REPRESENTATION OF AFFINE FINITE GEOMETRIES BY MEANS OF FINITE VECTOR SPACES

DISERTASI

oleh

KUSNO KROMODIHARDJO

INSTITUT TEKNOLOGI BANDUNG
1982

REPRESENTATION OF AFFINE FINITE GEOMETRIES BY MEANS OF FINITE VECTOR SPACES

DISERTASI

Untuk memperoleh gelar Doktor dalam
Ilmu Pasti dan Ilmu Pengetahuan Alam
pada Institut Teknologi Bandung
atas tanggungan Rektor:
Prof. Dr. Hariadi P. Soepangkat
Yang akan dipertahankan di muka
Sidang Terbuka Senat
Institut Teknologi Bandung
pada hari: Sabtu, 31 Juli 1982
pukul: 09.00 pagi
di: Jalan Surapati No. 1

oleh

KUSNO KROMODIHARDJO
Lahir di Wonosobo, 23 – 8 – 1931

INSTITUT TEKNOLOGI BANDUNG
1982

Promotor : Prof. Dr. D. Handali

Co-Promotor : Prof. Dr. H. J. A. Duparc

This dissertation has been printed by "Penerbit ITB" with financial support from Lieutenant General Wiyogo Admodarminto, Commander of The Second Region (Panglima Komando Wilayah Dua).

To my beloved wife and children
and to the memory of my parents

It is He who made the sun
To be a shining glory
And the moon to be a light
Of beauty, and measured out
Stages for her; that ye might
Know the number of years
And the count of time.
Nowise did God create this
But in truth and righteousness
Thus doth He explain His Signs
In detail, for those who
Understand

(Holy Quran, X: 5)

ACKNOWLEGEMENTS

The author is deeply grateful to Professor Daniel Handali for being his promotor.

He is also inbedted to Professor Herman Johan A Duparc from the Technische Hoge School at Delft, Netherland for being his co-promotor and for his valuable remarks, his suggestions and his advice concerning the English text of this dissertation.

Also he is grateful to Professor Doddy Tisna Amidjaja, former Rektor of ITB, who has made the desicion to allow him to enter the Graduate School of ITB, i.e. The SEKOLAH PASCA SARJANA INSTITUT TEKNOLOGI BANDUNG.

The author also thanks the late Professor Petrus A Surjadi who was able to find a co-promotor for him.

His thoughts also go to Mr. Rawuh who has introduced the concept of finite geometry for the first time to him.

He would like to thank the General Directorate of High Education for his sponsorship during the research.

He also would like to thank the Board of Directors of PT Asuransi Jiwasraya for some financial support.

Finally he expresses his gratitute to Dr. Bana Kartasasmita for his help and guidence and for his valuable advice on matters of English wordings.

ABSTRACT

Representation of finite geometries either by means of abelian finite groups or by means of marks of a Galois Field was developed by Robert D. Carmichael in the thirties. The emphasis was on projective finite geometries, while the Euclidean ones were mentioned very briefly and were considered as certain subsets of projective finite geometries. The concept of a vector space was not utilized by Carmichael [4].

In this dissertation I consider Affine finite geometries explicitly. The main idea is to introduce the concepts of parallelism and orthogonality, in those geometries, which are represented by means of finite vector spaces.

Beginning with a Galois Field $GF[p^n]$ we construct a k-dimensional vector space $V_k(GF[p^n])$. We call this space a k-dimensional Affine finite geometry of order p^n or a k-dimensional Affine finite space of order p^n.

The elements of this space are called points and particular subsets, namely subsets which can be written in the form $\{a + \mu b\}$, where a and b are elements of $V_k(GF[p^n])$ with $b \neq \bar{0}$ and $\mu \in GF[p^n]$, are called lines.

The terminologies "lying on" and "intersecting" are defined in a very obvious way.

Similarity among lines is defined by means of direction points (direction vectors) and two lines are said to be parallel if they are similar and disjoint.

The concept of standard pseudo inner product of two vectors is defined much in the same way as the standard inner product in $V_k(\mathbf{R})$ (or $\mathbf{R}^k$). Two vectors are said to be ortho gonal to each other if their standard inner product is zero and two lines are said to be orthogonal or perpendicular to each other whenever its respective direction vectors are orthogonal.

It is not impossible that a line might be orthogonal to itself. Such a line is called isotropic. As a consequence two lines which are parallel might be orthogonal to each other. This fact is something new, unexpected and rather surprising, especially when we consider the Affine finite plane.

Based on the vector equation of a plane in $\mathbf{R}^k$, especially in $\mathbf{R}^3$, a plane in $V_k(GF[p^n])$ is defined to be a subset which can be written in the form $\{a + \mu b + \theta c\}$, where $\mu, \theta \in GF[p^n]$ and b and c are two non zero vectors which are not similar.

Only planes in $V_3(GF[p^n])$ are considered in this dissertation. As expected coordinate equation of a plane, normal vector of a plane and many other notions have the same form as in the ordinary Affine geometry.

Since in finite systems counting theorems are important, one of the main problems here is the determination of the total number of lines and planes.

ABSTRAK

Penyajian geometri terhingga baik dengan grup abel terhingga maupun dengan unsur-unsur dari suatu medan Galois telah dikembangkan oleh Robert D Carmichael sekitar tahun tigapuluhan. Titik beratnya diletakkan pada geometri proyektif terhingga. Adapun geometry Euclides terhingga hanya disebut sepintas lalu saja dan dianggap sebagai anak himpunan tertentu dari geometri proyektif terhingga. Konsep ruang vektor belum digunakan oleh Carmichael [4].

Dalam disertasi ini saya meninjau geometri Afin terhingga secara eksplisit. Ide utamanya ialah memperkenalkan konsep-konsep kesejajaran dan ketegaklurusan, dalam geometri tersebut yang disajikan dengan ruang vektor terhingga.

Dimulai dengan suatu medan Galois $GF[p^n]$ kita bangun suatu ruang vektor berdimensi k yaitu $V_k(GF[p^n])$. Kita namakan ruang ini geometri Afin terhingga berdimensi k dan tingkat p^n atau ruang Afin terhingga berdimensi k dan tingkat p^n

Unsur-unsur ruang ini disebut titik dan anak himpunan-anak himpunan khusus yaitu anak himpunan yang dapat diucapkan dalam bentuk $\{a + \mu b\}$, dimana $a, b \in V_k(GF[p^n])$ dengan $b \neq \bar{0}$ dan $\mu \in GF[p^n]$, disebut garis.

Istilah-istilah "terletak pada" dan "berpotongan" didefinisikan dengan cara yang sangat eviden.

Pengertian searah antara dua garis didefinisikan dengan bantuan titik arah atau vektor arah dan dua garis dikatakan sejajar bila keduanya searah dan saling lepas.

Konsep hasilkali dalam baku palsu dari dua vektor didefinisikan dengan jalan yang serupa seperti hasilkali dalam baku pada $V_k(R)$ (R^k). Dua vektor dikatakan saling ortogonal jika hasilkali dalamnya nol dan dua garis dikatakan saling ortogonal atau saling tegaklurus bila vektor arah masing-masing saling tegaklurus.

Tidaklah mustahil bahwa suatu garis mungkin tegaklurus pada dirinya sendiri. Garis semacam itu disebut isotrop. Sebagai akibatnya dua garis yang sejajar mungkin saja saling tegaklurus.

Kenyataan ini menunjukkan sesuatu yang baru, tidak diduga dan agak mengejutkan, khususnya apabila kita tinjau Bidang Afine terhingga.

Berdasarkan persamaan vektor dari sebuah bidang dalam R^k, khususnya R^3, bidang dalam $V_k(GF[p^n])$ didefinisikan sebagai anak himpunan yang dapat diucapkan dalam bentuk $\{a + \mu b + \theta c\}$ dimana $a, b, c \in V_k(GF[p^n])$ dengan $b \neq \bar{0}$; $c \neq \bar{0}$ serta b tak searah dengan c dan $\mu, \theta \in GF[p^n]$.

Hanya bidang dalam $V_3(GF[p^n])$ akan dibahas di sini. Seperti yang diharapkan ternyata persamaan koordinat suatu bidang, vektor normal suatu bidang dan banyak konsep lainnya mempunyai bentuk yang sama seperti dalam geometri Afin yang biasa.

Karena dalam sistem-sistem terhingga teorema-teorema pembilangan (penghitungan) penting, maka salah satu masalah utama di sini yaitu menentukan banyaknya garis dan banyaknya bidang.

TABLE OF CONTENTS

	page
ACKNOWLEDGEMENTS	v
ABSTRACT	vi
ABSTRAK	vii
INTRODUCTION	1
CHAPTER I: FINITE VECTOR SPACES	3
1.1. Notation	3
1.2. Finite vector spaces	3
1.3. The vector space $V_k(GF[p^n])$	3
CHAPTER II: THE AFFINE FINITE GEOMETRY AFG(k, p^n)	4
2.1 Points and lines	4
2.2 Parallel lines	7
2.3 Number of lines	8
2.4 Orthogonality	9
CHAPTER III: THE AFFINE FINITE PLANE AFG(2, p^n)	15
3.1 Points and lines	15
3.2 Parallelism	15
3.3 Orthogonality	16
3.4 Illustration	18
3.5 A note on theorem 2.4.7	21
CHAPTER IV: THE AFFINE FINITE SPACE AFG(3, p^n)	22
4.1 Points and lines	22
4.2 Planes in AFG(2, p^n)	23
4.3 Lines and planes	30
4.4 Two planes	33
4.5 Coordinate representation of a plane	35
4.6 Orthogonality	38
4.7 Number of planes	44
4.8 Examples of 3-dimensional Affine finite geometries	47
CHAPTER V: TRANSFORMATIONS	52
5.1 Translations	52
5.2 Linear transformations	53
5.3 Affine transformations	54
5.4 Isometry	56
CHAPTER VI: THE PROJECTTIVE FINITE PLANE PFG(2, p^n)	58
6.1 The geometry PFG(2, p^n)	58
6.2 Some theorems in PFG(2, p^n)	58
6.3 An example of PFG(2, p^n)	60

GENERAL REMARKS 62

1. Midpoint in AFG(k, p^n) 62
2. Distance in AFG(k, p^n) 63
3. Quadratic forms in AFG(k, p^n) with k = 2 or 3 66
4. Finite geometry and a graph 67
5. Representation of finite geometries by means of sets 68
6. Quasi geometry 69

LIST OF SPECIAL SYMBOL 71

REFERENCES 73

THEOREMS (List I. Concerning the dissertation) 75

THEOREMS (List II. Not concerning the dissertation) 76

DALIL–DALIL (Daftar I. Mengenai disertasi) 77

DALIL–DALIL (Daftar II. Tidak mengenai disertasi) 78

RIWAYAT SINGKAT PROMOVENDUS 79

INTRODUCTION

Finite geometries can be set up in two ways, namely axiomatically [22] or by representation [4], [4a]. The most difficult one is the first.

Reprensentation of finite geometries by means of abelian finite groups has been done by Robert D Carmichael [4]. He began with an abelian finite group of prime power order $p^{(k+1)n}$ and of type (1, 1, 1,. . . ,1). A point is defined to be any subgroup of order p^n, while a line is defined to be a subgroup generated by two different subgroups which are points.

He called this geometry a k-space projective geometry and denoted it by $PG(k,p^n)$.

The two basic axioms of projective geometry in $PG(2, p^n)$ namely :

(i) Given two distinct points, there exists one and only one line passing through both points, and its dual

(ii) Two distinct lines intersect in one and only one point,

becomes true theorems.

He also gave a representation of finite projective geometry by means of "marks" which means elements of a Galois Field. A k-dimensional finite projective geometry is a set of (k + 1)--tuples $(\mu_0, \mu_1, \mu_2, \ldots, \mu_k)$, where $\mu_0, \mu_1, \mu_2, \ldots, \mu_k$ are elements of a Galois Field $GF[p^n]$ at least one of which is different from zero. He called such a (k + 1)–tuple a homogeneous coordinate.

Since the concept of a vector space has not been used, difficulties arose when such a coordinate will be added or will be multiplied by another element of the field $GF[p^n]$.

The emphasis of his work is finite projective geometry, while the Euclidean finite one was mentioned very briefly. By a Euclidean finite geometry is meant the set of (k +1)–tuples $(1, \mu_1, \mu_2 \ldots, \mu_k)$ where the μ_i 's are elements of a Galois Field GF $[p^n]$. Any such a (k + 1)–tuple is called a point. Hence the total number of points in that geometry is p^{nk}. He denoted this geometry by $EG(k, p^n)$.

I simply begin with a Galois Field $\Sigma = GF[p^n]$ and set up the vector space Σ^k over Σ, where Σ^k is the cartesian product of k factors, namely

$$\Sigma^k = \Sigma \times \Sigma \times \ldots \times \Sigma$$

in the very usual way. I denote this vector space by $V_k(\Sigma)$ or $V_k(GF[p^n])$ [3].

Any vector in $V_k(\Sigma)$ is defined to be a point and any subset $L \subseteq V_k(\Sigma)$ is called a line if and only if there exist points (vectors) a, $b \in V_k(\Sigma)$ with $b \neq \bar{0}$ such that

$$L = \{a + \theta b \mid \theta \in \Sigma\}$$

Here b is called a direction vector or direction point of L.

Furthermore a vector $c \neq \bar{0}$ is said to be similar to a vector $d \neq \bar{0}$ if and only if there exists an element $\mu \in \Sigma$ such that $c = \mu d$. Clearly similarity is an equivalence relation. Two lines are said to be similar if their direction vectors are similar and two lines are said to be parallel if they are similar and disjoint.

A subset $\Lambda \subseteq V_k(\Sigma)$ is said to be a plane if and only if there exist three vectors $a,b,c \in V_k(\Sigma)$ with $b \neq \bar{0}$, $c \neq \bar{0}$ where b and c are not similar, such that:

$$\Lambda = \{a + \mu b + \theta c \mid \mu, \theta \in \Sigma\}$$

In addition I introduce the standard pseudo inner product to define orthogonality.

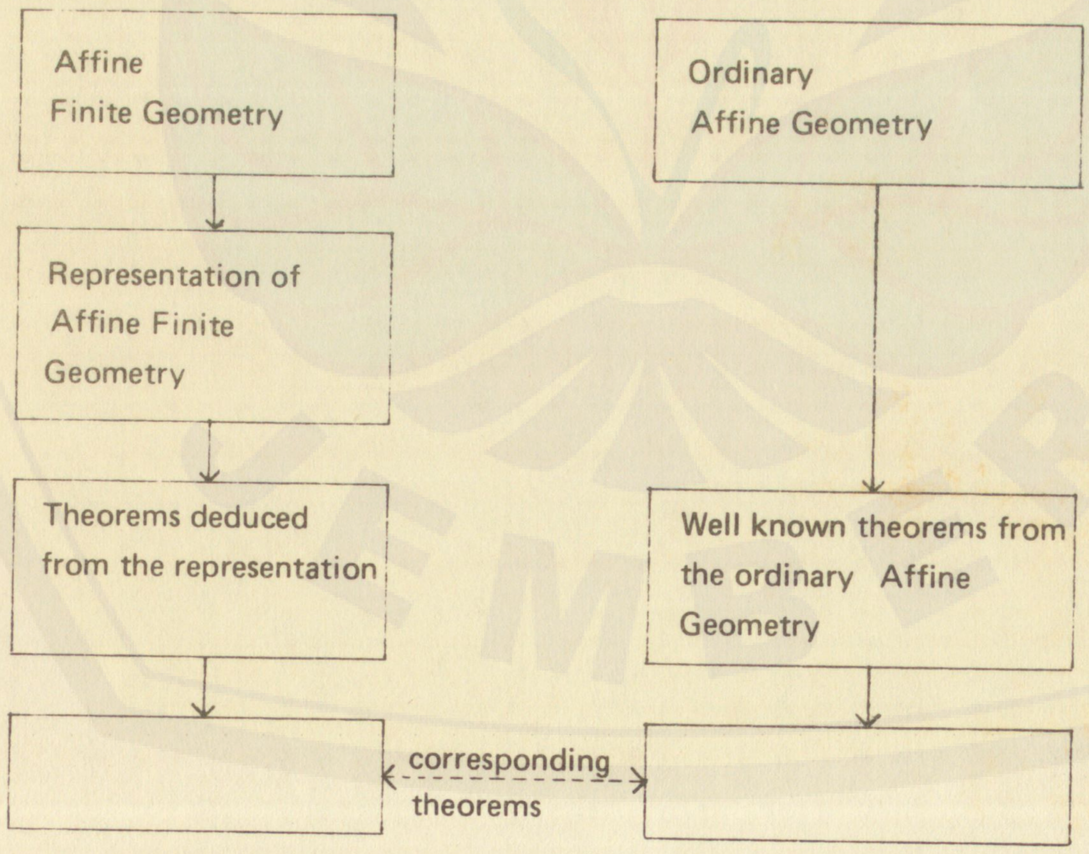
Then I call this $V_k(GF[p^n])$ a k-dimensional Affine Finite Geometry of order p^n and denote it by $AFG(k,p^n)$

The basic idea of this procedure is obvious. To build up finite geometries we search a representation of them. Then we deduce theorems. Finally we compare these theorems, which are discovered from the representation with the corresponding ones from the ordinary Affine geometry. We can see whether they are similar or not.

