ON FINITE LINEAR

AND

BAER STRUCTURES

by

Marta Sved, M.Sc.

A thesis submitted to the University of Adelaide
for the degree of Doctor of Philosophy.

Department of Pure Mathematics,
University of Adelaide,
South Australia

April, 1985

TABLE OF CONTENTS

This thesis contains no material which has been accepted for the award of any other degree or diploma in any University and, to the best of my knowledge and belief, contains no material previously published or written by another person, except when due reference is made in the text of the thesis.

I am willing to make this thesis available for photocopying and loan if it is accepted for the award of the degree.

ACKNOWLEDGEMENTS

I wish to thank my supervisor, Dr. L.R.A. Casse of the Pure Mathematics Department, University of Adelaide for his advice, help and constructive criticism. I also thank Dr. D. Parrott, of the same department for discussing with me my conjecture described at the end of Chapter 3. He drew my attention to results on cyclic groups of the general linear group GL(n,q) described in Huppert's book [37].

SUMMARY

The work is divided into three chapters, followed by an appendix describing computer programs developed for this work and used for experimentation, leading to conjectures which were subesequently proved and presented in the main part of the work. The computer programs can be used as a basis for further experimentation.

The first chapter of the thesis deals with incidence relations in the n-dimensional linear space over the finite field GF(q), where $q = p^h$. (Here h is a natural number and p a prime number.) The relations give rise to identities which can be interpreted as generalisations of known identities of binomial coefficients. Some of the enumerative formulae discussed in this chapter are used in the later part of the work, while others are explored for their intrinsic interest in highlighting the analogy between combinatorial structures: subsets of a set, and subspaces of a space.

The second and third chapters deal with projective geometries over finite fields $GF(q^2)$. Here the order of the underlying field is a perfect square $q^2 = p^{2h}$, an even power of some prime. These projective geometries are of special interest because of their subgeometries over GF(q). In the two dimensional case the substructures, called Baer-planes, have been investigated by several workers and a number of results discussed in this work were found earlier by others. The references listed include those works on which some of the investigations are based as well as those which contain results at which the present investigations arrived independently, by different methods. By the nature of the subject, the second chapter of this thesis, dealing with Baer-planes intertwines with the work of other authors. However, it appears that the Singer duality theorem and a theorem depending on it, dealing with a configuration of Baer-planes named here "Singer wreath"

are new results.

The third chapter deals with Baer-substructures of the n-dimensional projective space PG(n,q^2) over GF(q^2). These are structures isomorphic to projective spaces over GF(q) of dimension n or less. Their intersections give rise to structures, named Baer-complexes, which relate to projective spaces in a manner similar to the relation of partitions to sets. A number of properties of these Baer-complexes are established. The Singer duality theorem discussed in Chapter Two, is generalised in Chapter Three and earlier results are reviewed in this light.

FUNDAMENTAL CONCEPTS

Introduction

In traditional geometry properties of objects such as lines, curves, polygons or three dimensional configurations are established. These properties are metric or descriptive. While the former concern distances, angles, areas, volumes, the latter deal with relative positional connections. In classical (Euclidean) geometry - the theorems of Pappus, Desargues, Pascal are of descriptive nature. As a result of development, projective geometry has become an independent branch of geometry, exploring the descriptive properties of configurations, that is, incidence relations. The elements of three dimensional space are points, lines, planes. By assigning coordinates to the points, incidence relations such as intersections, collineations, coplanarities become simple problems of linear algebra. At this stage, geometry can be generalised in two directions. On one hand, the concept of dimension can be extended; abstract points which can be defined by n coordinates are introduced where n can be any natural number, not just 1, 2 or 3. On the other hand, the coordinates characterising the points can be chosen to be elements of some algebraic structure more general than the field of the real numbers. This way we arrive to finite geometries, or the geometries of finite combinatorial structures.

Two approaches to projective geometry were developed simultaneously. The first one is the axiomatic, purely geometrical approach, the starting point being the set of axioms on the primitive terms (such as points, lines, spaces), and deriving the theory from these. The other approach is the algebraic one, beginning with the concept of the general n-dimensional space, points being ordered sets of n numbers, where these numbers are elements of an algebraic field, infinite or finite, while linear spaces are sets of points, linearly dependent on finite sets of points, (basis-elements). Projective n-dimensional geometry is then presented as the set of subspaces of an n+1 dimensional linear space over a field, together with the incidence relations of these subspaces. It has been shown that for dimensions greater than two, the algebraic and axiomatic approach lead to the same result. This is not the case in two dimensions. The projective plane defined by the axioms of incidence (three in number) is a more general structure than the projective plane defined by its points given as triples of elements of an algebraic field, finite or infinite. Accordingly, the main stream of resarch on projective planes centers on finding and classifying projective planes other than Galois planes (i.e. planes where the coordinates of the points are elements of a finite field ([32], [17], [1], [35], [22]).

However, the aim of the present work is to explore combinatorial relationships in n-dimensional spaces, and where possible, extend results known, or more readily found in the two dimensional case to higher dimensions. Thus, throughout this work, the concept of projective planes will be restricted to Galois planes. In the few cases where results apply more generally, special mention will be made of this fact.

In this introductory chapter well known concepts will be summarised, notations, definitions and known results will be given. All the theory to be discussed is readily found in texts given as references, so proofs will be generally omitted.

1. Galois Fields

(E.g. [13], [31], [26].)

A finite field F is an extension of some finite prime-field. If p is the order of the prime-field, then p must be a prime number.

This number p is called the characteristic of F. The prime-field of F of characteristic p is isomorphic to Z_p, the field of residue classes modulo p. F can be represented, up to isomorphism, as a vectorspace over Z_p. Thus the order of F is

$p^h = q$ where h is a natural number.

The elements of F form an elementary abelian group under addition, since the order of each non-zero element is p. The elements belonging to $F\backslash\{0\}$ form a group under multiplication. Since the order of this group is

$$q - 1 = p^h - 1,$$

the multiplicative order of each non-zero element is a divisor of q - 1. Thus if

$$\alpha \in F\backslash\{0\}$$

then

$$\alpha^{q-1} = 1,$$

or more generally, if

$$\alpha \in F$$

then

$$\alpha^q - \alpha = 0.$$

Hence the elements of F are roots of

$$x^q - x = 0. \tag{1.1}$$

Since this polynomial has exactly q roots, and q is the number of elements in F, it follows that F is the splitting field of (1.1) over Z_p. Hence, in an abstract sense, all fields of order $q = p^h$ are identical.

So F is called the Galois field of order q and is denoted GF(q).

Furthermore, it can be shown that the multiplicative group of GF(q) is cyclic. If α is an element of order $q - 1$, that is, the powers of α run through all the non-zero elements of F = GF(q), then α is called a primitive element in GF(q).

The number of primitive elements in GF(q) is $\phi(q-1)$, where $\phi(n)$ is the Euler function of n, enumerating all positive integers less than n and coprime to it.

Field-automorphisms. It is immediate that the transformation

$$\tau : \alpha \to \alpha^p \text{ for all } \alpha \in GF(q)$$

is a field automorphism:

$$\tau(\alpha_1 + \alpha_2) = \tau(\alpha_1) + \tau(\alpha_2)$$

and

$$\tau(\alpha_1\alpha_2) = \tau(\alpha_1)\tau(\alpha_2)$$

and τ is a bijection, since $\tau(\alpha_1) - \tau(\alpha_2) = \tau(\alpha_1-\alpha_2)$. For $q = p^h$ this means h automorphisms. It can be also shown that these are the only automorphisms of GF(q). Hence GF(q) has exactly h automorphisms.

Conjugate roots

Let

$$f(x) = a_h x^h + \ldots + a$$

0

be an irreducible polynomial over Z_p, and let α be one of its roots. Then it follows from the automorphism theorem that the other roots are $\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}$, and these roots are said to be conjugate.

Sub-fields.

Let GF(q) and GF(q') be two Galois fields, where $q = p^h$ and $q' = p^{h'}$ and $h' > h$. Then GF(q) is a subfield of GF(q') if and only if h is a divisor of h'. An element α of GF(q') belongs to the subfield GF(q) if and only if

$$\alpha^q - \alpha = 0 \qquad \text{(cf 1.1)}$$

The automorphism theorem implies that if GF(q') is an extension field of GF(q), then the map

$$\alpha \to \alpha^q$$

is an automorphism where the fixed elements are those belonging to GF(q).

If $f(x) = a_n x^n + \ldots + a_0$ is an irreducible polynomial over GF(q), then its set of roots is

$$\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$$

where α is any one of the roots.

Quadratic extensions are of particular importance in this work. The following results are listed for this special case.

(i) GF(q) is a subfield of GF(q^2).

(ii) If α is a primitive element of GF(q^2) then the set $\{\alpha^{i(q+1)}\}$ $(i=1,..,q-1)$ represents all the elements of GF(q)$\setminus\{0\}$.

(iii) The mapping $\alpha \to \alpha^q$ is an involution of $GF(q^2)$.

(iv) If ε is a primitive element of $GF(q^2)$, then the set

$$\{m\varepsilon + n\},\ m,\ n \in GF(q) \tag{1.2}$$

represents uniquely the elements of $GF(q^2)$.

It is apparent that the relation of the extension field $GF(q^2)$ to $GF(q)$ is analogous to the relation of the field of complex numbers to the real field. This justifies the usage of referring to the elements of $GF(q)$ as the real elements of $GF(q^2)$.

2. General projective planes

[5], [26], [15], [21], [20] for Sections 2, 3, 4.

As pointed out in the Summary, this work is confined to the study of spaces over finite fields, so in the present summary of definitions, notations and results only such spaces will be considered, using the algebraic approach, while most texts indicated as references treat a wider field and use the two-way approach for establishing basic concepts and results. Since all the content of this introductory chapter is well known, the summary is restricted to material used in the following chapters. However, basics about general (not necessarily Galois-type) projective planes cannot be totally disregarded, so these are surveyed in this section.

The projective plane is an incidence structure:

$$\Pi = (P, L, I)$$

where $P = \{p\}$ is a set of objects called points, $L = \{\ell\}$ a set of objects called lines, the sets P and L are disjoint, and I is a subset of ordered pairs,

$$I \subset \{(p,\ell)\},$$

where $p \in P$, $\ell \in L$, subject to the following axioms.

I. For any two points p_1, $p_2 \in P$, there exists a unique line $\ell \in L$, incident with p_1 and p_2, that is

$$(p_1, \ell) \in I \text{ and } (p_2, \ell) \in I.$$

II. For any two lines ℓ_1, $\ell_2 \in L$, there exists a point $p \in P$, incident with both ℓ_1 and ℓ_2, that is

$$(p, \ell_1) \in I \quad \text{and } (p, \ell_2) \in I.$$

III. P contains four points such that no three of the four are incident with the same line.
(Such a set will be called briefly a non-degenerate quadrangle).

Immediate consequences

IIa It follows from I that the point incident with both lines ℓ_1 and ℓ_2 is unique.

IIIa. The plane Π contains four lines such that no three intersect in the same point.

Notations and definitions

The line ℓ, incident with p_1 and p_2 is denoted $\ell = p_1 + p_2$ and called the join of p_1 and p_2.

The point incident with ℓ_1 and ℓ_2 is denoted $p = \ell_1 \cap \ell_2$ and called the intersection of ℓ_1 and ℓ_2.

The principle of duality

From axioms I, II, III together with IIa and IIIa, it can be seen that the word "point" is interchangeable with the word "line", while interchanging the words "join" and "intersection". Thus for each theorem established for the projective plane, there is a valid dual theorem obtained by the above interchange.

Finite planes

To the axioms of the general projective plane add the assumption: there exists a line ℓ in P which is incident with only a finite number of points.

Let the number of points on the line ℓ be q+1, where q is called the order of the plane Π.

From the above assumption and the axioms the following can be deduced:

(i) $q \geq 2$ (this is Fano's postulate);

(ii) every line $\ell \in \Pi$ is incident with exactly q+1 points;

(iii) through each point p of Π there are exactly q+1 lines;

(iv) Π contains exactly $q^2 + q + 1$ points;

(v) Π contains exactly $q^2 + q + 1$ lines.

In Section 4 it will be shown that the number of choices for the order q of the projective plane is infinite.

3. Linear (vector) spaces over a field

The concern in this work is with finite spaces. In a more general treatment a linear space is a structure defined over a skew field (division ring). However, by Wedderburn's theorem [34], finite division rings are commutative, hence it is assumed here that the set of scalars forms a field.

A linear n-space V over a field k is the set of all n-tuples:

$$p = (a_1, a_2, \ldots, a_n)$$

where

$$a_i \in k \ (i=1,..,n) \qquad (3.1)$$

The ordered sets of field elements defined in (3.1) are called the points of the n-space. In particular the point

$\sigma = (0, 0, .., 0)$ is called the origin.

The a_j's in (3.1) are the coordinates of the point p. Alternatively they may be interpreted as the components of the vector p.

Defining scalar multiplication and addition of vectors the usual way, we can write down the vector

$$p = cp_1 + dp_2 \quad (c,d \in k).$$

Let $p_1 = (a_1, a_2, \ldots, a_n)$

$p_2 = (b_1, b_2, \ldots, b_n)$,

then

$$p = (ca_1 + db_1, ca_2 + db_2, \ldots., ca_n + db_n).$$

Linear subspaces

Let p_1, p_2, .., p_r be a set of points in a linear space V. Define the set

$$S = \{c_1p_1 + c_2p_2 + \ldots + c_rp_r\}$$
$$(c_i \in k \quad \text{for } i = 1,..r) \qquad (3.2)$$

to be the subspace spanned by p_1, p_2, ..., p_r. It follows from (3.2) that the origin σ is contained in every subspace.

Independence, basis, dimension

Definition : the points of the set $\{p_1, p_2, .., p_r\}$ are dependent, if some point of the set is in the subspace spanned by the others, or equivalently, if there exists a set

$$\{c_1, c_2, ..., c_r\} \quad (c_i \in k, i=1,..,r),$$

where not all the elements are equal to zero, such that

$$c_1p_1 + c_2p_2 + ... + c_rp_r = 0 \qquad (3.3)$$

Both definitions imply that a set of points containing σ is a dependent set.

The points $p_1, p_2, ..., p_r$ are independent if the equation (3.3) implies that

$$c_i = 0 \quad \text{for } i=1,..r.$$

A basis of a subspace is a set of independent points spanning the subspace. A subspace can be spanned by different sets of basis-elements, but the number of basis-elements in each basis is the same. The dimension of a subspace is defined as the number of basis-elements required to span it. Thus the dimension of V is n.

Zero dimension is assigned to the point σ, also called the null-space, and by the definition, the dimension of a line (through σ) is 1, of a plane (through σ) 2, and so on.

A subspace spanned by n-1 basis-elements is called a hyperplane. It is the solution-space of the single equation

$$a_1x_1 + a_2x_2 + ... + a_nx_n = 0 \qquad (3.4)$$

From the definition (3.2) it follows that it two points p_1 and p_2

belong to a subspace S, then so does any linear combination

$$c_1p_1 + c_2p_2 \quad (c_1,c_2 \in k).$$

Conversely, a subset of V, closed on addition and scalar multiplication is a subspace.

Intersection, sum-spaces, Grassman's identity

The set of points common to two subspaces S_1 and S_2 is again a subspace : $S_1 \cap S_2$.

The sum $S_1 + S_2$ of two subspaces S_1 and S_2 is defined as the set

$$\{p_1 + p_2 | \; p_1 \in S_1, \; p_2 \in S_2\}.$$

The union $S_1 \cup S_2$ is a proper subset of $S_1 + S_2$. $S_1 \cup S_2$ is not a subspace (unless $S_1 \subset S_2$ or $S_1 \supset S_2$). The smallest subspace containing $S_1 \cup S_2$ is $S_1 + S_2$.

The subspaces of the linear space V form a set, partially ordered by inclusion, and such that the meet of any two elements S_1 and S_2, which is $S_1 \cap S_2$ and the join of S_1 and S_2 which is $S_1 + S_2$ belong to the set. Hence the subspaces of a linear space form a lattice.

A very useful relation, known as Grassman's identity applies to the dimensions of the sum and intersection of any two subspaces S_1 and S_2. Denoting by dim S the dimension of a subspace S, the relation is

$$\dim(S_1 + S_2) + \dim(S_1 \cap S_2) = \dim S_1 + \dim S_2 \qquad (3.5)$$

Finite linear spaces

If k is a finite field, then a finite dimensional linear space over it is also finite. The linear space of n dimensions over the field

GF(q) is denoted by V(n,q).

The number of points in V(n,q) is q^n.

The number of r dimensional subspaces of V(n,q) is denoted by the symbol $\begin{bmatrix} n \\ r \end{bmatrix}_q$, where

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1) \ldots (q^{n-r+1}-1)}{(q-1)(q^2-1) \ldots (q^r-1)} \tag{3.6}$$

This result will be proved and discussed in detail in Chapter 1.

4. Projective spaces

Homogeneous coordinates

The historical development of projective geometry led to the introduction of homogeneous coordinates. The cartesian coordinate system characterises a point of the Euclidean plane by the coordinate pair

$$(\xi, \eta).$$

Writing $\xi = x/z$, $\eta = y/z$, the triple (x,y,z) is used to represent the point (ξ, η).

Using this representation, the ideal points of the Euclidean plane can be written as triples of type

$$(x,y,0)$$

and the ideal line is given by the equation

$$z = 0.$$

However, the choice of a homogeneous triple to replace the coordinate-pair is not unique. The triple (x,y,z) can be substituted by the triple

$(\rho x, \rho y, \rho z)$ where $\rho \neq 0$.

Hence the point in the plane is characterised by a set of triples, which form an equivalence class.

More generally, each point of an n-dimensional projective space is represented by an equivalence class of (n+1)-tuples. This can also be interpreted as an equivalence class of points of an (n+1)-dimensional linear space:

$$\rho(x_1, x_2, \ldots, x_{n+1}), \text{ where } \rho \neq 0.$$

Alternatively, the point in the n-dimensional projective space is represented by the set of points of a ray through the origin in the (n+1)-dimensional linear space, excluding the origin.

Galois planes

The Galois plane PG(2,q) over the field GF(q) is defined as a collection of points and lines described as follows.

A point in PG(2,q) is

$$p = \rho(x_1, x_2, x_3) \tag{4.1}$$

meaning an equivalence class of triples, where x_1, x_2, x_3 is some fixed set of three elements in GF(q) not all zero, and ρ ranges through all non-zero elements of GF(q). For most purposes, when identifying a point, the factor ρ may be omitted.

