NUMBER OF NEAR-VECTOR SPACES OVER FINITE FIELDS

WILASINEE CHOMJUN

A Thesis Submitted to the Graduate School of Naresuan University

in Partial Fulfillment of the Requirements

for the Master of Science Degree in Mathematics

December 2017

Thesis entitled "Number of Near-vector Spaces over Finite Fields"

by Miss Wilasinee Chomjun

has been approved by the Graduate School as partial fulfillment of the requirements for the Master of Science Degree in Mathematics of Naresuan University.

Oral Defense Committee

..... Chair

(Assistant Professor Somphong Jitman, Ph.D.)

..... Advisor

(Assistant Professor Kijti Rodtes, Ph.D.)

..... Internal Examiner

(Assistant Professor Umarin Pintoptang, Ph.D.)

Approved

.....

(Associate Professor Paisarn Muneesawang, Ph.D.)

Dean of the Graduate School

ACKNOWLEDGEMENT

First, I wish to express my sincerely gratitude to my advisor, Assistant Professor Dr. Kijti Rodtes for his guidance, encouragement and unmeasured amount of support. His vision and creative thinking are very helpful for developing my mathematical skill and that made it possible for me to construct the thesis.

I would like to thank Assistant Professor Dr. Somphong Jitman and Assistant Professor Dr. Umarin Pintoptang for many useful suggestions and comments for the thesis.

Finally, I would like to thank to my teachers and parents that always encourage and support everything to my success here.

Wilasinee Chomjun

Title	NUMBER OF NEAR-VECTOR SPACES OVER FINITE FIELDS
Author	Wilasinee Chomjun
Advisor	Assistant Professor Kijti Rodtes, Ph.D.
Academic Paper	Thesis M.S. in Mathematics, Naresuan University, 2017
Keywords	Finite fields, Near-vector spaces.

ABSTRACT

A slip on a paper concerning near-vector spaces is fixed. New characterization of near-vector spaces which is a generalization determined by finite fields is provided and the number (up to isomorphism) of these spaces is exhibited.

LIST OF CONTENTS

LIST OF TABLES

Table Page

CHAPTER I

INTRODUCTION

In 1974, the concept of near vector space was introduced and studied by Andre. Later several researchers, for example, Van der walt, Howell, Mayer and Tim Boykett, paid attention to investigate such concept. In 2010, Howell and Mayer classified near-vector spaces over finite fields of p (p is prime) elements up to isomorphism. Until 2014, they also extended the result to a finite field of p^n elements and presented in Theorem 2.2.13, [1] of the paper name "Near-vector spaces determined by finite fields"(in Journal of Algebra, 2014). They asserted that the number of near vector spaces $V = \mathbb{F}^{\oplus m}$ over a finite field $\mathbb{F} = GF(p^n)$ is exactly

$$\begin{pmatrix} m + \frac{\phi(p^n-1)}{n} - 2 \\ m-1 \end{pmatrix}$$

up to the isomorphism in Definition 2.2.7, where ϕ is the Euler's totient function. They calculated the number based on the distinct suitable sequences, (Definition 2.2.5, [1]). In other word, if A_1^* and A_2^* are determined by suitable sequences (S_1) and (S_2), respectively, then $(\mathbb{F}^{\oplus m}, A_1^*) \cong (\mathbb{F}^{\oplus m}, A_2^*)$ if and only if $(S_1) = (S_2)$.

However, for the case $\mathbb{F} = GF(3^3)$ and $m = 4$, it turns out that $(\mathbb{F}^{\oplus 4}, A_1^*) \cong (\mathbb{F}^{\oplus 4}, A_2^*)$, where $A_1^* = \{s_\alpha \,|\, \alpha \in \mathbb{F}\}$ and $A_2^* = \{t_\beta \,|\, \beta \in \mathbb{F}\}$ are constructed using the sequences $(S_1) = (1, 5, 7, 7)$ and $(S_2) = (1, 7, 17, 17)$, respectively, which are distinct suitable sequences. Accurately, the isomorphism is obtained by the group isomorphisms $\theta : \mathbb{F}^{\oplus 4} \longrightarrow \mathbb{F}^{\oplus 4}$ defined by $\theta(x_1, x_2, x_3, x_4) := (x_2, x_1^9, x_3, x_4)$ and $\eta : A_1^* \longrightarrow A_2^*$ defined by $\eta(s_\alpha) := t_{\alpha^5}$, which can be seen that;

$$\begin{aligned} \theta((x_1, x_2, x_3, x_4)s_\alpha) &= \theta(x_1\alpha, x_2\alpha^5, x_3\alpha^7, x_4\alpha^7) \\ &= (x_2\alpha^5, x_1^9\alpha^9, x_3\alpha^7, x_4\alpha^7) \\ &= (x_2\alpha^5, x_1^9(\alpha^5)^7, x_3(\alpha^5)^{17}, x_4(\alpha^5)^{17}) \end{aligned}$$

$$
\begin{aligned}
&= (x_2, x_1^9, x_3, x_4) t_{\alpha^5} \\
&= \theta(x_1, x_2, x_3, x_4)\eta(s_\alpha)
\end{aligned}
$$

for all $(x_1, x_2, x_3, x_4) \in \mathbb{F}^{\oplus 4}, s_\alpha \in A_1^*$. This contradicts to the main results of the paper. A slip can be found in the proof of Theorem 3.9 in [1] (line 17^{th} in the proof) in which there is using the isomorphism η to be $\eta(s_\alpha) = t_\alpha$. In fact, this should be $\eta(s_\alpha) = t_{\alpha^q}$, for some $1 \leq q \leq p^n - 1$ and $\gcd(q, p^n - 1) = 1$.

In this thesis, we fix the slip and provide a criteria for the classification of near-vector spaces $\mathbb{F}^{\oplus m}$ over a finite field $\mathbb{F} = GF(p^n)$. The number of near-vector spaces up to the isomorphism is also displayed based on subgroups lattice of the abelian group $G := U(p^n - 1)/\langle p \rangle$.

CHAPTER II

PRELIMINARIES

In this chapter, we give some definitions, notations, examples, and basic results, which are used in this research. This chapter is divided into two sections. The first section deals with fundamental algebra structures. Details and proofs about groups and fields can be found in [2] and [3]. The next one is about basic definitions and examples in near-vector spaces.

2.1 Fundamental Algebraic Structures

Definition 2.1.1. [2] Let G be a set with a binary operation, which is denoted by $\cdot$ and called the multiplication in G. G is called a *group* with respect to the multiplication, if the following manipulation rules hold:

$G1$ The associative law. That is, for all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

$G2$ There is an element in G, denoted by e, such that $a \cdot e = a$ for all $a \in G$.

$G3$ For any element $a \in G$, there is an element in G, denoted by a^{-1}, such that $a \cdot a^{-1} = e$.

Definition 2.1.2. [2] Let G be a group and the binary operation in G be denoted by $\cdot$. If the commutative law holds in G, i.e., for all $a, b \in G$, $ab = ba$, G is called an *abelian (or a commutative) group.*

Definition 2.1.3. [2] Let H be a subgroup of a group G. For each $a \in G$, the set $\{ah : h \in H\}$ (resp. $\{ha : h \in H\}$) is called a *left coset* (resp. right coset) of G relative to H and is denoted by aH (resp. Ha).

Proposition 2.1.4. [2] *Let G be a finite group and H be a subgroup of G. Then the number of left cosets of G relative to H is equal to the number of right cosets of G relative to H.*

Lemma 2.1.5. [2] *Let G be a finite group and H be a subgroup of G. Then any two left cosets of G relative to H contain the same number of elements.*

Definition 2.1.6. [3] A subgroup N of a group G is said to be *normal* if $aN = Na$ for all $a \in G$.

Theorem 2.1.7. [3] *Every subgroup of an abelian group is a normal subgroup.*

Definition 2.1.8. [3] Let N be a normal subgroup of a group G, then the group $G/N = \{aN : a \in G\}$ is called the *quotient group* or *factor group* of G by N.

Definition 2.1.9. [2] Let a be an element of a group G. If for any positive integer n, we have $a^n \neq e$, then a is called an *element of infinite order*. If there exists a positive integer n such that $a^n = e$, then a is called an *element of finite order* and the smallest positive integer n such that $a^n = e$ is called the *order of* a. The order of a is denoted by $ord(a)$.

Definition 2.1.10. [3] Let G be a group and $a \in G$. The set $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G which is called the *cyclic subgroup of G generated by a*.

A group G is called *cyclic* if there exists an element $a \in G$ with $G = \langle a \rangle$; in this case a is called *a generator of G*.

Example 2.1.11. *Let $G = \{1, -1, i, -i\} \subseteq \mathbb{C}$, (the group operation is the multiplication of complex numbers), $(G, \cdot)$ is a cyclic group, $G = \langle i \rangle$. Now, consider*

$$(1)^1 = 1, \text{ then } 1 \text{ has order } 1$$
$$(-1)^2 = 1, \text{ then } -1 \text{ has order } 2$$
$$(i)^4 = 1 \text{ but } (i)^2 \neq 1, \text{ then } i \text{ has order } 4$$
$$(-i)^4 = 1 \text{ but } (-i)^2 \neq 1, \text{ then } -i \text{ has order } 4.$$

Theorem 2.1.12. [2] *Let G be the cyclic group generated by an element $a \in G$. If G is of finite order n, then $ord(a) = n$ and*

$$G = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Proposition 2.1.13. [2] *Let $G = \langle a \rangle$ be a cyclic group of order n. For any integer k, a^k is a generator of G if and only if* $\gcd(k, n) = 1$.

Definition 2.1.14. [3] The *Euler ϕ−function* is the map $\phi : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $\phi(n) = 1$ for $n = 1$, and, for $n > 1, \phi(n)$ is the number of positive integer m with $1 \leq m < n$ and $\gcd(m, n) = 1$.

Proposition 2.1.15. [3] *The number of generators of a cyclic group, of order n is $\phi(n)$.*

Definition 2.1.16. [3] Let a, b, n be integers with $n > 0$. Then a is *congruent to b modulo n*, written $a \equiv b (\mathrm{mod}\, n)$ provides that n divides $a - b$.

Definition 2.1.17. [3] Let a and n be integers with $n > 0$. The *congruence class of a modulo n*, denote $[a]$ or $\bar{a}$, is the set of all those integers that are congruent to a modulo n, i.e.,

$$[a] = \{b : b \in \mathbb{Z} \text{ and } b \equiv a (\mathrm{mod}\, n)\},$$

where $b \equiv a (\mathrm{mod}\, n)$ means that $b - a = nk$ for some integer k. Thus

$$\begin{aligned} [a] &= \{b : b \in \mathbb{Z}, b \equiv a (\mathrm{mod}\, n)\}. \\ &= \{b : b = a + nk, k \in \mathbb{Z}\} \\ &= \{a + nk : k \in \mathbb{Z}\}. \end{aligned}$$

Theorem 2.1.18. [3] $a \equiv c (\mathrm{mod}\, n)$ *if and only if* $[a] = [c]$.

Definition 2.1.19. [3] A relation $\sim$ on a set S is

(i) reflexive : if $a \sim a$ for all $a \in S$.

(ii) symmetric : if $a \sim b$ implies $b \sim a$ for all $a, b \in S$.

(iii) transitive : if $a \sim b$ and $b \sim c$ imply $a \sim c$ for all $a, b, c \in S$.

A relation on S that has all of these properties is called an *equivalence relation* on S.

Definition 2.1.20. [3] Let $\sim$ be an equivalence relation on a set S. If $a \in S$, the *equivalence class* of a, denoted by $[a]$, is defined by

$$[a] = \{s \in S : s \sim a\} \subseteq S.$$

Theorem 2.1.21. [3] *(Lagrange's Theorem). If H is a subgroup of a finite group G, then $|H|$ is a divisor of $|G|$.*

Definition 2.1.22. [3] The *index of a subgroup H in G*, denote by $[G : H]$, is the number of left cosets (or right cosets) of H in G.

Proposition 2.1.23. [3] *If H is a subgroup of a finite group G, then*

$$[G : H] = |G|/|H|.$$

Corollary 2.1.24. [3] *If G is a finite group and $a \in G$, then the order of a divides $|G|$.*

Definition 2.1.25. [3] A mapping ϕ from a group G into a group G' is said to be a *homomorphism* if for all $a, b \in G$,

$$\phi(ab) = \phi(a)\phi(b).$$

Also, a homomorphism from a group G to itself is called an *endomorphism of G*. We denote $End(G)$ for the set of all homomorphisms on G.

Definition 2.1.26. [2] Let G and G' be two groups. Assume that a bijective map from G to G',

$$\sigma : a \longmapsto \sigma(a) \ (a \in G, \sigma(a) \in G')$$

and for any $a, b \in G$,

$$\sigma(ab) = \sigma(a)\sigma(b).$$

Then we say that G and G' are *isomorphic*, which is denoted by $G \cong G'$, and that σ is an isomorphic map from G to G', or in short, an *isomorphism*. An isomorphism from a group G to itself is called an *automorphism* of G. We write $Aut(G)$ for the set of all automorphisms of G.