As a side product I discuss in brief the Projective finite plane, deduced from the 3-dimensional Affine finite geometry $AFG(3,p^n)$ where lines through $\bar{0}$ are defined to be points and planes through $\bar{0}$ are defined to be lines.

In my remark I consider the possibility of defining distances and midpoints in $AFG(k,p^n)$ and investigating whether there is a relation between an Affine finite geometry and a graph.

The following scheme is the basic idea of this representation.



CHAPTER I

FINITE VECTOR SPACES

1.1 Notation

Let V be a vector space over the field Σ. Elements of V are denoted by the Italian letters a, b, c, . . . , x, y, z, while elements of Σ are denoted by the Greek letters $\alpha, \beta, \gamma, \mu, \theta, \ldots$

If $a \in V$ then the set of all multiples of a, namely

$\{\theta a \mid \theta \in \Sigma\}$

is denoted by Σa.

If a, b, $\in$ V. then the set $\{a + \theta b \mid \theta \in \Sigma\}$ is denoted

by $a + \Sigma b$,

and if a, b, c $\in$ V the set $\{a + \mu b + \theta c \mid \mu, \theta \in \Sigma\}$

is denoted by

$a + \Sigma b + \Sigma c$.

The k-dimensional vector space Σ^k over Σ is denoted by $V_k(\Sigma)$ [3].

1.2 Finite vector spaces

By a finite vector space V over the field Σ is meant a finite abelian group V which is a vector space over Σ. Obviously finite vector spaces are finite dimensional ones. We may have an infinite vector space over a finite field, for instance the trancendental extension of a finite field by adjunction of an indeterminate is an infinite vector space over the original finite field.

But we can not have a non zero finite vector space V over an infinite field, for if such a space V would exist we can select a non zero element $a \in V$ and form the set of all mutiples of a, which will be an infinite subset of V and thus contradicts the hypothesis that V is finite.

So we can state the following proposition:

PROPOSITION 1.2.1

There does not exist a non zero finite vector space over an infinite field.

1.3 The vector space $V_k(GF[p^n])$

So a non zero finite vector space V must be a finite one over a Galois $GF[p^n]$. Since two vector spaces over the same field, with the same dimension are isomorphic, hence for the investigation of finite vector spaces it is sufficient to consider the spaces $V_k(GF[p^n])$.

CHAPTER II

THE AFFINE FINITE GEOMETRY AFG(k, p^n)

2.1 Points and lines

Let Σ be a Galois Field GF[p^n]. We consider the k-dimensional vector space $V_k(\Sigma) = V_k(GF[p^n])$ over Σ. We are going to make this vector space a finite gometry by defining points and lines as follows:

DEFINITION 2.1.1
Any element of $V_k(\Sigma)$ is called a point.

DEFINITION 2.1.2
A subset $L \subseteq V_k(\Sigma)$ is called a line if and only if there exist points a and $b \in V_k(\Sigma)$ with $b \neq \bar{0}$ such that $L = a + \Sigma b$.

Hence this vector space $V_k(\Sigma)$ is called a k-dimensional Affine finite space of order p^n or an Affine finite geometry of dimension k and order p^n. The following statement is obvious.

COROLLARY 2.1.3
The total number of points in an Affine finite geometry of dimension k and order p^n is equal to p^{nk}.

We denote this geometry by AFG(k, p^n). If a line L in AFG(k, p^n) is represented by the formula $a + \Sigma b$, the point b is called a direction point or direction vector of L. It is denoted by d_L.

We say that a point b lies on L or L goes through b if and only if $b \in L$. A line L is called to intersect M if and only if $L \cap M \neq \emptyset$ and the fact that two lines K and N coincide is expressed by K = N.

PROPOSITION 2.1 4
The line $L = a + \Sigma b$ goes through the point a.

The following theorems are basic and plausible.

PROPOSITION 2.1.5
A line in AFG(k, p^n) contains exactly p^n points.

PROOF
This proposition is based on the property that in a vector space the relation $\theta x = \bar{0}$ implies $\theta = 0$ or $x = \bar{0}$.

Let L be a line in AFG(k, p^n) and let $L = a + \Sigma b$. Hence the total number of points in

L is at most p^n. Suppose there are $\theta_1, \theta_2 \in \Sigma$ such that $a + \theta_1 b = a + \theta_2 b$. Thus $\theta_1 b = \theta_2 b$. Or $(\theta_1 - \theta_2)b = 0$. Then according to the property just mentioned before this means that $\theta_1 = \theta_2$ since $b \neq 0$. Hence the number of points on L is equal to the number of possible choices of θ, i.e equal to p^n ∎

DEFINITION 2.1.6

A non zero vector a is said to be similar to a non zero vector b if and only if there exists a $\theta \in \Sigma$ such that $a = \theta b$. Notation: $a \backsim b$.

Obviously similarity is an equivalence relation.

PROPOSITION 2.1.7

Two direction points of a line are similar

PROOF

Let L be a line in AFG(k, p^n). and let L be represented by two different formulas, say $L = a + \Sigma b$ and $L = s + \Sigma t$.

Then according to a previous proposition a and s lie on L.

Hence we can write: $a = s + \mu t$ for some $\mu \in \Sigma$

and $s = a + \theta b$ for some $\theta \in \Sigma$

We consider two cases:

(i) $a \neq s$

(ii) $a = s$

In case (i) we have $\mu \neq 0$ and $\theta \neq 0$, while $a - s = \mu t = -\theta b$.

Hence $b = (-\theta)^{-1} \mu t$ which means that $b \backsim t$.

In the other case take a point $c \neq a$ on L. Then there exist σ and $\tau \in \Sigma$, both unequal zero such that:

$$c = a + \sigma b = s + \tau t = a + \tau t.$$

Hense $\sigma b = \tau t$ or $b = \sigma^{-1} \tau t$. This means $b \backsim t$. ∎

PROPOSITION 2.1.8

If a and b are two distinct points, then the line $L = a + \Sigma(b - a)$ goes through both points.

This is obvious since $a = a + 0(b - a)$ and $b = a + 1(b - a)$.

The following theorem is the fundamental one in geometry.

THEOREM 2.1.9 (The Fundamental Theorem)

Given two distinct points, there exists one and only one line passing through both points.

PROOF

(i) Existence

This has been stated in proposition 2.1.8. If we called those two points a and b, then one of the lines passing through both points is the line L represented by $L = a + \Sigma(b - a)$.

(ii) Uniqueness

Let M be another line passing through a and b. Since M is a line hence there exist points s and $t \neq \bar{0}$ such that $M = s + \Sigma t$. Since a, $b \in M$ this means that there exist α and $\beta \in \Sigma$ such that:

$$a = s + \alpha t \text{ and } b = s + \beta t.$$

Further let $x \in L$, hence

$$x = a + \gamma(b - a) = s + \alpha t + \gamma(\beta - \alpha)t = s + (\alpha + \gamma\beta - \gamma\alpha)t.$$

This means that $x \in M$. Therefore $L \subseteq M$. However L and M are both finite sets with the same number of elements, since both are lines. Hence L = M which means both lines coincide.

∎

REMARK

Another straight forward proof without using the conventional set inclusion can be done in the following way:

Let M be another line passing through a and b, then there exist points s and $t \neq \bar{0}$ such that $M = s + \Sigma t$. Since a and b are on M this means that there exist μ and $\theta \in \Sigma$ such that:

$$a = s + \mu t \text{ and } b = s + \theta t \qquad (*)$$

Hence $b - a = (\theta - \mu)t$. By hypothesis a differs from b, hence $b - a = (\theta - \mu)t \neq \bar{0}$. This implies that $\mu \neq \theta$. Then solving s and t from equation (*) we get:

$$t = (\theta - \mu)^{-1}(b - a) \quad \text{and} \quad s = a - \mu t = a - \mu(\theta - \mu)^{-1}(b - a).$$

Therefore:

$$M = s + \Sigma t = a - \mu(\theta - \mu)^{-1}(b - a) + \Sigma(\theta - \mu)^{-1}(b - a)$$
$$= \{a - \mu(\theta - \mu)^{-1}(b - a) + \sigma(\theta - \mu)^{-1}(b - a) \mid \sigma \in \Sigma\}$$
$$= \{a + (\sigma - \mu)(\theta - \mu)^{-1}(b - a) \mid \sigma \in \Sigma\} = \{a + \lambda(b - a) \mid \lambda \in \Sigma\} =$$
$$= a + \Sigma(b - a) \text{ which is identical to L.}$$

COROLLARY 2.1.10

Two distinct lines intersect in at most one point.

DEFINITION 2.1.11

Two lines are said to be similar if its direction vectors are similar.

Notation: $L \backsim M$.

This definition is well defined because of proposition 2.1.7. Clearly similarity among lines is an equivalence relation.

LEMMA 2.1.12

If two similar lines intersect, then they coincide.

PROOF

Suppose L and M are two lines such that $L \backsim M$ and $L \cap M \neq \emptyset$. Let $L = a + \Sigma b$ and $M = c + \Sigma d$ where $b \backsim d$. We may write $d = \theta b$. Hence $M = c + \Sigma(\theta b)$.

Take a point $q \in L \cap M$;

$q \in L$ hence $q = a + \lambda b$ for some $\lambda \in \Sigma$

$q \in M$ hence $q = c + \mu d$ for some $\mu \in \Sigma$

Further $q = c + \mu d = c + \mu\theta b$

Or $a + \lambda b = c + \mu\theta b$ hence $c = a + (\lambda - \mu\theta)b$.

For any point x on M one has $x = c + \sigma d = (a + (\lambda - \mu\theta)b) + \sigma\theta b = a + (\lambda - \mu\theta + \sigma\theta)b \in L$.

This means that $M \subseteq L$. Thus $M = L$. ■

PROPOSITION 2.1.13

Given a line $L = a + \Sigma b$, then for any μ and $\theta \in \Sigma$ with $\theta \neq 0$, the line $M = (a + \mu b) + \Sigma(\theta b)$ coincides with L.

PROOF

Since both lines L and M are passing through a and a + b they must coincide, according to theorem 2.1.9. ■

2.2 Parallel lines

One of the main ideas in this dissertation is to define the concept of parallelism, since Affine geometry is characterized by the existence of two non intersecting lines in a plane.

DEFINITION 2.2.1

Two lines L and M are said to be parallel to each other if and only if:

(i) $L \backsim M$

(ii) $L \cap M = \emptyset$

Notation: $L \mathbin{/\!/} M$

THEOREM 2.2.2

Given a line L and a point q not on L, then there exists one and only one line containing q wich is parallel to L.

PROOF

Let L be a line and q a point such that $q \notin L$. Since L is a line, it can be written as $L = a + \Sigma b$, where $a, b \in V_k(\Sigma)$ and $b \neq \overline{0}$.

Consider the line $M = q + \Sigma b$. Then M contains q and it is similar to L. It remains to be proved that $L \cap M = \emptyset$.

Assume that M intersects L. Since both lines are similar, according to Lemma 2.1.12 they coincide. Hence $q \in L$, which contradicts our hypothesis.

To show the uniqueness, suppose M′ is another line passing through q and parallel to L. So we have

$L \parallel M$

and $L \parallel M'$

$L \parallel M$ gives $L \backsim M$, thus $M \backsim L$. While $L \parallel M'$ means also $L \backsim M'$. Hence $M \backsim M'$ since similarity is transitive. Then according to Lemma 2.1.12 $M = M'$.

2.3 Number of lines

In this paragraph we want to determine the total number of lines in $AFG(k, p^n)$ beginning with

(i) The total number of lines passing through a given point;

(ii) the total number of lines parallel to a given line;

c.q the total number of lines with a certain direction;

(iii) the total number of lines in $AFG(k, p^n)$.

If nothing is mentioned, the word total number of lines means total number of distinct lines.

THEOREM 2.3.1

The total number of lines passing through a given point in $AFG(k, p^n)$ is equal to

$$\frac{p^{nk} - 1}{p^n - 1}$$

PROOF

Take a point a in $AFG(k, p^n)$. The total number of points different from a is $p^{nk} - 1$. So we can make $p^{nk} - 1$ lines through a. Each line contains $p^n - 1$ points different from a. Hence there are

$$\frac{p^{nk} - 1}{p^n - 1}$$ lines through the point a. ■

THEOREM 2.3.2

Given a line L in $AFG(k, p^n)$, there are exactly $p^{n(k-1)} - 1$ lines parallel to L.

PROOF

Since L contains p^n points, there are $p^{nk} - p^n$ points not on L. We can construct the same number of lines (one through each point) parallel to L. But each line contains p^n points.

Hence there are $\frac{p^{nk} - p^n}{p^n} = p^{n(k-1)} - 1$ different lines parallel to L. ■

COROLLARY 2.3.3

Given a line L in AFG(k, p^n), there are exactly $p^{n(k-1)}$ lines similar to L.

For futher purposes we introduce the word direction by saying that two lines have the same direction when they are similar. Furthermore we say that a line L has direction b when its direction vector (direction point) is similar to b.

THEOREM 2.3.4

The total number of lines in AFG(k, p^n) is equal to

$$p^{n(k-1)} \frac{p^{nk}-1}{p^n-1}$$

PROOF

There are $p^{nk}-1$ directions in AFG(k, p^n). Up to similarity the total number of distinct directions is

$$\frac{p^{nk}-1}{p^n-1}$$

In each direction there are $p^{n(k-1)}$ parallel lines. Hence the total number of lines is equal to

$$p^{n(k-1)} \frac{p^{nk}-1}{p^n-1}$$ ■

2.4 Orthogonality

We are now going to define the notion of standard pseudo inner product. Just for our purposes here we define it in the following way.

DEFINITION 2.4.1

The Standard Pseudo Inner Product (SPIP) of two vectors x and y $\in V_k(\Sigma)$ where

$x = (\xi_1, \xi_2, \ldots, \xi_k)$

and $y = (\eta_1, \eta_2, \ldots, \eta_k)$

is defined to be $\xi_1\eta_1 + \xi_2\eta_2 + \ldots + \xi_k\eta_k$ and will be denoted by x.y.

It can be verified easily that the standard pseudo inner product satisfies the following properties:

(i) $x.y = y.x$ for any $x,y \in V_k(\Sigma)$

(ii) $x.(y+z) = x.y + x.z$

(iii) $(x+y).z = x.z + y.z$

(ii)–(iii) for any $x,y,z \in V_k(\Sigma)$

(iv) $(\mu x).(\theta y) = \mu\theta\, x.y$, $\forall\ \mu.\theta \in \Sigma$ & $\forall\ x,y \in V_k(\Sigma)$

DEFINITION 2.4.2

Two vectors x and y are said to be mutually orthogonal if $x.y = 0$ (Notation $x \perp y$).

DEFINITION 2.4.3

Two lines L and M are said to be mutually orthogonal if $d_L.d_M = 0$ (Notation $L \perp M$).

PROPOSITION 2.4.4

Let L, M and N be lines. If $L \perp M$ and $M \parallel N$ then $L \perp N$.

PROOF

Let $L = a + \Sigma b$; $M = c + \Sigma d$ and $N = e + \Sigma f$.

Since $L \perp M$ hence $b.d = 0$.

$M \parallel N$ means $d \backsim f$ or $d = \theta f$ for some $\theta \in \Sigma$ with $\theta \neq 0$.