A line is a set of points in PG(2,q), satisfying the equation over GF(q)

$$a_1x_1 + a_2x_2 + a_3x_3 = 0 \tag{4.2}$$

where at least one of a_1, a_2, a_3 is different from 0. The set

$\{a_1, a_2, a_3\}$ can be replaced by $\rho\{a_1, a_2, a_3\}$, where $\rho \in GF(q)\backslash\{0\}$. The equation is well defined for the points of the line, for if one triple (x_1, x_2, x_3) satisfies (4.2), so do all the triples belonging to its equivalence class $\rho(x_1, x_2, x_3)$. The set of coefficients in (4.2) is called the set of line-coordinates and is denoted by

$$[a_1, a_2, a_3].$$

If p_1 and p_2 are any two distinct points on a line then the line can be represented as the set

$$\{c_1p_1 + c_2p_2\} \qquad (c_1, c_2 \in GF(q), \text{ not both zero}).$$

The number of points, also the number of lines in PG(2,q) is

$$(q^3-1)/(q-1) = \underline{q^2 + q + 1} .$$

It can be checked that all the axioms of the general projective plane, listed in Section 2 are satisfied.

The order of a Galois plane is $q = p^h$, where p is prime and h a natural number, hence there is an infinite number of choices for the order q.

Projective subspaces

It has already been noted that there is a 1-1 correspondence between the points of a projective n-space and the one-dimensional subspaces of a linear (n+1)-space. This is now generalised for the subspaces of the projective n-space. Subspaces of the projective n-space are defined as linear combinations of points of the projective space, in the same manner as for linear spaces. The concepts of linear dependence and independence for projective spaces also follow the definitions for linear spaces. Thus a point p of the projective n-space is independent of the projective subspace S if and only if the map of p in the linear (n+1)-space in independent of the map of S in the linear (n+1)-space. Assigning dimension 0 to the points of the projective space, dimension 1 to its lines, and so on, it follows from the above considerations that a bijection exists between the r-subspaces of the n-dimensional projective space and the (r+1)-subspaces of the (n+1)-dimensional linear space over the same field.

This mapping of the subspaces of the projective space to the subspaces of the linear space preserves inclusion, hence the lattice structure of the linear space induces a lattice structure of the projective space.

A basis of a projective subspace is a set of independent points which span the subspace. While in the case of the linear space a basis of an r-space contains r elements, the number being equal to the dimension of the subspace, it is seen from the above that an r-subspace of the projective n-space is spanned by r+1 basis-elements.

However, Grassman's identity as in (3.5) is still valid in the projective case, since the difference between numbers of basis-elements and dimensions is the same on both sides.

Some authors use the term "rank" for the number of basis-elements of the subspace, where

rank = dimension + 1.

A list of dimensions and ranks follows. The empty set is counted as a subspace, complying with the lattice structure of the set of projective subspaces.

	Dimension	No. of basis-elements (rank)
Empty set	-1	0
Point	0	1
Line	1	2
Plane	2	3
"Solid"	3	4
:		
Hyperplane	n-1	n
Whole space	n	n+1

Duality

The principle of duality for projective planes can be generalised for projective n-spaces. Hyperplanes are maximal dimensional proper subspaces of the n-space, their dimension being n-1. The points of a hyperplane are given by the points of the solution-space of the homogeneous linear equation

$$a_1x_1 + a_2x_2 + \dots + a_{n+1}x_{n+1} = 0 \qquad (4.3)$$

so the hyperplane h is determined by the n+1-tuple:

$$h = [a_1, a_2, \dots, a_{n+1}] \text{ where } a_i \in k \text{ (the field)}$$

$$(i=1,2,\dots,n+1),$$

not all the a_i's being equal to zero.

More precisely, as in the case of points, the hyperplane is determined by the set

$$\rho[a_1, a_2, \dots, a_{n+1}] \quad (\rho \in k, \rho \neq 0).$$

Again, in the equation (4.3) the vectors $(x_1, \dots, x_{n+1})$ and $[a_1,\dots, a_{n+1}]$ play equal roles.

A dual map of the projective space is introduced by interchanging points and hyperplanes, together with the words "contains" or "contained by", describing incidence.

General subspaces are determined by the intersection of a set of hyperplanes $\{h_i\}$, of which r are independent, meaning that r of the vectors $[a_1, a_2, \ldots, a_{n+1}]^{(i)}$ are linearly independent. A set of homogeneous linear equations of rank r is generated by these hyperplanes and so the solution-space is spanned by n+1-r basis-vectors $(x_1, \ldots, x_{n+1})^{(j)}$, hence the dimension of the intersection-space is

$$n-r.$$

At the same time, the dimension of the space spanned by the duals of the h_i vectors (r in number) is r-1.

Hence the sum of the dimensions of a subspace of the projective n-space and its dual is n-1.

The lattice of projective subspaces is associated with the dual lattice obtained by exchanging "meet" and "join". Each theorem of the projective space induces its dual.

Finite spaces

The projective n-space over the field GF(q) is denoted by

$$PG(n,q).$$

The number of points in PG(n,q) is

$$\frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + \ldots + q + 1 \qquad (4.4)$$

(equal to the number of lines (through σ) in V(n+1,q).

The number of r-dimensional subspaces of PG(n,q) can also be written down, assuming formula (3.6) for subspaces of V(n,q) and using the 1-1 correspondence between r-subspaces of PG(n,q) and (r+1)-subspaces of V(n+1,q).

The number of r-subspaces of PG(n,q) is

$$\begin{bmatrix} n+1 \\ r+1 \end{bmatrix}_q = \frac{(q^{n+1}-1)(q^n-1)\ \cdots\ (q^{n-r+1}-1)}{(q-1)(q^2-1)\ \cdots\ (q^n-1)} \tag{4.5}$$

5. Collineation Groups

[13], [5], [21].

A collineation (or automorphism) of a linear or projective space is a bijective map of the space to itself, which preserves incidence. The set of all collineations form a group, finite, if the space is finite.

The Group GL(n,q)

A transformation of the linear space V(n,q) such that the matrix of the transformation is non-singular is linear, hence it preserves incidence and is bijective, hence it is a collineation. All non-singular linear transformations of V(n,q) form a group under composition, denoted by GL(n,q).

The order of the group can be determined by counting all the bases of V(n,q):

$$|GL(n,q)| = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i-1). \tag{5.1}$$

Field automorphisms and collineations

Let τ be a field-automorphism of the field GF(q). The transformation τ on the points of V(n,q) takes

$$p = (a_1, a_2, \ldots, a_n)$$

to

$$\tau(p) = (\tau(a_1), \tau(a_2), \ldots, \tau(a_n))$$

for all $p \in V(n,q)$.

This transformation is again bijective and preserves incidence, hence it is a collineation.

A semilinear transformation is the composition of a linear transformation and a field automorphism. The group of semilinear transformations of $V(n,q)$ is denoted by

$$\Gamma L(n,q).$$

If q is the h^{th} power of some prime, then the order of the automorphism group of the field is h, hence the order of $\Gamma L(n,q)$ is

$$|\Gamma L(n,q)| = hq^{n(n-1)/2} \prod_{i=1}^{n} (q^i-1)$$

Finite projective groups

Homographies (called projectivities by some authors).

A homography is a transformation of $PG(n,q)$ induced by a non-singular linear transformation on the equivalence classes of points in $V(n+1,q)$ representing the points of $PG(n,q)$.

More explicitly:

Let p and p' be points of $PG(n,q)$, where

$$p = (a_1 \ \ a_2 \ \ \ldots \ a_{n+1})$$

$$p' = (b_1 \ \ b_2 \ \ \ldots \ b_{n+1})$$

and suppose that the homography takes p to p'.

Let P, P' be column-vectors, formed by the components of p and p' respectively. Let H be an $(n+1) \times (n+1)$ non-singular matrix over $GF(q)$, called the matrix of homography. Then

$$\rho P' = HP, \text{ where } \rho \in GF(q)\backslash\{0\} \qquad (5.2)$$

The group of homographies of $PG(n,q)$ is denoted by

$$PGL(n+1,q).$$

The order of $PGL(n+1,q)$ is

$$|PGL(n+1,q)| = q^{n(n+1)/2} \prod_{i=2}^{n+1} (q^i-1) \qquad (5.3)$$

As in the case of linear spaces, the composition of a homography and a field automorphism yields a collineation in PG(n,q). The converse can be stated as the

Fundamental Theorem of Projective Geometry

All collineations of PG(n,q) are of form

$$\tau H,$$

where H is a homography and τ a field automorphism.

The proof is omitted here, but note is taken of the fact that the fundamental theorem is the direct consequence of two equally important results:

Theorem A

The group of homographies of PG(n,q), which is the group PGL(n+1,q) is transitive on ordered sets of n+2 points, no n+1 linearly dependent.

Theorem B

A collineation leaving an ordered set of n+2 points, no n+1 linearly dependent, fixed, induces an automorphism of the field GF(q).

Theorem A can be stated in an even stronger form : there exists a unique homography which transforms an ordered set of n+2 points, no n+1 linearly dependent, into any other ordered set of n+2 points of the same structure in PG(n,q).

In particular, when the geometry is P(1,q), the geometry of the line, then there is a unique homography transforming an ordered set of three distinct points into any other ordered set of three distinct points.

It follows from the above that in coordinatising, any set of n+2 points, no n+1 dependent, can be chosen as the fundamental set:

$$\begin{matrix} (1 & 0 & .. & 0) \\ (0 & 1 & .. & 0) \\ \vdots \\ (0 & 0 & .. & 1) \\ (1 & 1 & .. & 1). \end{matrix}$$

Correlations

A correlation is a one to one mapping of a projective space to its dual. Points are mapped onto hyperplanes and hyperplanes onto points such that incidence relations are preserved : all points of a hyperplane map to hyperplanes containing the same point, and hyperplanes through a point to points in the same hyperplane. It follows that dependence and independence relations are preserved. One way of realising such a correlation is by mapping points $(a_1, a_2, \ldots, a_{n+1})$ to hyperplanes represented by vectors $[a_1, a_2, \ldots, a_{n+1}]$. The product of two correlations is a collineation.

6. Involutions, perspectivities, cyclic groups

[4], [19], [21]

This final section concentrates on subgroups of collineation groups of projective spaces which have relevance to this work.

Of special interest are those groups which leave certain configurations fixed. They are of significance not only in the case of Galois planes, but also in the general case.

The following definitions refer to general projective planes.

Closed configurations

A set of points and lines of the projective plane form a closed configuration if the intersection of any two lines and the join of any two points of the set belongs to the set.

Examples:

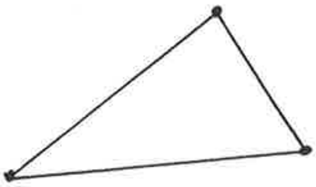
The empty set (vacuously),

the whole plane,

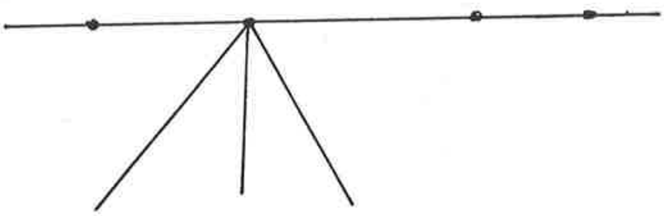
a single line with any number of points on it:

a single point, with any number of lines through it:

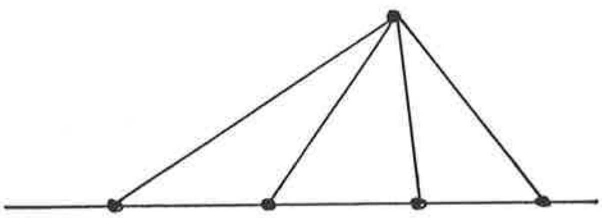
the sides and vertices of a triangle:



a line with some points on it and a number of lines through one of the points:



a line with some points on it, and an external point, with lines joining the external point to the selected points on the line:



Subplanes

If a closed configuration contains a non-degenerate quadrangle, then it follows from the axioms, that it is a projective plane. It is a subplane if it is properly contained in the projective plane of reference.

Example :

All Galois planes PG(2,q) have proper subplanes if $q = p^h$, where $h > 1$.

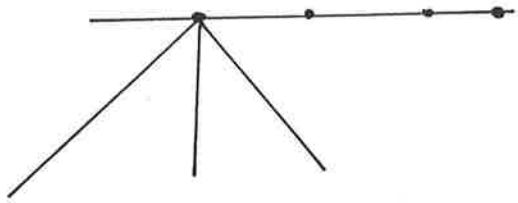
Dense sets (Baer sets)

If a closed configuration is such that each line of the projective plane contains a point of the configuration, and each point of the plane is on some line of the configuration, then the configuration is dense in the plane.

Non trivial examples in a plane of order q:

(i) a configuration of q+2 points and q+2 lines as shown in the figure:

(ii) a configuration of q+1 points and q+1 lines as shown:



Baer subplanes

A Baer subplane, or as it will be referred to subsequently, a Baer-plane is a proper subplane of the projective plane, dense in the plane.

All Galois planes of square order possess Baer-planes. They form the topic of Chapter 2.

Let θ be a collineation of the projective plane. The fixed set of the collineation: $F(\theta)$ is the set of points and lines which are mapped into themselves by θ.

$F(\theta)$ is a closed configuration for all θ.

An involution is a collineation of order 2.

A perspectivity is a collination which fixes all the lines through some point V, called the vertex of the perspectivity.

The following results hold for all projective planes.

1. If θ is an involution, then $F(\theta)$ is a dense set.

2. If θ is a perspectivity, then there is a line ℓ, called the axis of perspectivity, such that all the points on ℓ are fixed by the perspectivity. Conversely, if a collineation fixes all the points on a line ℓ, then it is a perspectivity, that is for some point V, all the lines through V are fixed by this collineation. The perspectivity is called a (V,ℓ)-perspectivity. It is called an elation if V is on ℓ, and a homology otherwise.
3. The (V,ℓ)-perspectivities, for a fixed pair (V,ℓ) form a group, denoted by $\Gamma(V,\ell)$. No element of $\Gamma(V,\ell)$, other than the identity, fixes any point of the plane P, other than V and the points on ℓ, and fixes no line of Π other than ℓ or the lines through V. The image of one (non-fixed) point or line determines the collineation.
4. If a closed set is dense in P, then it is either a Baer-plane, or the fixed set of some (V,ℓ) perspectivity.

(V,ℓ)-transitivity

The perspectivity group $\Gamma(V,\ell)$ is said to be transitive if for each pair of points p, p' such that V, p, p' are collinear and p and p' are not on ℓ, there exists an element $\theta \in \Gamma(V,\ell)$ such that

$$p' = \theta p.$$

In a finite projective plane of order q, $\Gamma(V,\ell)$ is transitive if and only if

$$|\Gamma(V,\ell)| = q \text{ and } V \in \ell \text{ (elation-group)}$$

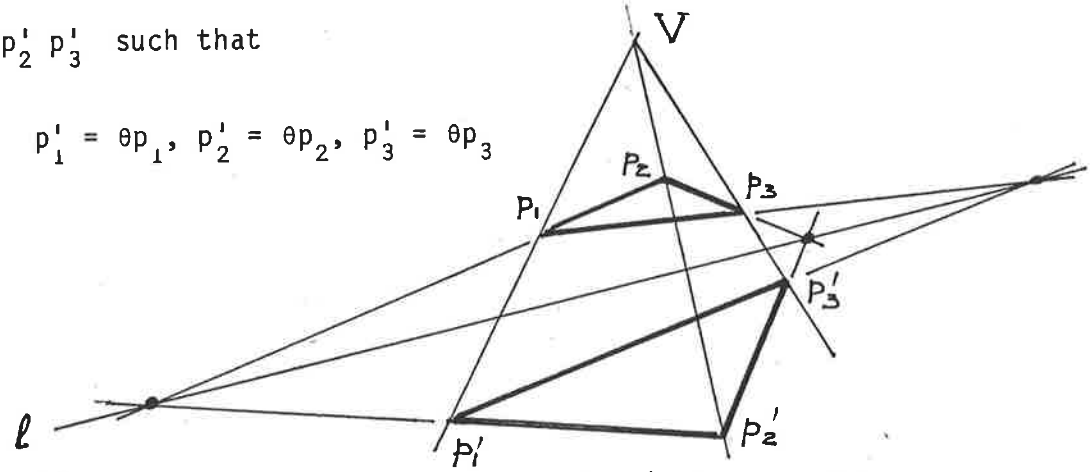
or

$$|\Gamma(V,\ell)| = q-1 \text{ and } V \notin \ell \text{ (homology group).}$$

Desargues configurations

Let θ be a (V,ℓ)-perspectivity, and the triangles $p_1\, p_2\, p_3$ and $p_1'\, p_2'\, p_3'$ such that

$$p_1' = \theta p_1,\ p_2' = \theta p_2,\ p_3' = \theta p_3$$



Then the 10 points : p_1, p_2, p_3, p_1', p_2', p_3', V, $p_1p_2 \cap \ell$, $p_2p_3 \cap \ell$, $p_1p_3 \cap \ell$ and the 10 lines : p_1p_2, p_1p_3, p_2p_3, $p_1'p_2'$, $p_2'p_3'$, $p_3'p_1'$, p_1p_1', p_2p_2', p_3p_3', ℓ are said to form a Desargues-configuration. (Here $p_1p_2 \cap \ell = p_1'p_2' \cap \ell$, and so on.)

By the classical Desargues-theorem, two triangles in the extended Euclidean plane are in perspective from a point, if and only if they are in perspective from a line, or (using the above definition), two triangles in perspective from a point, extend to a 10 point - 10 line Desargues configuration, as seen above.

For the general projective plane, the axioms do not imply Desargues' theorem, but projective planes which are subspaces of a higher dimensional space are Desarguesian.

Non-Desarguesian projective planes have been found in numbers ([32], [17], [1], [35]). However, some theorems on Desarguesian configurations apply to classes of projective planes wider than that of Desarguesian planes.

It was shown [22], that all finite projective planes admit Desarguesian configurations. This however does not imply the existence of non-trivial (V,ℓ)-perspectivity groups.

Of particular interest are those projective planes which are (V,ℓ)-Desarguesian. These are projective planes for which Desargues' theorem holds for a particular pair (V,ℓ).

Baer's Theorem [3]

A projective plane is (V,ℓ)-Desarguesian if and only if it is (V,ℓ)-transitive.

Thus the Galois plane is (V,ℓ)-Desarguesian and (V,ℓ)-transitive for all pairs (V,ℓ).

General projective planes, for which $q > 4$ have been completely classified by their sets of possible configurations of (V,ℓ)-pairs, for which (V,ℓ)-transitive collineation groups exist. This is the Lenz-Barlotti classification [35].

Singer's Theorem

Collineation groups of special interest are cyclic groups, generated by a single collineation σ, denoted by $\Xi = \langle\sigma\rangle$. If p is a point of the projective space (dimension ≥ 2), the orbit of p under the action of a collineation group Ξ is the set of points Ξp.

If the group $<\sigma>$ is transitive on the totality of points of a space, then the space is called cyclic. This is not always the case when the space is two-dimensional, hence cyclic projective planes form a special class of planes, with some existence problems still unresolved. However, Galois planes (2,q) are cyclic for all $q = p^h$, as all projective spaces PG(n,q) are cyclic. The cyclic nature of projective spaces plays a focal role in this present work, so the proof of the following fundamental theorem will be described in detail.