Definition 2.1.27. [2] Let $\mathbb{F}$ be a set with two binary operations $+$ and $\cdot$ (called *addition* and *multiplication*, respectively). $\mathbb{F}$ is called a *field* with respect to the addition and multiplication, if the following manipulation rules are fulfilled:

$F1$: $(\mathbb{F}, +)$ is an abelian group.

$F2$: $(\mathbb{F}^*, \cdot)$ is an abelian group, where $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$ and 0 is the additive identity of the group $(\mathbb{F}, +)$.

$F3$: $a(b + c) = ab + ac$ for all $a, b, c \in \mathbb{F}$.

We also say that $(\mathbb{F}, +, \cdot)$ is a field. $(\mathbb{F}, +)$ is called the *additive group* of the field $\mathbb{F}$ and $(\mathbb{F}^*, \cdot)$ is called the *multiplicative group* of $\mathbb{F}$.

Definition 2.1.28. [1] A *skew field* is a triple $(\mathbb{F}, +, \cdot)$ which satisfies :

$F1$: $(\mathbb{F}, +)$ is an abelian group.

$F2$: $(\mathbb{F}^*, \cdot)$ is a group, where $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$ and 0 is the additive identity of the group $(\mathbb{F}, +)$.

$F3$: $a(b + c) = ab + ac$ for all $a, b, c \in \mathbb{F}$.

Definition 2.1.29. [2] Let $\mathbb{F}$ be a field and e be its identity. If for any positive integer m, we have $me \neq 0$, then we say that the characteristic of $\mathbb{F}$ is 0 or that $\mathbb{F}$ is a *field of characteristic* 0. If there exists a positive integer m such that $me = 0$, then the smallest positive integer p satisfying $pe = 0$ is called the *characteristic* of $\mathbb{F}$ and $\mathbb{F}$ is called a *field of characteristic* p.

Theorem 2.1.30. [2] *Let $\mathbb{F}$ be any field, then the characteristic of $\mathbb{F}$ is either 0 or a prime p.*

Definition 2.1.31. [2] Let $p(x)$ be a polynomial with $\deg p(x) \geq 1$ in $\mathbb{F}[x]$. If $p(x)$ is a prime element in $\mathbb{F}[x]$, we say that $p(x)$ is an *irreducible* polynomial in $\mathbb{F}[x]$. Otherwise $p(x)$ is said to be *reducible.*

Definition 2.1.32. [2] Let $\mathbb{F}$ be a field. If the number of elements in $\mathbb{F}$ is infinite, $\mathbb{F}$ is called an *infinite field.* If the number of elements in $\mathbb{F}$ is finite, $\mathbb{F}$ is called a *finite field* or a *Galois field.* Here, $\mathbb{F} = GF(p^n)$ is a finite field with p^n elements, where p is a prime characteristic of $\mathbb{F}$ and n is a positive integer.

In fact, we can calculate all distinct elements in $\mathbb{F} = GF(p^n)$ by using the following proposition:

Proposition 2.1.33. [2] *Let $\mathbb{Z}_p$ be the prime field of characteristic p and $p(x)$ be an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$. Then $\mathbb{Z}_p[x]/_{(p(x))}$ is a finite field with p^n elements.*

Example 2.1.34. *Let $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$, which is an irreducible polynomial of degree 2 in $\mathbb{Z}_2[x]$. Then $\mathbb{Z}_2[x]/_{(x^2+x+1)}$ is a finite field of order 2^2 with the multiplication table:*

Table 1 The multiplication table of $\mathbb{Z}_2[x]/_{(x^2+x+1)}$

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

Theorem 2.1.35. [2] *Any two finite fields containing the same number of elements are isomorphic.*

Let $\mathbb{F} = GF(p^n) = \mathbb{F}_q$ be a finite field with p^n elements. The multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is of order $q-1$, every element of $\mathbb{F}_q^*$ is of finite order and its order is a divisor of $q-1$. Furthermore, $GF(p^n)$ has following results.

Proposition 2.1.36. [2] *Let $\mathbb{F}$ be a field of characteristic $p, p \neq 0, a, b$ be any two elements of $\mathbb{F}$, and n be any nonnegative integer, then*

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}.$$

Theorem 2.1.37. [2] *Let $\mathbb{F} = GF(p^n)$ be a finite field with p^n elements. Then $a^{p^n-1} = 1$ for all $a \in \mathbb{F}^*$.*

Theorem 2.1.38. [2] *The multiplicative group of any finite field is cyclic.*

In 2014, Howell and Mayer constructed a necessary condition on the positive integers q and r in which sufficient for the identity $(a^q + b^q)^r = (a^r + b^r)^q$ is true over a finite field, where $a, b \in \mathbb{F} = GF(p^n)$. They presented this a necessary condition in the form of following theorem:

Theorem 2.1.39. [1] *Let $q_1, q_2 \in \{1, 2, \ldots, p^n - 1\}$ with $\gcd(q_i, p^n - 1) = 1, (i = 1, 2)$ and $q_1 < q_2$. Then $(a^{q_1} + b^{q_1})^{q_2} = (a^{q_2} + b^{q_2})^{q_1}$ for all $a, b \in \mathbb{F}$ if and only if $q_1 \equiv q_2 p^l \bmod (p^n - 1)$ for some $l \in \{0, 1, \ldots, n-1\}$.*

Proposition 2.1.40. [1] *Let ψ_i be an automorphism of the group $(\mathbb{F}^*, \cdot)$, where $\mathbb{F} = GF(p^n)$ and the multiplicative group $U(p^n - 1) = \{k \in \mathbb{Z} : 1 \leq k \leq p^n - 1, \gcd(k, p^n - 1) = 1\}$. Then there exists $q_i \in U(p^n - 1)$ such that $\psi_i(x) = x^{q_i}$ for all $x \in \mathbb{F}^*$.*

2.2 Basic definitions and Examples in Near Vector Spaces

Let p be a prime, n be a positive integer and $\mathbb{F} = \mathrm{GF}(p^n)$, be a field of p^n elements. We first recall the definition of a near-vector space over a finite field $\mathbb{F}$.

Definition 2.2.1. [1] A pair (V, A) is called a *near-vector space* if:

1. $(V, +)$ is a group and A is a set of endomorphisms of V,
2. A contains the endomorphisms 0, id and $-id$,
3. $A^* = A\backslash\{0\}$ is a subgroup of the group $Aut(V)$,
4. A acts fixed point freely on V; i.e., for $x \in V$ and $\alpha, \beta \in A$, $x\alpha = x\beta$ implies that $x = 0$ or $\alpha = \beta$,
5. the quasi-kernel $Q(V)$ of V, generates V as a group. Here, $Q(V) = \{x \in V : \forall \alpha, \beta \in A, \exists \gamma \in A \text{ such that } x\alpha + x\beta = x\gamma\} \subseteq V$.

Remark:

(a) $-id \in A$ implies that $(V, +)$ is an abelian group, since by (2) : $x + y = (-x)(-1) + (-y)(-1) = (-x - y)(-1) = ((-(y + x))(-1) = y + x$. Also, the *dimension* of the near-vector space, $\dim(V)$, is uniquely determined by the cardinality of an independent generating set for $Q(V)$.

(b) Every vector space is a near vector space, that is we can consider vector space as near vector space under the scalar multiplication defined by

$$(x_1, \ldots, x_m)s_\alpha = (\alpha x_1, \ldots, \alpha x_m),$$

where $(x_1, \ldots, x_m) \in V$ and $A = \{s_\alpha : \alpha \in \mathbb{F}\}$.

Definition 2.2.2. [1] Two near-vector spaces (V_1, A_1) and (V_2, A_2) are *isomorphic*, written by $(V_1, A_1) \cong (V_2, A_2)$, if there are group isomorphisms $\theta : (V_1, +) \to$

$(V_2, +)$ and $\eta : (A_1^*, \cdot) \to (A_2^*, \cdot)$ such that $\theta(x\alpha) = \theta(x)\eta(\alpha)$ for all $x \in V_1$ and $\alpha \in A_1^*$.

In fact, the group isomorphism $\eta : (A_1^*, \cdot) \to (A_2^*, \cdot)$ can be extended to a semigroup isomorphism $\widehat{\eta} : A_1 \longrightarrow A_2$ by setting $\widehat{\eta}(0) = 0$ and $\widehat{\eta}(\alpha) = \eta(\alpha)$, for all $\alpha \in A_1^*$. For a near-vector space (V, A), the endomorphisms in A are sometimes called *scalars* and the action of these endomorphisms on the elements of V is sometimes called *scalar multiplication.*

Example 2.2.3. *Put* $(V_1, +) = (V_2, +) = (GF(5), +)$. *Let* $A_1 = \{s_\alpha : \alpha \in GF(5)\}$ *and* $A_2 = \{t_\alpha : \alpha \in GF(5)\}$, *where* $xs_\alpha := x\alpha$ *and* $xt_\alpha := x\alpha^3$ *for all* $x, \alpha \in GF(5)$. *Then, we show that* (V_1, A_1) *and* (V_2, A_2) *are near-vector spaces.*

1) $(V_1, +)$ *is a group. Moreover* $A_1 = \{s_\alpha : \alpha \in GF(5)\}$ *where* $xs_\alpha := x\alpha$.

Let $x, y \in V_1$. *Then*

$$\begin{aligned} (x+y)s_\alpha &= (x+y)\alpha \\ &= x\alpha + y\alpha \\ &= xs_\alpha + ys_\alpha. \end{aligned}$$

Thus s_α *is an endomorphism of* V_1. *Hence* A_1 *is the set of all endomorphisms of* V_1.

2) Let $x \in V_1$. *Then*

$$xs_0 = x(0) = 0$$

$$xs_1 = x(1) = x$$

$$xs_{-1} = x(-1) = -x.$$

3) We shall now show that $A_1^* \subseteq Aut(V_1)$. *Let* $s_\alpha \in A_1^*$. *Then* s_α *is an endomorphism. It suffices to show that* s_α *is a bijection.*

(i) Let $x, y \in V_1$ *and* $\alpha \in GF(5)\backslash\{0\}$. *Suppose that* $xs_\alpha = ys_\alpha$. *Then* $x\alpha = y\alpha$. *We have* $x\alpha - y\alpha = 0$. *Since* $\alpha \neq 0$, *so* $x - y = 0$. *Then* $x = y$. *Hence* s_α *is injective.*

(ii) Let $x \in V_1$ *and let* $s_\alpha \in A_1^*$. *So* α^{-1} *exists. Then* $x\alpha^{-1} \in V_1$. *We have* $(x\alpha^{-1})s_\alpha = (x\alpha^{-1})\alpha = x$. *Hence* s_α *is surjective. Next, we show that* A_1^* *is a subgroup of* $Aut(V_1)$. *Let* $A_1 = \{s_\alpha : \alpha \in GF(5)\}$. *Then* $A_1 = \{s_0, s_1, s_2, s_3, s_4\}$. *Thus* $A_1^* = A\backslash\{0\} = \{s_1, s_2, s_3, s_4\} \neq \emptyset$. *Let* $s_\alpha, s_\beta \in A_1^*$. *Then*

$$\begin{aligned} x(s_\alpha \circ s_\beta) &= x\alpha\beta \\ &= xs_{\alpha\beta}, \forall x \in GF(5). \end{aligned}$$

Thus $s_\alpha \circ s_\beta = s_{\alpha\beta}$. *Since* $\alpha\beta \in GF(5)\backslash\{0\}$, *so* $s_{\alpha\beta} \in A_1^*$ *and hence* $s_\alpha \circ s_\beta \in A_1^*$. *Let* $s_\alpha \in A_1^*$. *Then* $\alpha \neq 0$. *So* α^{-1} *exists and* $\alpha^{-1} \in GF(5)\backslash\{0\}$. *Thus* $s_{\alpha^{-1}} \in A_1^*$, *we have*

$$\begin{aligned} x(s_\alpha \circ s_{\alpha^{-1}}) &= x\alpha\alpha^{-1} \\ &= x(1) \\ &= x(id). \end{aligned}$$

We have $s_\alpha \circ s_{\alpha^{-1}} = id$. *Thus* $s_{\alpha^{-1}}$ *is the inverse of* s_α. *Hence* A_1^* *is a subgroup of* $Aut(V_1)$.

4) Let $x \in V_1$ *and* $s_\alpha, s_\beta \in A_1$. *Suppose that* $xs_\alpha = xs_\beta$ *and* $s_\alpha \neq s_\beta$. *Then* $x\alpha = x\beta$. *Since* $s_\alpha \neq s_\beta$, *we have* $\alpha \neq \beta$. *So* $\alpha - \beta \neq 0$. *Since* $x\alpha = x\beta$, *we have*

$$x\alpha - x\beta = 0$$

$$x(\alpha - \beta) = 0(\alpha - \beta)$$

$$xs_{(\alpha-\beta)} = 0s_{(\alpha-\beta)}.$$

Thus $s_{(\alpha-\beta)} \in A_1^* \subseteq Aut(V_1)$ *and* $s_{(\alpha-\beta)}$ *is injective. We conclude that* $x = 0$.