Hence $0 = b.d = b.\theta f = \theta\, b.f$, thus $b.f = 0$, since $\theta \neq 0$, which means that $L \perp N$. q.e.d. ■

Contrary to the classical Affine geometry, in AFG(k, p^n) it is not impossible that a line is orthogonal to itself. Such a line is called isotropic. The occurence of such a line is due to the pseudo inner product. It is not caused by the finiteness of the field Σ; neither is it caused by the finiteness of its characteristic. If a pseudo Hilbert space is defined to be a vector space endowed with a pseudo inner product, then such an isotropic line might occur in that space.

A space which contains no isotropic lines is called an anisotropic space. Otherwise it is called isotropic

Let us consider the space AFG(2, 2^1) namely the Affine finite plane of order 2. This plane contains the vector (1, 1) which is orthogonal to itself and hence any line with that direction is isotropic. In general we can state the following:

PROPOSITION 2.4.5

The space AFG(k, p^n) in which $k \geq p$ is isotropic.

PROOF

For k = p it can easily be seen that the vector (1,1,1, . . . ,1,1) is orthogonal to itself, hence any line with that direction is isotropic.

In the space AFG(k, p^n) with $k > p$, any vector of the form (1,0,1,0,0, . . . ,1,0, . . ,1) where p entries are equal to 1 and the others are zero, is orthogonal to itself and hence any line with that direction is isotropic, for the characteristic of GF[p^n] is equal to p, hence

$$(1,0,1,0, \ldots ,1).(1,0,1,0, \ldots ,1) = 1^2 + 1^2 + \ldots + 1^2 = p1 = 0.$$ ■

On the other hand take the plane AFG(2,3^1) = AFG(2,3). The number of distinct directions is equal to

$$\frac{p^{nk} - 1}{p^n - 1} = \frac{3^2 - 1}{3 - 1} = 4.$$

Those directions are represented by the vectors (1,0), (1,1), (1,2) and (0,1) and non of them is orthogonal to itself.

Hence the space AFG(2,3) is anisotropic. So we can make the following statement.

STATEMENT 2.4.6

There do exist anisotropic as well as isotropic spaces.

Sometimes we use synonym perpendicular instead of orthogonal. This is a geometric terminology, while the other is an algebraic one.

Furthermore, in the ordinary Affine geometry no matter the dimension, we have the following theorem:

Given a line L and a point b not on L, there exists one and only one line passing through b and intersecting L perpendicularly.

A question arises whether this theorem is still valid in the Affine finite geometry AFG(k, p^n). The answer will appear to be negative. A short investigation leads to the following result.

THEOREM 2.4.7

Given a line L in AFG(k, p^n) and a point b not on L then

(i) there exists one and only one line passing through b and intersecting L perpendicularly if the line L is anisotropic.

(ii) if L is isotropic then

either

(a) there does not exist a line through b and intersecting L perpendicularly

or

(b) any line passing through b and intersecting L is perpendicular to L.

PROOF

Let L be a line and let b be a point not on L.

Write $L = s + \Sigma t$.

Take a point $x \in L$. Then $x = s + \theta t$ for some $\theta \in \Sigma$.

Further let M be the line passing through x and b.

Then $M = b + \Sigma(b - x) = b + \Sigma(b - (s + \theta t))$.

The direction vector (direction point) of L is t and the direction vector of M is $b - s - \theta t$. For practical reasons let us abbreviate and denote these quantities by d_L and d_M respectively.

Now θ must be chosen in such a way that $M \perp L$. This means that θ must satisfy the equation

$$d_L \cdot d_M = 0 \qquad (*)$$

Hence $t.(b - s - \theta t) = 0$

or $t.b - t.s - \theta t.t = 0$

thus $\theta t.t = t.b - t.s$

(i) If $t.t \neq 0$, which means that $L \not\perp L$ i.e L is anisotropic, then $(t.t)^{-1}$ exists and $\theta = (t.t)^{-1}(t.b - t.s)$ which gives exactly one solution to the problem.

(ii) If $t.t = 0$, meaning that $L \perp L$ i.e L is isotropic, then there are two possibilities:

(a) t.b − t.s ≠ 0

In this case θ does not exist, since equation (*) can not be solved. So the line M does not exist.

(b) t.b − t.s = 0.

In this case any value of θ satisfies equation (*). This means that any line passing through b and intersecting L is perpendicular to L.

Since there are p^n points on L, there are exactly p^n lines passing through b and intercecting L perpendicularly. ■

In comparision with the corresponding theorem in ordinary Affine geometry, this is unexpected and of course not beautiful. It is due to the fact that the pseudo inner product does not necessarily statisfy the property $x.x \neq 0$ when $x \neq \bar{0}$. But in an anisotropic space the corresponding theorem is still valid. So we have the following:

COROLLARY 2.4.8

In an anisotropic space AFG(k, p^n), given a line L and a point b not on L, there exists one and only one line containing b and intersecting L perpendicularly.

EXAMPLES

Example 1

Take the Galois Field Z_5 (the integers modulo 5) and set up the Affine Finite Plane AFG(2,5) = $V_2(Z_5)$. On that plane take the line L = $\Sigma(1,1)$, in which $\Sigma = Z_5$. Further let b be the point (4,0). Clearly b does not lie on L, since L contains only the points (0,0), (1,1), (2,2), (3,3), and (4,4).

Let x be a point on L then $x = \mu(1,1)$. Now let M be the line passing through b and x, then its direction vector $d_M = b - x = (4,0) - \mu(1,1)$. While the direction vector of L is $d_L = (1,1)$. Choose now μ such that $d_M.d_L = 0$.

$$d_M.d_L = \{(4,0) - \mu(1,1)\}.(1,1) = 0,$$

$$\text{or } (4,0).(1,1) - \mu(1,1).(1,1) = 0,$$

$$4 - 2\mu = 0$$

$$2\mu = 4$$

$$\mu = 4(2)^{-1} = 4 \times 3 = 2.$$

Hence $x = 2(1,1) = (2,2)$

Then the line $M = b + \Sigma(b - x) = (4,0) + \Sigma((4,0) - (2,2))$

$$= (4,0) + \Sigma(2, -2)$$

$$= (4,0) + \Sigma(2,3).$$

Since L is anisotropic there exists one and only one line M passing through b and intersecting L perpendicularly.

Example 2

Take again the plane AFG(2,5). Further take the line $L = \Sigma(1,2)$ and the point $b = (2,1)$.

The point b does not lie on L since L contains only the points (0,0), (1,2), (2,4), (3,1) and (4,3). The direction vector of L is (1,2). So L is isotropic.

Let $x \in L$, then x can be written as $x = \theta(1,2)$. Consider the line M passing through b and x. Hence $M = b + \Sigma(b - x)$.

Its direction vector is $d_M = b \quad x = (2,1) - \theta(1,2)$. Now θ must be chosen such that $M \perp L$ or $d_M . d_L = 0$.

$$d_M . d_L = \{(2,1) - \theta(1,2)\} . (1,2) = 0 \qquad (*)$$

Hence θ must be solved from equation (*). After computation it gives

$$\theta\,(1,2).(1,2) = (2,1).(1,2) = 4 \qquad (**)$$

Since $(1,2).(1,2) = 1^2 + 2^2 = 1 + 4 = 0$, while the right hand side of equation (**) is not zero, this equation can not be solved.

Hence according to theorem 2.4.7 there does not exist a line passing through b and intersecting L perpendicularly

Example 3

Let $\Sigma = Z_5$ and consider the space $AFG(3,5) = V_3(\Sigma) = V_3(Z_5)$.
Let L be the line represented by

$L = (2,2,1) + \Sigma(1,2,0)$ and let b be the point (2,2,0).

It can be easily checked that b does not lie on L.

Now we determine a line M passing through b and intersecting L perpendicularly.
Let $x \in L$, hence $x = (2,2,1) + \mu(1,2,0)$ for some $\mu \in \Sigma$. Let M be the line containing both b and x, then

$$\begin{aligned} M &= b + \Sigma(b - x) \\ &= (2,2,0) + \Sigma[(2,2,0) - \{(2,2,1) + \mu(1,2,0)\}] \\ &= (2,2,0) + \Sigma[(0,0,4) - \mu(1,2,0)]. \end{aligned}$$

The direction vector of L is $d_L = (1,2,0)$ and the direction vector of M is $d_M = (0,0,4) - \mu(1,2,0)$.

Choose now μ such that $d_L . d_M = 0 \qquad (***)$

$$\begin{aligned} d_L . d_M &= (1,2,0).[(0,0,4) - \mu(1,2,0)] \\ &= (1,2,0).(0,0,4) - \mu(1,2,0).(1,2,0) \\ &= 0 - \mu 0 = 0 \text{ for any } \mu. \end{aligned}$$

Hence any value of μ satisfies equation (***).

This means that any line passing through b and intersecting L is perpendicular to L. Since there are five points on L, and thus there are five such lines, there exist exactly five lines passing through the point $b = (2,2,0)$ and intersecting the line $L = (2,2,1) + \Sigma(1,2,0)$ perpendicularly.

REMARKS

I. In case $L \perp L$, it seems that the point s from the expression $L = s + \Sigma t$ discussed in the proof of theorem 2.4.7 plays an important role in the determination of the line M. In reality this is not essential.

Since if $t.(b - s) = 0$ then $t.(b - x) = 0$ for any point $x \in L$, for an x on L can be written as

$$x = s + \mu t$$

hence $t.(b - x) = t.(b - (s + \mu t)) =$

$$= t.(b - s) - \mu t.t = 0 - 0 = 0.$$

II. Speaking about isotropic lines, we also have met such a thing in the classical analytic geometry with complex coefficients, namely the line $y = ix$, where $i = \sqrt{-1}$

III. Observing theorem 2.4.7 we can mention a somewhat related situation in a non Euclidean (elliptic) Geometry, i.e the geometry on the sphere.

Given a line L (great circle) and a point b not on L, then there exists one and only one line passing through b and intersecting L perpendicularly, if b is not a pole of L.

However if b is a pole of L, there are infinitely many lines passing through b and intersecting L perpendicularly.

CHAPTER III

THE AFFINE FINITE PLANE AFG(2, p^n)

3.1 Points and lines

We are dealing here with an Affine Finite Geometry of dimension two, namely the geometry AFG(k, p^n) with k = 2. According to a previous theorem the total number of points in the Affine finite plane AFG(2, p^n) is equal to p^{2n}. Further we have the following list about the number of lines.

1. The number of lines through a point is equal to

$$\frac{p^{2n} - 1}{p^n - 1} = p^n + 1$$

2. The number of parallel lines in a given direction is equal to p^n
3. The total number of lines is equal to

$$p^n\left(\frac{p^{2n} - 1}{p^n - 1}\right) = p^n\,(p^n + 1) = p^{2n} + p^n$$

3.2 Parallelism

In general two lines are said to be parallel if they are similar and their intersection is empty. On the plane however we have a special characterization of parallel lines.

THEOREM 3.2.1

Two lines in AFG(2, p^n) are parallel if and only if they do not intersect.

PROOF

(i) necessity:

If $L \parallel M$ then according to the definition of parallelism $L \cap M = \emptyset$.

(ii) sufficiency:

Suppose there are given two lines L and M such that $L \cap M = \emptyset$.

Let $L = q + \Sigma r$ and $M = s + \Sigma t$. Since $L \cap M = \emptyset$, there do not exist scalar μ and θ satisfying the following equation

$$q + \mu r = s + \theta t \qquad (*)$$

This means that the following system of linear equations

$$\left.\begin{aligned} \mu\rho_1 - \theta\tau_1 &= \sigma_1 - \varphi \\ \mu\rho_2 - \theta\tau_2 &= \sigma_2 - \varphi \end{aligned}\right\} \qquad (**)$$

where $q = (\varphi_1, \varphi_2)$; $r = (\rho_1, \rho_2)$; $s = (\sigma_1, \sigma_2)$ and $t = (\tau_1, \tau_2)$ has no solution.

Hence $\begin{vmatrix} \rho_1 & -\tau_1 \\ \rho_2 & -\tau_2 \end{vmatrix} = 0$ or $\rho_1\tau_2 = \rho_2\tau_1$

Since $t = (\tau_1, \tau_2)$ is a direction vector, at least one of the τ_i 's is not zero.

Suppose $\tau_2 \neq 0$. Then we distinguish two cases, i.e $\tau_1 = 0$ and $\tau_1 \neq 0$. In the first case one has

ρ_2 = arbitrary,

and $\rho_1 = 0$.

This means that $r \backsim t$.

The same conclusion will be got by supposing $\tau_1 \neq 0$ and $\tau_2 = 0$

In the second case, where both τ_1 and τ_2 are not zero, we have from $\rho_1\tau_2 = \rho_2\tau_1$ the relation

$$\rho_1\tau_1^{-1} = \rho_2\tau_2^{-1}$$

Putting $\rho_1\tau_1^{\;1} = \rho_2\tau_2^{-1} = \lambda$

one has $\rho_1 = \lambda\tau_1$

and $\rho_2 = \lambda\tau_2$

This means that $r = \lambda t$ or $r \backsim t$.

In any case we have $r \backsim t$. Thus $L \backsim M$. Since $L \cap M = \phi$, we have $L \mathbin{/\!/} M$. ∎

3.3 Orthogonality

In the previous chapter, we discussed the determination of a line M passing through a point b not on a given line L and intersecting L perpendicularly. Such a line always exists if the line L is anisotropic. In that case M is unique. If L is isotropic such a line might not exist. In the case k = 2 we can state the following theorem.

THEOREM 3.3.1

Given a line L on AFG(2, p^n) and a point b there exists one and only one line passing through b and perpendicular to L.

PROOF

Let L be a line on AFG(2, p^n) and let b be a point.

Write $L = s + \Sigma t = (\sigma_1, \sigma_2) + \Sigma\,(\tau_1, \tau_2)$.

Let M be a line through b, then M can be written as:

$$M = b + \Sigma m = (\beta_1, \beta_2) + \Sigma(\mu_1, \mu_2)$$

Choose m such that m.t = 0.

This is an equation in two unknowns which is linear and homogenous. Up to similarity its solution is unique. This completes the proof of our theorem, since two similar lines with a point in common coincide (see Lemma 2.1.12) ∎

Such a line always exists, even if L is isotropic. In that case M coincides with L if b is on L, while if b is not on L then M // L, so the line M does not intersect L.

If b is not on L, we have a special case of theorem 2.4.7 with k = 2. As a consequence of this theorem we have the following theorem on the plane.

THEOREM 3.3.2

If a line L is anisotropic and M is a line perpendicular to L then M intersects L.

PROOF

Assume $L \cap M = \phi$. Then according to theorem 3.2.1 L // M. This means that the direction vectors of L and M are similar. Let d_L and d_M be the direction vectors of L and M respectively, then $d_L \backsim d_M$ or $d_M = \theta d_L$ for some $\theta \in \Sigma$.

But $L \perp M$, hence

$$d_L . d_M = 0$$

$$\text{or} \quad d_L . (\theta d_L) = \theta\, d_L . d_L = 0$$

Since $\theta \neq 0$, one has $d_L . d_L = 0$, which means that L is isotropic. This contradicts our hypothesis and completes the proof of our theorem. ■

Theorem 3.3.1 which sounds like one of the fundamental theorems in the ordinary Affine plane might have been expected to be true.

PROPOSITION 3.3.3

If $L \perp M$ and $L \perp N$ and $M \neq N$ then M // N.

PROOF

Let $L = a + \Sigma b$,

$M = c + \Sigma d$

and $N = e + \Sigma f$.

$L \perp M$ leads to b.d = 0

$L \perp N$ leads to b.f = 0

Further put $b = (\beta_1, \beta_2)$; $d = (\delta_1, \delta_2)$ and $f = (\varphi_1, \varphi_2)$.