Theorem (Singer [27], [18])

Projective spaces PG(n,q) are cyclic : there exist cyclic groups acting transitively on the points and the hyperplanes of PG(n,q).

Proof

Let PG(n,q) be a projective space. The points are represented by (n+1)-vectors over the field GF(q), (or rather by equivalence classes of such vectors), hence they can be listed as elements of the field

$$GF(q^{n+1}).$$

Since Galois-fields have cyclic multiplicative groups (excluding the element 0), there exists some element $\alpha \in GF(q^{n+1})$ such that the set

$$\{\alpha^i | 0 \leq i < q^{n+1} - 1\}$$

gives the set of all non-zero elements of the field.

As $GF(q^{n+1})$ is an extension field of GF(q), there exists some irreducible polynomial equation of degree (n+1), such that α is one of its roots. Let this equation be

$$x^{n+1} = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0 \tag{6.1}$$

Equation (6.1) will be referred to as the <u>generating equation of the Singer-group.</u>

For the root α we have then

$$\alpha^{n+1} = c_n \alpha^n + c_{n-1} \alpha^{n-1} + \dots + c_1 \alpha + c_0 \tag{6.2}$$

Assign to α^{n+1} the vector determined by the coefficients on the left hand side of (6.2). Thus

$$\alpha^{n+1} \leftrightarrow (c_n, c_{n-1}, \dots, c_1, c_0) \tag{6.3}$$

Assign also to α^i $(0 \leq i \leq n)$ a vector which has only one non-zero component, which will be taken to be 1, and the first n-i and the last i components are zero. Thus

$$\left.\begin{array}{l} \alpha^0 \leftrightarrow (0\ \ 0\ \ \dots\ \dots\ \dots\ 1) = p_0 \\ \alpha^1 \leftrightarrow (0\ \ 0\ \ \dots\ \dots\ 1\ \ 0) = p_1 \\ \alpha^2 \leftrightarrow (0\ \ 0\ \ \dots\ 1\ \ 0\ \ 0) = p_2 \\ \quad\vdots \\ \alpha^n \leftrightarrow (1\ \ 0\ \ 0\ \ \dots\ \ 0) = p_n \end{array}\right| \tag{6.4}$$

Hence if for $i=1,2,\dots,(n+1)$ α^i is expressed as a linear combination of elements of the set

$$\{\alpha^0 = 1, \alpha, \alpha^2, \dots, \alpha^n\}$$

then the corresponding components of the vectors in (6.3) and (6.4) are the coefficients of the powers of α in the expansions.

Assume now inductively that

$$\alpha^j = a_n^{(j)} \alpha^n + a_{n-1}^{(j)} \alpha^{n-1} + \dots + a_1^{(j)} \alpha + a_0^{(j)}$$

Then

$$\alpha^{j+1} = a_n^{(j)}\alpha^{n+1} + a_{n-1}^{(j)}\alpha^n + \ldots + a_1^{(j)}\alpha^2 + a_0^{(j)}\alpha$$

Substituting for α^{n+1} at the right hand side of (6.2) we obtain

$$\alpha^{j+1} = a_n^{(j+1)}\alpha^n + a_{n-1}^{(j+1)}\alpha^{n-1} + \ldots + a_1^{(j+1)}\alpha + a_0^{(j+1)},$$

where

$$a_i^{(j+1)} = c_i a_n^{(j)} + a_{i-1}^{(j)} \text{ for } i=1 \text{ to } n$$

and

$$a_0^{(j+1)} = c_0 a_n^{(j)} \qquad (6.5)$$

Hence the transformation taking the vector $(a_n^{(j)} a_{n-1}^{(j)} .. a_1^{(j)}\ a_0^{(j)})$ assigned to α^j to the vector assigned to α^{j+1} is a linear transformation. In particular, the vectors (6.3) and (6.4) satisfy the general transformation - equation (6.5), so the matrix of the transformation is obtained immediately as

$$M = \begin{vmatrix} c_n & 1 & 0 & . & . & 0 \\ c_{n-1} & 0 & 1 & . & . & 0 \\ \vdots & & & & & \\ c_1 & 0 & 0 & . & . & 1 \\ c_0 & 0 & 0 & . & . & 0 \end{vmatrix} \qquad (6.6)$$

This matrix M will be referred to as the Singer matrix. The generating polynomial of the Singer group

$$x^{n+1} - c_n x^n - c_{n-1}x^{n-1} - \ldots - c_0$$

is the left-hand side of the characteristic equation of M, and α and its conjugates are the eigenvalues of M.

Let θ^* be the linear transformation induced by the matrix M. Since the set $\{\alpha^j\}$ gives all the elements of $GF(q^{n+1})\backslash\{0\}$, it follows that the cyclic group $<\theta^*>$ acts transitively on the non-zero vectors of $V(n+1,q)$, so there is a bijection between the set

$$\{\alpha^j | \ 0 \leq j < (q^{n+1} - 1)\}$$

and the $q^{n+1} - 1$ non-zero vectors of $V(n+1,q)$.

The points of $PG(n,q)$ are represented by equivalence classes of points in $V(n+1,q)$, each equivalence class having $q - 1$ elements.

Two vectors of $V(n+1,q)$:

$$v_1 = (a_n \ \ a_{n-1} \ \ .. \ a_0)$$

and

$$v_2 = (b_n \ \ b_{n-1} \ \ .. \ b_0)$$

represent the same point in $PG(n,q)$ if and only if

$$b_i = \rho a_i \qquad \text{for } i=0 \text{ to } n+1,$$

ρ being a constant for this set and a non-zero element of $GF(q)$.

Thus if α^{j_1} and α^{j_2} are assigned to v_1 and v_2 respectively, it follows that

$$\alpha^{j_2} = \rho \ \alpha^{j_1}$$

where $\rho = \alpha^r$ and since $\rho \in GF(q)$,

$$\rho^{q-1} = \alpha^{r(q-1)} = 1.$$

Since α is primitive, this happens if and only if $q^{n+1} - 1$ divides $r(q-1)$, or if r is a multiple of $(q^{n+1}-1)/(q-1)$. Thus the set $\{\alpha^j | \ 0 \leq j < (q^{n+1}-1)/(q-1)\}$ represents $(q^{n+1}-1)/(q-1)$ non-equivalent vectors of $V(n+1,q)$ and so represents all $(q^{n+1}-1)/(q-1)$ points of $PG(n,q)$.

The projective transformation (homography) induced by θ^* is denoted by σ for Singer transformation and

$$\Xi = \langle\sigma\rangle$$

is the cyclic Singer group, where

$$|\langle\sigma\rangle| = (q^{n+1}-1)/(q-1) \text{ for } PG(n,q).$$

The group $\Xi = \langle\sigma\rangle$ is said to act <u>regularly</u> on the points of PG(n,q) because

(i) it fixes no point in PG(n,q);

(ii) it is transitive on the points of PG(n,q).

<u>Note:</u> (For the purposes of the proof it was assumed that the roots of the generating equation (6.1) are primitive elements of $GF(q^{n+1})$, because the existence of primitive elements is known. It is sufficient to use a primitive element α for the bijection between the first $(q^{n+1}-1)/(q-1)$ powers of α and the points of PG(n,q). However, this is not necessary. It suffices to use any element of $GF(q^{n+1})$ which has $(q^{n+1}-1)/(q-1)$ successive powers which can be assigned to different points of PG(n,q).)

It remains to be shown that <u>Ξ acts</u> also <u>regularly</u> on the <u>hyperplanes</u> of PG(n,q).

Suppose h_1 is a hyperplane. Without loss of generality it may be assumed that

$$p_0 = (0 \;\; 0 \;\; . \;\; . \;\; 1) \in h_1.$$

Suppose that the length of the orbit of h_1 under the action of Ξ is L. This means that L is the <u>smallest</u> integer for which

$$\sigma^L(h_1) = h_1 \qquad (6.7)$$

Denote $R = (q^{n+1}-1)/(q-1)$, (the number of points of PG(n,q)).

Then $\sigma^R(h_\perp) = h_\perp$, since for all points p, $\sigma^R(p) = p$.

Thus L divides R.

By (6.7) $\sigma^L(p_0) = p_L$ is in $h_\perp$, hence p_{2L}, p_{3L} and so on are in $h_\perp$.

Let t be the <u>smallest</u> integer for which

$$p_{tL} = p_0.$$

Then R divides tL.

But L divides R and t is minimal, hence

$$t = R/L. \tag{6.8}$$

Suppose that the set $\{p_{kL} | k \text{ integer}\}$ does not include all the points of $h_\perp$. Then for a point $p_i \in h_\perp$, not in the cycle, there is another cycle of points

$$\{p_{i+kL} | k \text{ integer}\} \text{ in } h_\perp \text{ and disjoint from } \{p_{kL}\}.$$

So $h_\perp$ consists of cycles, each of length t. Denote $R_\perp = (q^n-1)/(q-1)$, the number of points in $h_\perp$.

Then t divides $R_\perp$ and by (6.8) it divides R, so t is a common divisor of R and $R_\perp$ where

$$R - R_\perp = q^n.$$

Hence R and $R_\perp$ are co-prime, and so $t = 1$.

Thus, by (6.8)

$$L = R = (q^{n+1}-1)/(q-1).$$

By (4.5) the number of hyperplanes in PG(n,q^2) is the same as the number of points. Thus the length of the orbit L is equal to the number of hyperplanes, so Ξ acts regularly on the hyperplanes in PG(n,q). This completes the proof. □

Difference Sets

Singer's theorem is valid for PG(2,q), hence Galois planes are cyclic. Here the hyperplanes are lines. Singer's theorem provides a natural ordering to the points and lines. Using orderings as before, we denote

$p_0 = (0 \;\; 0 \;\; 1)$
$p_1 = (0 \;\; 1 \;\; 0)$
$p_2 = (1 \;\; 0 \;\; 0)$
$p_3 = (c_2 \;\; c_1 \;\; c_0)$ where $x^3 = c_2x^2 + c_1x + c_0$

is the generating cubic.

For lines:

$\ell_0 = p_0p_1$
$\ell_1 = p_1p_2$
$\ell_2 = p_2p_3$ and so on.

The subscripts marking the points and lines are called Singer-indices.

If there is no ambiguity we may denote the points (or lines) by their Singer indices only.

The q+1 points on line ℓ_0 are

$D = \{0, 1, \ldots \}$

We show that these q+1 numbers denoting Singer indices of the points on line ℓ_0 form a perfect difference set modulo $(q^2 + q + 1)$.

This means that for all non-zero elements a of the set of residue classes modulo $(q^2 + q + 1)$, there is a unique pair (i,j) chosen out of the q+1 indices (mod $q^2 + q + 1$) in the set D, such that

$i - j = a \pmod{q^2 + q + 1}$.

Proof

There is a unique line ℓ_t containing the points 0 and a. Then 0 and a are the t^{th} images of two points on line ℓ_0. Let i,j be the Singer indices of these two points. Then

$$\left.\begin{array}{l} i + t = 0 \\ j + t = a \end{array}\right| \pmod{q^2 + q + 1},$$

hence $a = j - i \pmod{q^2 + q + 1}$.

Since the number of ordered pairs chosen out of the q+1 elements of the set D is

$$(q+1)q = q^2 + q,$$

it follows that each non-zero element of the $q^2 + q + 1$ Singer indices representing the points of PG(2,q) has just one representation as a difference. □

Note: If D is a perfect difference set, then so is the set D+s, where s (shift) is added to each of the elements of D, as $(i+s)-(j+s) = i - j$.

It follows that the Singer indices of any line in PG(2,q) form perfect difference sets $\pmod{q^2 + q + 1}$.

CHAPTER ONE

FINITE LINEAR SPACES AND GAUSSIAN COEFFICIENTS [30]

1.1 Introduction

Gaussian coefficients is the name given to a class of rational functions, playing a fundamental role in describing the structure of affine and projective spaces over a finite field. They will be denoted in this work by the symbol

$$\begin{bmatrix} n \\ r \end{bmatrix}_q$$

and defined for all $q \neq 1$ and non-negative integers n, r as

$$\begin{aligned}\begin{bmatrix} n \\ r \end{bmatrix}_q &= \frac{(q^n-1)(q^{n-1}-1) \ldots (q^{n-r+1}-1)}{(q-1)(q^2-1) \ldots (q^r-1)} \quad \text{when } 0 < r < n \\ &= 1 \text{ when } r = 0 \\ &= 0 \text{ otherwise.}\end{aligned} \qquad (1.1)$$

As the name shows, these rational functions were first studied by Gauss who proved their fundamental properties. The relation of these coefficients to linear spaces over finite fields was discovered later. They play also a basic role in the theory of partitions. However, in this work their study is linked with the study of linear spaces.

The notation used highlights the analogy between the Gaussian coefficients and the binomial coefficients

$$\begin{bmatrix} n \\ r \end{bmatrix} = \frac{n(n-1) \ldots (n-r+1)}{1 \,.\, 2 \ldots r}$$

In fact, we may write (1.1) as

$$\begin{aligned}\begin{bmatrix} n \\ r \end{bmatrix}_q &= \frac{(q^n-1) \ldots (q^{n-r+1}-1)}{(q-1)^r} \Bigg/ \frac{(q-1) \ldots (q^r-1)}{(q-1)^r} \\ &= \prod_{j=n-r+1}^{n} \sum_{i=0}^{j-1} q^i \Bigg/ \prod_{j=1}^{r} \sum_{i=0}^{j-1} q^i\end{aligned} \qquad (1.2)$$

for all $q \neq 1$ and $0 \leqslant r \leqslant n$.

If (1.2) is used as the defining formula for $\left[{n \atop r}\right]_q$ instead of (1.1), then the definition is valid for all q. In particular, when q = 1, the formula (1.2) yields the binomial $\binom{n}{r}$.

In this sense the Gaussians may be regarded as generalisations of the binomial coefficients and identities established for Gaussians must yield binomial identities for q = 1. We may say that Gaussian coefficients provide the connection between elements of the lattice of subspaces of a linear space in a manner analogous to the role played by binomial coefficients connecting the elements of the lattice of subsets of a set. The aim of this chapter is to explore these analogies, by looking first at the better known binomial relationships and finding the corespondent relations between Gaussians together with their implications to the structure of linear spaces. To this end we begin with the proof of the formula determining the number of subspaces of a linear subspace over a finite field, discussed already in the introductory chapter (cf. formula (3.6) in Introduction).

1.2 The Geometrical Meaning of the Gaussian Coefficients

The theorem proved below is well known, [13], [2], but for completeness the proof will be presented here.

Thereom 1.1 : Let V be a linear space of dimension n over the field GF(q), $q = p^h$ (p prime). The number of subspaces of dimension r is given by $\left[{n \atop r}\right]_q$.

Proof : (For brevity the subscript q is omitted whenever we deal with spaces over a fixed finite field. Subspaces of dimension r will be called shortly r-spaces.)

Each r-space of V can be specified by selecting a set of r linearly independent vectors out of the vectors of the n-space V, which has q^n-1 non-zero vectors.

Thus the first choice for a basis vector can be made in q^n-1 ways. For each successive basis vector we must exclude all the vectors of the spaces spanned by the basis vectors already fixed. Thus, the number of choices is

$$(q^n-1)(q^n-q) \;\ldots\; (q^n-q^{r-1})$$

However, the same r-space may be obtained by a different choice of basis elements. By reasoning similar to the above, the choice of r linearly independent vectors in a fixed r-space can be made in

$$(q^r-1)(q^r-q) \;\ldots\; (q^r-q^{r-1})$$

ways. Thus the number of r-spaces in the n-space V is

$$\frac{(q^n-1)(q^n-q)..(q^n-q^{r-1})}{(q^r-q^{r-1})(q^r-q^{r-2})..(q^r-1)} = \frac{q^{\binom{r}{2}}(q^n-1)..(q^{n-r+1}-1)}{q^{\binom{r}{2}}(q-1)..(q^r-1)}$$

where $q^{\binom{r}{2}} = q.\, q^2 \;..\; q^{r-1} = q^{(r(r-1))/2}$.

Simplifying, we obtain $\binom{n}{r}_q$ as claimed. □

1.3 Basic Properties of the Gaussian Coefficients

The fundamental properties of the binomial coefficients can be best visualised by exhibiting them in the Pascal triangle. Three properties of the binomials are immediately apparent and the elementary proofs of these properties are well known. We list here these for comparison with Gaussian coefficients. They are

(i) Unimodularity : $\binom{n}{r} > \binom{n}{r-1}$ for $r < 1/2\,(n+1)$

and

$\binom{n}{r} < \binom{n}{r-1}$ for $r > 1/2\,(n+1)$.

(ii) Symmetry: $\binom{n}{r} = \binom{n}{n-r}$.

(iii) Pascal's recursion: $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$.

For the Gaussian coefficients $\begin{bmatrix} n \\ r \end{bmatrix}_q$ tables are constructed by calculating the coefficients for q=2,3,4,5 and for small values of n. In addition the sums of the rows of the Gaussian tables are also shown.

$$\sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix}_q = G_n(q).$$

These sums are called Galois numbers.

Inspecting the tables, it is immediately apparent that properties (i) and (ii) of the binomials are also valid for Gaussians, while property (iii) does not hold. For Gaussians the Pascal recursion formula takes the form

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \begin{bmatrix} n-1 \\ r-1 \end{bmatrix}_q + q^r \begin{bmatrix} n-1 \\ r \end{bmatrix}_q \qquad (3.1)$$

or

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \begin{bmatrix} n-1 \\ r \end{bmatrix}_q + q^{n-r} \begin{bmatrix} n-1 \\ r-1 \end{bmatrix}_q \qquad (3.2)$$

These relations were known by Gauss, and their algebraic verification is easy, but it is omitted here. Instead, a combinatorial interpretation will be given to the fundamental relations as well as to more complex identities involving Gaussians.