5) The quasi-kernel $Q(V_1)$ *of* V_1 *consists of all those elements* x *of* V_1 *such that for every* $s_\alpha, s_\beta \in A_1$ *there exists a* $s_\gamma \in A_1$ *for which* $xs_\alpha + xs_\beta = xs_\gamma$. *Consider* $x \in V_1$ *and* $s_\alpha, s_\beta \in A_1$,

$$\begin{aligned} xs_\alpha + xs_\beta &= x\alpha + x\beta \\ &= x(\alpha + \beta) \end{aligned}$$

$$= xs_{\alpha+\beta}.$$

Hence $x \in Q(V_1)$, *so* $Q(V_1) = V_1$. *We have* $\langle Q(V_1)\rangle = \langle V_1\rangle = V_1$. *Since* $\alpha, \beta \in GF(5)$, *thus* $S_{\alpha+\beta} \in A_1$. *By (1)-(5), we have* (V_1, A_1) *is a near-vector space. Similarly* (V_2, A_2) *is a near vector-space. Moreover, we will show that* $(V_1, A_1) \cong (V_2, A_2)$. *Consider the group isomorphisms* $\theta : (V_1, +) \to (V_2, +)$ *defined by* $x \mapsto x$ *and* $\eta : (A_1^*, \cdot) \to (A_2^*, \cdot)$ *defined by* $s_\alpha \mapsto t_{\alpha^{1/3}}$, *where* $1/3$ *is the inverse of* 3 *in* $U(4)$ *which is* 2. *Let* $x \in V_1$ *and* $s_\alpha \in A_1^*$. *Then, we show that* $\theta(xs_\alpha) = \theta(x)\eta(s_\alpha)$ *which can be seen that*

$$\begin{aligned}
\theta(xs_\alpha) &= \theta(x\alpha) \\
&= x\alpha \\
&= x(\alpha^{1/3})^3 \\
&= xt_{\alpha^{1/3}}; \alpha^{1/3} \in GF(5), \forall \alpha \in GF(5) \\
&= \theta(x)\eta(s_\alpha).
\end{aligned}$$

Hence $(V_1, A_1) \cong (V_2, A_2)$.

Example 2.2.4. *Put* $V := \mathbb{F}^{\oplus 4}$ *where* $\mathbb{F} := GF(7^2)$ *and let each* $\alpha \in \mathbb{F}$ *act as an endomorphism on* V *by defining*

$$(x_1, x_2, x_3, x_4)\alpha = (x_1\alpha, x_2\alpha^5, x_3\alpha^5, x_4\alpha^5).$$

As in the previous example, it can be easy to show that $(V, \mathbb{F})$ *is a near-vector space but not a vector space which can be seen that for* $\alpha = 4$ *and* $(0,1,0,0) \in V$, *then*

$$\begin{aligned}
(0,1,0,0)4 + (0,1,0,0)4 &= (0,4^5,0,0) + (0,4^5,0,0) \\
&= (0,2,0,0) + (0,2,0,0) \\
&= (0,4,0,0) \\
&\neq (0,1,0,0) \\
&= (0,1,0,0)(4+4).
\end{aligned}$$

Hence it has no left distributive law and $(V, \mathbb{F})$ *is not a vector space.*

Definition 2.2.5. [1] A finite sequence of m integers $q_1, q_2, \ldots, q_m$ is called *suitable* with respect to $\mathbb{F} = GF(p^n)$ if

$(a) 1 \leqslant q_i \leqslant p^n - 1$ and $\gcd(q_i, p^n - 1) = 1$ for all $i = 1, \ldots, m$;

(b) no q_i can be replaced by a smaller q_i' that also satisfies (a) and such that $q_i \equiv q_i' p^l \bmod(p^n - 1)$ for some $l \in \{0, 1, \ldots, n-1\}$.

Suitable sequences are always written in non-decreasing order:

$$q_1 \leqslant q_2 \leqslant \cdots \leqslant q_m.$$

In order to construct a suitable sequence with respect to $\mathbb{F}$, we consider subgroup $\langle p \rangle$ of the multiplicative group $U(p^n - 1) = \{k \in \mathbb{Z} : 1 \leq k \leq p^n - 1$ and $\gcd(k, p^n - 1) = 1\}$, i.e.,

$$U(p^n - 1)/\langle p \rangle = \{k \langle p \rangle \,|\, k \in U(p^n - 1)\}.$$

Then select a list of the smallest members of all the cosets and write them down in non-decreasing order. Note that the number of elements in the list we can choose is $\phi(p^n - 1)/n$.

Example 2.2.6. *Let* $\mathbb{F} = GF(3^3)$, *then* $U(p^n - 1) = U(3^3 - 1) = U(26) = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$. *Furthermore, The set of cosets determined by* $\langle 3 \rangle$ *in the group* $U(3^3 - 1)$ *is given by* $\{\{1, 3, 9\}, \{5, 15, 19\}, \{7, 21, 11\}, \{17, 25, 23\}\}$. *The set of smallest elements* $\{1, 5, 7, 17\}$ *in these cosets determines all possible suitable sequences with respect to* $\mathbb{F}$ *of length four are*

$$(1,1,1,1), (1,1,1,5), (1,1,1,7), (1,1,1,17), (1,1,5,5), (1,1,7,7), (1,1,5,17),$$
$$(1,1,5,7), (1,1,7,17), (1,1,17,17), (1,5,5,7), (1,5,5,17), (1,5,7,7), (1,5,17,17),$$
$$(1,5,7,17), (1,5,5,5), (1,7,7,7), (1,17,17,17), (1,7,17,17), (1,7,7,17).$$

Recall that a (right) *near-field* is a triple $(\mathbb{F}, +, \cdot)$ that satisfies all the axiom of a skew-field, except perhaps the left distributive law $a \cdot (b + c) = a \cdot b + a \cdot c$.

Example 2.2.7. *Let* $\mathbb{F} = GF(3^2)$. *Denote the usual multiplication in* $\mathbb{F}$ *by* $\cdot$. *Define a new binary operation* $*$ *on* $\mathbb{F}$ *by:*

if b *is any element of* $\mathbb{F}$ *which is a square and* a *is any element of* $\mathbb{F}$, *then*

$$a * b = a \cdot b,$$

if b *is any element of* $\mathbb{F}$ *which is not a square and* a *is any element of* $\mathbb{F}$, *then*

$$a * b = a^3 \cdot b.$$

Thus the binary operation $*$ *is illustrated as in the table below:*

Table 2 The multiplication table of $\mathbb{F}$

$*$	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
2	0	2	1	$2x$	$2+2x$	$1+2x$	x	$2+x$	$1+x$
x	0	x	$2x$	2	$1+2x$	$x+1$	1	$2+2x$	$2+x$
$1+x$	0	$1+x$	$2+2x$	$2+x$	2	$2x$	$1+2x$	x	1
$2+x$	0	$2+x$	$1+2x$	$2+2x$	x	2	$1+x$	1	$2x$
$2x$	0	2	x	1	$2+x$	$2+2x$	2	$1+x$	$1+2x$
$1+2x$	0	$1+2x$	$2+x$	$1+x$	$2x$	1	$2+2x$	2	x
$2+2x$	0	$2+2x$	$1+x$	$1+2x$	1	x	$1+x$	$2x$	2

Therefore $\mathbb{F}$ *with the binary operation* $*$ *above is a (right)* near-field *of order 9, but* $(\mathbb{F}, +, \cdot)$ *is not a field.*

Theorem 2.2.8. [4] *Let* $(V, +)$ *be a group and let* $A = D \cup \{0\}$, *where* D *acts fixed point freely on group of automorphisms of* V. *Then* (V, A) *is a finite-dimensional near-vector space if and only if there exist a finite number of near-fields* $\mathbb{F}_1, \ldots, \mathbb{F}_m$, *semigroup isomorphisms* $\psi_i : (A, \circ) \to (\mathbb{F}_i, \cdot)$, *and an additive group isomorphism* $\phi : V \to \mathbb{F}_1 \oplus \cdots \oplus \mathbb{F}_m$ *such that if* $\phi(v) = (x_1, \ldots, x_m)$, *then* $\phi(v\alpha) = (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha))$ *for all* $v \in V, \alpha \in A$.

In the case of $\mathbb{F}_i = \mathbb{F}$ for all $i = 1, \dots m$, by the above theorem, all such near-vector spaces, which we now call *near-vector spaces over a finite field*, are determined by semigroup automorphisms $\psi_i : (\mathbb{F}, \cdot) \longrightarrow (\mathbb{F}, \cdot)$. Precisely, for a near-vector space (V, A) with $V = \mathbb{F}^{\oplus m} := \mathbb{F} \oplus \cdots \oplus \mathbb{F}$ and $A = \{s_\alpha \mid \alpha \in \mathbb{F}\}$, the scalar multiplication on V is given by

$$(x_1, \dots, x_m)s_\alpha = (x_1\psi_1(\alpha), \dots, x_m\psi_m(\alpha)),$$

for every $\alpha \in \mathbb{F}$.

Howell and Mayer stated that, two near vector spaces are isomorphic if they are determined by the same suitable sequences. Therefore, the number of near-vector spaces up to isomorphism as below:

Theorem 2.2.9. [1] *There are exactly* $\begin{pmatrix} m + \frac{\phi(p^n-1)}{n} - 2 \\ m - 1 \end{pmatrix}$ *m-dimensional near-vector spaces* $V = \mathbb{F}^{\oplus m}$ *(where* $\mathbb{F} = GF(p^n)$*), up to isomorphism. Each of these is completely determined by a suitable sequence* $1 = q_1 \leqslant q_2 \leqslant \cdots \leqslant q_m$ *with respect to* $GF(p^n)$*. Each such sequence* $1 = q_1 \leqslant q_2 \leqslant \cdots \leqslant q_m$ *defines the scalar multiplication*

$$(x_1, \dots, x_m)s_\alpha = (x_1\alpha^{q_1}, \dots, x_m\alpha^{q_m}),$$

where $\alpha \in \mathbb{F}$.

However, we found a slip in the proof of this Theorem in line 17^{th} in the proof. Therefore, we intend to fix the slip and provide a criteria for the classification of near-vector spaces $\mathbb{F}^{\oplus m}$ over a finite field $\mathbb{F} = GF(p^n)$.

CHAPTER III

MAIN RESULTS

This chapter is divided into two sections. In the first section, we present a necessary and sufficient condition for isomorphism of two near-vector spaces over a finite filed. The number of near-vector spaces over a finite field (up to isomorphism) is counted in the second section.

3.1 Classification of Near vector spaces

In this section, we denote (V, A) a near-vector spaces over a finite field where $V = \mathbb{F}^{\oplus m}$ which $(V, +)$ is an abelian group and A is a set of endomorphisms of V. By Proposition 2.1.40, semigroup automorphisms $\psi_i : (\mathbb{F}, \cdot) \longrightarrow (\mathbb{F}, \cdot)$ is given by $\psi_i(x) = x^{q_i}, \forall x \in \mathbb{F}^*$, for some $q_i \in U(p^n-1) := \{1 \leq q \leq p^n-1 \mid \gcd(q, p^n-1) = 1\}$. Let $A = \{s_\alpha \mid \alpha \in \mathbb{F}\}$, with the scalar multiplication on V given by

$$\begin{aligned}(x_1, \ldots, x_m)s_\alpha &= (x_1\psi_1(\alpha), \ldots, x_m\psi_m(\alpha)) \\ &= (x_1\alpha^{q_1}, \ldots, x_m\alpha^{q_m}).\end{aligned}$$

for every $\alpha \in \mathbb{F}$.

We will need the following two lemmas in connection with this construction:

Lemma 3.1.1 (confront Lemma 3.6 in [1]). *Let σ be any permutation of the indices $\{1, 2, ..., m\}$ and $\widetilde{A}_\sigma = \{\sigma_\alpha \mid \alpha \in \mathbb{F}\}$, with the scalar multiplication on V given by*

$$(x_1, \ldots, x_m)\sigma_\alpha = (x_1\alpha^{q_{\sigma(1)}}, \ldots, x_m\alpha^{q_{\sigma(m)}}),$$

for all $\alpha \in \mathbb{F}$. Then $\widetilde{A}^*$ is a subgroup of $Aut(V)$ and $(\mathbb{F}^{\oplus m}, A) \cong (\mathbb{F}^{\oplus m}, \widetilde{A}_\sigma)$.