Then b.d = 0 leads to $\beta_1\delta_1 + \beta_2\delta_2 = 0$ (I)

and b.f = 0 leads to $\beta_1\varphi_1 + \beta_2\varphi_2 = 0$ (II)

Since b is direction vector, then at least one of the β_i's, say β_2, is not zero. After multiplying equation II by δ_1 and equation I by φ_1 we have:

$$\beta_1\delta_1\varphi_1 + \beta_2\delta_2\varphi_1 = 0 \qquad \text{(Ia)}$$

$$\beta_1\varphi_1\delta_1 + \beta_2\varphi_2\delta_1 = 0 \qquad \text{(IIa)}$$

Subtracting equation Ia from equation IIa we get:

$$\beta_2\delta_2\varphi_1 = \beta_2\varphi_2\delta_1.$$

From $\beta_2 \neq 0$ we conclude that:

$$\delta_2\varphi_1 = \varphi_2\delta_1$$

Consider three cases:

(i) $\delta_1 = 0$;

(ii) $\delta_2 = 0$;

(iii) both δ_1 and δ_2 are unequal zero.

(δ_1 and δ_2 cannot both zero simultaneously, since $d = (\delta_1, \delta_2)$ is a direction vector).

In case (i) we have $\varphi_1 = 0$ and φ_2 arbitrary.

This means that $d \backsim f$. Hence $M \mathbin{/\!/} N$, since $M \neq N$.

In case (ii) we have $\varphi_2 = 0$ and φ_1 arbitrary which means $M \mathbin{/\!/} N$ similarly.

In case (iii) we have:

$$\varphi_1\delta_1^{-1} = \varphi_2\delta_2^{-1}$$

Putting

$$\varphi_1\delta_1^{-1} = \varphi_2\delta_2^{-1} = \theta$$

we get $\varphi_1 = \theta\delta_1$ and $\varphi_2 = \theta\delta_2$

which means $f = \theta d$ hence $f \backsim d$ and $N \mathbin{/\!/} M$. ■

This proposition which can be considered as the converse of proposition 2.4.4 is no longer true in spaces of dimension higher than two.

3.4 Illustrations

To get a more concrete picture of these finite geometries, we can draw a diagram of such a geometry by plotting all the points, especially for the Affine finite plane. In fact those points may be plotted arbitrarily without any arrangement. Then a real line can be drawn through points which lie on one line.

But if we plot those points in a square array some advantages will be gained. It can be seen easily for instance how many lines go through one point, how many lines there are in a given direction, what is the total number of lines, whether two lines are prependicular a.s.o. It looks like a coordinate system (Cartesian coordinate system) in $\mathbf{R}^2$.

ILLUSTRATION 1

The plane AFG(2, 2) contains 4 points and six lines. There are three lines through each point and in a given direction there are two lines. See figure 1a, 1b and figure 2.

figure 1 a

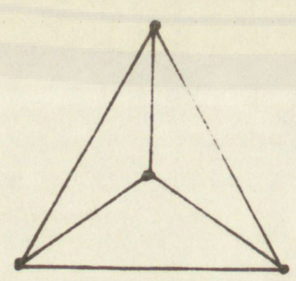


figure 1 b

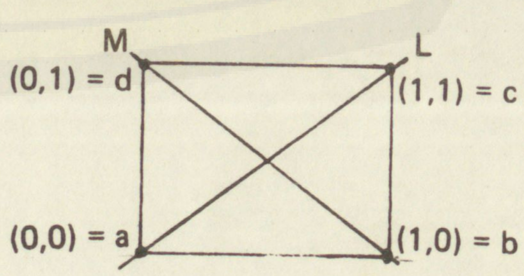


figure 2

The plane AFG(2, 2) = $V_2(Z_2)$ where Z_2 is the field of integers module 2.

Let $Z_2 = \{0.1\} = \Sigma$ and call the points (0, 0) = a; (0, 1) = d; (1, 1) = c and (1, 0) = b. Further call the line ac = L. then we have $L = \Sigma c = \Sigma(1, 1) = \{(0, 0), (1, 1)\} = \{a, c\}$. Call the line bd = M, then $M = d + \Sigma(b - d) = (0, 1) + \Sigma(1, 1) = \{(0, 1), (1, 0)\} = \{d, b\}$. L and M are parallel but mutually orthogonal, since they do not intersect and $d_L . d_M = c.c = (1, 1).(1, 0)] = 0$.

Here k = 2; p = 2 and n = 1. therefore

(i) the total number of points is equal to $2^2 = 4$;

(ii) the total number of lines through one point is equal to

$$\frac{p^{nk} - 1}{p^n - 1} = \frac{2^2 - 1}{2 - 1} = 3.$$

(iii) the number of lines = $p^{n(k-1)} \left(\frac{p^{nk} - 1}{p^n - 1} \right) = 2.3 = 6$,

(iv) the number of parallel lines in a given direction is equal to $p^{n(k-1)} = 2$

ILLUSTRATION 2

Take the Galois Field $\Sigma = GF[3^1] = Z_3$ = the field of integers module 3 and set up the finite geometry AFG(2, 3) = $V_2(Z_3)$, i.e the Affine finite plane of order 3.

Here k = 2, p = 3 and n = 1. After computation we have:

(i) the number of points = 9;

(ii) the number of lines through one points = 4;

(iii) the number of parallel lines in a given direction = 3;

(iv) total number of lines = 12.

See figure 3. Call (0, 0) = o then on figure 3 we can see the four lines through o. They are

$K = \Sigma(0, 1) = \{(0, 0), (0, 1), (0, 2)\}$.

$L = \Sigma(1, 1) = \{(0, 0), (1, 1), (2, 2)\}$;

$M = \Sigma(2, 1) = \{(0, 0), (2, 1), (1, 2)\}$;

and $N = \Sigma(1, 0) = \{(0, 0), (1, 0), (2, 0)\}$.

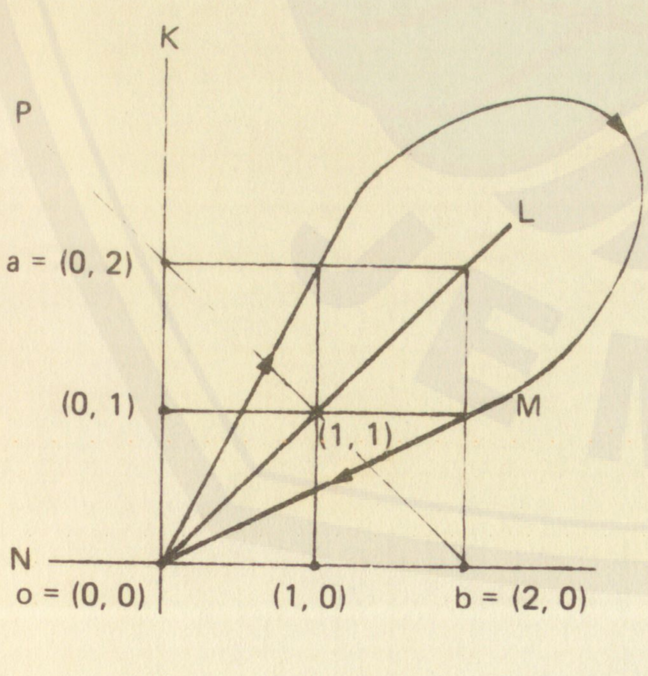


figure 3

Further the line P through a = (0, 2) and b = (2, 0) can be written as:

$$P = a + \Sigma(b - a) = (0, 2) + \Sigma(2, -2) =$$
$$= (0, 2) + \Sigma(2, 1)$$
$$= \{(0, 2), (1, 1), (2, 0)\}.$$

On the other hand P // M, since they do not intersect (according to theorem 3.2.1). In fact direction vectors are $d_P = (2, 1)$ and $d_M = (2, 1)$ respectively.

Furthermore P ⊥ L, since $d_P . d_L = (2, 1). (1, 1) = 0$.

Looking at figure 3 it seems that P is "really" perpendicular to L. On figure 4 it can be seen the three parallel lines in the direction (1, 1), namely the lines L, R and S.

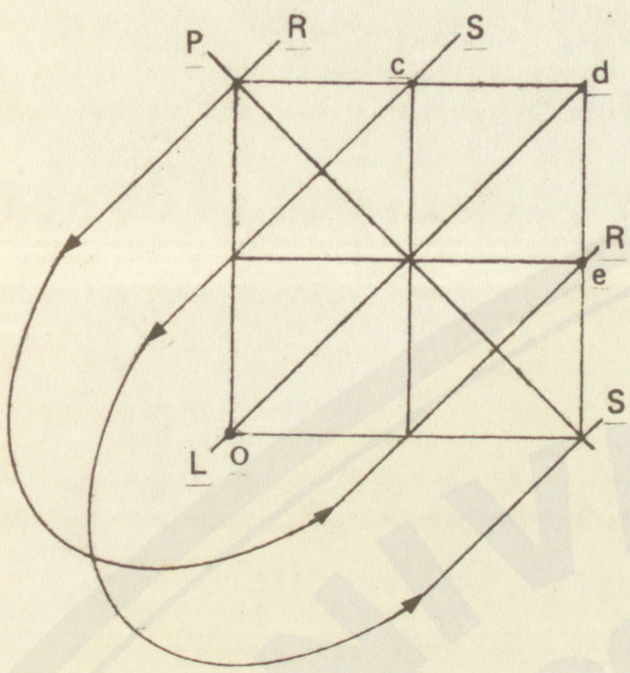


figure 4

As we have seen before, the Affine finite plane AFG(2, 3) is anisotropic. So given a line and a point not on that line, there always exists a line through that point and intersecting the given line perpendicularly.

Let us take the line P in figure 4 and the points

c = (1, 2), d = (2, 2) and e = (2, 1)

No one of these points lies on P. Then :

* S is the line through c and intersecting P perpendicularly.;

** L is the line passing through d and intersecting P perpendicularly;

*** R is the line passing through e and intersecting P perpendicularly.

ILLUSTRATION 3

Take the Galois Field $\Sigma = GF[2^2]$ obtaining from Z_2 by root adjunction of the equation $x^2 + x + 1 = 0$. If one of the roots is called θ we have :

$$\Sigma = GF[2^2] = \{0, 1, \theta, \theta + 1\}.$$

Build up the Affine finite plane $AFG(2, 2^2) = V_2(\Sigma)$.

See figure 5.

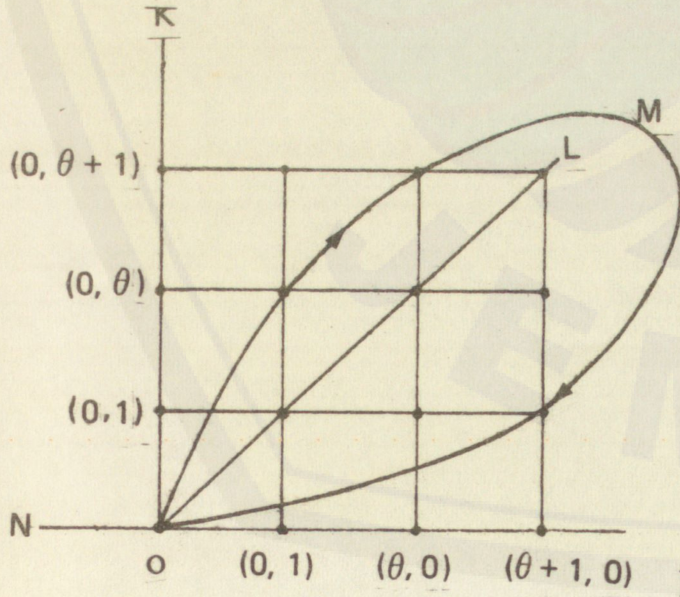


figure 5

There are 16 points on this plane. Through each point there are $2^2 + 1 = 5$ lines.

In a given direction there are 4 parallel lines and the total number of lines is equal to

$2^4 + 2^2 = 20$.

Let L be the line $\Sigma(1, 1)$. It is isotropic. Through each point outside L there does not exist a line which intersect L perpendicularly.

Through o = (0, 0) there are five lines, namely the lines

$K = \Sigma(0, 1)$; $L = \Sigma(1, 1)$; $M = \Sigma(1, \theta)$;

$N = \Sigma(1, 0)$; and $P = \Sigma(\theta, 1)$.

Only four of them are drawn in figure 5. The line P is not drawn in the figure. It can be seen in this figure that $M = \Sigma(1, \theta)$ contains the points

(0, 0), (1, θ), (θ, θ + 1) and (θ + 1, 1);

while K = Σ(0, 1) contains the points (0, 0), (0, 1), (0, θ), (0, θ + 1);

L = Σ(1, 1) contains the points (0, 0), (1, 1), (θ, θ) and (θ + 1, θ + 1);

N = Σ(1, 0) contains the points (0, 0), (1, 0), (θ, 0), (θ + 1, 0);

and P = Σ(θ, 1) contains the points (0, 0), (θ, 1), (θ + 1, θ) and (1, θ + 1).

3.5 A note on theorem 2.4.7

From theorem 2.4.7 it is known that in AFG(k, p^n) if L is an anisotropic line, and b a point not lying on L, then there exists one and only one line through b and intersecting L perpendicularly.

If L is isotropic and b a point not lying on L, then either there does not exist a line through b and intersecting L perpendicularly or any line passing through b and intersecting L is perpendicular to L. This is true for k $\neq$ 2. But on the plane we have only one possibility, which can be stated as follows :

THEOREM 3.5.1

Given an isotropic line on the Affine finite plane AFG(2, p^n) and a point b not lying on L, then there does not exist a line passing through b and intersecting L perpendicularly.

PROOF

According to theorem 3.3.1 there exists one and only one line passing through b and perpendicular to L. Let M be the unique line given by the theorem. It remains to be proved that M does not intersect L.

Since b $\notin$ L and b $\in$ M we have M $\neq$ L. By hypotesis L $\perp$ L then we have

L $\perp$ L

L $\perp$ M

Hence on account of L $\neq$ M one has, according to theorem 3.3.3, the property L // M. Therefore L $\cap$ M = $\emptyset$, or M does not intersect L. Since M is the only line perpendicular to L, this means that there does not exist a line through b and intersecting L perpendicularly ■

CHAPTER V

TRANSFORMATIONS

5.1 Translations

Take the vector space $V_k(\Sigma)$, where Σ is a Galois Field GF$[p^n]$. For shortness we use the notation Σ^k instead of $V_k(\Sigma)$.

Consider this space as an Affine finite geometry of dimension k, namely AFG(k, p^n).

A mapping $f : \Sigma^k \longrightarrow \Sigma^k$ of the form $f(x) = x + a$, in which a is a fixed vector is called a translation in AFG(k, p^n). If we denote such a translation by T_a, then we have

$T_a : x \longmapsto x + a.$

The set of all translations under succesive mapping forms an abelian group, which is obviously nothing but the left (or right) regular representation of the additive group $(\Sigma^k, +)$.

Hence we have the following theorem.

THEOREM 5.1.1

The set of all translations in AFG(k, p^n) under succesive mapping forms a group which is isomorphic to the additive group $(\Sigma^k, +)$.

THEOREM 5.1.2

Under a translation a line is transformed either into a parallel line or into itself.

PROOF

Let L be a line and let T_a be a translation. Since L is a line. it can be represented by:

$L = s + \Sigma q$, with $q \neq \bar{0}$;

this means

$L = \{ s + \theta q \mid \theta \in \Sigma \}.$

$$\begin{aligned} \text{Hence } T_a(L) &= \{(s + \theta q) + a \mid \theta \in \Sigma\} \\ &= \{(s + a) + \theta q \mid \theta \in \Sigma\} \\ &= (s + a) + \Sigma q \ , \end{aligned}$$

and this is a representation of a line, with direction vector q. Therefore $T_a(L)$ is either a line parallel to L or the line L itself. ∎

Clearly if $a \backsim d_L$ then $T_a(L) = L$ and if $a \not\backsim d_L$ then $T_a(L) \,/\!/\, L$.

THEOREM 5.1.3

If L and M are two lines such that $L \perp M$ and T a translation then $T(L) \perp T(M)$.

PROOF

This is obvious, since under a translation the direction vector of a line does not change ■

REMARK

In AFG(k, p^n) with $k > 3$, a plane can be defined in a way similar to what we have done in AFG(3, p^n) namely as follows:
A subset Λ of AFG(k, p^n) is said to be a plane if there exist a, b, c $\in$ AFG(k, p^n) with $b \neq \bar{0}$, $c \neq \bar{0}$ and b $\not\sim$ c such that $\Lambda = a + \Sigma b + \Sigma c$.

Then it can be shown easily that under a translation a plane is carried either into another parallel plane or into itself.