Gaussian tables

q = 2

$$G_n = \sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix}$$

										G_n
n=0	1									1
n=1	1	1								2
n=2	1	3	1							5
n=3	1	7	7	1						16
n=4	1	15	35	15	1					67
n=5	1	31	155	155	31	1				374
n=6	1	63	651	1395	651	63	1			2825
n=7	1	127	2667	11811	11811	2667	127	1		29212
n=8	1	255	10795	97155	200787	97155	10795	255	1	417199

q = 3

n=0	1									1
n=1	1	1								2
n=2	1	4	1							6
n=3	1	13	13	1						28
n=4	1	40	130	40	1					212
n=5	1	121	1210	1210	121	1				2664
n=6	1	364	11011	33880	11011	364	1			56632
n=7	1	1093	99463	925771	925771	99463	1093	1		2052656
n=8	1	3280	896260	25095280	75913222	25095280	896260	3280	1	127902864

q = 4

$G_n = \sum_{r=0}^{n} \begin{bmatrix} n \\ r \end{bmatrix}$

									G_n
n=0	1								1
n=1	1	1							2
n=2	1	5	1						7
n=3	1	21	21	1					44
n=4	1	85	357	85	1				529
n=5	1	341	5797	5797	341	1			12278
n=6	1	1365	93093	376805	93093	1365	1		565723
n=7	1	5461	1490853	24208613	24208613	1490853	5461	1	51409856

q = 5

n=0	1								1
n=1	1	1							2
n=2	1	6	1						8
n=3	1	31	31	1					64
n=4	1	156	806	156	1				1120
n=5	1	781	20306	20306	781	1			42176
n=6	1	3906	508431	2558556	508431	3906	1		3583232
n=7	1	19531	12714681	320327931	320327931	12714681	19531	1	666124288

For the binomial coefficients, that is, for the case, q=1, the Galois number $G_n(1)$ is well known and can be listed as property (iv) of the binomials:

(iv) $$\sum_{r=0}^{n} \binom{n}{r} = 2^n = G_n(1).$$

One way of proving (iv) for binomials is by using recursion:

$$G_n = 2\, G_{n-1}.$$

By a suitable interpretation the recursion formula will be generalised for q > 1. It is clear from the tables that here G_n increases more rapidly with n. The recursion formula for Gaussians is

$$G_n = 2\, G_{n-1} + (q^{n-1}-1)G_{n-2} \tag{3.3}$$

Before proving (3.1), (3.2), (3.3) by their geometrical interpretation to be done in the next section, the unimodularity and symmetry of the Gaussians can be settled.

Unimodularity : This is verified exactly the same way as for binomials.

Symmetry : We recall the combinatorial interpretation of the relation

$$\binom{n}{r} = \binom{n}{n-r}.$$

When choosing r out of a set of n, we choose simultaneously n-r elements to be left behind. The corresponding interpretation for Gaussians is not quite as direct. Two alternatives can be given.

(a) Orthogonal complements

Fix a basis and coordinate system, and define the inner product of the vectors

$$\underset{\sim}{x} = (x_1, x_2, \ldots, x_n),\ \underset{\sim}{y} = (y_1, y_2, \ldots, y_n)$$

in the usual way as

$$p = \sum_{i=1}^{n} x_i y_i$$

Two vectors are orthogonal if this inner product is zero. Let V_r be an r dimensional subspace of V_n (dimension n). The orthogonal complement of V_r is the set of vectors orthogonal to all the vectors of V_r. These form a subspace of V_n of dimension n-r. Thus there is a bijection from the r-spaces of V_n to their orthogonal complements which are (n-r)-spaces.

(b) Duality

The r-spaces of V_n can be mapped to the (n-r)-spaces of the dual space of V_n defined by the q^n linear transformations of V_n to itself.

1.4 Subset and Subspace Intersections

The basic difference between binomials, which count subsets and Gaussians which count subspaces manifests itself in the greater complexity of intersection relations of the latter.

The general intersection relation from which the special cases can be deduced, is analogous to the count of the number of k-sets intersecting a fixed r-subset R of the n-set S_n in a fixed f-set F.

This count is

$$\binom{n-r}{k-f},$$

for there are k-f elements of S_n to be chosen to complete the fixed f-set, and these must be selected out of n-r elements of S_n which are not contained in R.

The corresponding relation for linear subspaces can be summarised in the following theorem.

Theorem 1.2

Let V be an n dimensional linear space over GF(q), R and F fixed subspaces of V of dimensions r and f respectively and $F \subset R$.

The number of k-spaces which intersect the subspace R exactly in F is

$$N_{k,r,f} = \begin{bmatrix} n-r \\ k-f \end{bmatrix} q^{(k-f)(r-f)} \qquad (4.1)$$

(Note: for q = 1 the formula agrees with the binomial coefficient calculated above.)

Proof

Choose a basis for V by beginning with a set

$$X = \{\underset{\sim}{x}_1, \underset{\sim}{x}_2, \ldots, \underset{\sim}{x}_f\}$$

of basis vectors spanning F, and complete it to a basis for R by the independent set

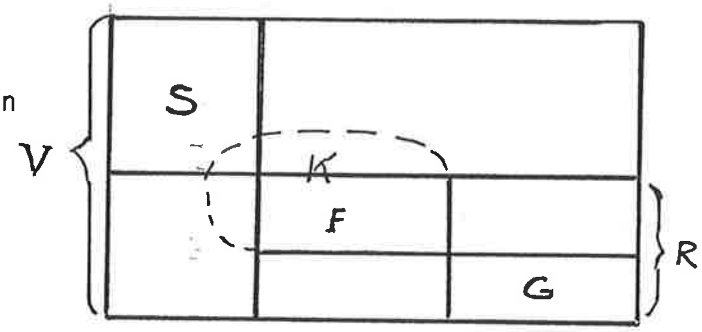
$$Y = \{\underset{\sim}{y}_1, \underset{\sim}{y}_2, \ldots, \underset{\sim}{y}_g\}$$

where $y_i \in R$ (i=1,..,g) and g = r-f.

Complete this to a V-basis by choosing a third linearly independent set:

$$Z = \{z_1, z_2, \ldots, z_s\}$$

where $s = n-r$.



The sets X,Y,Z are to span spaces F,G,S mutually orthogonal. Let K be a k-space in V such that $K \cap R = F$.

A basis for K may be chosen by completing the set X with the linearly independent set

$$W = \{\underset{\sim}{w}_1, \underset{\sim}{w}_2, \ldots, \underset{\sim}{w}_\ell\}$$

where $\ell = k-f$.

Each element $\underset{\sim}{w}_i$ of W belongs to the space spanned by S and G, hence has a unique decomposition

$$\underset{\sim}{w}_i = \underset{\sim}{\bar{z}}_i + \underset{\sim}{\bar{y}}_i$$

where $\underset{\sim}{\bar{z}}_i \in S$ and $\underset{\sim}{\bar{y}}_i \in G$. Moreover the set of the components

$$\{\underset{\sim}{\bar{z}}_1, \underset{\sim}{\bar{z}}_2, \ldots, \underset{\sim}{\bar{z}}_\ell\}$$

must consist of <u>ℓ linearly independent</u> vectors. Suppose that they are dependent, hence some linear combination of the $\underset{\sim}{\bar{z}}_i$ components vanishes. Then we have a vector in K with all its basis components in G, contradicting the requirement that $K \cap R = F$, thus $K \cap G = 0$. Conversely, any linearly independent set of ℓ vectors belonging to S gives rise to a linearly independent set

$$\{\bar{z}_i + \bar{y}_i\},\ \bar{z}_i \in S,\ \bar{y}_i \in G \qquad (i=1,2,..,\ell)$$

whatever the vectors $\bar{y}_i$ are. The set $\{\bar{y}_i\}$ need not be independent.

Each admissible k-space determines uniquely its Z_ℓ component, where $Z_\ell \subseteq S$ and is of dimension $\ell = k-f$.

The number of ℓ-spaces in S is $\left[{s \atop \ell}\right]$. Each of these gives rise to a Z_ℓ component of a class of admissible k-spaces. Each k-space belonging to the same class is determined by the choice of the $\{\bar{y}_i\}$ set, $\bar{y}_i \in G$, $(i=1,..,\ell)$. Once the Z_ℓ component is fixed, the set of k-spaces determined by it is independent of the basis $\{\bar{z}_i\}$ $(z_i \in Z_\ell,\ i=1,..,\ell)$ chosen for it. Different choices for the $\{\bar{y}_i\}$ components to complement a given $\{\bar{z}_i\}$ basis give rise to different k-spaces, for if $\bar{z}_i + \bar{y}_i^{(1)}$ is a basis element of the k-space K, the vector $\bar{z}_i + \bar{y}_i^{(2)}$ is in K if and only if $\bar{y}_i^{(2)} = \bar{y}_i^{(1)}$. Since the number of vectors (including the zero vector) in G is q^g, each of the ℓ basis vectors of Z_ℓ can be complemented independently in q^g ways, so the same Z_ℓ component determines

$$(q^g)^\ell$$

admissible k-spaces. Thus the number of k-spaces intersecting R <u>exactly in F</u> is

$$\left[{s \atop \ell}\right] q^{g\ell}$$

Setting $s = n-r$, $\ell=k-f$, $g = r-f$ gives the result (4.1). □

We write down now important special cases of (4.1).

(a) Number of k-spaces containing a fixed r space

Here F = R, hence the number is

$$\begin{bmatrix} n-r \\ k-r \end{bmatrix}.$$

In particular the number of k-spaces containing a fixed vector is

$$\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}.$$

(b) Number of k-spaces K for which $K \cap R = 0$ (the null space)

Here f = 0, hence the number is

$$\begin{bmatrix} n-r \\ k \end{bmatrix} q^{kr}.$$

By abuse of terminology we will say that the k-spaces are "disjoint" from R.

(c) Number of k-spaces which do not contain a given line

This is a special case of (b) with r = 1, hence the number is

$$\begin{bmatrix} n-1 \\ k \end{bmatrix} q^{k}.$$

(d) Number of complementary spaces of an r-space in V

The number of subspaces of dimension n-r and disjoint from the given r-space R are wanted here. This is again a special case of (b), where k = n-r. Thus the required number is

$$q^{r(n-r)}.$$

(Note that when q=1, i.e. when we deal with sets instead of spaces, the number of complementary sets is 1.)

Relations (3.1) and (3.2) of the previous section can be interpreted now. We recall the combinatorial interpretation of the Pascal recursion formula:

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

The r-subsets of an n-set fall into two classes: those which contain a fixed element and those which do not contain it. The two terms on the right hand side of the formula signify the number of sets belonging to each class.

Similarly, we consider the r-spaces in an n-space. Those subspaces which contain a fixed vector, which is a 1-dimensional subspace are

$$\left[{n-1 \atop r-1}\right] \text{ in number, by (a).}$$

Those r-spaces in V which do not contain the fixed vector in question give the count

$$\left[{n-1 \atop r}\right] q^r \quad \text{by (c).}$$

Hence

$$\left[{n \atop r}\right] = \left[{n-1 \atop r-1}\right] + q^r\left[{n-1 \atop r}\right].$$

Now we use the symmetry relation to obtain

$$\left[{n \atop n-r}\right] = \left[{n-1 \atop n-r}\right] + q^r\left[{n-1 \atop n-1-r}\right]$$

and setting $k = n-r$ we obtain the alternative formula

$$\left[{n \atop k}\right] = \left[{n-1 \atop k}\right] + q^{n-k}\left[{n-1 \atop k-1}\right]$$

as stated in (3.2).

This last formula can also be given a dual interpretation. The first term on the right hand side gives the number of k-spaces which are contained in a fixed (n-1)-space (hyperplane) of V. Since the left hand side counts all k-spaces of V, the second term gives the remaining k-spaces. Hence we obtain another useful relation :

(e) The number of k-spaces not contained in a fixed hyperplane of V is

$$q^{n-k}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}.$$

In particular, q^{n-1} is the number of lines not contained in a fixed hyperplane. This follows also from (d).

Next, we prove the recursion formula for the Galois numbers G_n stated in (3.3). We note first that if q=1, $G_n=2^n$ as indicated before. This can be proved by establishing a recursion: all subsets of an (n+1)-set are obtained by considering first all the subsets of one of its n-subsets and then adding the element left out to each of the subsets already accounted for. Thus when q=1,

$$G_{n+1} = 2\ G_n.$$

This reasoning is then modified for q > 1. Let $\underset{\sim}{v}$ be a fixed vector in the (n+1)-dimensional vector space V_{n+1}. Then

$$G_{n+1} = N_1 + N_2$$

where N_1 is the number of all the subspaces containing $\underset{\sim}{v}$ and N_2 the number of subspaces not containing $\underset{\sim}{v}$.

The number of k-spaces in V_{n+1} containing $\underset{\sim}{v}$ is $\begin{bmatrix} n \\ k-1 \end{bmatrix}$ and those not containing $\underset{\sim}{v}$ is $\begin{bmatrix} n \\ k \end{bmatrix} q^k$, so we have

$$G_{n+1} = \sum_{k=1}^{n+1} \begin{bmatrix} n \\ k-1 \end{bmatrix} + \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} q^k$$

$$= \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} + \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} q^k = G_n + \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} q^k \qquad (4.2)$$

The second term on the right hand side is the count of the incidences of all the subspaces of V_n with the points contained by them.

Another way of counting these incidences is obtained by counting first all the subspaces containing a fixed non-zero vector.

By (a) in Section 1.4, a fixed vector is contained in $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ k-spaces and hence in

$$\sum_{k=1}^{n} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} = \sum_{k=0}^{n-1} \begin{bmatrix} n-1 \\ k \end{bmatrix} = G_{n-1} \text{ subspaces.}$$

Since the number of non-zero vectors of G_{n-1} is q^n-1, the number of incidences is

$$(q^n-1)G_{n-1}.$$

To this we add G_n as the number of incidences of the zero vector with all the subspaces. Thus

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} q^k = (q^n-1)G_{n-1} + G_n.$$

Substituting this in (4.2) we obtain the recursion

$$G_{n+1} = 2\,G_n + (q^n-1)G_{n-1} \text{ of (3.3).}$$

1.5 Summation Identities

In this section interpretative proofs are given to some known Gaussian identities together with proofs of identities not known by the author. All these identities are treated as q-generalisations of known binomial identities.

The binomial identity dealing with addition of the elements in a diagonal of the Pascal triangle is

$$\sum_{r=k}^{n} \binom{r-1}{k-1} = \binom{n}{k}.$$

The combinatorial meaning of this identity to be adopted for Gaussians is as follows.

Arrange the elements of an n-set in a fixed order

$$a_1, a_2, \ldots, a_k, \ldots, a_n.$$

We keep this order in the k-sets selected out of the n-set. We put then all the k-sets with the common last element a_r into one class ($k \leq r \leq n$).

The number of the k-sets in this class is

$$\binom{r-1}{k-1}.$$

Summation of the number of sets in all classes gives the identity.

The corresponding relation for Gaussian, known and proved by Gauss is

$$\sum_{r=k}^{n} \begin{bmatrix} r-1 \\ k-1 \end{bmatrix} q^{r-k} = \begin{bmatrix} n \\ k \end{bmatrix} \tag{5.1}$$

The right hand side represents the number of k-subspaces on an n-space.

On the left hand side we do the counting by arranging fixed subspaces dimensions k, k+1, ..., n respectively and such that

$$M_k \subset M_{k+1} \subset \ldots \subset M_r \subset \ldots \subset M_n.$$

Taking M_k as the first k-space we proceed by finding all k-spaces contained in M_{k+1}, with the exclusion of M_k. The number of these is

$$\begin{bmatrix} k \\ k-1 \end{bmatrix} q \quad \text{by (e) of section 4.}$$

(This number is equal to $\begin{bmatrix} k+1 \\ k \end{bmatrix}-1$.)

Suppose now that all the k-spaces contained in M_{r-1} have already been counted. Since M_{r-1} is a hyperplane of M_r, we can use (e) again to find the number of k-spaces included in M_r, but not in M_{r-1}. This is $\begin{bmatrix} r-1 \\ k-1 \end{bmatrix} q^{r-k}$. Continuing in this manner we finish the counting by considering the k-spaces contained in $V = M_n$ but not in M_{n-1}. This proves (5.1). □

Another well known binomial identity is known as the Van der Monde convolution:

$$\sum_{r=0}^{k} \binom{m}{r}\binom{n}{k-r} = \binom{m+n}{k}.$$

The interpretation: Count the k-subsets of an (m+n) set, by separating the set into an m-set and an n-set, then selecting r elements from the m-set and (k-r) elements from the n-set for all values of r such that $0 \leqslant r \leqslant k$.

The Gaussian generalisation of this is

$$\sum_{r=0}^{k} \begin{bmatrix} m \\ r \end{bmatrix}\begin{bmatrix} n \\ k-r \end{bmatrix} q^{(k-r)(m-r)} = \begin{bmatrix} m+n \\ k \end{bmatrix} \qquad (5.2)$$

This can now be proved by a reasoning similar to the above. Consider the vector space

$$V = M + N$$

where M, N have dimensions m and n respectively.

By Theorem 1.2, the number of k-spaces of V intersecting M in a fixed r-space is

$$\begin{bmatrix}(m+n)-m\\k-r\end{bmatrix} q^{(k-r)(m-r)}.$$

Since there are $\begin{bmatrix}m\\r\end{bmatrix}$ r-spaces in M, the number of k-spaces intersecting M in some r-space is

$$\begin{bmatrix}m\\r\end{bmatrix}\begin{bmatrix}n\\k-r\end{bmatrix} q^{(k-r)(m-r)},$$

(since there are $\begin{bmatrix}m\\r\end{bmatrix}$ choices for the r-space in the m-space).

Summing for r = 0 to k yields (5.2).

Note that this formula is not symmetrical in m and n (unlike the Van der Monde formula for sets), but using the symmetry relation of Gaussians, various equivalent forms can be written down.

(Formula (5.2) is a special case of a generalisation of the Van der Monde identity found in [7].)

A binomial identity similar to the convolution formula, but not as well known is

$$\sum_{j=k}^{n-k} \binom{j}{k}\binom{n-j}{k} = \binom{n+1}{2k+1}.$$

Combinatorial Proof:

An (n+1)-set is arranged in fixed order. The (2k+1)-sets chosen out of it are classified, according to the centrally placed element: if the (j+1)th element is "central" in the chosen 2k+1 set where $k \leqslant j \leqslant n-k$, then there are k elements of a lower and k elements of a higher index in the chosen set. Therefore the number of sets with the $j+1^{th}$ element central, is

$$\binom{j}{k}\binom{n-j}{k}.$$

Summing for all the admissible j-values, the number of all (2k+1)-sets is obtained.

Generalisation for Gaussians:

$$\sum_{j=k}^{n-k} \left[{j \atop k}\right]\left[{n-j \atop k}\right] q^{(j-k)(k+1)} = \left[{n+1 \atop 2k+1}\right] \qquad (5.3)$$

Proof:

We proceed similarly to the proof of (5.1). Consider the series of subspaces

$$M_{k+1} \subset M_{k+2} \subset \ldots \subset M_j \subset M_{j+1} \subset \ldots \subset M_{n+1-k}$$

of the (n+1)-space V, where the subscripts indicate the dimensions. We count the (2k+1)-spaces in the (n+1)-space V containing M_{k+1}, next those (2k+1)-spaces which contain (k+1)-spaces of $M_{k+2} \setminus M_{k+1}$, and so on, finishing with the (2k+1)-spaces containing (k+1)-spaces of $M_{n+1-k} \setminus M_{n-k}$.