Proof. We want to show that $\widetilde{A}^*$ is a subgroup of $Aut(V)$. First, we show that $\widetilde{A}^* \subseteq Aut(V)$. Let $\widetilde{A}_\sigma = \{\sigma_\alpha \mid \alpha \in \mathbb{F}\}$, where $(x_1, \ldots, x_m)\sigma_\alpha = (x_1\alpha^{q_{\sigma(1)}}, \ldots, x_m\alpha^{q_{\sigma(m)}})$

and $(x_1,\ldots,x_m),(y_1,\ldots,y_m)\in\mathbb{F}^{\oplus m}$. Then

$$\begin{aligned}(x_1+y_1,\ldots,x_m+y_m)\sigma_\alpha &= ((x_1+y_1)\alpha^{q_\sigma(1)},\ldots,(x_m+y_m)\alpha^{q_\sigma(m)})\\ &= ((x_1\alpha^{q_\sigma(1)}+y_1\alpha^{q_\sigma(1)}),\ldots,(x_m\alpha^{q_\sigma(m)}+y_m\alpha^{q_\sigma(m)}))\\ &= (x_1\alpha^{q_\sigma(1)},\ldots,x_m\alpha^{q_\sigma(m)})+(y_1\alpha^{q_\sigma(1)},\ldots,y_m\alpha^{q_\sigma(m)})\\ &= (x_1,\ldots,x_m)\sigma_\alpha+(y_1,\ldots,y_m)\sigma_\alpha.\end{aligned}$$

Thus σ_α is an endomorphism of $\mathbb{F}^{\oplus m}$. Next we show that σ_α is a bijection. Let $(x_1,\ldots,x_m),(y_1,\ldots,y_m)\in\mathbb{F}^{\oplus m}$, $\sigma_\alpha\in\widetilde{A}_\sigma$ and suppose that

$$(x_1,\ldots,x_m)\sigma_\alpha=(y_1,\ldots,y_m)\sigma_\alpha.$$

Then $(x_1\alpha^{q_\sigma(1)},\ldots,x_m\alpha^{q_\sigma(m)})=(y_1\alpha^{q_\sigma(1)},\ldots,y_m\alpha^{q_\sigma(m)})$. We have

$$((x_1\alpha^{q_\sigma(1)}-y_1\alpha^{q_\sigma(1)}),\ldots,(x_m\alpha^{q_\sigma(m)}-y_m\alpha^{q_\sigma(m)}))=(0,\ldots,0).$$

Thus $((x_1-y_1)\alpha^{q_\sigma(1)},\ldots,(x_m-y_m)\alpha^{q_\sigma(m)})=(0,\ldots,0)$. Since $\alpha\neq 0$, we have $\alpha^{q_\sigma(i)}\neq 0$. So $(x_i-y_i)=0$. We conclude that $x_i=y_i$, for all $i=1,2,\ldots,m$ and $(x_1,\ldots,x_m)=(y_1,\ldots,y_m)$. Therefore σ_α is injective. Furthermore, let $(x_1,\ldots,x_m)\in\mathbb{F}^{\oplus m}$ and $\sigma_\alpha\in\widetilde{A}^*$. Then $\alpha\neq 0$. Thus α^{-1} exists and

$$\begin{aligned}(x_1\alpha^{-q_\sigma(1)},\ldots,x_m\alpha^{-q_\sigma(m)})\sigma_\alpha &= (x_1\alpha^{-q_\sigma(1)}\alpha^{q_\sigma(1)},\ldots,x_m\alpha^{-q_\sigma(m)}\alpha^{q_\sigma(m)})\\ &= (x_1,\ldots,x_m).\end{aligned}$$

Hence σ_α is surjective. Finally, we show that $\widetilde{A}^*$ is a subgroup of $Aut(V)$. Let $\sigma_\alpha,\sigma_\beta\in\widetilde{A}^*$. Then

$$\begin{aligned}(x_1,\ldots,x_m)(\sigma_\alpha\circ\sigma_\beta) &= ((x_1,\ldots,x_m)\sigma_\alpha)\sigma_\beta\\ &= (x_1\alpha^{q_\sigma(1)},\ldots,x_m\alpha^{q_\sigma(m)})\sigma_\beta\\ &= (x_1\alpha^{q_\sigma(1)}\beta^{q_\sigma(1)},\ldots,x_m\alpha^{q_\sigma(m)}\beta^{q_\sigma(m)})\\ &= (x_1(\alpha\beta)^{q_\sigma(1)},\ldots,x_m(\alpha\beta)^{q_\sigma(m)})\\ &= (x_1,\ldots,x_m)\sigma_{\alpha\beta},\end{aligned}$$

for all $(x_1, \ldots, x_m) \in \mathbb{F}^{\oplus m}$. Thus $\sigma_\alpha \circ \sigma_\beta = \sigma_{\alpha\beta}$ but $\alpha\beta \in \mathbb{F}\backslash\{0\}$. So $\sigma_{\alpha\beta} \in \widetilde{A}^*$. Let $\sigma_\alpha \in \widetilde{A}^*$. Then $\alpha \neq 0$. So α^{-1} exists and $\alpha^{-1} \in \mathbb{F}\backslash\{0\}$. We have $\sigma_{\alpha^{-1}} \in \widetilde{A}^*$. Thus $\sigma_\alpha \circ \sigma_{\alpha^{-1}} = \sigma_{\alpha\circ\alpha^{-1}} = \sigma_1 = id$. Hence $\sigma_{\alpha^{-1}}$ is the inverse of σ_α. Therefore $\widetilde{A}^*$ is a subgroup of $\mathrm{Aut}(V)$. By considering the group isomorphisms $\theta : \mathbb{F}^{\oplus m} \to \mathbb{F}^{\oplus m}$ defined by $(x_1, \ldots, x_m) \mapsto (x_{\sigma(1)}, \ldots, x_{\sigma(m)})$ and $\eta : A^* \to \widetilde{A}^*$ defined by $s_\alpha \mapsto \sigma_\alpha$. Then

$$\begin{aligned}
\theta(vs_\alpha) &= \theta((x_1, \ldots, x_m)s_\alpha) \\
&= \theta(x_1\alpha^{q_1}, \ldots, x_m\alpha^{q_m}) \\
&= (x_{\sigma(1)}\alpha^{q_{\sigma(1)}}, \ldots, x_{\sigma(m)}\alpha^{q_{\sigma(m)}}) \\
&= (x_{\sigma(1)}, \ldots, x_{\sigma(m)})\sigma_\alpha \\
&= \theta(x_1, \ldots, x_m)\sigma_\alpha \\
&= \theta(v)\eta(s_\alpha).
\end{aligned}$$

Hence $(\mathbb{F}^{\oplus m}, A) \cong (\mathbb{F}^{\oplus m}, \widetilde{A}_\sigma)$. □

Example 3.1.2. *For* $\mathbb{F} = GF(3^3)$, *denote* $A_1 = \{s_\alpha : \alpha \in \mathbb{F}\}$ *and* $A_2 = \{t_\alpha : \alpha \in \mathbb{F}\}$, *where*

$$(x_1, x_2, x_3, x_4)s_\alpha = (x_1\alpha^5, x_2\alpha^7, x_3\alpha^7, x_4\alpha^{17})$$

$$(x_1, x_2, x_3, x_4)t_\alpha = (x_1\alpha^7, x_2\alpha^5, x_3\alpha^{17}, x_4\alpha^7).$$

Then $(\mathbb{F}^{\oplus 4}, A_1) \cong (\mathbb{F}^{\oplus 4}, A_2)$.

For each $q_i \in U(p^n - 1)$ with $i = 1, \ldots, m$, there is a permutation σ such that $\sigma(q_1) \leq \cdots \leq \sigma(q_m)$. Thus, it is enough to consider the action of A in terms of the non-decreasing sequences.

Lemma 3.1.3. *Let* $A = \{s_\alpha : \alpha \in \mathbb{F}\}$ *act on* V *by*

$$(x_1, \ldots, x_m)s_\alpha = (x_1\alpha^{q_1}, \ldots, x_m\alpha^{q_m}),$$

for all $\alpha \in \mathbb{F}$ *and* $\widetilde{A} = \{t_\alpha : \alpha \in \mathbb{F}\}$ *acts on* V *by*

$$(x_1, \ldots, x_m)t_\alpha = (x_1\alpha^{q_1p^{l_1}}, \ldots, x_m\alpha^{q_mp^{l_m}}),$$

where $l_1, \ldots, l_m \in \{0, 1, \ldots, n-1\}$. *Then* $\overline{A}^*$ *is a subgroup of* $Aut(V)$ *and* $(\mathbb{F}^{\oplus m}, A) \cong (\mathbb{F}^{\oplus m}, \overline{A})$.

Proof. We want to show that $\overline{A}^*$ is a subgroup of $Aut(V)$. First, we show that $\overline{A}^* \subseteq Aut(V)$. Let $\overline{A} = \{t_\alpha : \alpha \in \mathbb{F}\}$, where $(x_1, \ldots, x_m)t_\alpha = (x_1\alpha^{q_1 p^{l_1}}, \ldots, x_m\alpha^{q_m p^{l_m}})$ and $(x_1, \ldots, x_m), (y_1, \ldots, y_m) \in \mathbb{F}^{\oplus m}$. Then

$$\begin{aligned}(x_1 + y_1, \ldots, x_m + y_m)t_\alpha &= ((x_1 + y_1)\alpha^{q_1 p^{l_1}}, \ldots, (x_m + y_m)\alpha^{q_m p^{l_m}}) \\ &= ((x_1\alpha^{q_1 p^{l_1}} + y_1\alpha^{q_1 p^{l_1}}), \ldots, (x_m\alpha^{q_m p^{l_m}} + y_m\alpha^{q_m p^{l_m}})) \\ &= (x_1\alpha^{q_1 p^{l_1}}, \ldots, x_m\alpha^{q_m p^{l_m}}) + (y_1\alpha^{q_1 p^{l_1}}, \ldots, y_m\alpha^{q_m p^{l_m}}) \\ &= (x_1, \ldots, x_m)t_\alpha + (y_1, \ldots, y_m)t_\alpha.\end{aligned}$$

Thus t_α is an endomorphism of $\mathbb{F}^{\oplus m}$. Next we show that t_α is a bijection. Let $(x_1, \ldots, x_m), (y_1, \ldots, y_m) \in \mathbb{F}^{\oplus m}$, $t_\alpha \in \overline{A}^*$ and suppose that

$$(x_1, \ldots, x_m)t_\alpha = (y_1, \ldots, y_m)t_\alpha.$$

Then $(x_1\alpha^{q_1 p^{l_1}}, \ldots, x_m\alpha^{q_m p^{l_m}}) = (y_1\alpha^{q_1 p^{l_1}}, \ldots, y_m\alpha^{q_m p^{l_m}})$. We have

$$(x_1\alpha^{q_1 p^{l_1}} - y_1\alpha^{q_1 p^{l_1}}, \ldots, x_m\alpha^{q_m p^{l_m}} - y_m\alpha^{q_m p^{l_m}}) = (0, \ldots, 0).$$

Thus $((x_1 - y_1)\alpha^{q_1 p^{l_1}}, \ldots, (x_m - y_m)\alpha^{q_m p^{l_m}}) = (0, \ldots, 0)$. Since $\alpha \neq 0$, we have $\alpha^{q_i p^{l_i}} \neq 0$. So $(x_i - y_i) = 0$. We conclude that $x_i = y_i$, for all $i = 1, 2, \ldots, m$. and $(x_1, \ldots, x_m) = (y_1, \ldots, y_m)$. Therefore t_α is injective. Furthermore, let $(x_1, \ldots, x_m) \in \mathbb{F}^{\oplus}$ and $t_\alpha \in \overline{A}^*$. Then $\alpha \neq 0$. Thus α^{-1} exists and

$$\begin{aligned}(x_1\alpha^{-(q_1 p^{l_1})}, \ldots, x_m\alpha^{-(q_m p^{l_m})})t_\alpha &= (x_1\alpha^{-(q_1 p^{l_1})}\alpha^{q_1 p^{l_1}}, \ldots, x_m\alpha^{-(q_m p^{l_m})}\alpha^{q_m p^{l_m}}) \\ &= (x_1(\alpha^{-1}\alpha)^{q_1 p^{l_1}}, \ldots, x_m(\alpha^{-1}\alpha)^{q_m p^{l_m}}) \\ &= (x_1, \ldots, x_m).\end{aligned}$$