5.2 Linear transformations

The space AFG(k, p^n) is the vector space $V_k(\Sigma) = \Sigma^k$.
Hence a linear transformation in AFG(k, p^n) is a linear transformation in $V_k(\Sigma)$. Such a transformation can be represented by a $k \times k$ matrix with entries in Σ.

We are dealing here with finite sets. Therefore any injective mapping is surely surjective and thus bijective. In this case the adjectives injective, surjective and bijective are equivalent.

DEFINITION 5 2.1

An injective linear transformation in AFG(k, p^n) is called nonsingular.

THEOREM 5.2.2

The set of all nonsingular transformations in AFG(k, p^n) constitutes a group under successive mapping. This group is called the full linear groups and is detoned by $\mathcal{L}_k(\Sigma)$.

PROOF

The set of all bijective mapping from Σ^k onto itself under successive mapping constitutes a group. which is called the group of transformations of AFG (k, p^n).
Let us call this group $\mathcal{G}$, then it is sufficient to prove that $\mathcal{L}_k(\Sigma)$ is a subgroup of $\mathcal{G}$.

Let f, g $\in \mathcal{L}_k(\Sigma)$, then for any x, y $\in \Sigma^k$ and any $\alpha, \beta \in \Sigma$ we have

$$\begin{aligned}(fg)(\alpha x + \beta y) &= f[g(\alpha x + \beta y)] = f[\alpha g(x) + \beta g(y)], \text{ since g is linear}\\ &= \alpha f[g(x)] + \beta f[g(y)], \text{ since f is linear,}\\ &= \alpha(fg)(x) + \beta(fg)(y).\end{aligned}$$

Therefore $fg \in \mathcal{L}_k(\Sigma)$.

Further we want to show that $f^{-1} \in \mathcal{L}_k(\Sigma)$ whenever $f \in \mathcal{L}_k(\Sigma)$ by showing that $f^{-1}(\mu x + \theta y) = \mu f^{-1}(x) + \theta f^{-1}(y)$ for any $x, y \in \Sigma^k$ and any $\mu, \theta \in \Sigma$.

Take the element $\mu f^{-1}(x) + \theta f^{-1}(y)$ and consider $f\{\mu f^{-1}(x) + \theta f^{-1}(y)\}$.
Since f is ~~linear~~, $f\{\mu f^{-1}(x) + \theta f^{-1}(y)\} = \mu ff^{-1}(x) + \theta ff^{-1}(y) =$

$= \mu I(x) + \theta I(y)$ where I is the identity map,

$= \mu x + \theta y$.

Hence $f^{-1}(\mu x + \theta y) = f^{-1}[f\{\mu f^{-1}(x) + \theta f^{-1}(y)\}] =$

$= I\{\mu f^{-1}(x) + \theta f^{-1}(y)\}$

$= \mu f^{-1}(x) + \theta f^{-1}(y)$

This means that

$f^{-1} \in \mathcal{L}_k(\Sigma)$ whenever $f \in \mathcal{L}_k(\Sigma)$.

Hence $\mathcal{L}_k(\Sigma)$ is a subgroup of $\mathcal{G}$. ■

NOTE

This theorem is well known. Further more the full linear group $\mathcal{L}_k(\Sigma)$ is isomorphic to the group of all nonsingular $k \times k$ matrices with entries in Σ.
This is the reason why this group is denoted by

$\mathcal{L}_k(\Sigma)$.

5.3 Affine Transformations

A nonsingular linear transformation followed by a translation is called an affine transformation. If T is a linear transformation and a a fixed vector in $V_k(\Sigma)$, then an affine transformation is a mapping of the form:

$f(x) = T(x) + a$.

Affine transformations include the nonsingular linear transformations (a = 0) as well as all translations, namely an affine transformation in which T is the identity mapping. The following theorem is also well known in the ordinary Affine Geometry.

THEOREM 5.3.1

The set of all affine transformations in AFG(k, p^n) constitutes a group, called the affine group and it is denoted by $\mathcal{A}_k(\Sigma)$. It contains as subgroups the full linear group and the group of translations.

PROOF

Let f and g be two affine transformations. Then each of them is a mapping of the form

$$f(x) = T(x) + a$$

and

$$g(x) = S(x) + b$$

where T and S are nonsingular linear transformations.

Hence, by using column matrix notation for vectors, we have

$$\begin{aligned}(fg)(x) &= f(S(x) + b) = T(S(x) + b) + a \\ &= T(S(x)) + T(b) + a \\ &= (TS)(x) + T(b) + a.\end{aligned}$$

So the product of two affine transformations is an affine transformation.

Furthermore the inverse of an affine tranformation is also an affine transformation. In fact if $y = f(x)$, where $f \in \mathcal{A}_k(\Sigma)$,
then $y = T(x) + a$,
hence $x = T^{-1}(y - a) = T^{-1}(y) - T^{-1}(a)$
and this means that $f^{-1} \in \mathcal{A}_k(\Sigma)$.

The group of translations in 5.1 is also called the translation group. It is denoted by $\mathcal{T}(\Sigma^k)$.

THEOREM 5.3.2

The translation group is a normal subgroup of the affine group.

PROOF

Clearly it is a subgroup.

Further let $f \in \mathcal{A}_k(\Sigma)$ and $g \in \mathcal{T}(\Sigma^k)$, then f is mapping of the form $f(x) = T(x) + a$ and g is a mapping of the form $g(x) = x + b$.

$$\begin{aligned}(fgf^{-1})(x) &= (fg)f^{-1}(x) = (fg)(T^{-1}(x) - T^{-1}(a)) \\ &= f(T^{-1}(x) - T^{-1}(a) + b) \\ &= T(T^{-1}(x) - T^{-1}(a) + b) + a \\ &= x - a + T(b) + a = x + T(b).\end{aligned}$$

Hence fgf^{-1} is a translation. This completes the proof. ■

THEOREM 5.3.3

$\mathcal{L}_k(\Sigma) \cong \mathcal{A}_k(\Sigma)/\mathcal{T}(\Sigma^k)$

PROOF

Define a mapping ψ from $\mathcal{A}_k(\Sigma)$ into $\mathcal{L}_k(\Sigma)$ as follows:
if $f \in \mathcal{A}_k(\Sigma)$, then f is of the form

$f(x) = T(x) + b$;

now put $\psi(f) = T$

Surely ψ is surjective. It remains to be proved that ψ is homomorphic.
Let f, $g \in \mathcal{A}_k(\Sigma)$ then there exist T, $S \in \mathcal{L}_k(\Sigma)$ and a, $b \in \Sigma^k$ such that

$$f(x) = T(x) + a$$

and $g(x) = S(x) + b$.
Then from $(fg)(x) = f(S(x) + b) = T(S(x) + b) + a =$

$$= TS(x) + T(b) + a,$$

one concludes $\psi(fg) = TS = \psi(f) \cdot \psi(g)$.
For the kernel of ψ one has

Kern $\psi = \{ f \in \mathcal{A}_k(\Sigma) \mid \psi(f) = I \}$, where I is the identity mapping. This means that f is a translation. So we have

Kern $\psi = T(\Sigma^k)$,

hence $\mathcal{L}_k(\Sigma) \cong \mathcal{A}_k(\Sigma)/T(\Sigma^k)$. ■

The full linear group $\mathcal{L}_k(\Sigma)$ is isomorphic to the group of all nonsingular $k \times k$ matrices with entries in Σ.
It is known from linear algebra [13] that the number of all nonsingular $k \times k$ matrices with entries from a field Σ with q element is equal to

$$(q^k - 1)(q^k - q)(q^k - q^2) \ldots (q^k - q^{k-1}).$$

Here we have $q = p^n$. Hence the order of the full linear group $\mathcal{L}_k(\Sigma)$ is.

$$(p^{nk} - 1)(p^{nk} - p^n)(p^{nk} - p^{2n}) \ldots (p^{nk} - p^{n(k-1)}).$$

COROLLARY 5.3.4

The order of the affine group $\mathcal{A}_k(\Sigma)$ is equal to the product of the order of the translation group $T(\Sigma^k)$ and the order of the full linear group $\mathcal{L}_k(\Sigma)$, and therefore equal to

$$p^{nk}(p^{nk} - 1)(p^{nk} - p^n)(p^{nk} - p^{2n}) \ldots (p^{nk} - p^{n(k-1)}).$$

5.4 Isometry

In abstract algebra we have the concept of isomorphy. Two algebraic structures are said to be isomorphic if there exists a bijective mapping from the first structure onto the second one which preserves all operations.

In geometry we have the concept of isometry. We define this notion as follows:

DEFINITION 5.4.1

A geometry G_1 is said to be isometric to a geometry G_2 if there exists a bijective mapping f from G_1 onto G_2, such that if L is a line in G_1 then f(L) is a line in G_2.

THEOREM 5.4.2

Any plane in AFG(3, p^n) is isometric to the geometry AFG(2, p^n).

PROOF

Let Λ be a plane in AFG(3, p^n). So Λ can be represented by:

$$\Lambda = a + \Sigma b + \Sigma c, \text{ where } b \neq \bar{0};$$
$$c \neq \bar{0} \text{ and } b \not\sim c.$$

Define the mapping

$$f : \Lambda \longrightarrow AFG(2, p^n) \text{ as follows:}$$
$$f(a + \theta b + \mu c) = \theta(1, 0) + \mu(0, 1).$$

Then it remains to be proved that:

(i) f is surjective,

(ii) f is injective,

(iii) f transforms a line into a line.

(i) Clearly f is surjective, since given any point $x \in AFG(2, p^n)$ then $x = \alpha(1, 0) + \beta(0, 1)$. Hence $\alpha b + \beta c$ is one of its pre-images.

(ii) Suppose that $f(x) = f(y)$

and let $x = a + \theta_1 b + \mu_1 c$,

$y = a + \theta_2 b + \mu_2 c$.

Then $f(x) = \theta_1(1, 0) + \mu_1(0, 1)$

and $f(y) = \theta_2(1, 0) + \mu_2(0, 1)$,

hence $\theta_1(1, 0) + \mu_1(0, 1) = \theta_2(1, 0) + \mu_2(0, 1)$.

Since (1, 0) and (0 1) are linearly independent this implies that

$\theta_1 = \theta_2$ and $\mu_1 = \mu_2$

hence x = y, thus f is injective.

(iii) Let L be a line in Λ. Then it can be represented by

$$L = a + \mu_1 b + \mu_2 c + \Sigma(\theta_1 b + \theta_2 c)$$

with rank $(\theta_1 \quad \theta_2) \neq 0$

Then for any $\sigma \in \Sigma$ one has

$$f[a + \mu_1 b + \mu_2 c + \sigma(\theta_1 b + \theta_2 c)] = f[a + (\mu_1 + \sigma\theta_1)b + (\mu_2 + \sigma\theta_2)c]$$
$$= (\mu_1 + \sigma\theta_1)(1, 0) + (\mu_2 + \sigma\theta_2)(0, 1) = \mu_1(1, 0) + \mu_2(0, 1) + \sigma(\theta_1(1, 0) + \theta_2(0, 1)),$$

i.e $f(L) = \mu_1(1,0) + \mu_2(0, 1) + \Sigma(\theta_1(1, 0) + \theta_2(0, 1))$.

Hence f(L) is a line in AFG(2, p^n) since rank $(\theta_1 \quad \theta_2) \neq 0$.

Therefore Λ is isometric to AFG(2, p^n). ■

It can be seen easily that isometry is an equivalence relation.

A plane in AFG(3, p^n) is also called a subgeometry of AFG(3, p^n).

CHAPTER VI

THE PROJECTIVE FINITE PLANE PFG(2, p^n)

6.1 The geometry PFG(2, p^n)

In this chapter we want to give the idea of projective finite planes, i.e projective finite geometries of dimension two which can be built up from 3-dimensional Affine Finite geometries, namely AFG(3, p^n).

Starting with a 3-dimensional Affine finite geometry AFG(3, p^n) we build up a new geometry by defining points and lines in the following way.

DEFINITION 6.1.1

Any line through the point o (zero vector) in AFG(3, p^n) is called a point.

DEFINITION 6.1.2

Any plane in AFG(3, p^n) through the point o (zero vector) is called a line.

We call this new geometry a projective finite geometry of dimension two or a projective finite plane and denote it by PFG(2, p^n), a geometry in which the underlying set is $V_3(\Sigma)$. In fact considered as a vector space we have

PFG(2, p^n) = AFG(3, p^n).

It will be shown that the fundamental theorem and the principle of duality are valid in this new geometry.

6.2 Some theorems in PFG(2, p^n)

Two lines in PFG(2, p^n) are two planes in AFG(3, p^n) which are passing through the point o. Since the intersection of two different planes is a line, we can state the fundamental theorem in the plane PFG(2, p^n) as follows:

THEOREM 6.2.1

Two different lines in PFG(2, p^n) intersect in one and only one point.

On the other hand, according to corollary 4.2.13 we have the following.

THEOREM 6.2.2

Given two different points in PFG(2, p^n) there exists one and only one line containing both points.

Furthermore the total number of points in PFG(2, p^n) is equal to the number of lines in AFG(3, p^n) passing through one point.

Hence we can state the following.

THEOREM 6.2.3

The total number of points in PFG(2, p^n) is equal to $p^{2n} + p^n + 1$.
Apply theorem 2.3.1 with $k = 3$. ■

Since the number of lines in PFG(2, p^n) is equal to the number of planes through one point AFG(3, p^n) we can state

THEOREM 6.2.4

The total number of lines in PFG(2, p^n) is equal to $p^{2n} + p^n + 1$.
See theorem 4.7.6. ■

To determine the total number of points on a line, we look back to corollary 4.2.7. The total number of points on a line in PFG(2, p^n) is equal to the total number of lines in a plane through one point in the Affine space AFG(3, p^n). So we can state

THEOREM 6.2.5

Each line in PFG(2, p^n) contains $p^n + 1$ points.
See corollary 4.2.7 as it is stated before. ■

Finally the total number of lines through one point in the plane PFG(2, p^n) is equal to the total number of planes through one line in the space AFG(3, p^n). Then according to theorem 4.7.5 we can state the following.

THEOREM 6.2.6

Through each point in PFG(2, p^n) there are exactly $p^n + 1$ lines. ■

Using the word "incident", the principle of duality can be easily formulated. It says that interchanging the words "point" and "line" in a true statement gives another true statement. The latter is called the dual statement of the former and vice versa. The following list of statements will show this.

STATEMENT 6.2.7

a. Two points are incident with exactly one line.
b. Two lines are incident with exactly one point.
c. Incident with one point there are exactly $p^n + 1$ lines.
d. Incident with one line there are exactly $p^n + 1$ points.
e. The total number of points is equal to $p^{2n} + p^n + 1$.
f. The total number of lines is equal to $p^{2n} + p^n + 1$. ■

REMARK

We have defined points in PFG(2, p^n) to be one-dimensional subspaces of $V_3(\Sigma)$. While lines are defined to be two-dimensional subspaces of $V_3(\Sigma)$.

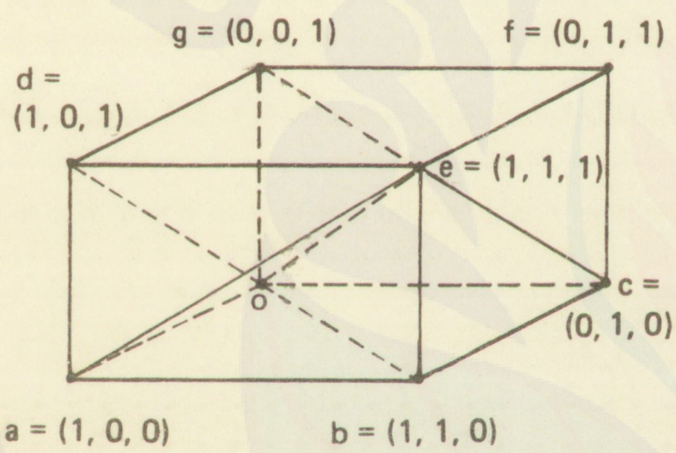
The role of the origin (the zero vector) is not essential here. We may take an arbitrary point in AFG(3, p^n) not necessarily the point zero and define points to be lines through that point, while lines can be defined to be planes through that point. Then all theorems remain valid.