Using (e) of section 4, we find that the number of (k+1)-spaces contained in

$$M_{j+1} \setminus M_j$$

is

$$q^{(j+1)-(k+1)}\left[{(j+1)-1 \atop (k+1)-1}\right] = q^{j-k}\left[{j \atop k}\right].$$

By Theorem 1.2, the number of (2k+1)-spaces of V intersecting M_{j+1} in a fixed k+1-space is

$$\left[{(n+1)-(j+1) \atop (2k+1)-(k+1)}\right] q^{((2k+1)-(k+1))((j+1)-(k+1))}$$

$$= \left[{n-j \atop k}\right] q^{k(j-k)}$$

hence the number of (2k+1)-spaces containing (k+1)-spaces of

$$M_{j+1} \setminus M_j$$

is

$$\begin{bmatrix} j \\ k \end{bmatrix} \begin{bmatrix} n-j \\ k \end{bmatrix} q^{(k+1)(j-k)}$$

This gives the general term of the sum on the left hand side of (5.3) with j varying from k to (n-k).

This identity can be generalised to

$$\sum_{j \geq k} \begin{bmatrix} j \\ k \end{bmatrix} \begin{bmatrix} n-j \\ \ell \end{bmatrix} q^{(\ell+1)(j-k)} = \begin{bmatrix} n+1 \\ k+\ell-1 \end{bmatrix} \qquad (5.4)$$

The proof of (5.3) can be adapted with no change in the reasoning.

To finish this section one more binomial summation is discussed which can be naturally extended to a Gaussian identity:

$$\sum_{r=k}^{n} \binom{r}{k} \binom{n}{r} = \binom{n}{k} 2^{n-k}$$

leads to

$$\sum_{r=k}^{n} \begin{bmatrix} r \\ k \end{bmatrix} \begin{bmatrix} n \\ r \end{bmatrix} = \begin{bmatrix} n \\ k \end{bmatrix} G_{n-k} \qquad (5.5)$$

In the combinatorial identity both sides represent the number of ways in which an n-set can be divided into three sets, one of which has the fixed cardinality k. On the left hand side the division is made by first selecting an r-set out of the n-set, where r must be at least as much as k. An n-set is then selected out of the r-set. The number of ways this can be done is $\binom{n}{r}\binom{r}{k}$. Summing for r gives all possible partitions satisfying the preset condition. On the right hand side the k-set is chosen first. For each choice there are 2^{n-k} partitions of the remaining elements.

We reason the same way for establishing (5.5), counting the number of ways in which an n-space can be partitioned into three <u>orthogonal</u> subspaces, one of them of fixed dimension k.

1.6 Alternating Sums. The Inversion Theorem

A large number of well known binomial identities involve sums with terms of strictly alternating signs. There are corresponding alternating Guassian sums. To show the connection between these and the binomial sums it is necessary to generalise the Inclusion-Exclusion principle of combinatorics.

A general treatment of generalised (Möbius) inversion relations in (locally) finite partially ordered sets is given in [25]. In this chapter, a proof of the inversion theorem in the partially ordered set of subspaces of a linear space is given, using only the results of the previous sections. Alternative, simple proof can be found in [8].

Theorem 1.3 (Inversion)

Let V be a finite linear space over the finite field GF(q), the dimension of V being n. Denote by S,T any of the subspaces (including V and 0) of V and define the functions f(S), g(S), h(S) on the subspaces with the following properties

$$g(S) = \sum_{T\subseteq S} f(T) \quad \text{and} \quad h(S) = \sum_{T\supseteq S} f(T).$$

Then, for all $S \subseteq V$

(a) $$f(S) = \sum_{T\subseteq S} \overline{\mu}(T)g(T) \text{ and}$$

(b) $$f(S) = \sum_{T\supseteq S} \underline{\mu}(T)h(T)$$

where

$$\overline{\mu}(T) = (-1)^k q^{\binom{k}{2}}, \quad k = \dim S - \dim T \text{ for (a)}$$

and

$$\underline{\mu}(T) = (-1)^k q^{\binom{k}{2}}, \quad k = \dim T - \dim S \text{ for (b).}$$

Note:

(i) For our purposes, f, g, h are integer valued functions but they may represent mappings to any ring.

(ii) The set of subspaces of V, partially ordered by inclusion has V for a natural upper bound and the 0-space for a natural lower bound. However, upper and lower bounds S_{max} and S_{min} may be imposed by defining $f(S) = 0$ for $S \supset S_{max}$ and $S \subset S_{min}$. The sums defining $g(S)$ and $h(S)$ are finite and hence well defined.

Proof

(a) Let the dimension of S be m, and denote by $S^{(k)}$ any subspace of S of dimension m-k. (In particular $S^{(0)} = S$.)

Then

$$g(S) = \sum_{T \subseteq S} f(T) = f(S) + \sum_{T \subset S} f(T)$$

$$= f(S) + \sum_{k=1}^{m} \sum_{S^{(k)} \subset S} f(S^{(k)}) \tag{6.1}$$

Hence

$$f(S) = g(S) - \sum_{k=1} \sum_{S^{(k)} \subset S} f(S^{(k)}) \tag{6.2}$$

More generally, we may apply (6.1) to any $S^{(k)}$ subspace of S and hence obtain

$$f(S^{(k)}) = g(S^{(k)}) - \sum_{i=k+1}^{m} \sum_{S^{(i)} \subset S^{(k)}} f(S^{(i)}) \tag{6.3}$$

Substituting expression (6.3) for k=1,2,... into (6.2) we obtain at some stage

$$f(S) = g(S) + \sum_{i=1}^{k-1} \overline{\mu}(i) \sum_{S^{(i)} \subset S} g(S^{(i)}) + R_{k-1} \tag{6.4}$$

where the remainder term is

$$R_{k-1} = \sum_{i=k}^{m} c_i \sum_{S^{(i)} \subset S} f(S^{(i)}).$$

We note here that the coefficients of the $g(S^{(i)})$ and $f(S^{(i)})$ terms depend only on the structure of the P.O. set of subspaces considered and not on the functions f and g. Furthermore, another application of (6.3) to (6.4) affects only R_{k-1} and leaves the first part unchanged.

Write

$$R_{k-1} = c_k \sum_{S^{(k)} \subseteq S} f(S^{(k)}) + \sum_{S^{(k)} \subseteq S} \sum_{i=k+1}^{m} c_i \sum_{S^{(i)} \subseteq S^{(k)}} f(S^{(i)}).$$

Apply now (6.3) to each $f(S^{(k)})$, substitute into (6.4) to obtain

$$f(S) = g(S) + \sum_{i=1}^{k-1} \bar{\mu}(i) \sum_{S^{(i)} \subset S} g(S^{(i)})$$

$$+ c_k \sum_{S^{(k)} \subset S} g(S^{(k)}) + R_k \qquad (6.5)$$

Hence R_k is the new remainder term containing $f(S^{(i)})$ terms for $i=k+1$ to m.

We can now write $\bar{\mu}(k) = c_k$ and write down (6.5) in the form

$$g(S) = f(S) - \sum_{i=1}^{k} \bar{\mu}(i) \sum_{S^{(i)} \subset S} g(S^{(i)}) - R_k \qquad (6.6)$$

and compare the coefficient of $f(S^{(k)})$ in (6.1) to (6.6).

Note that R_k contains only $f(S^{(i)})$ terms for $k+1 \leq i \leq m$, hence $f(S^{(k)})$ contributes to the sums $g(S^{(i)})$ for $0 \leq i \leq k$ only.

Let $S^{(k)}$ be a fixed subspace. Then $f(S^{(k)})$ contributes to $g(S^{(i)})$ if and only if $S^{(k)} \subseteq S^{(i)}$.

By (a) in section 1.4, the number of $S^{(i)}$ spaces (i.e. spaces of dimension (m-i) of S, containing $S^{(k)}$) is given by

$$\left[{m-(m-k) \atop (m-i)-(m-k)}\right] = \left[{k \atop k-i}\right] = \left[{k \atop i}\right].$$

Thus the contribution of $f(S^{(k)})$ to the term

$$\bar{\mu}(i) \sum_{S^{(i)} \subset S} g(S^{(i)}) \text{ is } \bar{\mu}(i)\left[{k \atop i}\right]$$

and so the coefficient of $f(S^{(k)})$ contained in (6.6) is

$$-\sum_{i=1}^{k} \bar{\mu}(i)\left[{k \atop i}\right]$$

and this must be equal to 1, the coefficient of $f(S^{(k)})$ in (6.1).

Hence

$$1 + \sum_{i=1}^{k} \bar{\mu}(i)\left[{k \atop i}\right] = 0.$$

Writing $\bar{\mu}(0) = 1$, we write down this last equation as a recursion formula for $\bar{\mu}(k)$. Since $\left[{k \atop k}\right] = 1$, we obtain

$$\bar{\mu}(k) = -\sum_{i=0}^{k-1} \bar{\mu}(i)\left[{k \atop i}\right]. \qquad (6.7)$$

Using this to evaluate $\bar{\mu}(k)$, we obtain

$$\bar{\mu}(0) = 1,\ \bar{\mu}(1) = -1,\ \bar{\mu}(2) = q,\ \bar{\mu}(3) = -q^3 = -q^{1+2}.$$

We continue by induction, assuming that for $0 \leq i < k$

$$\bar{\mu}(i) = (-1)^i q^{\binom{i}{2}}.$$

(Since $\binom{i}{2} = 0$ when i=0 or 1, this is also true for those two values.)

Using (3.1) of section 1.3 and the inductive hypothesis we write (6.7) as

$$\overline{\mu}(k) = -1 - \sum_{i=2}^{k-1} (-1)^i q^{\binom{i}{2}} \left(\begin{bmatrix} k-1 \\ i-1 \end{bmatrix} + q^i \begin{bmatrix} k-1 \\ i \end{bmatrix}\right) \tag{6.8}$$

All terms of the right hand side, excepting the last one cancel out and we obtain

$$\overline{\mu}(k) = (-1)^k q^{\binom{k-1}{2}} . q^{k-1} \begin{bmatrix} k-1 \\ k-1 \end{bmatrix} = (-1)^k \; q^{\binom{k}{2}}$$

as claimed.

(b) The proof is similar to (a). The modification is that we denote with $S^{(k)}$ any subspace of V containing S and of dimension m+k. We have

$$\begin{aligned} h(S) &= \sum_{T \supseteq S} f(T) = f(S) + \sum_{T \supset S} f(T) \\ &= f(S) + \sum_{k=1}^{n-m} \sum_{S^{(k)} \supset S} f(S^{(k)}). \end{aligned} \tag{6.9}$$

Then for k=0,1,2,...

$$f(S^{(k)}) = h(S^{(k)}) - \sum_{i=k+1}^{n-m} \sum_{S^{(i)} \supset S^{(k)}} f(S^{(i)}) \tag{6.10}$$

and after successive substitutions

$$f(S) = h(S) + \sum_{i=1}^{k-1} \underline{\mu}(i) \sum_{S^{(i)} \supset S} h(S^{(i)}) + R_{k-1} \tag{6.11}$$

with the remainder term

$$R_{k-1} = \sum_{i=k}^{n-m} c_i \sum_{S^{(i)} \supset S} f(S^{(i)})$$

and corresponding to (6.6) we have

$$h(S) = f(S) - \sum_{i=1}^{k} \underline{\mu}(i) \sum_{S^{(i)} \supseteq S} h(S^{(i)}) - R_k \qquad (6.12)$$

Here $f(S^{(k)})$ contributes to $h(S^{(i)})$ if and only if the subspace $S^{(k)} \supseteq S^{(i)}$, where $S^{(k)}$, $S^{(i)}$ are subspaces of dimensions m+k, m+i respectively, both containing S.

Hence we must determine the number of the (m+i)-spaces in an (m+k)-space which contain a fixed m-space.

By (a) of section 1.4 this is

$$\left[{(m+k)-m \atop (m+i)-m}\right] = \left[{k \atop i}\right].$$

Thus we obtain for $\underline{\mu}(k)$ the same recursion formula (6.7) as for $\overline{\mu}(k)$.

$$\underline{\mu}(k) = -\sum_{i=0}^{k-1} \underline{\mu}(i)\left[{k \atop i}\right]$$

and so

$$\underline{\mu}(k) = (-1)^k q^{\binom{k}{2}}.$$

In (a), k = dim S - dim $S^{(k)}$, while in (b) k = dim $S^{(k)}$ - dim S. This completes the proof. □

The arguments used in the proof are valid for q = 1, i.e. for the case of subsets. Here $\underline{\mu}(k) = (-1)^k = \overline{\mu}(k)$. The result gives the combinatorial Inclusion-Exclusion principle as a special case.

Let Ω be a set of objects and P a set of properties. Let the variables S, T represent subsets of P, and use the notation $S^{(i)}$ for subsets of P consisting of i properties. Denote by f(S) the number, (or more generally the combined "weight") of those elements of Ω which have <u>exactly</u> the <u>properties S</u>, by h(S) the number (weight) of elements of Ω having at least the properties S, and by g(S) of those having at most properties S, hence

$$h(S) = \sum_{T \supseteq S} f(T) \quad \text{and} \quad g(S) = \sum_{T \subseteq S} f(T)$$

as before. The inversion formula for h(S) gives

$$f(S) = \sum_{T \supseteq S} (-1)^k h(T) \tag{6.13}$$

where $k = |T| - |S|$.

In particular, if $S = \phi$ (the empty set of properties) $h(\phi) = |\Omega|$, or (the weight of Ω), the whole set of objects, since there is no restriction on them. The relation (6.13) can then be written as

$$f(\phi) = |\Omega| - \sum_{S^{(1)}} h(S^{(1)}) + \sum_{S^{(2)}} h(S^{(2)}) + \ldots + (-1)^{|P|} h(P)$$

This last equation represents the classical Inclusion-Exclusion principle.

1.7 Examples of Binomial and Gaussian Alternating Sums

The best known example of an alternating sum of binomials is

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} \ldots (-1)^n \binom{n}{n} = 0.$$

Using the notations of the previous section this result can be obtained by setting $f(\phi) = 1$ for the empty set and for each subset S of an n-set have $f(S) = 0$.

Then for all subsets S of an n-set N, we have

$$g(S) = \sum_{T \subseteq S} f(T) = 1$$

and by inversion

$$\sum_{i=0}^{n} \binom{n}{i}(-1)^i = f(N) = 0 \quad \text{for all } n > 0.$$

The result translates immediately into the Gaussian relation

$$\sum_{i=0}^{n} \left[{n \atop i}\right]\mu(i) = \left[{n \atop 0}\right]-\left[{n \atop 1}\right]+\left[{n \atop 2}\right]q + \ldots + (-1)^i\left[{n \atop i}\right]q^{\binom{i}{2}} +$$

$$+ \ldots + (-1)^n\left[{n \atop n}\right] = 0 \qquad (7.1)$$

We can recognise that (7.1) is the same as the recursion formula (6.7).

Another well known alternating bionomial sum is

$$\sum_{j=1}^{n} (-1)^j j\binom{n}{j} = 0.$$

We can give two different interpretations to this relation, and accordingly obtain two different Gaussian identities.

(i) We use the Inclusion-Exclusion principle to determine the number of those (n-1)subsets of an n-set which <u>do not contain</u> any of the elements 1,2,..,n knowing that the answer is 0.

Let Ω be the set of (n-1)-sets and the property P is defined in the following way:

P_j : the subset contains the element j (j=1,2,..,n),

P_{jk} : the subset contains the elements j and k, and so on.

$$|\Omega| = \binom{n}{n-1} = \binom{n}{1} = n.$$

The number of (n-1)-sets containing j is $\binom{n-1}{n-2}$. Hence the sum of the numbers of (n-1)-sets with properties P_1, P_2, .., P_n respectively is $n\binom{n-1}{n-2}$. The number of (n-1)-sets with properties P_i and P_j is $\binom{n-2}{n-3}$. The sum of the numbers is $\binom{n}{2}\binom{n-2}{n-3}$.

We proceed in this manner and applying the Inclusion-Exclusion principle we find that

$$\sum_{r=0}^{n-1} (-1)^r \binom{n}{r} \binom{n-r}{n-r-1} = 0$$

Setting $\binom{n-r}{n-r-1} = \binom{n-r}{1} = (n-r)$ we obtain

$$\sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r) = 0 \text{ or writing } j = (n-r)$$

$$\sum (-1)^j j \binom{n}{j} = 0.$$

This interpretation can be used directly for (n-1)-spaces in an n-dimensional linear space, by fixing a basis $v_1, v_2, \ldots, v_j \ldots, v_n$ and then using the Inclusion-Exclusion principle in the above manner to determine the number of hyperplanes not containing any vector of the given basis.

By reasoning identical to the above assign property P_j to those hyperplanes which contain v_j. Their number (by (a) in Section 1.4) is $\left[{n-1 \atop n-2}\right]$, hence the corresponding sum for $j=1,2,\ldots,n$ is

$$\binom{n}{1}\left[{n-1 \atop n-2}\right].$$

Similarly, the number of hyperplanes containing a fixed set of r of the given basis-vectors, hence the subspace spanned by them, is

$$\left[{n-r \atop n-r-1}\right] = \left[{n-r \atop 1}\right] \qquad \text{(section 1.4(a))}$$

and since there are $\binom{n}{r}$ ways of choosing the r basis-vectors, the corresponding sum in the Inclusion-Exclusion formula is

$$(-1)^r \binom{n}{r}\left[{n-r \atop 1}\right].$$

Thus the number of hyperplanes not containing any of the basis elements $v_1, v_2, \ldots, v_n$ is

$$\sum_{r=0}^{n-1} (-1)^r \binom{n}{r} \begin{bmatrix} n-r \\ 1 \end{bmatrix}.$$

This sum however is <u>not 0</u>.

We can count this sum by determining the number of hyperplanes with equations

$$\sum_{i=1}^{n} a_i x_i = 0 \quad (a_i \in GF(q))$$

not containing any of the unit-vectors

(1 0 0 .. 0), (0 1 0 .. 0), .. (0 0 0 .. 1).

Choosing $a_1 = 1$ and $a_i \neq 0$ $(i=2,..,n)$ there are $(q-1)^{n-1}$ possible choices which determine the admissible hyperplanes.

Hence

$$\sum_{r=0}^{n-1} (-1)^r \binom{n}{r} \begin{bmatrix} n-r \\ 1 \end{bmatrix} = (q-1)^{n-1} \qquad (7.2)$$

The result (7.2) is easy to verify algebraically and does not yield results when n-subspaces are considered instead of hyperplanes. A more interesting result ensues from the alternative method.

(ii) Using the inversion theorem, define $f(S) = 1$ if S is a subset of an n-set containing one element or if S is a subspace of dimension 1 of an n-space; otherwise, in both cases let $f(S) = 0$.