Hence t_α is surjective. Finally, we show that $\overline{A}^*$ is a subgroup of $Aut(V)$. Let $t_\alpha, t_\beta \in \overline{A}^*$. Then

$$(x_1, \ldots, x_m)(t_\alpha \circ t_\beta) = ((x_1, \ldots, x_m)t_\alpha)t_\beta$$

$$\begin{aligned} &= (x_1\alpha^{q_1p^{l_1}}, \ldots, x_m\alpha^{q_mp^{l_m}})t_\beta \\ &= (x_1\alpha^{q_1p^{l_1}}\beta^{q_1p^{l_1}}, \ldots, x_m\alpha^{q_mp^{l_m}}\beta^{q_mp^{l_m}}) \\ &= (x_1(\alpha\beta)^{q_1p^{l_1}}, \ldots, x_m(\alpha\beta)^{q_mp^{l_m}}) \\ &= (x_1, \ldots, x_m)t_{\alpha\beta}. \end{aligned}$$

for all $(x_1, \ldots, x_m) \in \mathbb{F}^{\oplus m}$. Thus $t_\alpha \circ t_\beta = t_{\alpha\beta}$ but $\alpha\beta \in \mathbb{F}\backslash\{0\}$. So $t_{\alpha\beta} \in \overline{A}^*$. Let $t_\alpha \in \overline{A}^*$. Then $\alpha \neq 0$. So α^{-1} exists and $\alpha^{-1} \in \mathbb{F}\backslash\{0\}$. We have $t_{\alpha^{-1}} \in \overline{A}^*$. Thus $t_\alpha \circ t_{\alpha^{-1}} = t_{\alpha\circ\alpha^{-1}} = t_1 = id$. Hence $t_{\alpha^{-1}}$ is the inverse of t_α. Therefore $\overline{A}^*$ is a subgroup of $\mathrm{Aut}(V)$. By considering the group isomorphisms $\theta : \mathbb{F}^{\oplus m} \to \mathbb{F}^{\oplus m}$ defined by $(x_1, \ldots, x_m) \mapsto (x_1^{p^{l_1}}, \ldots, x_m^{p^{l_m}})$ and $\eta : A^* \to \overline{A}^*$ defined by $s_\alpha \mapsto t_\alpha$. Let $v = (x_1, \ldots, x_m) \in \mathbb{F}^{\oplus m}$ and $s_\alpha \in A^*$. Then

$$\begin{aligned} \theta(vs_\alpha) &= \theta((x_1, \ldots, x_m)s_\alpha) \\ &= \theta(x_1\alpha^{q_1}, \ldots, x_m\alpha^{q_m}) \\ &= ((x_1\alpha^{q_1})^{p^{l_1}}, \ldots, (x_m\alpha^{q_m})^{p^{l_m}}) \\ &= (x_1^{p^{l_1}}\alpha^{q_1p^{l_1}}, \ldots, x_m^{p^{l_m}}\alpha^{q_mp^{l_m}}) \\ &= (x_1^{p^{l_1}}, \ldots, x_m^{p^{l_m}})t_\alpha \\ &= \theta(x_1, \ldots, x_m)t_\alpha \\ &= \theta(v)\eta(s_\alpha). \end{aligned}$$

Hence $(\mathbb{F}^{\oplus m}, A) \cong (\mathbb{F}^{\oplus m}, \overline{A})$. □

Example 3.1.4. *For* $\mathbb{F} = GF(3^3)$, *denote* $A_1 = \{s_\alpha : \alpha \in \mathbb{F}\}$ *and* $A_2 = \{t_\alpha : \alpha \in \mathbb{F}\}$, *where*

$$(x_1, x_2, x_3, x_4)s_\alpha = (x_1\alpha^7, x_2\alpha^5, x_3\alpha^{17}, x_4\alpha^7)$$

$$(x_1, x_2, x_3, x_4)t_\alpha = (x_1\alpha^{21}, x_2\alpha^5, x_3\alpha^{23}, x_4\alpha^{11}).$$

Then $(\mathbb{F}^{\oplus 4}, A_1) \cong (\mathbb{F}^{\oplus 4}, A_2)$.

So, we can now only concentrate on the smallest element in the class $\overline{q}_i \in G$, for each $i = 1, \ldots, m$; namely, the action of A is in the form of a suitable sequence.

Thus, the classification of near-vector spaces over finite fields depends on semigroup automorphisms ψ_i's and their actions. Moreover, by Lemma 3.1.1 and 3.1.3, we have $A = \{s_\alpha \mid \alpha \in \mathbb{F}\}$, $\widetilde{A}_\sigma = \{\sigma_\alpha \mid \alpha \in \mathbb{F}\}$ and $\overline{A} = \{t_\alpha \mid \alpha \in \mathbb{F}\}$. Then

$$(\mathbb{F}^{\oplus m}, A) \cong (\mathbb{F}^{\oplus m}, \widetilde{A}_\sigma) \quad \text{and} \quad (\mathbb{F}^{\oplus m}, A) \cong (\mathbb{F}^{\oplus m}, \overline{A}).$$

This motivates us to consider the group $G := U(p^n - 1)/\langle p \rangle$, where the operation is the usual multiplication modulo $p^n - 1$ and $\langle p \rangle = \{1, p, \ldots, p^{n-1}\}$. By the above discussion, we can identify the action of A on $\mathbb{F}^{\oplus m}$ by a non-decreasing sequence of length m on G. Precisely, if $A = \{s_\alpha \mid \alpha \in \mathbb{F}\}$ acts on $\mathbb{F}^{\oplus m}$ by

$$(x_1, \ldots, x_m)s_\alpha = (x_1\alpha^{q_1}, \ldots, x_m\alpha^{q_m}),$$

then we identify this action by the sequence

$$(S) := (q_1, \ldots, q_m).$$

A non-decreasing sequence $(S) = (q_1, \ldots, q_m)$ in which q_i is the smallest element in the class $\overline{q}_i \in G$ for each $i = 1, \ldots, m$, is a suitable sequence of length m.

Furthermore, if $q \in G$ and $(S) = (q_1, \ldots, q_m)$ is a suitable sequence of length m on G and $A = \{s_\alpha \mid \alpha \in \mathbb{F}\}$ is identified by (S), then $(\mathbb{F}^{\oplus m}, A) \cong (\mathbb{F}^{\oplus m}, A')$, where $A' = \{s'_\alpha \mid \alpha \in \mathbb{F}\}$ is identified by $(S') := q(S) := (qq_1, \ldots, qq_m)$. Here, the isomorphism is derived by

$$\theta' : \mathbb{F}^{\oplus m} \longrightarrow \mathbb{F}^{\oplus m}; (x_1, \ldots, x_m) \mapsto (x_1, \ldots, x_m) \text{ and } \eta' : A^* \longrightarrow A'^*; s_\alpha \mapsto s'_{\alpha^{1/q}}.$$

Example 3.1.5. *For* $\mathbb{F} = GF(3^3)$, *denote* $A_1 = \{s_\alpha : \alpha \in \mathbb{F}\}$ *and* $A_2 = \{t_\alpha : \alpha \in \mathbb{F}\}$, *where*

$$(x_1, x_2, x_3, x_4)s_\alpha = (x_1\alpha^7, x_2\alpha^5, x_3\alpha^{17}, x_4\alpha^7)$$

$$(x_1, x_2, x_3, x_4)t_\alpha = (x_1\alpha^1, x_2\alpha^5, x_3\alpha^{17}, x_4\alpha^{17}).$$

Then $(\mathbb{F}^{\oplus 4}, A_1) \cong (\mathbb{F}^{\oplus 4}, A_2)$.

Therefore, to classify and count (up to isomorphism) all near-vector spaces $\mathbb{F}^{\oplus m}$ over a finite filed $\mathbb{F}$, it is enough to deal with the set of all suitable sequences on G of length m with 1 in the first position, and we denote this set by $St(1, m, G)$. We also define an equivalent relation $\sim$ on the set $St(1, m, G)$ by, for suitable sequences (S_1) and (S_2) in $St(1, m, G)$,

$$(S_1) \sim (S_2) \iff (\mathbb{F}^{\oplus m}, A_1) \cong (\mathbb{F}^{\oplus m}, A_2), \tag{3.1.1}$$

where A_1 and A_2 are determined by (S_1) and (S_2) respectively.

Since $G = U(p^n - 1)/\langle p \rangle$, where $\langle p \rangle = \{1, p, \ldots, p^{n-1}\}$, we can represent the group G explicitly as $G = \{1, q_2, \ldots, q_{\frac{\phi(p^n-1)}{n}}\} \subseteq U(p^n - 1)$, where q_i is the smallest element in the coset of $\langle p \rangle$ containing q_i. Thus the product of q_i and q_j in G will be $q_k \in G$ whose its coset $\overline{q_k} := q_k \langle p \rangle$ contains the remainder of $q_i q_j$ divided by $p^n - 1$. The theorem below is a main tool that is used in the proof of the main result.

Theorem 3.1.6 (confront Theorem 2.2 in [1]). *Let $\mathbb{F} = \mathrm{GF}(p^n)$ and $q_i, q_j \in G$. Then, $(\alpha^{q_i} + \beta^{q_i})^{q_j} = (\alpha^{q_j} + \beta^{q_j})^{q_i}$ for all $\alpha, \beta \in \mathbb{F}$ if and only if $q_i = q_j$.*

Proof. ($\Leftarrow$) Suppose that $q_i = q_j$. Then $\alpha^{q_i} = \alpha^{q_j}$ for all $\alpha, \beta \in \mathbb{F}$. Thus

$$(\alpha^{q_i} + \beta^{q_i})^{q_j} = (\alpha^{q_j} + \beta^{q_j})^{q_i}$$

for all $\alpha, \beta \in \mathbb{F}$.

($\Rightarrow$) Let $q_i, q_j \in G$. For each $\alpha, \beta \in \mathbb{F}$, we have $(\alpha^{q_i} + \beta^{q_i})^{q_j} = (\alpha^{q_j} + \beta^{q_j})^{q_i}$. By Theorem 2.1.39, we have $q_i \equiv q_j p^l (\mathrm{mod}\, p^n - 1)$ for some $l \in \{0, 1, \ldots, n-1\}$. Since $q_i, q_j \in G$, $q_i = q_j$. □

For a given suitable sequence $(S) = (1, q_2, \ldots, q_m)$, we denote $S := \{1, \ldots, q_N\}$ the order set (strictly increasing) of all distinct elements in (S).

Theorem 3.1.7. *Let $(\mathbb{F}^{\oplus m}, A_1)$ and $(\mathbb{F}^{\oplus m}, A_2)$ be near-vector spaces, where A_1 and A_2 are determined by suitable sequence (S_1) and (S_2), respectively. Then*

$(\mathbb{F}^{\oplus m}, A_1) \cong (\mathbb{F}^{\oplus m}, A_2)$ *if and only if there is* $q \in S_1$ *such that* $S_1 = qS_2$ *and the occurrences of* $qq'_j \in (S_1)$ *and* $q'_j \in (S_2)$ *are the same for each* $j = 1, \ldots, N$, *where* $N = |S_1| = |S_2|$.

Proof. Suppose that $(\mathbb{F}^{\oplus m}, A_1) \cong (\mathbb{F}^{\oplus m}, A_2)$. So there exist group isomorphisms $\theta : \mathbb{F}^{\oplus m} \longrightarrow \mathbb{F}^{\oplus m}$ and $\eta : A_1^* \longrightarrow A_2^*$ such that

$$\theta((x_1, x_2, ..., x_m)s_\alpha) = \theta(x_1, x_2, ..., x_m)\eta(s_\alpha).$$

Suppose $(S_1) = (1 = q_1, q_2, \ldots, q_m)$ and $(S_2) = (1 = q'_1, q'_2, \ldots, q'_m)$. Then the actions of A_1, A_2 on $\mathbb{F}^{\oplus m}$ are explicitly given by

$$(x_1, x_2, ..., x_m)s_\alpha = (x_1\alpha^{q_1}, x_2\alpha^{q_2}, ..., x_m\alpha^{q_m}),$$

$$(x_1, x_2, ..., x_m)t_\gamma = (x_1\gamma^{q'_1}, x_2\gamma^{q'_2}, ..., x_m\gamma^{q'_m}),$$

for each $\alpha, \gamma \in \mathbb{F}$ and each $(x_1, x_2, \ldots, x_m) \in \mathbb{F}^{\oplus m}$.

Since $\mathbb{F}^*$ is a cyclic group, $\mathbb{F}^* = \langle a \rangle$ for some $a \in \mathbb{F}^*$. Suppose $\eta(s_a) = t_b$, for some $b \in \mathbb{F}^* = \langle a \rangle$. Thus, there exists an integer $1 \leq q_\circ < p^n - 1$ such that $b = a^{q_\circ}$. Since η is an isomorphism, we have $\mathrm{ord}(s_a) = \mathrm{ord}(t_b) := k$. So

$$(1, 1, \ldots, 1) = (1, 1, \ldots, 1)(t_b)^k = (1, 1, \ldots, 1)t_{b^k} = (b^{kq'_1}, b^{kq'_2}, \ldots, b^{kq'_m}),$$

and then $b^k = 1$ (because $\gcd(q'_i, p^n - 1) = 1$). If $\mathrm{ord}(b) = l < k$, then

$$(t_b)^l = t_{b^l} = t_1 = id.$$

This implies that $\mathrm{ord}(t_b) \leq l < k$, which is a contradiction. So, $\mathrm{ord}(b) = k$. Similarly, $\mathrm{ord}(a) = k$ and thus $k = |\mathbb{F}^*| = p^n - 1$. Since $b = a^{q_\circ}$ and a, b have the same orders, $\gcd(q_\circ, p^n - 1) = 1$; namely, $q_\circ \in U(p^n - 1)$. Therefore, for the given isomorphism η, there must exist $q_\circ \in U(p^n - 1)$ such that, for each non zero $\alpha (= a^r)$ in $\mathbb{F}$,

$$\eta(s_\alpha) = \eta(s_{a^r}) = (\eta(s_a))^r = (t_{a^{q_\circ}})^r = t_{(a^{q_\circ})^r} = t_{\alpha^{q_\circ}}.$$