6.3 An Example of PFG(2, p^n)

The famous seven points geometry can be represented by the projective finite plane PFG(2, 2). Consider as a vector space we have in fact

PFG(2, 2) = AFG(3, 2) = V_3(GF[2])

In this geometry there are $2^2 + 2^1 + 1 = 7$ points and also 7 lines. Each line contains $2^1 + 1 = 3$ points and through each point there are three lines. See figure 12 as an illustration.



figufe 12

Consider the space AFG(3, 2). It consists of the points o = (0, 0, 0); a = (1, 0, 0); b = (1, 1, 0); c = (0, 1, 0); d = (1, 0, 1); e = (1, 1, 1); f = (0, 1, 1) and g = (0, 0, 1).

The points in PFG(2, 2) are the lines in AFG(3, 2) passing through the point o. These are the lines oa, ob, oc, od, oe, of and og. Seven in number.

Moreover the lines in PFG(2, 2) are the planes in AFG(3, 2) passing through o. Those are oadg, oabc, ocfg, obeg and the other three planes are obdf. odec, and oaef, also seven in number. Each line in PFG(2, 2) contains 3 points, which means that each plane through o in AFG(3, 2) contains three lines through o.

From the figure one sees easily the existence of the six planes oadg, oabc, ocfg, odec and oaef. Further the point f lies in the plane obd.

Since the plane obd can be represented by

$$obd = \Sigma b + \Sigma d = \{o, b, d, d + b = f\},$$

hence the points o, b, d, and f lie in one plane, the seventh plane through o in our geometry, i.e the geometry AFG(3, 2).

Through each point there are three lines in PFG(2, 2), which means that through any line in AFG(3, 2) containing o, there are three planes. For example through the line og we have the planes oadg, obeg, and ocfg. A similar fact can also be seen easily for the planes through oa, through oc and through oe.

But not so easy for the lines od, of and ob. For example the planes through od are oadg, odec and last but not least odbf.
(see the determination of all points in the plane obd!).

GENERAL REMARKS

1. Midpoint in AFG(k, p^n)

Without using the concept of a distance, the midpoint of two points in the Affine finite geometry AFG(k, p^n) can be defined provided that $p \neq 2$.

Let a and b be two points in AFG(k, p^n) where $p \neq 2$. The point $(1 + 1)^{-1}(a + b)$ is called the midpoint of a and b.

Something which should be expected is the following statement.

If a and b are two distinct points, then the midpoint of a and b is lying on the line through a and b.

In fact this statement is true, since the line passing through a and b can be represented by $a + \Sigma(b - a)$, while their midpoint is $(1 + 1)^{-1}(a + b) = 2^{-1}(a + b) = 2^{-1}a + 2^{-1}b$ (by using the symbol 2 for 1 + 1), which can be written in the form $a + \mu(b - a)$ with $\mu = 2^{-1}$, since

$$a + 2^{-1}(b - a) = a + 2^{-1}b - 2^{-1}a = (1 - 2^{-1})a + 2^{-1}b = (2.2^{-1} - 2^{-1})a + 2^{-1}b =$$
$$= 2^{-1}(2 - 1)a + 2^{-1}b = 2^{-1}a + 2^{-1}b = 2^{-1}(a + b) = (1 + 1)^{-1}(a + b).$$

Furthermore we can state following theorem similar to the one we have had in the ordinary Affine geometry:

If a, b and c are non collinear points in AFG(k, p^n) with $p \neq 2$ and m_{ac} is the midpoint of a and c. then abcd is a parallelogram if and only if m_{ac} is the midpoint m_{bd} of b and d.

Only the sufficient condition will be proved here.

Let d be the point satisfying the condition stated in the theorem, then

$$m_{ac} = 2^{-1}(a + c) = m_{bd} = 2^{-1}(b + d).$$

Hence

$$2^{-1}d = 2^{-1}a + 2^{-1}c - 2^{-1}b,$$

therefore

$$d = a + c - b.$$

Then it remains to be proved that the line L_{ad}, i.e the line passing through a and d is parallel to L_{bc} (the line passing through b and c) and L_{ab} is parallel to L_{dc}.

Clearly this is true since the direction vector of $L_{ad} = d - a = c - b$ and the direction vector of $L_{bc} = c - b$.

Similarly the direction vector of L_{ab} is similar to the direction vector of L_{dc}. QED.

COROLLARY

The diagonals of a parallelogram in AFG(k, 2^n) do not intersect.

To illustrate what is going on, let us consider figure 13.

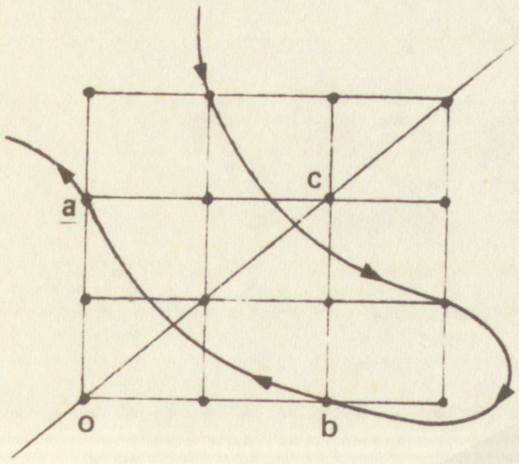


figure 13

Consider the plane AFG(2, 2^2), where the Galois Field $\Sigma = GF[2^2]$ can be obtained from Z_2 by root adjunction of the equation $x^2 + x + 1 = 0$. If one of its roots is called μ, we have

$$\Sigma = \{0, 1, \mu, \mu + 1\}.$$

Take the points $o = (0, 0)$; $b = (\mu, 0)$ and $a = (0, \mu)$. The vertex c of the parallelogram oacb can be found by determining the intersection of the line L passing through a and parallel to ob and the line M passing through b and parallel to oa. After computation we obtain $c = (\mu, \mu)$.

Here the diagonals oc and ab do not intersect, since

$ab = a + \Sigma(b - a) = (0, \mu) + \Sigma(\mu, -\mu) = (0, \mu) + \Sigma(\mu, \mu) =$
$= (0, \mu) + \Sigma(1, 1)$, which contains the points
$(0, \mu)$, $(1, \mu + 1)$, $(\mu, 0)$ and $(\mu + 1, 1)$ while the line $oc = \Sigma c = \Sigma(\mu, \mu) =$
$= \Sigma(1, 1)$ contains 4 other points i.e $(0, 0)$, $(1, 1)$, (μ, μ) and $(\mu + 1, \mu + 1)$.

In figure 13, if we draw a straight line through a and b, it seems that the diagonals oc and ab intersect at the point (1, 1).

As a second example consider figure 13a. In the plane AFG(2, 5) take the points $o = (0, 0)$; $q = (3, 0)$ $r = (3, 3)$ and $s = (0, 3)$.

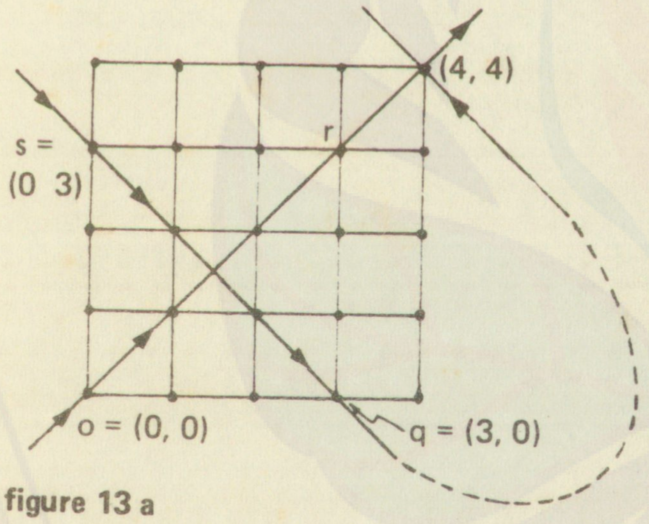


figure 13 a

Then oqrs is a parallelogram since $o + r = q + s$. The diagonal $or = \Sigma r = \Sigma(3, 3) = \Sigma(1, 1)$. It contains (0, 0), (1, 1), (2, 2), (3, 3) and (4, 4). On the other hand, the diagonal sq can be represented by $sq = s + \Sigma(s - q) = (0, 3) + \Sigma(-3, 3) =$ $= (0, 3) + \Sigma(2, 3)$. So sq contains the points: $(0, 3) = s$, (2, 1), (4, 4), (1, 2) and $(3, 0) = q$.

In figure 13 a one sees that the line sq does not intersect or.

In fact both diagonals intersect at the point (4, 4). Thus the point (4, 4) is the midpoint of o and r also the midpoint of s and q.

2. Distance in AFG(k, p^n)

A distance can be defined by means of the lenght of a vector.
So the distance of two points a and b in AFG(k, p^n) will be defined to be the length of the vector $b - a$.

If a non-directed distance is required, the concept of the length of a vector must be defined in such a way that the length of the vector $b - a$ is equal to the length of the vector $a - b$.

It can be done by means of the standard pseudo inner product. Since $\sqrt{x}$ does not always exist in an arbitrary field, we define the length of a vector in a vector space over a field of characteristic p in the following way:

The length of $x = \sqrt[p]{x.x}$ and denote it by $\| x \|$.

Then a circle in the plane AFG(2, 2^n) with centre at the origin has an equation of the form $\xi_1^2 + \xi_2^2 = \theta$.

It is necessary to be noted that by defining the length in such a way there is no guarantee that a vector of the form (0, 0, . . . , μ, 0, 0, 0) in AFG(k, p^n) has length μ. Only in the case p = 2 this is true, since the length of the vector (0, 0, . . . , μ,0, 0, 0) in AFG(k, 2^n) is equal to

$$\sqrt{(0, 0, \ldots, \mu, 0\ 0, 0) . (0, 0, \ldots, \mu, 0, 0, 0)} = \sqrt{\mu^2} = \mu.$$

Using the idea of the p-norm in the classical Banach Space L^p [19], where

$$\| f \|_p = [\int_0^1 | f |^p]^{1/p}$$

we may define the length of a vector in AFG(k, p^n) as follows:

$$\| x \| = (\sum_{i=1}^{k} \xi_i^p)^{1/p}$$

However in a field of characteristic p we have

$$(\sum_{i=1}^{k} \xi_i^p) = (\sum_{i=1}^{k} \xi_i)^p$$

Hence we have $\| x \| = \sum_{i=1}^{k} \xi_i$, where $x = (\xi_1, \xi_2, \ldots, \xi_k)$.

Any vector of the form (0, 0, . . . , θ, . . . , 0, 0, 0) has length θ, but in general the length of a vector x is not equal to the length of $-$ x.

So by defining the length of a vector in this way, where the distance between two points a and b has to be equal to the length of the vector b $-$ a, we have to do with a directional distance. Therefore we call this a directional distance and we denote the directional length of the vector x by $\| x \|_{dir}$.

Especially in a vector space over a field of characteristic 2, both definitions of distances are equivalent, for

$$\| x \| = (x.x)^{1/2} = (\sum_{i=1}^{k} \xi_i^2)^{1/2} = ((\sum_{i=1}^{k} \xi_i)^2)^{1/2} = \sum_{i=1}^{k} \xi_i = \| x \|_{dir}$$

It is worth to be noted that over a field of characteristic 2, $\| x \|_{dir} = \| -x \|_{dir}$. This is due to the fact that over a field of characteristic 2, we have

$$-x = -(\xi_i, \xi_2, \ldots, \xi_k) = (-\xi_1, -\xi_2, \ldots, \xi_k) = (\xi_1, \xi_2, \ldots, \xi_k) = x.$$

The following theorem, which should be true is rather surprising.

THEOREM

Given two points a and b in AFG(k, p^n) with $p \neq 2$ and their midpoint m_{ab}, then the distance from a to m_{ab} is equal to the distance from m_{ab} to b.

PROOF

The distance from a to $m_{ab} = \| m_{ab} - a \|$, while the distance from m_{ab} to $b = \| b - m_{ab} \|$. Since $m_{ab} = 2^{-1}(a + b)$, hence

$$\begin{aligned} m_{ab} - a &= 2^{-1}(a + b) - a = 2^{-1}a + 2^{-1}b - a \\ &= 2^{-1}b + 2^{-1}a - a = 2^{-1}b + (2^{-1} - 1)a \\ &= 2^{-1}b + (2^{-1}.1 - 2^{-1}.2)a = 2^{-1}b + 2^{-1}(1 - 2)a \\ &= 2^{-1}b + 2^{-1}(-1)a = 2^{-1}b - 2^{-1}a. \end{aligned}$$

While

$$b - m_{ab} = b - 2^{-1}(a + b) = 2^{-1}b - 2^{-1}a = m_{ab} - a.$$

Therefore $\| m_{ab} - a \| = \| b - m_{ab} \|$. QED.

Another possible definition of the length of a vector will be the standard pseudo inner product of that vector with itself.

Then the distance of two points a and b is equal to

$$(b - a).(b - a) = (a - b).(a - b).$$

If $\Sigma = Z_p$ for some prime p, it is possible to define a real distance in AFG(k, p), namely in the following way.

The distance of a and b, where $a = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $b = (\beta_1, \beta_2, \ldots, \beta_k)$ is defined to be $\sum_{i=1}^{k} (\alpha_i - \beta_i)^2$ in which the computation has to be done in $\mathbf{Z}$, not in $\mathbf{Z}_p$.

Thus for example the distance of the points a = (0, 1, 1, 0) and b = (0, 0, 0, 1) in AFG(4, 2) is not equal to 1 but equal to 3.

The distance of (3, 4) and (2, 1) in AFG(2, 5) is equal to 10 and no zero.

An application of AFG(k, 2) can be found in coding theory in which a real distance is defined as we have done in the last case.

SOME EXAMPLES

1. Take the plane AFG(2, 3). Then the equation of the unit circle, namely the circle with centre at the origin and radius 1 has the form.

$$(x.x)^{1/3} = 1$$

or $\quad x.x = 1$

or $\quad \xi_1^2 + \xi_2^2 = 1$

where $x = (\xi_1, \xi_2)$.

It consists of the points (0, 1), (1, 0), (2, 0) and (0, 2). See figure 14. On the other hand,

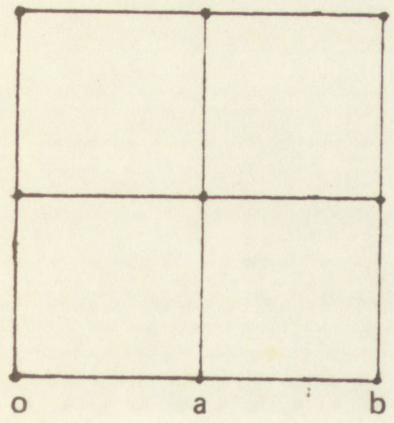


figure 14

let us take the points o = (0, 0), a = (1, 0) and b = (2, 0).

Clearly a lies on the line ob.

However, the distance from o to a is equal to the distance from a to b but also equal to the distance from o to b, since ob = $\| (2, 0) \| = (2^2 + 0^2)^{1/3} =$ $= (1)^{1/3} = 1$.

2. Consider the plane AFG(2, 2^2) with
$\Sigma = \{0, 1, \mu, \mu + 1\}$. where $\mu^2 = \mu + 1$.

Take the point (μ, 0). The distance from o = (0, 0) to that point is equal to the lenght of the vector (μ, 0). So we have

distance of (0, 0) and (μ, 0) = $\| (\mu, 0) \|$
$= ((\mu, 0).(\mu, 0))^{1/2} = (\mu^2)^{1/2} = \mu$.

We have here $\| (\mu, 0) \| = \mu$, while in example 1 we had $\| (2, 0) \| = 1 \neq 2$.
$\| (\mu, 0) \| = \mu$ in AFG(2, 2^2) is due to the fact that over a field of characteristic 2 we have had $\| x \| = \| x \|_{dir}$.

3. Another example that $\| (0, 0, \ldots, \mu, 0, 0) \| \neq \mu$ can be seen in the following one:
Consider the vector x = (0, θ, 0) in $V_3(\Sigma)$, where $\Sigma = GF[3^2]$
$= \{0, 1, 2, \theta, \theta + 1, \theta + 2, 2\theta, 2\theta + 1, 2\theta + 2\}$, in which $\theta^2 = \theta + 1$.