Then in the case of subsets

$$g(S) = \sum_{T \subseteq S} f(T) = |S|$$

and in the case of subspaces

$$g(S) = \sum_{T \subseteq S} f(T) = \begin{bmatrix} k \\ 1 \end{bmatrix},$$

where k is the dimension of S. The inversion theorem gives for sets:

$$\sum_{j=0}^{n} (-1)^j (n-j) \binom{n}{n-j} = 0$$

which is the same as the relation

$$\sum_{j=0}^{n} (-1)^j j \binom{n}{j} = 0 \text{ of (i).}$$

For subspaces we obtain a relation different from (7.2) namely

$$\sum_{j=0}^{n} (-1)^j \left[{n-j \atop 1}\right]\left[{n \atop n-j}\right] q^{\binom{j}{2}} = 0 \quad (n > 1). \tag{7.3}$$

The last identity can be generalised by letting f(S) = 1 for all m-subsets of an n-set, or m-spaces in an n-space respectively, and setting f(S) = 0 otherwise.

If S is a k-set or k-space respectively, where k > m, then

$$g(S) = \sum_{T \subseteq S} f(T) = \binom{k}{m}$$

for the case of sets, with the resulting binomial identity

$$\sum_{j=0}^{n-m} (-1)^j \binom{n}{n-j}\binom{n-j}{m} = 0 \quad (n > m)$$

For Gaussians we get in the same way

$$\sum_{j=0}^{n-m} (-1)^j \left[{n \atop n-j}\right]\left[{n-j \atop m}\right] q^{\binom{j}{2}} = 0. \tag{7.4}$$

The same method yields a further pair of relations, by setting f(S) = 1 for <u>all</u> subsets (subspaces). These are:

$$\sum (-1)^j \binom{n}{n-j} 2^{n-j} = 1$$

and

$$\sum (-1)^j \left[{n \atop n-j}\right] G_{n-j} q^{\binom{j}{2}} = 1 \tag{7.5}$$

(Note: The above binomial identity can be obtained by a direct application of the Inclusion-Exclusion principle to count those sets, which do not contain any of the elements (1,2,..,n). The answer is 1, corresponding to the empty set.)

We conclude this discussion with two more examples, using less trivial f functions. The first one is the identity

$$\sum_{k=0}^{n-1} (-1)^k (n-k) \binom{n}{n-k} 2^{n-k} = 2n$$

which generalises to

$$\sum_{k=0}^{n-1} (-1)^k q^{\binom{k}{2}} (n-k) \begin{bmatrix} n \\ n-k \end{bmatrix} G_{n-k} = 2n \qquad (7.6)$$

Let r be the dimension of a subspace S of the n-dimensional space V. Define f(S) = r. Then

$$g(S) = \sum_{T \subseteq S} f(T) = \sum_{j=0}^{r} j \begin{bmatrix} r \\ j \end{bmatrix} = \frac{1}{2} r \, G_r,$$

since

$$2 \sum_{j=0}^{r} j \begin{bmatrix} r \\ j \end{bmatrix} = \sum_{j=0}^{r} j \begin{bmatrix} r \\ j \end{bmatrix} + \sum_{j=0}^{r} j \begin{bmatrix} r \\ r-j \end{bmatrix} =$$

$$= \sum_{j=0}^{r} j \begin{bmatrix} r \\ j \end{bmatrix} + \sum_{j=0}^{r} (r-j) \begin{bmatrix} r \\ j \end{bmatrix} = \sum_{j=0}^{r} r \begin{bmatrix} r \\ j \end{bmatrix}.$$

The inversion theorem (a) then gives (7.6).

Another known alternating binomial identity is

$$\sum_{k=0}^{m} (-1)^k \binom{m}{k} \binom{n-k}{m} = 1.$$

One interpretation of this is given by counting those m-subsets of an n-set which contain exactly the m elements of a given set M.

One possible translation of this relation to Gaussian is

$$\sum_{k=0}^{m} (-1)^k \begin{bmatrix} m \\ k \end{bmatrix} \begin{bmatrix} n-k \\ m \end{bmatrix} q^{\binom{k}{2}} = q^{m(n-m)} \tag{7.7}$$

Proof

Let M be a fixed m-space in the n-space V.

Let K be a k-space in M. Define f(K) as the number of those (n-m)-spaces which intersect M exactly in K. By Theorem 1.2

$$f(K) = \begin{bmatrix} n-m \\ (n-m)-k \end{bmatrix} q^{n-m-k)(m-k)} = \begin{bmatrix} n-m \\ k \end{bmatrix} q^{(n-m-k)(m-k)}$$

In particular for K being the 0-space we have

$$f(0) = q^{(n-m)m}$$

(the number of complement-spaces of M, c.f. section 1.4(d)).

Then $h(K) = \sum_{S \supseteq K} f(S)$, hence h(K) enumerates all those (n-m)-spaces of V which contain K.

By (a) of Section 4,

$$h(K) = \begin{bmatrix} n-k \\ (n-m)-k \end{bmatrix} = \begin{bmatrix} n-k \\ m \end{bmatrix}.$$

(In particular, $h(0) = \begin{bmatrix} n \\ m \end{bmatrix}$.)

A direct application of the inversion theorem (b) gives the identity (7.7).

Gaussian coefficients will be frequently used in Chapter 3 in the study of Baer-spaces of higher dimensions.

CHAPTER TWO

ON THE BAER STRUCTURE OF GALOIS PLANES OF SQUARE ORDER

2.1 Introduction

In Section 5 of the introductory chapter a Baer-plane was defined as a projective plane of finite order, embedded in a large projective plane and dense in it. The following theorem gives a necessary condition for the existence of a proper subplane within a finite projective plane.

Bruck's Theorem [12]

If Π is a finite projective plane of order q and can be extended to a projective plane Π' of order q', then either

(i) $q' = q^2$,

or

(ii) $q' \geq q^2 + q$.

The proof of this theorem implies that in case (i) the subplane is dense in the larger projective plane. Hence a projective plane can possess a Baer-plane only if its order is a perfect square.

Galois planes of type $PG(2,q^2)$ $(q \geq 2)$ possess Baer-planes, for the points in $PG(2,q^2)$ with coordinates belonging to $GF(q)$ (dividing through by a constant if necessary) form a subplane : $PG(2,q)$. In the subsequent work this Baer-plane will be called the "real" Baer-plane and denoted by B_0.

It follows immediately that there is a large number of Baer-planes in $PG(2,q^2)$. Any homography produces a Baer-plane. The converse is also true. Any Baer-plane B_1 is a homographical image of B_0. This is not obvious, since by the Fundamental Theorem of Projective Geometry a general collineation is the product of a homography and a field automorphism. Thus by choosing a non degenerate quadrangle in B_1 to be the homographical image of the fundamental points (1 0 0), (0 1 0), (1 0 0) and (1 1 1) (always possible by the fundamental theorem), it must also be ascertained that the homography determines fully B_1. This is proved, e.g. in [14] by J. Cofman. A short alternative argument is used here to prove the statement, because the same argument can be used for higher dimensions to be discussed in the next chapter.

It suffices to show that a field automorphism τ of GF(q) leaves B_0 invariant (though not necessarily pointwise). All points of B_0 have coordinates belonging to GF(q), so all of the coordinates satisfy the equation

$$x^q - x = 0 \tag{1.1}$$

If τ is a field automorphism, then

$$(\tau x)^q - (\tau x) = \tau(x^q - x) = \tau(0) = 0,$$

hence the transformed points are again in B_0.

In particular, if the automorphism takes the coordinates of the points to their <u>conjugates</u> in GF(q^2), that is

$$x \to x^q$$

then B_0 remains <u>pointwise fixed</u>, since by (1.1) the elements of GF(q) are equal to their conjugates. Hence this particular field-automorphism induces an <u>involution</u> in PG($2,q^2$), with <u>B_0 being its fixed set</u>.

The number of Baer-planes in PG($2,q^2$) can be determined next.

This is obtained by dividing the total number of homographics of $PG(2,q^2)$ by the number of those which leave B_0 invariant, that is the number of homographics of PG(2,q).

Denote the number of Baer-planes by N. Then

$$N = |PGL(3,q^2)|/|PGL(3,q)|,$$

and by (5.4) of the introductory chapter,

$$N = q^6(q^4-1)(q^6-1)/q^3(q^2-1)(q^3-1)$$

$$= q^3(q^3+1)(q^2+1) \qquad (1.2)$$

The investigations leading to this work began with a computer search surveying points, lines and a Singer orbit of Baer-planes in PG(2,25). Questions of interest in the geometry of the plane $PG(2,q^2)$ are:

(i) intersection configurations of Baer-planes;

(ii) partitioning of $PG(2,q^2)$ by Baer-planes;

(iii) structures of special sets of Baer-planes.

The findings resulting from the early investigations were published in [28], (1981).

Before these results could be published, the paper [10] by R.C. Bose, T.W. Freeman, D.G. Glynn appeared proving the intersection-theorem of Baer-planes (Theorem 2.1) in this chapter), together with a count of the possible intersection configurations. The proofs of these, given in this chapter, are independent of the above, using different methods. The intersection theorem was also proved simultaneously by K. Vedder [33].

The problem of partitioning a projective plane by Baer-planes was treated by T.G. Room and P.B. Kirkpatrick in [24]. Theorem (2.12) of this chapter is proved in [24] for PG(2,9), but there is nothing new in the proof for PG(2,q^2), the general case. This result was needed for interpreting the formula for the number of Baer-planes disjoint from a given Baer-plane, obtained earlier by indirect means.

Another approach to partitioning, independently found and published in [28] was later found to have appeared in [36] by P. Yff (1974), where it was quoted as a result of R.H. Bruck (1960). A survey of partitions and spreads appeared in [20].

Baer-planes have been intensively studied by several workers (as the short survey above indicates). They have proved to be useful tools for constructing non-desarguesian projective planes (cf D.R. Hughes and F.C. Piper [21], Chapter on Derivation Sets), also for constructing arcs in projective planes [6].

This chapter may be regarded as an introduction to Chapter 3. Results discussed here are pointers to the more general structure of projective spaces of higher dimensions.

2.2 The Intersection of Two Baer-Planes

Definition

Two Baer-planes B_1 and B_2 of a general projective plane Π of order q^2 are said to share a line ℓ in Π, if $q+1$ points of ℓ belong to each B_1 and B_2.

If, in particular

$$B_1 \cap \ell = B_2 \cap \ell$$

and $|B_1 \cap \ell| = |B_2 \cap \ell| = q+1$, then B_1 and B_2 are said to <u>share the line ℓ pointwise</u>.

<u>Note</u> : It is sufficient to ascertain that <u>two</u> points of ℓ belong to each of B_1 and B_2, for it follows then that $\ell \cap B_1$ and $\ell \cap B_2$ each contain $q+1$ points. The sets of points in $\ell \cap B_1$ and $\ell \cap B_2$ may be disjoint, intersecting or identical.

<u>Theorem 2.1</u>

The number of points common to two Baer-planes B_1 and B_2 of a projective plane Π of order q^2 is equal to the number of lines shared by B_1 and B_2.

<u>Proof</u>

Observe first that for each Baer-plane B of Π there are $q+1$ lines of B through each point of B, while exactly <u>one</u> line of B goes through a point of Π <u>external</u> to B. This is so because B is dense in Π and lines belonging to B intersect within B.

Dually, each line of B contains $q+1$ points of B, while each line of Π external to B intersects B in exactly one point.

Denote by <u>r</u> the number of points in $B_1 \cap B_2$, and by <u>s</u> the number of lines shared by B_1 and B_2.

Let I be the number of <u>incidences</u> of the <u>points of B_1</u> with the <u>lines of B_2</u>.

By the above observation, the r points <u>internal</u> in B_2 make $r(q+1)$ incidences with lines of B_2, while the rest of the points of B_1, $q^2+q+1-r$ in number, are external to B_2, hence result each in one incidence only. Hence

$$I = r(q+1) + q^2 + q + 1 - r \qquad (2.1)$$

On the other hand, s lines of B_2 belong to B_1, hence give s(q+1) incidences with its points, while the remaining $q^2+q+1-s$ lines of B_2 are external to B_1, hence each makes one incidence with some point of B_1. Hence

$$I = s(q+1) + q^2 + q + 1 - s \qquad (2.2)$$

Comparing (2.1) and (2.2) it is found that r = s as claimed. □

Corollary

Two Baer-planes have no common line if and only if they are pointwise disjoint.

Theorem 2.1 is valid for Baer-planes of a general projective plane. The next lemma is also valid generally. It concerns the nature of the intersection of two Baer-planes.

Lemma 2.2

The intersection of two Baer-planes is a closed configuration (cf. Introduction, Section 6).

Proof

If two points p_1 and p_2 belong to $B_1 \cap B_2$, then $p_1, p_2 \in B_1$, so their join : $p_1 + p_2 \in B_1$. Similarly $p_1 + p_2 \in B_2$. Hence $p_1 + p_2 \in B_1 \cap B_2$.

In the same way, if the lines ℓ_1 and ℓ_2 belong to each of B_1 and B_2, so does their intersection $\ell_1 \cap \ell_2$. □

If the projective plane is a Galois plane $PG(2,q^2)$, then the following theorem imposes more restrictions on the intersection configurations of two Baer-planes belonging to it.

Theorem 2.3 (cf. also [14])

If two Baer-planes in $PG(2,q^2)$ share 3 points on a line ℓ of $PG(2,q^2)$, then they share q+1 points of ℓ. (They share the line ℓ pointwise.)

Proof

Denote the three points on ℓ shared by the two Baer-planes by p_1, p_2, p_t.

Without loss of generality the fundamental points of $PG(2,q^2)$ can be chosen as

$$p_1 = (0\ 1\ 0),\ p_2 = (1\ 0\ 0),$$

(hence they are two of the given points), while

$$p_0 = (0\ 0\ 1) \quad \text{and } p_s = (1\ 1\ 1)$$

are two points in one of the Baer-planes, on some line through p_t (the third given point of intersection). Thus one of the given Baer-planes is taken to be B_0, the real Baer-plane, while the other one is denoted by B_1.

It follows from the construction that $p_t = (1\ 1\ 0)$. Consider a homography taking $\underline{B_1 \text{ to } B_0}$ and leaving $\underline{p_1 \text{ and } p_2 \text{ fixed}}$.

The matrix of this homography is of form

$$A = \begin{vmatrix} \alpha_1 & 0 & * \\ 0 & \alpha_2 & * \\ 0 & 0 & * \end{vmatrix},$$

where all entries are elements of $GF(q^2)$, the asterisks in the third column stand for unspecified elements, and α_1, α_2 and the last entry in the third column are non-zero.

The homography takes p_t to $p_u \in \ell \cap B_0$, where

$$p_u = (\alpha_1, \alpha_2, 0).$$

Since $p_u \in B_0$, it follows that $\alpha_1/\alpha_2 \in GF(q)$.

Let $p \in \ell \cap B_1$ where p is different from p_1, p_2, p_t. Without loss of generality

$$p = (x \quad 1 \quad 0)$$

then the homography takes p to p', where

$$p' = (\alpha_1 x \quad \alpha_2 \quad 0).$$

Since $p' \in B_0$, $\alpha_1 x/\alpha_2 \in GF(q)$ and so $x \in GF(q)$. This means that all the points of $\ell \cap B_1$ belong to B_0. Hence B_1 and B_0 intersect in q+1 points of ℓ as claimed. □

It follows immediately that the intersection of two distinct Baer-planes in $PG(2,q^2)$ have 0, 1, 2 or q+1 points in common with any line. Furthermore, by Lemma 2.2 the intersection is a closed configuration and it cannot contain a non-degenerate quadrangle, because such a quadrangle determines exactly one Baer-plane. Hence we arrive to the following theorem.

<u>Theorem 2.4</u>

Two Baer-planes in $PG(2,q^2)$ can only intersect in one of the following configurations:

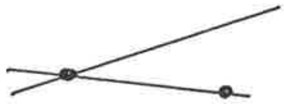
(1) the empty set, ϕ (1)

(2) one point and one line

(i) the point is on the line  (2i)

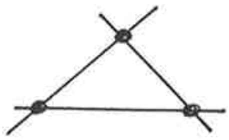
(ii) the point is external to the line,  (2ii)

(3) two points and two lines as shown,



(3)

(4) three points and three lines forming a triangular configuration,



(4)

(5) q+1 points on a line and q+1 lines going through one point of that line

(5)

(6) q+2 points and q+2 lines q+1 points being collinear and q+1 lines concurrent.

(6)

Proof

By Theorem 2.1 the number of points and number of lines in the intersection must be the same. In cases (1) and (2) there is nothing to prove. In case (3) one of the lines must be the join of the two points and one of the points must be the intersection of the two lines since the configuration is closed. In case (4) the configuration consists of 3 non-collinear points and their 3 joins. In cases (5) and (6) the configurations contain more than two points of one line ℓ. By Theorem (2.3) the number of points on that line must then be q+1. If no more than these q+1 points belong to the intersection, then there must be q+1 lines, one of which is the join of the points. The remaining q lines must all intersect in one of the q+1 points, otherwise a point external to ℓ would be added to the configuration. In case (6) an external point is added to the q+1 points of ℓ. The q+1 lines joining the external point to the points of ℓ close the configuration. No more than 1 external point can be added to the q+1 points of ℓ, since the configuration cannot contain a quadrangle. This completes the proof.

□

Note:

Theorem (2.4) does not establish the existence of all the listed configurations. It will be shown later that they are all realised and the number of Baer-planes intersecting a fixed Baer-plane of PG$(2,q^2)$ will be calculated.

2.3 Baer-planes and perspectivity Groups, Slots, Bunches and Clusters

Recall the result in the Introduction : Desarguesian planes are (V,ℓ)-transitive for all (V,ℓ)-pairs in the planes: if V is any fixed point of the plane and ℓ any line with all its points fixed, then the homography-group with the above fixed set is transitive on the points of $m\setminus\{V,m \cap \ell\}$, where m is any line through V. The homographies belonging to the group are perspectivities, more specifically homologies if V is not on ℓ, and elations otherwise.

Before discussing the action of perspectivity groups or Baer-planes, the following theorem is needed.

(Note: in the following statement and proof, points are marked by capitals, lines by small letters, to make distinctions between duals clearer.)

Theorem 2.5

If ℓ is a line in PG$(2,q^2)$, A, B, C three distinct points on the line, and P an arbitrary point of the plane, not on ℓ, then there exist Baer-planes in PG$(2,q^2)$ containing A, B, C and P.

Dually : If a, b, c are three lines in the plane, through a point P, and ℓ some other line of the plane, not through P, then there are Baer-planes containing a, b, c and ℓ.

Proof

Let P' be a point on the line PC, distinct from P or C. (Since $q^2+1\geq 5$, the choice for P' is not unique.) Then A, B, P', P determine a non-degenerate quadrangle, hence a Baer-plane, which contains C, which is the intersection of AB and PP'.

The dual statement is proved similarly, noting that a quadrilateral (non-degenerate) also determines uniquely a Baer-plane, since any four intersection points of the four sides forming a non-degenerate quadrangle determine a unique Baer-plane containing the four lines (hence the other intersection points). □

Recall next Lemma 2.2. All Baer-planes sharing the points A, B, C on the line ℓ, share q+1 points of line ℓ. The dual of this lemma implies that if two Baer-planes share three lines a, b, c through the point P, then they have q+1 lines through P in common.