Let $S_1 = \{1, \ldots, q_{N_1}\} \subseteq G = U(p^n - 1)/\langle p \rangle$ be the order set (strictly increasing) of all elements in the sequence (S_1). Suppose that, for each $i = 1, \ldots, N_1$, the occurrence of q_i in (S_1) is l_{1i}. Then $l_{1i} \geq 1$ for each $i = 1, \ldots, N_1$ and

$$l_{11} + \cdots + l_{1N_1} = m. \tag{3.1.2}$$

Now, for each $1 \leq k \leq N_1$, consider the constant subsequence $(q_k, \ldots, q_k)$ (length l_{1k}) of (S_1). Let $e_i = (0, \ldots, 1, \ldots, 0)$, with 1 in position i, and zeros elsewhere, $1 \leqslant i \leqslant m$. Suppose that

$$\theta(e_i) = (\omega_{i,1}, \ldots, \omega_{i,m})$$

for some $\omega_{i,j} \in \mathbb{F}, k \leqslant i \leqslant k + l_{1k}, 1 \leqslant j \leqslant m$. Also, for $\alpha \in \mathbb{F}$, we have

$$\theta(e_i s_\alpha) = \theta(0, \ldots, \alpha^{q_i}, \ldots, 0),$$

$$\theta(e_i)\eta(s_\alpha) = (\omega_{i,1}, \ldots, \omega_{i,m})t_{\alpha^{q_0}} = (\omega_{i,1}\alpha^{q_0 q'_1}, \ldots, \omega_{i,m}\alpha^{q_0 q'_m})$$

and thus

$$\theta(0, \ldots, \alpha^{q_i}, \ldots, 0) = \theta(e_i s_\alpha) = (\omega_{i,1}\alpha^{q_0 q'_1}, \ldots, \omega_{i,m}\alpha^{q_0 q'_m})$$

for $k \leqslant i \leqslant k + l$, and α^{q_i} in the i^{th} position. Hence, with α in the k^{th} position,

$$\theta(0, \ldots, \alpha, \ldots, 0) = \theta(e_k s_{\alpha^{1/q_k}}) = (\omega_{k,1}\alpha^{q_0 q'_1/q_k}, \ldots, \omega_{k,m}\alpha^{q_0 q'_m/q_k}).$$

Consequently, for $\alpha, \beta \in \mathbb{F}$,

$$\theta(0, \ldots, \alpha+\beta, \ldots, 0) = \theta(e_k s_{(\alpha+\beta)^{1/q_k}}) = (\omega_{k,1}(\alpha+\beta)^{q_0 q'_1/q_k}, \ldots, \omega_{k,m}(\alpha+\beta)^{q_0 q'_m/q_k}).$$

We also have

$$\begin{aligned}
\theta(0, \ldots, \alpha+\beta, \ldots, 0) &= \theta(e_k s_{\alpha^{1/q_k}}) + \theta(e_k s_{\beta^{1/q_k}}) \\
&= (\omega_{k,1}\alpha^{q_0 q'_1/q_k}, \ldots, \omega_{k,m}\alpha^{q_0 q'_m/q_k}) + (\omega_{k,1}\beta^{q_0 q'_1/q_k}, \ldots, \omega_{k,m}\beta^{q_0 q'_m/q_k}) \\
&= (\omega_{k,1}(\alpha^{q_0 q'_1/q_k} + \beta^{q_0 q'_1/q_k}), \ldots, \omega_{k,m}(\alpha^{q_0 q'_m/q_k} + \beta^{q_0 q'_m/q_k})).
\end{aligned}$$

Since e_k is non-zero, at least one of $\omega_{k,1}, \ldots, \omega_{k,m}$ is non-zero, say $\omega_{k,r} \neq 0$, where r is minimal with respect to this property. Then, we have

$$\omega_{k,r}(\alpha^{q_0 q'_r/q_k} + \beta^{q_0 q'_r/q_k}) = \omega_{k,r}(\alpha+\beta)^{q_0 q'_r/q_k}.$$

Thus,

$$\alpha^{q_\circ q'_r/q_k} + \beta^{q_\circ q'_r/q_k} = (\alpha+\beta)^{q_\circ q'_r/q_k} \tag{3.1.3}$$

for all $\alpha, \beta \in \mathbb{F}$.

By Theorem 3.1.6 in [1], the equation (3.1.3) happens if and only if $\frac{q_\circ q'_r}{q_k} \in \overline{1} = \langle p \rangle$; equivalently, if and only if $qq'_r = q_k$, where $q \in G$ such that $q_\circ \in q\langle p \rangle$. This also implies that $\omega_{k,j} = 0$ if $qq'_j \neq q_k$, for each $j = 1, \ldots, m$. Assume that $(q'_r, \ldots, q'_{r+l'})$ is the constant subsequence of maximal length of the sequence (S_2) and satisfies $q_k = qq'_r = \cdots = qq'_{r+l'}$. Then

$$\theta(e_i) = (0, \ldots, 0, \omega_{i,r}, \ldots, \omega_{i,r+l'}, 0, \ldots, 0),$$

for each $i = k, \ldots, k + l_{1k}$. If $l' < l_{1k}$, then $\{\theta(e_k), \ldots, \theta(e_{k+l_{1k}})\}$ is a linearly dependent set in the vector space $\mathbb{F}^{\oplus m}$ over $\mathbb{F}$. So, there exists $\alpha_0^{q_\circ}, \ldots, \alpha_{l_{1k}}^{q_\circ} \in \mathbb{F}$, not all zero, such that

$$0 = \sum_{i=0}^{l_{1k}} \theta(e_{k+i}) t_{\alpha_i^{q_\circ}} = \sum_{i=0}^{l_{1k}} \theta(e_{k+i} s_{\alpha_i}) = \theta\left(\sum_{i=0}^{l_{1k}} e_{k+i} s_{\alpha_i}\right).$$

Then, $0 = \sum_{i=0}^{l_{1k}} e_{k+i} s_{\alpha_i} = \sum_{i=0}^{l_{1k}} v_i$, where $v_i = (0, \ldots, 0, \alpha_i^{q_k}, 0, \ldots, 0)$, with $\alpha_i^{q_k}$ in position $k+i$ and zero elsewhere, $0 \leq i \leq l_{1k}$. This is a contradiction because $\{v_0, \ldots, v_{l_{1k}}\}$ is a linearly independent set in the vector space $\mathbb{F}^{\oplus m}$ over $\mathbb{F}$. Hence $l' \geq l_{1k}$.

Now, let $S_2 = \{q'_1, \ldots, q'_{N_2}\} \subseteq G$ be the order set (strictly increasing) of all elements in the sequence (S_2). Suppose also that, for each $j = 1, \ldots, N_2$, the occurrence of q'_j in (S_2) is l'_{2j}. Then $l'_{2j} \geq 1$ for all $j = 1, \ldots, N_2$ and

$$l'_{21} + \cdots + l'_{2N_2} = m. \tag{3.1.4}$$

Therefore, for each $q_k \in S_1$, there exist $q'_r \in S_2$ such that $qq'_r = q_k$; namely, $S_1 \subseteq qS_2$ and $l_{1k} \leq l'_{2r}$. However, by (3.1.2) and (3.1.4), we conclude that $S_1 = qS_2$ and the occurrence of $q_k \in (S_1)$ is the same as occurrence of $q^{-1}q_k = q'_r \in (S_2)$. Moreover, since $1 \in S_1 \cap S_2$, $q \in S_1$ and $q^{-1} \in S_2$.

Conversely, we assume the assumptions and then define $\eta : A_1^* \longrightarrow A_2^*$ by $\eta(s_\alpha) = t_{\alpha^q}$, for each $\alpha \in \mathbb{F}$. For $S_1 = \{1, \ldots, q_N\}$ and $S_2 = \{1, \ldots, q'_N\}$, let l_j and l'_j be the occurrences of $q_j \in (S_1)$ and $q'_j \in (S_2)$, respectively. Define a permutation $\rho : \{1, ..., N\} \longrightarrow \{1, ..., N\}$ by setting $\rho(j) := n_j$ if $qq'_j = q_{n_j}$, for each $j = 1, \ldots, q_N$. Now, for each $k = 1, \ldots, N$, we set

$$m_{\rho(k)} := \sum_{j<\rho(k)} l_j \quad \text{and} \quad m'_k := \sum_{j=1}^{k} l'_j,$$

and set $m_1 = 0 = m'_0$. For each $i \in \{1, \ldots, m\}$ such $m'_{k-1} < i \leq m'_k$, we define

$$\sigma(i) := m_{\rho(k)} + j,$$

where $i = m'_{k-1} + j$. Then $\sigma : \{1, \ldots, m\} \longrightarrow \{1, \ldots, m\}$ is a permutation satisfying the property that $qq'_i = q_{\sigma(i)}$, for all $i \in \{1, \ldots, m\}$. By setting $s_i := qq'_i/q_{\sigma(i)} \bmod(p^n - 1)$ for each $i = 1, \ldots, m$, we see that $s_i \in \overline{1} = \langle p \rangle$. So, the function $\theta : \mathbb{F}^{\oplus m} \longrightarrow \mathbb{F}^{\oplus m}$ defined by

$$\theta(x_1, x_2, \ldots, x_m) = (x_{\sigma(1)}^{s_1}, x_{\sigma(2)}^{s_2}, \ldots, x_{\sigma(m)}^{s_m}),$$

is a group isomorphism, by Theorem 3.1.6 in [1]. Moreover, for $\alpha \in \mathbb{F}$ and $(x_1, x_2 \ldots, x_m) \in \mathbb{F}^{\oplus m}$,

$$\begin{aligned}
\theta((x_1, x_2, \ldots, x_m)s_\alpha) &= \theta(x_1\alpha^{q_1}, x_2\alpha^{q_2}, \ldots, x_m\alpha^{q_m}) \\
&= ((x_{\sigma(1)}\alpha^{q_{\sigma(1)}})^{s_1}, (x_{\sigma(2)}\alpha^{q_{\sigma(2)}})^{s_2}, \ldots, (x_{\sigma(m)}\alpha^{q_{\sigma(m)}})^{s_m}) \\
&= (x_{\sigma(1)}^{s_1}\alpha^{q_{\sigma(1)}s_1}, x_{\sigma(2)}^{s_2}\alpha^{q_{\sigma(2)}s_2}, \ldots, x_{\sigma(m)}^{s_m}\alpha^{q_{\sigma(m)}s_m}) \\
&= (x_{\sigma(1)}^{s_1}\alpha^{qq'_1}, x_{\sigma(2)}^{s_2}\alpha^{qq'_2}, \ldots, x_{\sigma(m)}^{s_m}\alpha^{qq'_m}) \\
&= (x_{\sigma(1)}^{s_1}, x_{\sigma(2)}^{s_2}, \ldots, x_{\sigma(m)}^{s_m})t_{\alpha^q} \\
&= \theta(x_1, x_2, \ldots, x_m)\eta(s_\alpha)
\end{aligned}$$

Therefore $(\mathbb{F}^{\oplus m}, A_1) \cong (\mathbb{F}^{\oplus m}, A_2)$. □

3.2 Number of Near vector spaces

As in the previous section, we also denote by G the group $U(p^n-1)/\langle p\rangle$ and 1 by the identity of G and the number (up to the isomorphism) of near-vector spaces $\mathbb{F}^{\oplus m}$ over a finite field $\mathbb{F}$ is based on the number (up to the relation $\sim$ in (3.1.1) of equivalent classes in $St(1,m,G)$.

In this section, we let S be the set of all distinct elements in the suitable sequence (S) on G. By Theorem 3.1.7, we know that if $|S_1| \neq |S_2|$, then $(S_1) \nsim (S_2)$. Thus, the total number of near-vector spaces up to the isomorphism is

$$\sum_{i=1}^{\min(m,|G|)} T(i),$$

where $T(i)$ denote the number (up to $\sim$) of suitable sequences (S) of length m with $|S| = i$.

It is clear that, for $i = 1$, then $T(1) = 1$. Now, we consider $T(N)$ for $2 \leq N \leq \min(m,|G|)$. Let $St(1,m,N)$ denote the set of all possible distinct $(\neq)$ suitable sequences (S) having length m, $|S| = N$ and 1 in the first position. By basic combinatorics, there are suitable sequences in $St(1,m,N)$:

$$\binom{|G|-1}{N-1}\binom{m-1}{N-1} := t_N$$

For a suitable sequence $(S) \in St(1,m,N)$ having the set $S = \{1 = q_1, q_2, \ldots, q_N\}$, by Theorem 3.1.7, it means that equivalent class can be explicit as

$$[(S)] := \{(S), q_2^{-1}(S), \ldots, q_N^{-1}(S)\}.$$

Here, $q_j^{-1}(S)$ it means the suitable sequence obtained from (S) by multiplying elements in each position of the sequence by q_j^{-1} and then rearrange their entry in non-decreasing order. By the discussion above, each class in $St(1,m,N)/\sim$ contains N elements, then $T(N) = (t_N)/N$.

However, it can occur that $|[(S)]| < N$ that is $q_i^{-1}(S) = q_j^{-1}(S)$, for some

$1 \leq i \neq j \leq N$ or equivalently $q(S) = (S)$ for some $q \in S$ ($q = q_i q_j^{-1} \in S$, because $1 \in S$). Now, we consider the cases $|[(S)]| < N$, as the following.