Then $\| x \| = \| (0, \theta, 0) \| = (x.x)^{1/3} = (\theta^2)^{1/3} = 2\theta + 2$,
since $(2\theta + 2)^3 = 2^3(\theta + 1)^3 = 2(\theta^3 + 1) = 2(\theta^2\theta + 1)$
$= 2[(\theta + 1)\theta + 1] = 2(\theta^2 + \theta + 1) = 2(\theta + 1 + \theta + 1)$
$= 2(2\theta + 2) = 2^2(\theta + 1) = \theta + 1 = \theta^2$

Here we have $\| (0, \theta, 0) \| \neq \theta$.

4. The sphere of radius 2 with centre at (1, 1, 1) in AFG(3, 3) has the equation

$$(\xi_1 - 1)^2 + (\xi_2 - 1)^2 + (\xi_3 - 1)^2 = 2^3;$$

which can be written as

$$(\xi_1 - 1)^2 + (\xi_2 - 1)^2 + (\xi_3 - 1)^2 = 2, \text{ since } 2^3 = 2.$$

3. Quadratic forms in AFG(k, p^n) with k = 2 or 3

In AFG(2, p^n) an expression of the form:

$$f(\xi_1, \xi_2) = \alpha_{11}\xi_1^2 + \alpha_{12}\xi_1\xi_2 + \alpha_{22}\xi_2^2 + \beta_1\xi_1 + \beta_2\xi_2 + \gamma$$

is called a quadratic form, simillarly the expression

$$\alpha_{11}\xi_1^2 + \alpha_{12}\xi_1\xi_2 + \alpha_{22}\xi_2^2 + \alpha_{13}\xi_1\xi_3 + \alpha_{33}\xi_3^2 + \alpha_{23}\xi_2\xi_3 + \beta_1\xi_1 + \beta_2\xi_2 + \beta_3\xi_3 + \gamma$$

is called a quadratic form in AFG(3, p^n).

Using matrix notation, that form can be written as:

$(\xi_1\ \xi_2\ \xi_3)\ A\ (\xi_1\ \xi_2\ \xi_3)^t + B\ (\xi_1\ \xi_2\ \xi_3)^t + \gamma$, where $B = (\beta_1\ \beta_2\ \beta_3)$ and

$$A = \begin{bmatrix} \alpha_{11} & 2^{-1}\alpha_{12} & 2^{-1}\alpha_{13} \\ 2^{-1}\alpha_{12} & \alpha_{22} & 2^{-1}\alpha_{23} \\ 2^{-1}\alpha_{13} & 2^{-1}\alpha_{23} & \alpha_{33} \end{bmatrix} \quad \text{provided } p \neq 2.$$

By a coordinate transformation, in this case a translation such a form can be reduced to the following one:

$(\eta_1\ \eta_2\ \eta_3)\ A\ (\eta_1\ \eta_2\ \eta_3)^t + \delta$ provided A is non-singular.
A similar result holds for a quadratic form in AFG(2, p^n).

In general such a quadratic form is called a quadratic form over the field $\Sigma = GF[p^n]$ and an equation of the form

$xAx^t + \gamma = 0$

in which $x = (\xi_1\ \xi_2\ \dots\ \xi_k)$ will be called a quadratic equation in k variables over Σ or a quadratic equation in Σ^k. In particular if Σ is a Galois field it is called a quadratic equation in AFG(k, p^n), where $\Sigma = GF[p^n]$.

G. Birkhoff and S. Mac Lane have derived and proved the following theorem [3]:
By non-singular trnasformations of the variables, a quadratic form xAx^t in k variables over any field of characteristic $p \neq 2$ can be reduced to a diagonal form,

$\delta_1\eta_1^2 + \delta_2\eta_2^2 + \dots + \delta_r\eta_r^2$, each $\delta_i \neq 0$.
The number r is called the rank of the given quadratic form.
This rank is equal to the rank of the matrix A of the original form.

This theorem can be applied to any quadratic form over any field of characteristic $p \neq 2$, in particular over any Galois field $GF[p^n]$ with $p \neq 2$.

Then we can define ellipses, hyperbolas and parabolas in the Affine finite plane AFG(2, p^n), but it appears that there is no difference between an ellipse and a hyperbola.

Similarly in AFG(3, p^n) we can define ellipsoids, paraboloids and hyperboloids, but also here these notions are not all different.

4. Finite Geometry and a graph

A graph is a non-void set with one or more relations, usually denoted by $(G, E_1, E_2, \dots)$ hence (G, E_1, E_2) in the case of two relations and (G, E) in the case of only one relation.

By a simple graph is meant a finite set with only one relation which is symmetric and antireflexive, meaning that there exists no point x such that xEx. A simple graph can be drawn by a diagram which is called the diagram representation of that graph. The points represent the elements of that graph and the relation is represented by lines. The symmetry means that the graph is non-directed. The anti-reflexivity means there are no loops.

Furthermore by a graph is meant a simple graph [12].

Examples of graphs can be seen in figure 15, in which each of them is represented by a diagram.

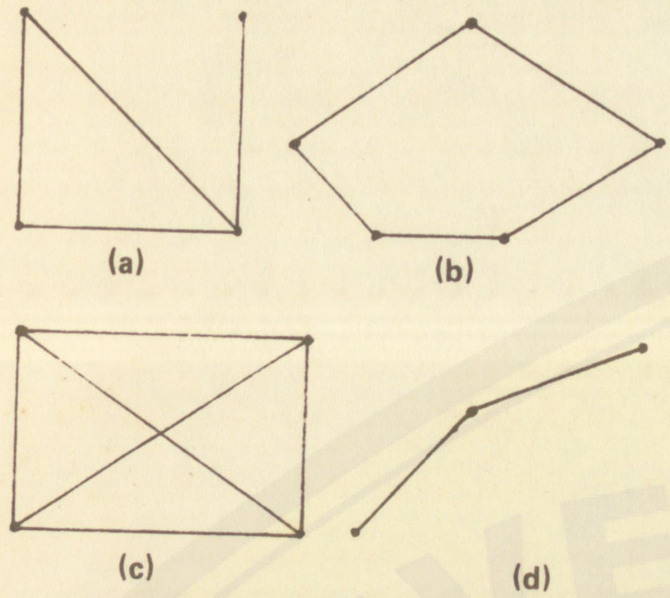


figure 15

If two elements of a graph have a relation, in the diagram representation both points are connected by a line; then they are called adjacent. A graph is called complete if any two elements are adjacent. See figure 15c.

There cannot be much said about the relation between a finite geometry and a graph. In fact in an Affine finite geometry any two points lie in a line. Hence some Affine finite geometries are complete graphs. But we cannot say in general that any Affine finite geometry is a complete graph. Why? Because in an Affine finite geometry three different points might be collinear, and thus only one line goes through those points, while in a complete graph three different points are connected to each other by three different lines.

A complete graph with m points is denoted by K_m. Hence we have for instance the following relation between an Affine finite geometry and a graph.

$AFG(1, 2) = K_2$

$AFG(2. 2) = K_4$

But in general it is difficult to say much about $AFG(k, p^n)$ with $k \neq 2$, and $p^n \neq 2$, even $AFG(1, 3)$ cannot be considered as K_3, since there is only one line through those three points.

A cylcle with m points is denoted by C_m and a path with m points is denoted by P_m. Hence we have

$AFG(1, 2) = K_2 = P_2$

in fact

$AFG(1, 3) = P_3$

5. Representation of finite geometries by means of sets

Although very limited, it is not impossible to set up a representation of finite geometries by means of sets. Difficulties are predictable. These arise since there is no structure.

Begining with a non-empty finite set S with N elements, we define any subset with q elements as points and any subset with L elements as lines. Evidently L must be greater than q. We denote this geometry by FG(N, q, L). In case q = 1, which means that any element of S is defined to be a point, we use the shortened notation

FG(N, L) instead of FG(N, 1, L).

Then we observe that the finite geometry FG(3, 2) is the smallest, may be unknown, finite projective geometry, which satisfies the following theorems:

I. Given two distinct points there exists one and only one line passing through both points.
II. Two different lines intersect in the exactly one point.

On the other hand the finite geometry FG(4, 2) is isometric with AFG(2, 2), while the finite geometry FG(N, 2) with any number $N > 4$ is a Lobatsevskian geometry.

A question arises whether such a geometry can be developed with $p \neq 1$ and $L \neq 2$. Finally we can write the following relation between these geometries and graphs.

$FG(3, 2) = C_3 = K_3$

$FG(2, 2) = AFG(1, 2) = P_2 = K_2$

In general we can state that

$FG(N, N) = P_N$

and in particular

$AFG(1, p^n) = FG(p^n, p^n) = P_{p^n}$.

6. Quasi Geometry

Instead of a Galois Field we can take a finite commutative ring χ with identity and construct the finite module

$\chi \times \chi \times \cdots \times \chi = \chi^k$ over χ.

Then we may define any element of χ^k to be a point and any subset of the form $a + \chi b$, where $b \neq 0$ to be a line. Then we have built up what is called a finite quasi geometry satisfying the following properties:

I. A line contains at most m points, where m is the number of elements of the ring χ.
II. Given two distinct points, there exists at least one line passing through both points.
III. Two different lines might intersect in two different points.
IV. The total number of points is m^k.
V. A line might contain another line as a proper subset.

Parallelism between two lines is defined in a similar way like we have done in a previous chapter in this thesis.

Then in a quasi plane it might happen that two non parallel lines do not intersect.

As an illustration of this so called quasi geometry, let us consider the quasi geometry built up from $Z_4 \times Z_4$. See figure 16.

Set $Z_4 = \chi$.

Further let L be the line passing through the points $o = (0, 0)$ and $a = (1, 0)$. Then L can be represented by:

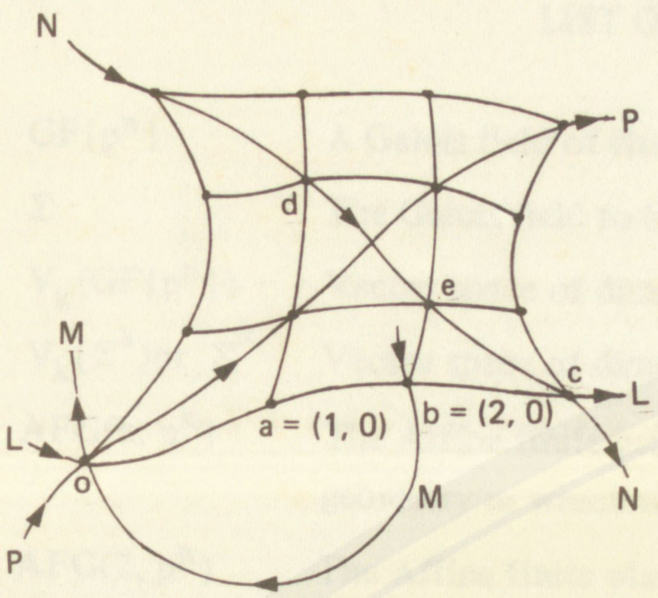


figure 16

$L = 0 + \chi a = \chi a = \chi(1, 0) = \{\mu(1, 0) \mid \mu \in \chi\}$.
It contains the points $o = (0, 0)$, $a = (1, 0)$, $b = (2, 0)$ and $c = (3, 0)$.

On the other hand, let M be the line passing through o and $b = (2, 0)$. Then M can be represented by: $M = o + \chi b = \chi b = \{\theta(2, 0) \mid \theta \in \chi\} = \{(0, 0), (2, 0)\}$. Thus M only contains the points $o = (0, 0)$ and $b = (2, 0)$.

Here we can see that there are two different lines passing through two different points, namely o and b. As it has been stated before the line M is a proper subset of the line L.

Consider now the line N passing through $d = (1, 2)$ and $e = (2, 1)$.
It can be represented by: $N = d + \chi(e - d) = (1, 2) + \chi(1, -1) = (1, 2) + \chi(1, 3)$.
After computations it turned out that N contains the points

$d = (1, 2)$, $e = (2, 1)$, $(3, 0) = c$ and the point $(0, 3)$.

Also consider the line P which is passing through o and the point $(1, 1)$. Clearly $P = \chi(1, 1)$ and it contains the points $o = (0, 0)$, $(1, 1)$, $(2, 2)$ and $(3, 3)$.
Hence P does not intersect N. However, both lines are not parallel since the direction "vector" of N is $(1, 3)$ and the direction "vector" of P is $(1, 1)$ and both are not similar.

NOTE

1. Since a finite integral domain is a field, to buildup a finite quasi geometry, the ring to be considered must be a ring with zero divisors.
2. Building up a quasi geometry from the ring **Z**, i.e the ring of integers, we obtain an infinite quasi geometry. In the quasi plane $\mathbf{Z} \times \mathbf{Z}$ it might happen that two non parallel lines do not intersect.

Take for example the line L passing through $(0, 0)$ and $(1, 1)$ and the line M passing through $(1, 0)$ and $(0, 1)$. Clearly both lines do not intersect. However, both lines have distinct directions (direction "vectors").

The direction of L is $d_L = (1, 1)$ while the direction of M is $d_M = (1, 0) - (0, 1) = (1, -1)$. Clearly both directions are not similar. Hence $L \nparallel M$.

LIST OF SPECIAL SYMBOLS

$GF[p^n]$	A Galois field of characteristic p with p^n elements
Σ	The Galois field to be considered
$V_k(GF[p^n])$	Vector space of dimension k over $GF[p^n]$
$V_k(\Sigma^k)$ or Σ^k	Vector space of dimension k over the field Σ
$AFG(k, p^n)$	The Affine finite geometry of dimension k and order p^n, i.e. the geometry in which the underlying set is $V_k(GF[p^n])$
$AFG(2, p^n)$	The Affine finite plane of order p^n
$AFG(3, p^n)$	The Affine finite space of order p^n, i.e the Affine finite space of dimension 3 and order p^n
$PFG(2, p^n)$	The projective finite plane of order p^n, i.e the projective finite geometry whose underlying set is $V_3(GF[p^n])$
a, b, c, x, y, . . . except k, p and n	Small italic letters are used to denote vectors or points, i.e elements of $V_k(\Sigma)$ or points in $AFG(k, p^n)$
$\alpha, \beta, \theta, \mu, \ldots$	Small Greek letters are used to denote elements of Σ
$A, \Gamma, \Delta, \ldots$ except Σ	Greek capitals are used to denote planes in $AFG(3, p^n)$
$\bar{0}$	The zero vector in $V_k(\Sigma)$
0	zero element of Σ
o	small italic letter 0 to denote the point of origin, i.e the zero vector $\bar{0}$
1	identity element of Σ
2	symbol for 1 + 1
d_L	direction vector of the line L
n_Γ	normal vector of the plane Γ
$\backsim$	similar
$/\!/$	parallel
$\not\backsim$	not similar
$\nparallel$	not parallel
$\perp$	perpendicular to
$\not\perp$	not perpendicular to
$a + \Sigma b$	notation for the set $\{a + \mu b \mid \mu \in \Sigma\}$

$a + \Sigma b + \Sigma c$	notation for the set $\{a + \mu b + \theta c \mid \mu, \theta \in \Sigma\}$
$x.y$	Standard Pseudo Innerproduct of x and y
$\mathbf{Z}$	Ring of integers
$\mathbf{Z}_m$	Ring of integers modulo m
$\mathbf{Z}_p$	Field of integers modulo p, where p is prime
$(\Sigma^k, +)$	Additive group of Σ^k
$\mathcal{A}_k(\Sigma)$	Affine group of $V_k(\Sigma)$
$\mathcal{T}(\Sigma^k)$	Translation group of $V_k(\Sigma)$
$\mathcal{L}_k(\Sigma)$	Full linear group of $V_k(\Sigma)$
m_{ab}	midpoint of a and b
$\lVert x \rVert$	ordinary length of x
$\lVert x \rVert_{dir}$	directional length of x
rank (A)	rank of the matrix A
x^t	transposed of the matrix x
■	a mark to indicate the end of a proof
$\mathcal{P}(S)$	power set of the set S
$\ominus$	symmetric difference

REFERENCES

[1] Baer, R. *Linear Algebra and Projective Geometry.* Academic Press Inc. Publishers, New York, N. Y, 1952.

[2] Bell, R. J. T. *Coordinate Geometry of Three Dimensions.* Mac Millan and Co., Limited St. Martin's Street, London, 1950.