Definitions

(a) Let A, B, C be three points on a line ℓ in $PG(2,q^2)$. The set of q+1 points of ℓ belonging to a Baer-plane through A, B, C is called a slot on ℓ.

(b) Let a, b, c be three lines of $PG(2,q^2)$ through a point P. The set of q+1 lines through P belonging to a Baer-plane containing a, b, and c (that is segments of q+1 points of each of these lines), is called a bunch through P.

Theorem 2.6

For a given line ℓ, and a given point V, not on ℓ in $PG(2,q^2)$, and a given slot s on ℓ, there are exactly q+1 Baer-planes which share the point V and the slot s. They partition the points on each of the q+1 lines joining V and the points of s (excluding V and s).

Proof

By Theorem 2.5 there exists a Baer-plane B_1, containing V and s. Then a (V,ℓ)-homology θ takes B_1 into some Baer-plane (possibly itself). This new Baer-plane is fully determined by a non-degenerate quadrangle, and since V and s are already fixed, an image of any point $X \in B_1 \setminus \{V \cup s\}$ determines a Baer-plane. On the other hand, since the plane $PG(2,q^2)$ is (V,ℓ)-transitive for any choice of V and ℓ, any point X' on some line m through V, m belonging to B_1, is a θ-image of the point X on $B_1 \cap m$, where θ is a (V,ℓ)-homology, and X and X' are distinct, from V or points of s. Hence, every point X of $m \setminus \{V, m \cap \ell\}$ belongs to exactly one Baer-plane containing V and s. The three points V, $m \cap \ell$ and X' determine a slot on the line m. Thus all images of X within this slot determine the same Baer-plane.

Hence the number of Baer-planes sharing V and the slot s on ℓ is equal to the number of slots on some line m, joining V and a point of s, such slot containing V and $m \cap s$. Since there are q-1 more points on each slot, and by Theorem 2.3 these sets of q-1 points must be disjoint, the number of admissible slots on m is

$$(q^2+1-2)/(q-1) = q+1.$$

This concludes the proof. □

Definition

A family, consisting of q+1 Baer-planes sharing a slot s on a line ℓ and a point V not on ℓ, is called a (V,s)-homology cluster.

Theorem 2.7

Let ℓ be a line in $PG(2,q^2)$, A a point on ℓ, s a slot on ℓ, and b a bunch through A such that s and b belong to the same Baer-plane B_1.

Then there are exactly q Baer-planes which share the slot s and the bunch b. The points, excluding A, of the q lines of $b\setminus\{\ell\}$ are partitioned by the Baer-planes into disjoint sets, each containing q points.

Proof

Choose in the fixed Baer-plane B_1 a point X, not belonging to s. Let m be the line AX. Let θ' be an (A,ℓ)-elation taking X to X' where $X' \in m\setminus\{A\}$. It is known (cf. Introduction, Section 6) that θ' is fully determined by X', hence X' also determines uniquely a Baer-plane B_2 (possibly identical to B_1), which is the image of B_1. The point X' can be arbitrarily chosen on $m\setminus\{A\}$, since $PG(2,q^2)$ is (A,ℓ)-transitive. Let $s_m = B_2 \cap m$, thus s_m is a slot on the line m. Let X" be another point of s_m. By the transitivity property, X" determines some transformation θ'', belonging to the (A,ℓ)-elation group. Hence X" also determines uniquely some Baer-plane B_3, which contains X", b and s, (since B_3 is an image of B_1).

Then the Baer-planes B_2 and B_3 are identical, since they share at least one non-degenerate quadrilateral conisting of two lines of b, different from m, and two lines joining X" to two points of s, different from A, (noting that X" belongs to B_2 since it is a point of s_m). Hence the slot s_m determines a unique Baer-plane containing s and m.

Conversely, if $Y \in m\setminus s_m$, then the unique Baer-plane determined by the (A,ℓ)-elation taking X to Y must differ from B_2, since it contains a point on m, which does not belong to $B_2 \cap m$.

Hence the number of Baer-planes sharing a slot s on ℓ and an associated bunch b through the point $A \in s$ is equal to

$(q^2+1-1)/q = q,$

since by the above, the set of points of $m\backslash\{A\}$ is partitioned into disjoint sets, each containing $q+1-1 = q$ points. □

Definition

A family, consisting of q Baer-planes, sharing a slot s on a line ℓ together with a fixed bunch through A, where A is a point of s, is called an (A,s)-elation cluster.

2.4 The Existence of the Intersection Configurations of Two Baer-planes

Theorem 2.8

There exist seven possible configurations of intersections of Baer-planes in $PG(2,q^2)$.

Proof

Theorem 2.4 gives a listing of 1; 2(i),(ii); 3, 4, 5, 6 to the only possible configurations in which two Baer-planes in $PG(2,q^2)$ may intersect. Theorems 2.6 and 2.7 will be used to construct and count all Baer-planes intersecting a fixed Baer-plane in each of the configurations from 6 down to 2(i) and 2(ii). The total number of these is found to be less than N-1, where

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

denotes the total number of Baer-planes in $PG(2,q^2)$ (cf. 1.2). Thus N_0, the number of Baer-planes disjoint from B_0 can be also found by a simple subtraction. The procedure then is to begin with configuration (6) and do the constructions and counting successively in the cases, in an order reverse to the listing.

Without loss of generality, the fixed Baer-plane can be taken to be in all cases, the real Baer-plane B_0. This is used as a reference, but does not make any difference to the arguments in the proofs.

Case 6

To determine the number of Baer-planes sharing q+2 points and q+2 lines with B_0, we count the number of (V,s)-homology clusters to which B_0 belongs. Each cluster is determined by fixing within B_0 a point V and a line ℓ of $PG(2,q^2)$ belonging to B_0.

For V we have a free choice out of the q^2+q+1 points of B_0. For ℓ, a line must be chosen which does not contain V, hence there are

$$q^2+q+1-(q+1) = q^2 \text{ choices.}$$

Thus B_0 belongs to

$$q^2(q^2+q+1) \quad \text{clusters.}$$

By Theorem 2.6 there are q Baer-planes other than B_0 in each cluster, the clusters forming disjoint classes of Baer-planes. Hence the number of Baer-planes intersecting B_0 in configuration (6) is

$$\underline{N_{q+2} = q^3(q^2+q+1)} \qquad (4.1)$$

Case 5

To find the number of Baer-planes intersecting B_0 in exactly q+1 points of a line (and the same number of lines), we have to find the number of (A,s)-elation clusters to which B_0 belongs. The point A can be chosen within B_0 in q^2+q+1 ways. Since there are q+1 lines of B_0 through A, there are q+1 choices for the slot s containing A. Thus the required number of elation-clusters is $(q^2+q+1)(q+1)$.

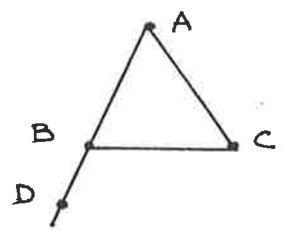
In each elation-cluster there are q-1 Baer-planes other than B_0 by Theorem (2.7). Thus the number of Baer-planes intersecting B_0 in configuration (5) is

$$N_{q+1} = (q^2-1)(q^2+q+1) \qquad (4.2)$$

Case 4

The intersection is a triangular configuration of three points and three lines.

Let the points A, B, C be fixed in B_0. Let D be any point on the line AB, not belonging to B_0. Then A, B, D determine uniquely a slot s of q+1 points on the line AD. Next we find the number of



Baer-planes containing the point C and the slot s (hence the points A and B) and no other point of B_0. All these Baer-planes belong to the (C,s)-homology cluster determined by A, B, C and D. This cluster consists of q+1 Baer-planes. However, we must exclude Baer-planes containing points on CA or CB, other than A, B, C and belonging to B_0.

By Theorem 2.6 there is a unique Baer-plane B_1 which shares with B_0 the slot $AC \cap B_0$ and belongs to the (C,s)-cluster. Likewise, there is a unique Baer-plane B_2 which shares with B_0 the slot $BC \cap B_0$ and belongs to the (C,s) cluster. Moreover, B_1 and B_2 are distinct, for no Baer-plane shares with B_0 more points than those in a slot and a point external to the slot. Thus B_1 and B_2 are the only two Baer-planes belonging to the (C,s) cluster, and sharing with B_0 some points on CA or CB other than A, B or C. So the numbers of admissible Baer-planes belonging to the (C,s) cluster is

$$q+1-2 = q-1.$$

The number of slots on the line AB, containing the points A and B is

$$(q^2-1)/(q-1) = q+1$$

(as seen before in the proof of Theorem 2.6).

Thus there is a choice of q slots, other than the slot belonging to B_0, on the line AB, through A and B, each of them determining a (C,s) cluster. Hence, for a fixed triangle ABC in B_0 there are

$$q(q-1)$$

Baer-planes intersecting B_0 in exactly A, B, and C.

The choice of the three non collinear points A, B, C in B_0 can be made in

$$\frac{(q^2+q+1)(q^2+q)q^2}{3!} \quad \text{ways,}$$

(choosing A, B, C in order, then obtaining the number of unordered triples).

Hence the number of Baer-planes intersecting B_0 in configuration (4), is

$$N_3 = \frac{(q^2+q+1)(q^2+q)q^2}{3!}\, q(q-1)$$

$$= (q^2+q+1)q^4(q^2-1)/3! \qquad (4.3)$$

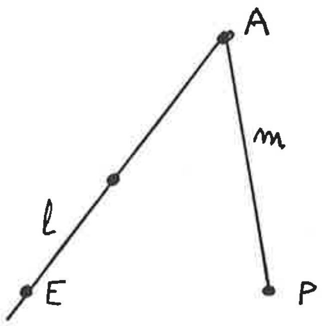
Note

While q > 2, and plane B_1 intersects B_0 in exactly 3 points, the points are necessarily non-collinear. This is not the case when q=2. Case 5 applies to the situation when two Baer-planes in PG(2,4) intersect in 3 collinear points, and case 4, when the points are non-collinear.

Thus, for PG(2,4) there are $(2^2+2+1)(2^2-1) = 21$ Baer-planes intersecting B_0 in 3 collinear points and $(2^2+2+1)2^4(2^2-1)/3! = 56$ Baer-planes intersecting it in 3 non-collinear points. Hence the total number of Baer-planes in PG(2,4) intersecting B_0 in 3 points is 77.

Case 3

Let A, B be fixed points and ℓ, m fixed lines of B_0 such that ℓ = AB and A = $\ell \cap m$. The admissible Baer-planes to be counted are those which intersect B_0 in A, B, ℓ and m and no other points or lines.



Let P be a point of $m \setminus \{A\}$, not belonging to B_0, and s a slot on ℓ, determined by A, B and E where E $\notin B_0$. We show that there is exactly one admissible Baer-plane containing P and s.

All Baer-planes through P and s belong to the (P,s)-homology cluster which consists of q+1 Baer-planes, all different from B_0. Let C be a point of $B_0 \cap m \setminus \{A\}$. Then the quadrangle EBPC determines the unique Baer-plane B_1, which contains also the point A, hence belongs to the (P,s)-cluster. Since B_1 is then different from B_0, it shares no other points with B_0 on the line m, than A and C. Thus, each point of $B_0 \cap m \setminus \{A\}$ determines a unique Baer-plane of the (P,s)-cluster, and these planes are distinct, q in number, all of them inadmissible. This leaves exactly one Baer-plane, $\overline{B}$ in the cluster. $\overline{B}$ is admissible, for it shares on ℓ only the points A and B with B_0, on m only the point A, and it cannot contain a point $P' \in B_0 \setminus \{\ell \cup m\}$, otherwise the line EP' and hence $EP' \cap m$ belongs to $\overline{B} \cap B_0$, which is a contradiction, since $EP' \cap m \neq A$. This proves the claim.

$\overline{B}$ intersects $m \setminus \{A\}$ in q points. Hence the number of admissible planes containing the slot s in ℓ is equal to the number of slots on m, each consisting of the point A and a set of q points, disjoint from all the other slots. The number of these slots is then

$$(q^2+1-(q+1))/q = q-1$$

Since, as seen before, the slot s on ℓ can be chosen in q ways, (if it is to contain exactly the two given points A and B of B_0, and no more) it follows that there are

q(q-1) admissible Baer-planes for each fixed A, B, ℓ, m set in B_0.

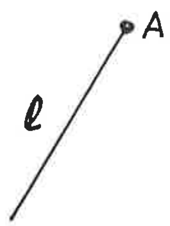
The number of choices for the above sets can be obtained by considering the number of selections for A and B, which uniquely determine ℓ, and then choose m through A, giving $\underline{(q^2+q+1)(q^2+q)q}$ selections of the above ordered set.

Thus the number of Baer-planes intersecting B_0 in two points and two lines is

$$\begin{aligned} N_2 &= (q^2+q+1)(q^2+q)q(q-1)q \\ &= (q^2+q+1)q^3(q^2-1) \qquad (4.4) \end{aligned}$$

Case 2(i)

Let ℓ and A be a fixed line and point of B_0 and $A \in \ell$. The admissible Baer-planes now are those which intersect B_0 in A and ℓ and no other elements.



As a first step, we count

(a) the number of slots on line ℓ which contain A, but no other point of B_0,

(b) dually : the number of bunches through A which contain ℓ, but no other line of B_0.

The count is the same for (a) and (b).

The total number of slots containing A on ℓ is

$$\binom{q^2}{2}/\binom{q}{2} = q^2(q^2-1)/q(q-1) = q^2 + q,$$

because there are $\binom{q^2}{2}$ ways of picking 2 points on ℓ which determine a slot together with A, and there are $\binom{q}{2}$ pairs of points different from A within each slot consisting of q+1 points.

Fix now a point on $\ell \cap B_0 \setminus \{A\}$. This can be done in q ways. As it was shown earlier, the number of slots containing A, the selected point but no other point of B_0, is q. Thus q^2 slots contain exactly two points of $B_0 \cap \ell$. Finally, subtract q^2+1 from the total number of slots, taking into account the single slot which belongs to B_0. Hence the count for both (a) and (b) is

$$(q^2+q)-(q^2+1) = \underline{q-1}.$$

Next consider the cluster of Baer-planes which contain a slot s on ℓ, and a bunch b through A, such that s contains no other point than A and b contains no other line of B_0 than ℓ.

This is an (A,b)-elation cluster, consisting of <u>q Baer-planes</u>, <u>all</u> of which are <u>admissible</u>, since none of the lines of the bunch contain any point of B_0, other than A. Hence any of the planes belonging to this cluster intersect B_0 in A and ℓ and no other element.

Since the choice of slots and bunches of the desired property, can be done in (q-1) ways for each, it follows that for a given A and ℓ the number of admissible Baer-planes is

$$q(q-1)^2.$$

The choice of A and ℓ in B can be made in $(q^2+q+1)(q+1)$ ways, hence the total number of Baer-planes intersecting B_0 in one line and one point contained by the line is

$$N_1^{(1)} = (q^2+q+1)(q+1)q(q-1)^2 \qquad (4.5)$$

Case 2(ii)

Let ℓ and A be a fixed line and point in B_0, A not on ℓ. A Baer-plane is admissible if it intersects B_0 in A and ℓ, but no other point or line.

Consider an (A,s)-homology cluster, where s is a slot on the line ℓ, not containing any point of B_0. All admissible Baer-planes must belong to such a homology-cluster, since each must contain A and ℓ, but cannot intersect ℓ in a point belonging to B_0. All q+1 Baer-planes belonging to such a homology cluster are admissible, for no line of the bunch through A can belong to B_0, otherwise its intersection with ℓ would be a point of B_0. So no line of the bunch contains a point of B_0 other than A.

Next the number of slots on ℓ, not containing any point of B_0 must be calculated:

Reasoning similarly as before we have

(a) the total number of slots on ℓ = $\binom{q^2+1}{3}/\binom{q+1}{3}$

$= q(q^2+1)$

(b) the number of slots containing one fixed point of B_0 is using the result in case 1(i)

$= q-1,$

hence the total number of slots containing some unique point of B_0 on ℓ is $(q+1)(q-1)$.

(c) the number of slots containing exactly two fixed points of $B_0 \cap \ell$ is (as seen before) q, hence the number which contains exactly some fixed pair of points in $B_0 \cap \ell$ is

$$\binom{q+1}{2} q.$$

(d) there is 1 Baer-plane, namely B_0, which contains more than 2 points of $B_0 \cap \ell$.

Hence the required number of suitable slots is

$$q(q^2+1)-(q-1)(q+1) - q^2(q+1)/2 - 1 = 1/2\, q(q-1)(q-2).$$

Since each (A,s)-cluster contains q+1 admissible Baer-planes, if s has no point in B_0, the total number of admissible Baer-planes, for A and ℓ fixed is

$$1/2\, q(q^2-1)(q-2)$$

The number of ways in which the point A and the line ℓ can be selected, is

$$(q^2+q+1)q^2,$$

and so the number of Baer-planes intersecting B_0 in one line and one point, the point not on the line is

$$N_1^{(2)} = 1/2\, q^3(q^2+q+1)(q^2-1)(q-2) \qquad (4.6)$$

Using now the result (1.2) for the total number N of Baer-planes in $GF(q^2)$, we can calculate N_0, the number of Baer-planes disjoint from B_0:

$$N_0 = N - N_{q+2} - N_{q+1} - N_3 - N_2 - N_1^{(1)} - N_1^{(2)}. \qquad (4.7)$$

Substituting into each term on the right hand side of (4.7) the appropriate result given by (1.2), (4.1), (4.2), (4.3), (4.4), (4.5) and (4.6), we obtain after simplification that

$$N_0 = \frac{q^4(q-1)^3(q+1)}{3} \qquad (4.8)$$

This completes the counts of all the configurations listed in Theorem (4.4), hence completes the proof of Theorem (4.8). □

Compare the expression (4.8) with the order Λ_0 of the homography group which leaves B_0 invariant. By (5.4) in the introduction,

$$\Lambda_0 = |PGL(3,q)| = q^3(q^3-1)(q^2-1).$$

Hence N_0 may be written down as

$$N_0 = (q^2-q)\frac{\Lambda_0}{3(q^2+q+1)} \qquad (4.9)$$

An interpretation of this result is given in Section 8 of this Chapter.

2.5 The Action of Cyclic (Singer) Groups of Homographies

Singer's theorem plays a fundamental role in describing the structure of the projective plane $PG(2,q^2)$. It was treated generally, (for spaces of n dimensions) in detail in the Introduction (Section 6). It is convenient to recall here some definitions and notations which will be used throughout. In this chapter only planes are considered, hence the following apply to two dimensions only.

The Singer group is a cyclic group of homographies, acting regularly on the points and lines of $PG(2,q)$. Since this chapter deals with Baer-planes in the projective plane of square order : $PG(2,q^2)$, it will be necessary to distinguish between a Singer group acting on the projective plane $PG(2,q^2)$ and the Singer group acting on the Baer-plane $B_0 = PG(2,q)$. Hence, whenever necessary we use subscripts q or q^2 in the notation.