Proposition 3.2.1. *For a suitable sequence $(S) \in St(1, m, N)$, $|[(S)]| < N$ if and only if*

1. *S is a disjoint union of cosets in G/H such $H \subseteq S$, for some non-trivial subgroup H of G in which $|H|$ is a common factor of $m, N, |G|$, and*
2. *elements in (S) coming from the same cosets have the same occurrences.*

Proof. ($\Rightarrow$) Suppose that $|[(S)]| < N$. Then $q(S) = (S)$, for some $q \in S$. This implies that $qS = S$. We claim that $q^k S = S$ for all $k \in \mathbb{N}$. If $q^k S = S$, then $q^{k+1} S = q^k(qS) = q^k S = S$. By mathematical induction, we have the claim. Since $1 \in S$ and $q^k S = S$ for all $k \in \mathbb{N}$, we have $q^k \in S$ for all $k \in \mathbb{N}$. So $\langle q \rangle \subseteq S$. Now, we can write $S = \{1, q, q^2, \ldots, q^{r-1}, q_{r+1} \ldots, q_N\} = \langle q \rangle \sqcup \{q_{r+1}, \ldots, q_N\}$, where $r = \text{ord}(q)$ and $\sqcup$ is the disjoint union. By using the fact that $q^k S = S$, for all $k \in \mathbb{N}$ again, we have $q^k q_{r+1} \in S$, for all $k \in \mathbb{N}$. Then $q_{r+1} \langle q \rangle \subseteq S$. Thus we can write $S = \langle q \rangle \sqcup q_{r+1} \langle q \rangle \sqcup \{q_{2r+1}, \ldots, q_N\}$. After continuously repeating this process, we can write

$$S = \langle q \rangle \sqcup q_{r+1} \langle q \rangle \sqcup q_{2r+1} \langle q \rangle \sqcup \cdots \sqcup q_{N-r+1} \langle q \rangle \tag{3.2.1}$$

We conclude that S is a union of cosets in $G/\langle q \rangle$. Since $r|N$, $q^N = 1$. By using the fact that $q(S) = (S)$, the occurrences for qq' and q' must be equal for each $q' \in S$. We claim that elements in S coming from the same coset in $G/\langle q \rangle$ must be the same occurrences. Let $q' \in S$. If the occurrences for $q^k q'$ and q' are equal, then $q^{k+1} q', q^k q'$ and q' have the same occurrences. By mathematical induction, the occurrences for $q^k q'$ and q' must be equal for all $k \in \mathbb{N}$. Let $q'_1, q'_2 \in q' \langle q \rangle$. Then $q'_1 = q' q^{k_1}$ and $q'_2 = q' q^{k_2}$ for some $k_1, k_2 \in \mathbb{N}$. So the occurrences for q'_1 and q'_2 are the same as the

occurrences for q'. Thus, we have the claim. Denote $q'_0 = 1$ and $q'_j = q_{jr+1}$, where $j = 1, 2, \ldots, N-r+1$. Let m_k be the occurrences of q'_k, where $k = 0, 1, \ldots, N-r+1$. By (3.2.1), we can conclude that $m = r(m_0 + m_1 + \cdots + m_{N-r+1})$. Thus $r|m$.

($\Leftarrow$) Suppose that H is a non trivial subgroup of G in which its order divides $\gcd(m, N, |G|)$. Let S be a disjoint union of $N/|H|$-elements in G/H and elements in (S) coming from the same cosets have the same occurrences. Let $q \in H$ and $q' \in S$. Since S is a disjoint union in G/H, we have $qq' \in S$. Then $q' \in q^{-1}S$. Note that the occurrences for q' and qq' are equal in (S). Since the occurrences for qq' in (S) are equal to the occurrences for q' in $q^{-1}(S)$, we have the occurrences for q' in (S) and in $q^{-1}(S)$ are equal. Hence $q^{-1}(S) = (S)$. Suppose that q_1, q_2 are in the same coset in G/H. Then $q_2 = q_1 q$ for some $q \in H$. We have

$$(q_2)^{-1}(S) = (q_1 q)^{-1}(S) = (q_1)^{-1}q^{-1}(S) = (q_1)^{-1}(S).$$

Thus $(q_1)^{-1}(S) = (q_2)^{-1}(S)$. Since $[(S)] := \{(S), q_2^{-1}(S), \ldots, q_N^{-1}(S)\}$, we conclude that $[(S)]$ contains at most $N/|H|$ sequences. □

An instant resultant of this proposition is as follow.

Corollary 3.2.2. *If* $\gcd(m, N, |G|) = 1$, *then* $T(N) = (t_N)/N$. *In particular, if* $\gcd(m, |G|) = 1$, *then the total number of near-vector space up to the isomorphism is*

$$\sum_{N=1}^{\min(m,|G|)} (t_N)/N$$

and

$$\begin{pmatrix} |G|-1 \\ N-1 \end{pmatrix} \begin{pmatrix} m-1 \\ N-1 \end{pmatrix} = t_N$$

is divisible by N *for each* $N = 1, 2, \ldots, \min(m, |G|)$.

For $\emptyset \neq H \leq G$ such that $|H|$ is a divisor of $\gcd(m, N, |G|)$, we denote $St(H, m, N)$ the set of all suitable sequences (S) of length m satisfying (1) and (2) in Proposition 3.2.1.

Proposition 3.2.3. *Let H, K be subgroups of G such that $|H|$ and $|K|$ are the divisors of* $\gcd(m, N, |G|)$. *Then $St(K, m, N) \subseteq St(H, m, N)$ if $H \leq K$.*

Proof. Suppose that $H \leq K$. Let $(S) \in St(K, m, N)$. Then S is a disjoint union of cosets in G/K. Since each coset in G/K can be written as a$|K|/|H|$ disjoint union of cosets in G/H, we have that S is also a disjoint union of cosets in G/H and elements in (S) coming from the same cosets in G/H have the same occurrences. Thus $(S) \in St(H, m, N)$. Hence $St(K, m, N) \subseteq St(H, m, N)$. □

The proof of Proposition 3.2.1 also asserts that if $|[(S)]| < N$, then this class contains at most $N/|H|$ sequences. In fact, we have:

Proposition 3.2.4. *Each $[(S)]$, where $(S) \in St(H, m, N)$, contains exactly $N/|H|$ sequences if and only if $H \not\leq K$ for any subgroup $K \neq H$ of G such that $|K|$ is a divisor of* $\gcd(m, N, |G|)$.

Proof. ($\Rightarrow$) Suppose that $H \lneq K$ for some subgroup K of G such that $|K|$ is a divisor of $\gcd(m, N, |G|)$. Let $(S) \in St(K, m, N)$. So $(S) \in St(H, m, N)$. By the assumption of Proposition 3.2.1, $[(S)]$ contains at most $N/|K|$ sequences, which is exactly not $N/|H|$ sequences.

($\Leftarrow$) Suppose that $|[(S)]| < N/|H|$. Then there are disjoint cosets $[q], [q']$ in G/H such that $q^{-1}(S) = q'^{-1}(S)$, or equivalently, $q(S) = (S)$ for some $q \notin H$. Again, $q^i(S) = (S)$, for all $i \in \mathbb{N}$ and hence $q^i S = S$. Since $H \subseteq S$, we have $q^i H \subseteq q^i S = S$ for all $i \in \mathbb{N}$. Hence $\langle q \rangle H \subseteq S$. Since G is abelian, $K := \langle q \rangle H$ is a subgroup of G. We see that $H \lneq K$. Let $q' \in K$. Then $q' = q^i h$ for some $i \in \mathbb{N}$. and $h \in H$. We claim that $q'(S) = (S)$ for all $q' \in K$. Since $h(S) = (S)$ and $q^i(S) = (S)$ for all $i \in \mathbb{N}$, we have $q'(S) = q^i h(S) = q^i(S) = (S)$. Thus $q'(S) = (S)$ for all $q' \in K$ and we have the claim. Now, we can write

$$S = K \sqcup \{q_{r+1}, \ldots, q_N\} = K \sqcup q_{r+1}K \sqcup \cdots \sqcup q_{N-r+1}K,$$

where $|K| = r$. Then $r|N$ and S is an $N/|K|$ disjoint union of coset in G/K. Let $q'_1, q'_2 \in q'K$. Then $q'_1 = q'q^{i_1}h_1$ and $q'_2 = q'q^{i_2}h_2$. Since $q(S) = (S)$, the occurrences for qq' and q' must be equal for each $q' \in S$. Note that the occurrences for $q'q^{i_1}h_1$ and $q'q^{i_1}$ must be equal in (S) and the occurrences for $q'q^{i_2}h_2$ and $q'q^{i_2}$ must be equal in (S). By the same process in the proof of Proposition 3.2.1, the occurrences for q^iq' and q' must be equal for all $i \in \mathbb{N}$. Thus the occurrences for q'_1 and q'_2 are the same as the occurrences for q'. This also implies that m is divisible by r. Hence $|K|$ is a common factor of $m, N, |G|$. □

By Proposition 3.2.1 and the proof above, yields us to conclude that:

Corollary 3.2.5. *For a suitable sequence $(S) \in St(1, m, N)$, if $||[(S)]|| \neq N$, then $||[(S)]|| = N/|H|$ for some subgroup $H \leq G$ such that $|H|$ is a divisor of* $\gcd(m, N, |G|)$.

Proof. Suppose that $||[(S)]|| \neq N/|H|$. By Proposition 3.2.1, $(S) \in St(H', m, N)$. for some $H' \leq G$ such that $|H'|$ is a divisor of $\gcd(m, N, |G|)$. Let H be the largest subgroup of G which contains H' and $|H|$ is a divisor of $\gcd(m, N, |G|)$. By Proposition 3.2.4, $[(S)]$ contains exactly $N/|H|$ sequences. □

This motivates us to consider all possible subgroups of G that their orders are divisors of $\gcd(m, N, |G|)$. Let $\{d_1, \ldots, d_l\}$ be the set of all divisors of $\gcd(m, N, |G|)$ and suppose without loss of generality that $d_1 < \cdots < d_l$. Suppose, for each d_i, there are k_i distinct subgroups of order d_i; we refer to these subgroups by H_{ij}, for each $1 \leq i \leq l$ and $1 \leq j \leq k_i$. Denote $S_{d_i}(G, N) := \{H_{ij} \,|\, 1 \leq j \leq k_i\}$, for each $i = 1, \ldots, l$.

Lemma 3.2.6. *Let $H_1, H_2 \in S_{d_i}(G, N)$, for some $1 \leq i \leq l$ such $H_1 \neq H_2$. If there is a suitable sequence $(S) \in St(H_1, m, N) \cap St(H_2, m, N)$, then $(S) \in St(K, m, N)$ for some $K \in S_{d_j}(G, N)$ such that $d_j > d_i$ and $H_1H_2 \subseteq K$.*

Proof. Assume that $(S) \in St(H_1, m, N) \cap St(H_2, m, N)$. Thus $h_1(S) = (S)$ for all $h_1 \in H_1$ and $h_2(S) = (S)$ for all $h_2 \in H_2$. Let $h \in H_1H_2$. Then $h = h_1h_2$, for some $h_1 \in H_1, h_2 \in H_2$. We have $h(S) = h_1h_2(S) = h_1(S) = (S)$. Thus $h(S) = (S)$, for all $h \in H_1H_2$. Since $1 \in S$ and $hS = S$, we have $h \in S$. So $H_1H_2 \subseteq S$. Now, we can write $S = H_1H_2 \sqcup \{q_{r+1}, \ldots, q_N\}$, where $|H_1H_2| = r$. By using the same process as the proof of Proposition 3.2.1,

$$H_1H_2 \sqcup q_{r+1}H_1H_2 \sqcup \cdots \sqcup q_{N-r+1}H_1H_2.$$

Then $r|N$ and S is an $N/|H_1H_2|$ disjoint union of coset in G/H_1H_2. By using the fact that $h(S) = (S)$, the occurrence for hq' and q' must be equal for each $q' \in S$. Let $q'_1, q'_2 \in q'H_1H_2$. Then $q'_1 = q'h$ and $q'_2 = q'g$ for some $h, g \in H_1H_2$. So the occurrence for q'_1 and q'_2 are the same as the occurrence for q'. By the same process in the proof of Proposition 3.2.1, we can conclude that $r|m$. Hence $|H_1H_2|$ is a common factor of $m, N, |G|$. Thus $(S) \in St(H_1H_2, m, N)$, which complete the proof. □