[3] Birkhoff, G and Mac Lane, S. *A Survey of Modern Algebra.* Revised Edition. The Mac Millan Company, New York, 1953.

[4] Carmichael, R. D. *Finite Geometry and the Theory of Groups.* American Journal of Mathematics, Vol. LII, 1930, p 745–788.

[4a] ––– *Introduction to the Theory of Groups of Finite Order.* Dover Publications, Inc., 1937.

[5] Coolidge, J. L. *The Elements of Non-Euclidean Geometry.* Oxford At The Clarendon Press, 1909.

[6] Coxeter, H. S. M. *Introduction to Geometry.* Third Printing, John Wiley & Sons, Inc. Toronto, New York, London, January 1953.

[7] Fishback, W. T. *Projective and Euclidean Geometry.* John Wiley & Sons, Inc. New York, London, Sydney, Toronto,1969.

[8] Fraleigh, J. B. *A First Course in Abstract Algebra.* Addison-Wesley Publishing Company, Reading Massachusets, Menlo Park California, London, Sydney, Manila, 1971.

[9] Greub, W. H. *Linear Algebra.* Springer-Verlag Berlin, Heidelberg, New York. Kinokuniya Book-Store Co., Ltd. Tokyo Japan, Third Edition, 1967.

[10] Hall Jr, M. *The Theory of Groups.* The Mac Millan Company, New York, 1959.

[11] Halmos, P. R. *Finite-Dimensional Vector Spaces.* Second Edition, D. Van Nostrand Company, Inc., Princeton, New Jersey, Toronto, New York, London, 1958.

[12] Harary, F. *Graph Theory.* Addison-Wesley Publishing Company, Reading, Massachusetts, Menlo Park California, London, Amsterdam, Don Mills, Ontario, Sydney, Third Printing, October 1972.

[13] Jacobson, N. *Lectures in Abstract Algebra. Vol. II.* D. Van Nostrand Company, Inc. Princeton, New Jersey, Toronto, New York, London, 1953.

[13a] ––– *Lectures in Abstract Algebra. Vol. III.* D. Van Nostrand Company, Inc. Princeton, New Jersey, Toronto, New York, London, 1964.

[14] Jerger, M and Eckmann, B. *Vector Geometry and Linear Algebra.* English translation Interscience Publishers, London, 1967.

[15] Kromodihardjo, K. *Representation of Euclidean Finite Geometries by Means of Finite Vector Spaces.* Sains Malaysiana, Vol. II. No. 2, July 1973, p 65–75.

[15a] ––– *Orthogonality in EG (k, p^n).* Sains Malaysiana. Vol. IV, No. 1, 1975, p 37–40.

[16] Lang, S. *Algebra.* Addison-Wesley Publishing Company, Reading, Massachusetts. Menlo Park, California. London. Don Mills, Ontario. Revised Printing, January 1971.

[17] Mac Lane, S and Birkhoff, G. *Algebra.* The Mac Millan Company, Collier-Mac Millan Limited, London, 1967.

[18] McCarthy, P. J. *Algebraic Extensions of Fields.* Consulting Editor, George Springer, Indiana University 1966.

[19] Royden, H. L. *Real Analysis.* Second Edition. The Mac Millan Company, New York, Collier-Mac Millan Limited, London, 1968.

[20] Struik, D. J. *Analytic and Projective Geometry.* Addison-Wesley Publishing Company, Inc., Cambridge 42, Massachusetts, 1953.

[21] Todd, J. A. *Projective and Analytic Geometry.* London, Sir Isaac Pitman & Sons, Ltd, First Published 1947, Revised and Reprinted 1954, Reprinted 1958.

[22] Veblen and Bussey. *Finite Projective Geometry.* Transaction American Mathematical Society, Vol. VII, 1906, p 241–259.

[23] Veblen, O and Young, J. W. *Projective Geometry. Vol. I.* Ginn and Company, Boston, New York, Chicago, London, Atlanta, Dallas, Columbus, San Francisco, 1916.

[23a] ––– *Projective Geometry. Vol. II.* By Oswald Veblen, Ginn and Company, Boston, New York, Chicago, London, Atlanta, Dallas, Columbus, San Francisco, 1917.

[24] Waerden, B. L. van der, *Modern Algebra. Vol. I.* Revised English Edition. Frederick Ungar Publishing Co., New York, 1953.

[25] Wilder, R. L. *Introduction to The Foundations of Mathematics* Second Edition. John Wiley & Sons, Inc., New York, London, Sydney, Toppan Company Ltd., Tokyo, Japan, 1965.

THEOREMS

(LIST I. Concerning the dissertation)

1. Given two distinct points in AFG(k, p^n) there exists one and only one line passing through both points.
2. Given a line L in AFG(k, p^n) and a point q not lying on L, there exists one and only one line passing through q and parallel to L.
3. Given an isotropic line L in AFG(k, p^n) and a point b not lying on L then either

   there does not exist a line passing through b and intersecting L perpendicularly

   or

   any line passing through b and intersecting L is perpendicular to L.
4. The total number of lines passing through one point in AFG(k, p^n) is equal to $\frac{p^{nk} - 1}{p^n - 1}$.
5. In a given direction in AFG(k, p^n) there exist $p^{n(k-1)}$ parallel lines.
6. The total number of lines AFG(k, p^n) is equal to $p^{n(k-1)} \frac{p^{nk} - 1}{p^n - 1}$.
7. Given three non-collinear points in AFG(3, p^n) there exists one and only one plane containing those points.
8. If L is an isotropic line in AFG(3 p^n) and b a point lying on L, then the plane passing through b and perpendicular to L is containing L.
9. The number of planes perpendicular to a given line in AFG(3, p^n) is equal to p^n.
10. The total number of planes in AFG(3, p^n) is equal to $p^n(p^{2n} + p^n + 1)$.
11. The number of planes containing a given line in AFG(3. p^n) is equal to $p^n + 1$.
12. The number of planes passing through a certain point in AFG(3, p^n) is equal to $p^{2n} + p^n + 1$.
13. The set of all affine transformations in AFG(k, p^n) under successive mapping constitutes a group of order $p^{nk}(p^{nk} - 1)(p^{nk} - p^n)(p^{nk} - p^{2n})(p^{nk} - p^{3n}) \ldots (p^{nk} - p^{n(k-1)})$.
14. Any plane in AFG(3, p^n) is isometric to the geometry AFG(2, p^n).
15. Given two distinct points in the projective finite plane PFG(2, p^n), there exists one and only one line passing through both points.
16. Two different lines in PFG(2, p^n) intersect in one and only one point.
17. In the plane PFG(2, p^n) each line contains $p^n + 1$ points and through each point there exist $p^n + 1$ lines.
18. The total number of points in PFG(2, p^n) is equal to the total number of lines and it is equal to $p^{2n} + p^n + 1$.

THEOREMS

(LIST II. Not concerning the dissertation)

1. In finite systems counting theorems are important.
2. If S is a set and $\{A_1, A_2, \ldots, A_n\}$ a finite collection of subsets of S, then $\langle \mathcal{P}(\bigcup_{i=1}^{n} A_i), \ominus \rangle = \sum_{i=1}^{n} \langle \mathcal{P}(A_i), \ominus \rangle$.
3. If $\{A_\alpha\}_{\alpha \in \Lambda}$ is a collection of subsets of a set S, then $\langle \mathcal{P}(\bigcap_{\alpha} A_\alpha), \ominus \rangle = \bigcap_{\alpha} \langle \mathcal{P}(A_\alpha), \ominus \rangle$.
4. For any set S, with cardinality $\neq 1$, the Frattini subgroup of $\langle P(S), \ominus \rangle$ is trivial.
5. If a is a singleton subset of a set S then $\langle \mathcal{P}(S - a), \ominus \rangle$ is a maximal subgroup of $\langle \mathcal{P}(S), \ominus \rangle$ of index two.
6. Mathematical terminology in this country must be uniformed.
7. As long as the situation remains unchanged in Indonesia, it is very difficult to receive a doctor degree in mathematics.

DALIL – DALIL

(DAFTAR I. Mengenai disertasi)

1. Melalui dua buah titik yang berlainan dalam AFG(k, p^n) terdapat satu dan hanya satu garis.
2. Melalui suatu titik di luar sebuah garis dalam AFG(k, p^n) terdapat satu dan hanya satu garis yang sejajar dengan garis yang pertama.
3. Diberikan sebuah garis isotrop L dalam AFG(k, p^n) dan suatu titik di luarnya maka:

   atau tidak terdapat satu garispun yang melalui titik tadi dan memotong L tegaklurus.
   atau setiap garis yang melalui titik tadi dan memotong L tegaklurus pada L.

4. Banyaknya garis melalui sebuah titik dalam AFG(k, p^n) ada $\frac{p^{nk} - 1}{p^n - 1}$ buah
5. Dalam AFG(k, p^n) banyaknya garis sejajar dengan suatu arah tertentu ada $p^{n(k-1)}$ buah.
6. Banyaknya garis dalam AFG(k, p^n) ada $p^{n(k-1)} \frac{p^{nk} - 1}{p^n - 1}$ buah.
7. Melalui tiga buah titik yang tidak segaris dalam AFG(3, p^n) terdapat satu dan hanya satu bidang.
8. Jika L sebuah garis isotrop dalam AFG(3, p^n) dan b suatu titik padanya, maka bidang yang melalui b dan tegaklurus pada L melalui L.
9. Banyaknya bidang yang tegaklurus pada suatu garis dalam AFG(3, p^n) ada p^n buah.
10. Banyaknya bidang dalam AFG(3, p^n) ada $p^n(p^{2n} + p^n + 1)$ buah.
11. Banyaknya bidang melalui sebuah garis dalam AFG(3, p^n) ada $p^n + 1$ buah.
12. Banyaknya bidang melalui sebuah titik dalam AFG(3, p^n) ada $p^{2n} + p^n + 1$ buah.
13. Himpunan semua transformasi afin dalam AFG(k, p^n) terhadap pemetaan komposisi membentuk sebuah group yang bertingkat
    $p^{nk}(p^{nk} - 1)(p^{nk} - p^n)(p^{nk} - p^{2n})(p^{nk} - p^{3n}) \ldots (p^{nk} - p^{n(k-1)})$.
14. Setiap bidang dalam AFG(3, p^n) isometrik dengan bidang AFG(2, p^n).
15. Melalui dua buah titik yang berlainan dalam bidang proyektif terhingga PFG(2, p^n) terdapat satu dan hanya satu garis.
16. Dua buah garis yang berlainan dalam PFG(2, p^n) berpotongan pada satu dan hanya satu titik.
17. Dalam bidang PFG(2, p^n) setiap garis memuat $p^n + 1$ buah titik dan melalui sebuah titik terdapat $p^n + 1$ buah garis.
18. Banyaknya titik dalam PFG(2, p^n) sama dengan banyaknya garis dan banyaknya $p^{2n} + p^n + 1$.

DALIL – DALIL

(DAFTAR II. Tidak mengenai disertasi)

1. Dalam sistem-sistem terhingga dalil-dalil penghitungan adalah penting.
2. Jika $\{A_1, A_2, \ldots, A_n\}$ suatu koleksi terhingga dari anakhimpunan-anakhimpunan dari suatu himpunan S maka $\langle \mathcal{P}(\bigcup_{i=1}^{n} A_i), \ominus \rangle = \sum_{i=1}^{n} \langle \mathcal{P}(A_i), \ominus \rangle$.
3. Jika $\{A_\alpha\}_{\alpha \in \Lambda}$ suatu koleksi anakhimpunan-anakhimpunan dari suatu himpunan S maka $\langle \mathcal{P}(\bigcap_{\alpha} A_\alpha), \ominus \rangle = \bigcap_{\alpha} \langle \mathcal{P}(A_\alpha), \ominus \rangle$.
4. Untuk setiap himpunan S, dengan kardinal $\neq 1$, subgrup Frattini dari grup $\langle P(S), \ominus \rangle$ adalah subgrup trivial.
5. Jika a suatu anakhimpunan tunggal dari himpunan S maka $\langle \mathcal{P}(S - a), \ominus \rangle$ merupakan suatu subgrup maximal dari $\langle \mathcal{P}(S), \ominus \rangle$ dengan indeks dua.
6. Istilah matematika di negeri kita harus diseragamkan.
7. Selama keadaan di Indonesia masih seperti sekarang ini, sulit sekali bagi seseorang untuk memperoleh gelar doktor dalam matematika.

RIWAYAT SINGKAT PROMOVENDUS

Dilahirkan di Wonosobo, Jawa Tengah pada tanggal 23 Agustus 1931. Anak bungsu dari tigabelas bersaudara. Ayahnya seorang pedagang bernama Kromodihardjo.

Masuk HIS (SD zaman kolonial Belanda) di Wonosobo tahun 1937. Waktu balatentara Jepang menduduki Indonesia ia masih duduk di kelas lima, kemudian masuk kelas lima Sekolah Rakyat (bekas HIS) di masa Jepang.

Setamatnya dari SR masuk SMP Negeri I di Yogyakarta lalu melanjutkan ke SMA-B Negeri I di kota yang sama. Pada tahun 1951 mengikuti kuliah di Fakultas Ilmu Teknik Universitas Indonesia di Bandung (kini ITB) pada jurusan Elektroteknika sampai mendapat izajah P2. Lalu pada tahun 1955 pindah ke Fakultas Ilmu Pasti dan Ilmu Pengetahuan Alam, Universitas Indonesia di Bandung (yang kemudian bersatu dengan Fakultas Ilmu Teknik menjadi ITB). Lulus sarjana muda ilmu pasti pada tahun 1957 dan lulus sarjana ilmu pasti pada tahun 1958.

Sejak lulus sarjana muda, menjadi asisten semi akademis pada Fakultas Ilmu Teknik Bagian Ilmu Dasar dan diberi tugas memberi kuliah ilmu ukur proyektip untuk bagian Geodesi. Tahun 1959 tugas belajar ke Amerika Serikat dan kembali ke tanah air pada tahun 1961 tanpa membawa gelar tambahan. Pada tahun 1966 mengajukan permohonan lagi untuk belajar di Amerika Serikat tetapi tidak disetujui kementerian P dan K.

Tahun 1972 sampai dengan 1974 bertugas mengajar di Malaysia. Selama bertugas di sana melakukan penelitian di bidang aljabar dan ilmu ukur. Sewaktu masih bertugas di Malaysia mengajukan permohonan ke senat ITB untuk promosi doktor dengan judul disertasi.
"SUBGRUP FRATTINI ADITIF DARI SUATU RING BOOLE YANG ATOMIK DENGAN UNSUR KESATUAN".
Tetapi tidak dapat terlaksana, karena yang akan menjadi promotornya sekonyong-konyong mengundurkan diri. Kemudian oleh Prof. Doddy A Tisna Amidjaja didaftarkan sebagai peserta Sekolah Pasca Sarjana ITB, Stratum -3, pada tahun 1977 – 1978 dengan mendapat beasiswa dari P dan K selama satu tahun. Namun demikian tetap menghadapi kesulitan karena tidak adanya promotor.

Akhirnya pada tahun 1979, atas usaha almarhum Prof. Surjadi promovendus berhasil mendapatkan seorang promotor/ resminya co-promotor yaitu Prof. H.J.A Duparc dari Technische Hoge School di Delft, Negeri Belanda. Tetapi topik risetnya diganti dengan Geometri Terhingga yang akhirnya menjelma menjadi disertasi ini dengan judul seperti tertera di depan.

Sejak dari SD kelas enam promovendus sudah tertarik pada ilmu pasti dan sudah memulai belajar aljabar sedikit. Sewaktu duduk di bangku SMP kelas I semua pelajaran ilmu pasti untuk SMA tiga tahun yaitu aljabar, goniometri, ilmu ukur ruang dan ilmu ukur melukis telah selesai dipelajari hingga menginjak awal kelas II SMP. Kemudian di bangku SMP kelas II sudah belajar sendiri ilmu hitung diferensial dan integral. Dan di SMP kelas III mulai belajar persamaan diferensial.

Sejak tahun 1957 hingga kini menjadi anggota staf pengajar departemen Matematika ITB (dulunya fakultas teknik bagian ilmu dasar).

Telah berkeluarga dan mempunyai seorang istri dengan empat orang anak, seorang wanita dan tiga pria.