries of one is a scalar multiple of the other. In other words, for all $A, B \in S L_{n}\left(\mathbb{Z}_{m}\right), A \sim_{R} B$ if and only if there is a scalar matrix $C$ such that $A=B C$.

To determine the order of $P S L_{n}\left(\mathbb{Z}_{m}\right)$ we need to first determine the number of elements $x \in \mathbb{Z}_{m}$ such that $x^{n}=1$. Then each such $x$ will correspond to exactly one scalar matrix $x I_{n}$ in the center of $S L_{n}\left(\mathbb{Z}_{m}\right)$. The multiplicative group of integers modulo $m, \mathbb{Z}_{m}^{\times}$is a finite abelian group. By the Fundamental Theorem of Finitely Generated Abelian Groups, $\mathbb{Z}_{m}^{\times}$isomorphic to a direct product of cyclic groups, $C_{n_{1}} \times C_{n_{2}} \times \cdots \times C_{n_{s}}$ where $n_{j} \geq 2$ and $n_{j+1} \mid n_{j}$ for all $j=1, \ldots, s-1$ and $\prod_{j=1}^{s} n_{j}=\phi(m)$. We will call the integers $n_{j}$ the characteristic factors of $\mathbb{Z}_{m}^{\times}$. There is a simple algorithm for obtaining the characteristic factors of $\mathbb{Z}_{m}^{\times}$from the prime factorization of $m$. The proof of which is rather long. The reader is referred to Shanks [18] pages 92-108.

Theorem 15.4. Let $G=C_{n_{1}} \times C_{n_{2}} \times \cdots \times C_{n_{s}}$. Then the number of elements $x \in G$ such that $x^{n}=1_{G}$ is equal to $\prod_{i=1}^{s} g c d\left(n, n_{i}\right)$ where $1_{G}$ is the identity in $G$.

Proof. By Theorems $12.9,12.10$, and 12.11 we have that the number of solutions to $x^{n}=$ $1_{G}$ in $C_{n_{i}}$ is $\operatorname{gcd}\left(n, n_{i}\right)$. So for each component $g_{i}$ in the tuple $\left(g_{1}, g_{2}, \ldots, g_{s}\right)$ we have $\operatorname{gcd}\left(n, n_{i}\right)$ choices. Each choice is made independently. So there are $\prod_{i=1}^{s} \operatorname{gcd}\left(n, n_{i}\right)$ elements $x \in G$ that satisfy $x^{n}=1_{G}$

So we have: If $m$ is such that $C_{n_{1}} \times C_{n_{2}} \times \cdots \times C_{n_{s}}$ are the characteristic factors of $\mathbb{Z}_{m}^{\times}$then

$$
\left|P S L_{n}\left(\mathbb{Z}_{m}\right)\right|=\frac{\prod_{j=1}^{k}\left(p_{j}^{\left(\alpha_{j}-1\right) n^{2}}{ }_{\left.\gamma_{n, p_{j}}\right)}\right.}{\phi(m) \prod_{i=1}^{s} \operatorname{gcd}\left(n, n_{i}\right)}
$$

The order of the projective special linear group over $\mathbb{Z}_{m}$ for $n=2$ and $m \geq 1$ is sequence A300915.
$1,6,12,24,60,72,168,96,324,360,660,288,1092,1008,720 \ldots$
Table 45: Order of $P S L_{2}\left(\mathbb{Z}_{m}\right)$ for $m \geq 1$. A300915

## References

[1] The correspondence theorem for groups, Mathematics Stack Exchange, https://math.stackexchange.com/q/955460 (version: 2014-10-02).
[2] Elementary abelian group, Wikipedia, The Free Encyclopedia, 2018, http://en.wikipedia.org/wiki/ElementaryAbelianGroup.
[3] Finite field, Wikipedia, The Free Encyclopedia, 2018, https://en.wikipedia.org/wiki/Finitefield.
[4] q-analog, Wikipedia, The Free Encyclopedia, 2018, http://en.wikipedia.org/wiki/Qanalog.
[5] Sheldon Axler, Linear algebra done right, 3 ed., Springer, 2015.
[6] Jonathon Azose, A tiling interpretation of $q$-binomial coefficients, 2007, https://www.math.hmc.edu/seniorthesis/archives/2007/jazose/jazose-2007-thesis.pdf.
[7] Miklos Bóona, Introduction to enumerative combinatorics, McGraw Hill Higher Education, 2007.
[8] David Ellerman, The number of direct-sum decompositions of a finite vector space, arXiv 1603 (2016), 1-11.
[9] Philippe Flajolet and Robert Sedgewick, Analytic combinatorics, Cambridge University Press, 2009.
[10] D Dummit R Foote, Abstract algebra, Wiley, 2003.
[11] Joseph Gallian, Contemporary abstract algebra, Brooks/Cole, 2013.
[12] Groupprops, Order formulas for linear groups, 2018, https://groupprops.subwiki.org/wiki/Order/formulas/for/linear/groups.
[13] Donald Knuth, Subspaces subsets and partitions, Journal of Combinatoial Theory 10 (1977), 107-109.
[14] Barbara Margolius, Permutations with inversions, 2018, http://academic.csuohio.edu/bmargolius/homepage/inversions/invers.htm.
[15] Yan Sun Pete McNeely, q-binomial coefficients and the q-binomial theorem, 2012, https://pdfs.semanticscholar.org/8cf4/eeba260dfc96677044eb40465daa7e400e23.pdf.
[16] Kent Morrison, Integer sequences and matrices over finite fields, Journal of Integer Sequences 9 (2006), 1-25.
[17] Joseph Rotman, An introduction to the theory of groups, Springer Verlag, 1995.
[18] D. Shanks, Solved and unsolved problems in number theory, Chelsea Publishing Co., 1962.
[19] J Overby W Traves and J Wojdylo, On the keyspace of the hill cipher, 2000, http://jeff.over.bz/papers/undergrad/on-the-keyspace-of-the-hill-cipher.pdf.
[20] Vinroot, The multiplicative group of a finite field, Math 430 Spring 2013, 2013, www.math.wm.edu/ vinroot/430513 multfinitefield.pdf.
[21] C Vinroot, An enumeration of flags in finite vector spaces, The Electronic Journal of Combinatorics 19 (2012), 1-4.
[22] A Nijenhuis A Solow H Wilf, bijective methods in the theory of finite vector spaces, Journal of Combinatoial Theory 37 (1984), 80-84.
[23] E Calabi H Wilf, On the sequential and random selection of subspaces over a finite field, Journal of Combinatoial Theory 22 (1977), 107-109.

I, Geoffrey Critzer , hereby submit this thesis/report to Emporia State University as partial fulfillment of the requirements for an advanced degree. I agree that the Library of the University may make it available to use in accordance with its regulations governing materials of this type. I further agree that quoting, photocopying, digitizing or other reproduction of this document is allowed for private study, scholarship (including teaching) and research purposes of a nonprofit nature. No copying which involves potential financial gain will be allowed without written permission of the author. I also agree to permit the Graduate School at Emporia State University to digitize and place this thesis in the ESU institutional repository.


[^0]:    ${ }^{1}$ The reader is asked to forgive us here for this abuse of notation. We acknowledge that the quantity