We observe that if $(S) \in St(H, m, N)$, then $[(S)] \subseteq St(H, m, N)$. Thus, by Proposition 3.2.4 and Lemma 3.2.6, $St(H_{lj}, m, N)/\sim$ contains exactly

$$\begin{pmatrix} \frac{|G|}{d_l} - 1 \\ \frac{N}{d_l} - 1 \end{pmatrix} \begin{pmatrix} \frac{m}{d_l} - 1 \\ \frac{N}{d_l} - 1 \end{pmatrix} /(N/d_l)$$

equivalent classes (each class has exactly N/d_l suitable sequences), for each $j = 1, \ldots, k_l$. However, for $i < l$, $St(H_{ij}, m, N)$ may contain some $(S) \in St(H_{sj}, m, N)$ (and hence all $St(H_{sj}, m, N)$), for some $s > i$ and $1 \leq j \leq k_s$ which these equivalent classes, $[(S)]$, have order less than N/d_i. Now, for each $1 \leq i \leq l$ and $1 \leq j \leq k_i$, we define

$$\overline{S}(H_{ij}) := \{(S) \in St(H_{ij}, m, N) \mid |[(S)]| = N/d_i\},$$

$$t(N, d_i) := \begin{pmatrix} \frac{|G|}{d_i} - 1 \\ \frac{N}{d_i} - 1 \end{pmatrix} \begin{pmatrix} \frac{m}{d_i} - 1 \\ \frac{N}{d_i} - 1 \end{pmatrix}$$

and $C_s(H_{ij})$ to be the set of all subgroups of order d_s of G containing H_{ij}, for each $1 \leq s \leq l$. By the above discussion, Proposition 3.2.1, 3.2.4, Lemma 3.2.6 and by basic combinatorics, we compute directly that:

$$|\overline{S}(H_{lj})| = t(N, d_l), \quad \text{for each } j = 1, \ldots, k_l, \tag{3.2.2}$$

$$|\overline{S}(H_{(l-1)j}| = t(N, d_{l-1}) - |C_l(H_{(l-1)j})|t(N, d_l), \quad \text{for each } j = 1, \ldots, k_{l-1}, \tag{3.2.3}$$

and, for $2 \leq v < l$, $1 \leq j \leq k_{l-v}$,

$$|\overline{S}(H_{(l-v)j}| = t(N, d_{l-v}) - \left[\sum_{s=l-v+1}^{l-1} \sum_{H \in C_s(H_{(l-v)j})} |\overline{S}(H)|\right] - |C_l(H_{(l-v)j})|t(N, d_l). \tag{3.2.4}$$

Since $\overline{S}(H_{ij})$'s are all distinct sets, there are exactly $\sum_{i=1}^{l} \frac{d_i}{N} \sum_{j=1}^{k_i} |\overline{S}(H_{ij})|$ equivalent classes of order less than N. So, there must be $\frac{1}{N}\left[t_N - \sum_{i=1}^{l} \sum_{j=1}^{k_i} |\overline{S}(H_{ij})|\right]$ equivalent classes of order N. Therefore, the following is immediate.

Theorem 3.2.7. *The total number of near-vector spaces $\mathbb{F}^{\oplus m}$ over a finite field $\mathbb{F}$ is exactly $\sum_{N=1}^{\min(m,|G|)} T(N)$ which each $T(N)$ is explicitly as*

$$\frac{t_N}{N} + \frac{1}{N} \sum_{i=1}^{l} (d_i - 1) \sum_{j=1}^{k_i} |\overline{S}(H_{ij})|,$$

where $1 < d_1 < \cdots < d_l$ are all divisors of $\gcd(m, N, |G|)$ and $H_{ij} \in S_{d_i}(G, N)$, for each $i = 1, \ldots, l$ and $j = 1, \ldots, k_i := |S_{d_i}(G, N)|$. Here, $|\overline{S}(H_{ij})|$'s can be read from (3.2.2), (3.2.3) and (3.2.4), recursively.

We see from this theorem that the number of near-vector spaces depends on the subgroups lattice of G. For example, in the case $n = 3, p = 3$, we have $G_1 = U(26)/\langle 3 \rangle = \{1, 5, 7, 17\}$ and, in the case $n = 2, p = 5$, we have $G_2 = U(24)/\langle 5 \rangle = \{1, 7, 13, 19\}$. Their group structures are illustrated as in the group tables below:

Table 3 Group table of G_1

G_1	1	5	7	17
1	1	5	7	17
5	5	17	1	7
7	7	1	17	5
17	17	7	5	1

Table 4 Group table of G_2

G_2	1	7	13	19
1	1	7	13	19
7	7	1	19	13
13	13	19	1	7
19	19	13	7	1

We see that G_1 has only one subgroup of order 2, which is $\{1, 17\}$, whereas G_2 has three subgroups of order 2, which are $\{1, 7\}$, $\{1, 13\}$ and $\{1, 19\}$. By direct calculation (listing all possible suitable sequences and then grouping them), we have tables of the number of near-vector spaces on $\mathbb{F}^{\oplus m}$ corresponding to G_1 and G_2, with $m = 4, 5, 6, 7, 8$ as below:

Table 5 The number of near-vector spaces on $GF(3^3)$

$T(N)$; G_1	$m = 4$	$m = 5$	$m = 6$	$m = 7$	$m = 8$
$N = 1$	1	1	1	1	1
$N = 2$	5	6	8	9	11
$N = 3$	3	6	10	15	21
$N = 4$	1	1	3	5	10
Total	10	14	22	30	43

Table 6 The number of near-vector spaces on $GF(5^2)$

$T(N)$; G_2	$m=4$	$m=5$	$m=6$	$m=7$	$m=8$
$N=1$	1	1	1	1	1
$N=2$	6	6	9	9	12
$N=3$	3	6	10	15	21
$N=4$	1	1	4	5	11
Total	11	14	24	30	45

In fact, this calculation agrees with the calculation using Theorem 3.2.7.

Example 3.2.8. *Let* $n=2, p=7$, *then* $G=U(48)/\langle 7\rangle=\{1,5,11,13,17,19,25,41\}$. *Thus group structures is illustrated as in the group tables below:*

Table 7 Group table of G

G	1	5	11	13	17	19	25	41
1	1	5	11	13	17	19	25	41
5	5	25	1	17	19	41	11	13
11	11	1	25	41	13	17	5	19
13	13	17	41	25	11	1	19	5
17	17	19	13	11	1	5	41	25
19	19	41	17	1	5	25	13	11
25	25	11	5	19	41	13	1	17
41	41	13	19	5	25	11	17	1

We see that G *has three subgroups of order* 2, *which are* $\{1,17\}$, $\{1,25\}$ *and* $\{1,41\}$ *also* G *has three subgroups of order* 4, *which are* $\{1,5,11,25\}$, $\{1,13,19,25\}$ *and* $\{1,17,25,41\}$. *By using Theorem 3.2.7, we have a table of the number of near-vector spaces on* $\mathbb{F}^{\oplus m}$ *corresponding to* G *with* $m=4,5,6,7,8,9,10,11,12$ *as below:*

Table 8 The number of near-vector spaces on $GF(7^2)$

$T(N)$; G; m	4	5	6	7	8	9	10	11	12
$N=1$	1	1	1	1	1	1	1	1	1
$N=2$	12	14	19	21	26	28	33	35	40
$N=3$	21	42	70	105	147	196	252	315	385
$N=4$	12	30	92	150	314	420	744	900	1,456
Total	46	87	182	277	488	645	1,030	1,251	1,882

CHAPTER IV

CONCLUSIONS

In this chapter, we list all main results of this thesis below.

1. Let σ be any permutation of the indices $\{1, 2, ..., m\}$ and $\widetilde{A}_\sigma = \{\sigma_\alpha \,|\, \alpha \in \mathbb{F}\}$, with the scalar multiplication on V is given by

$$(x_1, \ldots, x_m)\sigma_\alpha = (x_1\alpha^{q_\sigma(1)}, \ldots, x_m\alpha^{q_\sigma(m)}),$$

for all $\alpha \in \mathbb{F}$. Then $\widetilde{A}^*$ is a subgroup of $\mathrm{Aut}(\mathbb{F}^{\oplus m})$ and $(\mathbb{F}^{\oplus m}, A) \cong (\mathbb{F}^{\oplus m}, \widetilde{A}_\sigma)$.

2. Let $A = \{s_\alpha : \alpha \in \mathbb{F}\}$ acts on V by

$$(x_1, \ldots, x_m)s_\alpha = (x_1\alpha^{q_1 p^{l_1}}, \ldots, x_m\alpha^{q_m p^{l_m}}),$$

where $l_1, \ldots, l_m \in \{0, 1, \ldots, n-1\}$ and $\overline{A} = \{t_\alpha : \alpha \in \mathbb{F}\}$ acts on V by

$$(x_1, \ldots, x_m)t_\alpha = (x_1\alpha^{q_1}, \ldots, x_m\alpha^{q_m}),$$

for all $\alpha \in \mathbb{F}$. Then $\overline{A}^*$ is a subgroup of $\mathrm{Aut}(V)$ and $(\mathbb{F}^{\oplus m}, A) \cong ((\mathbb{F}^{\oplus m}, \overline{A})$.

3. Let $\mathbb{F} = \mathrm{GF}(p^n)$ and $q_i, q_j \in G$. Then, $(\alpha^{q_i} + \beta^{q_i})^{q_j} = (\alpha^{q_j} + \beta^{q_j})^{q_i}$ for all $\alpha, \beta \in \mathbb{F}$ if and only if $q_i = q_j$.

4. Let $(\mathbb{F}^{\oplus m}, A_1)$ and $(\mathbb{F}^{\oplus m}, A_2)$ be near-vector spaces, where A_1 and A_2 are determined by suitable sequence (S_1) and (S_2), respectively. Then $(\mathbb{F}^{\oplus m}, A_1) \cong (\mathbb{F}^{\oplus m}, A_2)$ if and only if there is $q \in S_1$ such that $S_1 = qS_2$ and the occurrences of $qq'_j \in (S_1)$ and $q'_j \in (S_2)$ are the same for each $j = 1, \ldots, N$, where $N = |S_1| = |S_2|$.

5. For a suitable sequence $(S) \in St(1, m, N)$, $|[(S)]| < N$ if and only if

   1. S is a disjoint union of cosets in G/H such $H \subseteq S$, for some non-trivial subgroup H of G in which $|H|$ is a common factor of $m, N, |G|$, and

2. elements in (S) coming from the same cosets have the same occurrences.

6. If $\gcd(m, N, |G|) = 1$, then $T(N) = (t_N)/N$. In particular, if $\gcd(m, |G|) = 1$, then the total number of near-vector space up to the isomorphism is

$$\sum_{N=1}^{\min(m,|G|)} (t_N)/N$$

and

$$\binom{|G|-1}{N-1}\binom{m-1}{N-1} = t_N$$

is divisible by N for each $N = 1, 2, \ldots, \min(m, |G|)$.

7. Let H, K be subgroups of G such that $|H|$ and $|K|$ are the divisors of $\gcd(m, N, |G|)$. Then $St(K, m, N) \subseteq St(H, m, N)$ if $H \leq K$.

8. Each $[(S)]$, where $(S) \in St(H, m, N)$, contains exactly $N/|H|$ sequences if and only if $H \not\leq K$ for any subgroup $K \neq H$ of G such that $|K|$ is a divisor of $\gcd(m, N, |G|)$.

9. For a suitable sequence $(S) \in St(1, m, N)$, if $|[(S)]| \neq N$, then $|[(S)]| = N/|H|$ for some subgroup $H \leq G$ such that $|H|$ is a divisor of $\gcd(m, N, |G|)$.

10. Let $H_1, H_2 \in S_{d_i}(G, N)$, for some $1 \leq i \leq l$ such $H_1 \neq H_2$. If there is a suitable sequence $(S) \in St(H_1, m, N) \cap St(H_2, m, N)$, then $(S) \in St(K, m, N)$ for some $K \in S_{d_j}(G, N)$ such that $d_j > d_i$ and $H_1 H_2 \subseteq K$.

11. The total number of near-vector spaces $\mathbb{F}^{\oplus m}$ over a finite filed $\mathbb{F}$ is exactly $\sum_{N=1}^{\min(m,|G|)} T(N)$ which each $T(N)$ is explicitly as

$$\frac{t_N}{N} + \frac{1}{N}\sum_{i=1}^{l}(d_i - 1)\sum_{j=1}^{k_i}|\overline{S}(H_{ij})|,$$

where $1 < d_1 < \cdots < d_l$ are all divisors of $\gcd(m, N, |G|)$ and $H_{ij} \in S_{d_i}(G, N)$, for each $i = 1, \ldots, l$ and $j = 1, \ldots, k_i := |S_{d_i}(G, N)|$. Here, $|\overline{S}(H_{ij})|$'s can be read from (3.2.2); (3.2.3) and (3.2.4), recursively.

REFERENCES

REFERENCES

1. Howell KT, Meyer JH. Near-vector spaces determined by finite fields. J Algebra. 2014;398:55-62.

2. Zhexian W. Lectures on finite fields and Galois rings. Beijing: World Scientific; 2003.

3. Joseph J. A first course in abstract algebra with applicatios. Pllinois: University of Illinois at Urbana-Champaign; 2006.

4. Vanderwalt APJ. Matrix near-rings contained in 2-primitive near-rings with minimal subgroups. J Algebra. 1992;148:296-304.

5. Andre J. Lineare algebra uber Fastkorpern. Math Z. 1974;136:295-313.

6. Howell KT, Meyer JH. Finite dimensional near-vector spaces over finite fields. J Comm Algebra. 2010;38:86-93.