Thus $\Xi_q = \langle\sigma_q\rangle$ acts on $PG(2,q)$

and $\Xi_{q^2} = \langle\sigma_{q^2}\rangle$ acts on $PG(2,q^2)$.

Here σ_q is a homography with matrix

$$M = \begin{vmatrix} c_2 & 1 & 0 \\ c_1 & 0 & 1 \\ c_0 & 0 & 0 \end{vmatrix} \qquad (5.1)$$

where $x^3 = c_2x^2 + c_1x + c_0$ (5.2)

is the generating cubic equation (cf. Introduction) and c_2, c_1, c_0 are elements of $GF(q)$.

For σ_{q^2} we write the matrix of homography and generating cubic equation in the same forms (5.1) and (5.2) respectively, with the understanding that in this case c_2, c_1, c_0 are elements of $GF(q^2)$.

The Singer groups induce natural orderings of the points and lines in $PG(2,q)$ and $PG(2,q^2)$.

Denoting by $\sigma(p)$, $\sigma^2(p) = \sigma(\sigma(p))$, ..., $\sigma^k(p)$, .. the successive Singer transforms of a point p, we denote by p_0 the point $(0\ 0\ 1)$, in $PG(2,q)$ (or $PG(2,q^2)$).

Then by Singer's theorem, the set

$$\{\sigma_q^k(p_0) \mid 0 \leq k < q^2+q+1\} \qquad (5.3)$$

consists of q^2+q+1 different points of $PG(2,q)$ and

$$\sigma_q^{q^2+q+1}(p_0) = p_0.$$

Hence all the points of PG(2,q) are represented by the set (5.3).

We denote by

$$p_k = \sigma_q^k(p_0) \tag{5.4}$$

The subscript k characterising the point p_k is called the Singer-index of the point. It is defined as the exponent (mod q^2+q+1) in the equation (5.4).

(Note: The subscript q or q^2 may be dropped if there is no ambiguity.)

Thus

$$\left.\begin{array}{l} p_0 = (0 \quad 0 \quad 1) \\ p_1 = \sigma(0 \quad 0 \quad 1) = (0 \quad 1 \quad 0) \\ p_2 = \sigma^2(0 \quad 0 \quad 1) = (1 \quad 0 \quad 0) \\ p_3 = \sigma^3(0 \quad 0 \quad 1) = (c_2 \quad c_1 \quad c_0) \end{array}\right| \tag{5.5}$$

and so on.

We observe that

$$p_{k+s} = \sigma^{k+s}(p_0) = \sigma^s(\sigma^k(p_0)) = \sigma^s(p_k).$$

The difference s between the Singer indices of two points is called the Singer-shift.

The lines of PG(2,q) are also ordered cyclically by the group

$$\Xi = \langle\sigma\rangle.$$

The choice of the line ℓ_0 is arbitrary. Unless stated otherwise in some particular case, we take for ℓ_0 the join of p_0 and p_1.

Hence

$$\ell_0 = p_0 + p_1, \text{ in short notation } p_0p_1$$
$$\ell_1 = \sigma(p_0+p_1) = \sigma(p_0) + \sigma(p_1) = p_1p_2$$
$$\ell_3 = \sigma^2(p_0+p_1) = \sigma^2(p_0) + \sigma^2(p_1) = p_2p_3$$

and generally

$$\ell_k = \sigma^k(\ell_0) = p_kp_{k+1} \tag{5.6}$$

The set

$$\{\sigma_q^k(\ell_0) | 0 \leqslant k < q^2+q+1\} \tag{5.7}$$

represents all the lines of PG(2,q).

The exponent k (mod q^2+q+1) in equation (5.6) is called the <u>Singer-index of the line ℓ_k</u>.

The difference between the indices of two lines (mod q^2+q+1) is called the <u>Singer-shift of the lines</u>.

We recall here that if the points

$$p_{i_0}, p_{i_1}, \ldots, p_{i_q} \text{ are collinear,}$$

then the indices $i_0, i_1, \ldots, i_q$ form a perfect difference set (cf. Introduction).

We also observe here the useful fact that if the point p_i is on the line ℓ_k, then the point p_{i+s} is on the line ℓ_{k+s}.

We conclude this section by tabulating the points and the lines of PG(2,4) to illustrate Singer ordering. Two different generating cubics are used in the two tables to determine the Singer cycle. PG(2,4) is the smallest projective plane of square order, so it is the smallest projective plane which possesses Baer-planes. In the case of PG(2,4) the ordering can be done by hand-calculation, while for projective planes of higher order, this is done by computer. In each of the two tables the points and lines of the real Baer-plane, i.e. the points the lines with coordinates in GF(2) are circled in.

TABLES OF SINGER LISTING IN PG(2,4)

(α is root of $\alpha^2+\alpha+1 = 0$ over GF(2))

Table 1a

Generating cubic : $x^3 = x^2+x+\alpha$

(Circled points and lines belong to real subplane)

(Circled entries shown in bold.)

Points	(x_1,x_2,x_3)	Lines (each line is given by the set of the indices of its points)					
P_0	(0, 0, 1)	**ℓ_0**	**0**	**1**	4	**14**	16
P_1	(0, 1, 0)	**ℓ_1**	**1**	**2**	5	**15**	17
P_2	(1, 0, 0)	ℓ_2	**2**	3	6	16	18
P_3	(1, 1, α)	ℓ_3	3	4	**7**	17	19
P_4	(0, α, 1)	ℓ_4	4	5	8	18	**20**
P_5	(α, 1, 0)	ℓ_5	5	6	9	19	**0**
P_6	(1, α^2, 1)	**ℓ_6**	6	**7**	10	**20**	**1**
P_7	(1, 0, 1)	**ℓ_7**	**7**	8	11	**0**	**2**
P_8	(1, 0, α)	ℓ_8	8	9	12	**1**	3
P_9	(α, 1, α^2)	ℓ_9	9	10	13	**2**	4
P_{10}	(α^2, 1, α^2)	ℓ_{10}	10	11	**14**	3	5
P_{11}	(α, 0, 1)	ℓ_{11}	11	12	**15**	4	6
P_{12}	(1, α, α)	ℓ_{12}	12	13	16	5	**7**
P_{13}	(1, 1, α^2)	ℓ_{13}	13	**14**	17	6	8
P_{14}	(0, 1, 1)	**ℓ_{14}**	**14**	**15**	18	**7**	9
P_{15}	(1, 1, 0)	ℓ_{15}	**15**	16	19	8	10
P_{16}	(0, 1, α)	ℓ_{16}	16	17	**20**	9	11
P_{17}	(1, α, 0)	ℓ_{17}	17	18	**0**	10	12
P_{18}	(1, α, α^2)	ℓ_{18}	18	19	**1**	11	13
P_{19}	(α, 1, 1)	**ℓ_{19}**	19	**20**	**2**	12	**14**
P_{20}	(1, 1, 1)	**ℓ_{20}**	**20**	**0**	3	13	**15**

Table 1b

Generating cubic : $x^3 = \alpha x^2 + \alpha x + \alpha$
(Circled points and lines belong to real subplane)

Points	(x_1, x_2, x_3)	Lines (each line is given by the set of the indices of its points)					
P_0	(0, 0, 1)	**ℓ_0**	**0**	**1**	6	**8**	18
P_1	(0, 1, 0)	**ℓ_1**	**1**	**2**	7	**9**	19
P_2	(1, 0, 0)	**ℓ_2**	**2**	**3**	**8**	10	20
P_3	(1, 1, 1)	**ℓ_3**	**3**	4	**9**	11	**0**
P_4	$(1, 1, \alpha^2)$	ℓ_4	4	5	10	12	**1**
P_5	$(\alpha^2, 1, \alpha)$	ℓ_5	5	6	11	13	**2**
P_6	$(0, \alpha^2, 1)$	ℓ_6	6	7	12	14	**3**
P_7	$(\alpha^2, 1, 0)$	ℓ_7	7	**8**	13	15	4
P_8	(0, 1, 1)	**ℓ_8**	**8**	**9**	14	**16**	5
P_9	(1, 1, 0)	ℓ_9	**9**	10	15	17	6
P_{10}	$(\alpha, 1, 1)$	ℓ_{10}	10	11	**16**	18	7
P_{11}	$(1, 1, \alpha)$	ℓ_{11}	11	12	17	19	**8**
P_{12}	$(\alpha, 0, 1)$	ℓ_{12}	12	13	18	20	**9**
P_{13}	$(\alpha, 1, \alpha)$	ℓ_{13}	13	14	19	**0**	10
P_{14}	$(\alpha^2, \alpha, 1)$	ℓ_{14}	14	15	20	**1**	11
P_{15}	$(\alpha^2, 0, 1)$	**ℓ_{15}**	15	**16**	**0**	**2**	12
P_{16}	(1, 0, 1)	**ℓ_{16}**	**16**	17	**1**	**3**	13
P_{17}	$(1, \alpha, 1)$	ℓ_{17}	17	18	**2**	4	14
P_{18}	$(0, 1, \alpha^2)$	ℓ_{18}	18	19	**3**	5	15
P_{19}	$(1, \alpha^2, 0)$	ℓ_{19}	19	20	4	6	**16**
P_{20}	$(1, \alpha, \alpha)$	ℓ_{20}	20	**0**	5	7	17

2.6 Singer Duality of Baer-Planes

We begin with the observation made in the last section that if a point p_i lies on the line ℓ_j, then the point p_{i+s} lies on the line ℓ_{j+s}.

Put in particular $s = -(i+j)$, then we obtain the result:

p_i lies on ℓ_j, if and only if p_{-j} lies on ℓ_{-i}.

Note: In this section we refer to the plane $PG(2,q^2)$, hence the Singer group here is

$$\Xi_{q^2} = \langle \sigma_{q^2} \rangle$$

and indices are taken modulo (q^4+q^2+1).

The above result suggests the establishment of the duality map ν_0, from the points of $\Pi = PG(2,q^2)$ to its lines, and from its lines to its points, defined the following way:

$$\left.\begin{array}{l} \nu_0(p_i) = \ell_{-i} = \overline{p_i(0)} \\ \nu_0(\ell_i) = p_{-i} = \overline{\ell_i(0)} \end{array}\right| \qquad (i=0,1,..,q^4+q^2) \qquad (6.1)$$

where $\overline{p_i(0)}$, $\overline{\ell_i(0)}$ are points and lines of the projective plane $\overline{\Pi}$, dual to Π.

It follows immediately that

$\overline{p_i(0)}$ lies on $\overline{\ell_j(0)}$ if and only if p_{-j} lies on ℓ_{-i}, hence if and only if p_{-j+s} lies on ℓ_{-i+s} for all s (mod q^4+q^2+1).

Thus the more general duality map ν_s may be defined:

$$\left.\begin{array}{l} \nu_s(p_i) = \ell_{-i+s} = \overline{p_i(s)} \\ \nu_s(\ell_i) = p_{-i+s} = \overline{\ell_i(s)} \end{array}\right| \quad (i=0,1,..,q^4+q^2) \qquad (6.2)$$

Let p_{i_1}, p_{i_2}, p_{i_3}, p_{i_4} be the vertices of a non-degenerate quadrangle in B_0, the real Baer-plane in PG$(2,q^2)$. Then, (denoting by $\overline{\Pi}$ the ν_s dual of Π):

the dual image of B_0 in $\overline{\Pi}$ is real if and only if ℓ_{-i_1+s}, ℓ_{-i_2+s}, ℓ_{-i_3+s}, ℓ_{-i_4+s} are real lines.

The above is referred to as Condition R.

This is so, because in this case the dual map of the quadrangle p_{i_1}, p_{i_2}, p_{i_3}, p_{i_4} is again a non-degenerate quadrangle with real vertices, hence it determines uniquely the real Baer-plane B_0 in $\overline{\Pi}$.

An equivalent form of Condition R is as follows:

The image of the real Baer-plane in Π = PG$(2,q^2)$ is the real Baer-plane of $\overline{\Pi}$ if and only if there exist in B_0 a non-degenerate quadrangle with vertices p_{i_1}, p_{i_2}, p_{i_3}, p_{i_4} and a non-degenerate quadrilateral with sides ℓ_{j_1}, ℓ_{j_2}, ℓ_{j_3}, ℓ_{j_4} such that

$$j_r - j_t = -(i_r - i_t) \quad (\text{mod } q^4+q^2+1)$$

for

$$r,t = 1, 2, 3, 4 \text{ and } r \neq t.$$

Theorem 2.9

A unique number s can be found such that the duality map ν_s, defined as in (6.2), maps the real Baer-plane of Π = PG$(2,q^2)$ to the real Baer-plane of $\overline{\Pi} = \nu_s(\Pi)$.

<u>Proof</u>

It suffices to ascertain that Condition R is satisfied, that is, a non-degenerate quadrangle p_{i_1}, p_{i_2}, p_{i_3}, p_{i_4} can be found, such that its vertices are real points and the duals ℓ_{s-i_1}, ℓ_{s-i_2}, ℓ_{s-i_3}, ℓ_{s-i_4} are real lines, for a suitably chosen s.

Let ℓ_0, ℓ_1 and ℓ_2 (indexed as in Section 5) be the lines p_0p_1, p_1p_2, p_2p_3 with equations

$$\begin{aligned} x_1 &= 0 && (\ell_1) \\ x_3 &= 0 && (\ell_2) \\ c_0x_2 - c_1x_3 &= 0 && (\ell_3) \end{aligned}$$

using the coordinates of p_0, p_1, p_2, p_3 as in (5.5).

Using the line-coordinate notation $[u_1 \; u_2 \; u_3]$ to describe a line of which the equation is $u_1x_1 + u_2x_2 + u_3x_3 = 0$, we write

$$\left.\begin{aligned} \ell_0 &: [1 \;\; 0 \;\; 0\,] \\ \ell_1 &: [0 \;\; 0 \;\; 1] \\ \ell_2 &: [0 \;\; c_0 \; - c_1] \end{aligned}\right| \qquad (6.3)$$

and

$$\ell_{-1} : [c_2 \;\; 1 \;\; 0] \quad \Big| \quad (\text{as } [1\;0\;0]M = [c_2 \;\; 1 \;\; o])$$

The lines ℓ_0 and ℓ_1 are real, so each of them contains q+1 points belonging to B_0.

Let this list of real points be as follows:

$$\left.\begin{aligned} \ell_0 &: p_0 \; p_1 \; p_{i_2} \; \cdots \; p_{i_q} \\ \ell_1 &: p_1 \; p_2 \; p_{i_2+1}, \; \cdots \; p_{i_q+1} \end{aligned}\right| \qquad (6.4)$$

Since ℓ_1 is obtained from ℓ_0 by a Singer-shift equal to 1, the points in the second line of (6.4) belong indeed to ℓ_1. That these points also belong to B_0 follows from the fact that the Singer transformation σ_{q^2} with matrix M as in (5.1) takes a point

$(0, f, g)$ of ℓ_0, where $f, g \in GF(q)$

to $(f, g, 0)$ in ℓ_1.

Suppose that the dual map ν_s takes the line ℓ_0 to the point p_s, as in (6.2).

Then ℓ_1 has as dual the point p_{s-1}, while the points

$p_0, p_1, \ldots, p_{i_q}$

and

$p_1, p_2, \ldots, p_{i_q+1}$

have as duals the lines

$\ell_s, \ell_{s-1}, \ldots, \ell_{s-i_q}$

and

$\ell_{s-1}, \ell_{s-2}, \ldots, \ell_{s-i_q-1}$ respectively.

We look for a duality map which satisfies the following condition.

Condition S.

The transformation σ_{q^2} takes all real lines through p_s into real lines through p_{s-1}.

We note here that Condition S represents the dual of the statement that all real points of ℓ_0 are taken by σ_{q^2} to real points of ℓ_1, and so it represents a condition necessary to be satisfied by s to make $\nu_s(B_0)$ the real Baer-plane of $\overline{\Pi}$.

Suppose that

$p_s = (x_1\ x_2\ x_3)$.

Then the line

$$\ell = [a_1 \ a_2 \ a_3]$$

goes through p_s if and only if

$$a_1x_1 + a_2x_2 + a_3x_3 = 0 \qquad (6.5)$$

This line ℓ is real if and only if a_1, a_2, a_3 (divided by a common factor if necessary) belong to GF(q).

The transformation $\sigma_{q^2}^{-1}$ takes the line $[a_1 \ a_2 \ a_3]$ into a line $[b_1 \ b_2 \ b_3]$ such that the matrix equation

$$[b_1 \ b_2 \ b_3] = [a_1 \ a_2 \ a_3]M$$

is satisfied, where M is the Singer matrix of σ_{q^2}.

From this we have

$$[b_1 \ b_2 \ b_3] = [c_2a_1 + c_1a_2 + c_0a_3 \quad a_1 \quad a_2] \qquad (6.6)$$

Referring now to Condition S, the choice of s, hence of p_s must be made so that for the fixed triple $(x_1 \ x_2 \ x_3)$ and for all real triples $(a_1 \ a_2 \ a_3)$ which satisfy equation (6.5), all triples $(b_1 \ b_2 \ b_3)$ obtained by (6.6) are also real.

Write $c_i = \alpha_i + \varepsilon\beta_i$ (i=1,2,3), where ε is a primitive element of the extension-field $GF(q^2)$ over GF(q) and α_i, $\beta_i \in GF(q)$. (cf. Introduction, Section 1).

Then Condition S is satisfied if and only if

$$\beta_2a_1 + \beta_1a_2 + \beta_0a_3 = 0$$

for each of the q+1 vectors $[a_1\ a_2\ a_3]$, representing real lines, which satisfy (6.5).

This happens if and only if

$$p_s = (\beta_2\ \beta_1\ \beta_0) \tag{6.7}$$

Next it must be shown that if s is chosen to satisfy (6.7) then Condition R is fulfilled.

(i) The General Case

As a first step we show that if (6.7) is satisfied, then the lines ℓ_s, ℓ_{s-1}, ℓ_{s-2} are real.

Since p_s is real by definition and Condition S is satisfied, it follows that the point p_{s-1} is also real. Thus

$\ell_s = p_{s-1}p_s$ is real.

Moreover, since ℓ_{s-1} is one of the real lines through p_s, the transformation $\sigma_{q^2}^{-1}$ takes it to a real line which is ℓ_{s-2}.

It remains to be shown that ℓ_s is real. By the use of matrix M, the point p_{s+1} is determined.

$$p_{s+1} = (c_2\beta_2 + \beta_1 \quad c_1\beta_2 + \beta_0 \quad c_0\beta_2)$$

(Note: p_{s+1} is not generally real.)

The equation of the line ℓ_s is

$$\begin{vmatrix} x_1 & x_2 & x_3 \\ \beta_2 & \beta_1 & \beta_0 \\ c_2\beta_2+\beta_1 & c_1\beta_2+\beta_0 & c_0\beta_2 \end{vmatrix} = 0 \tag{6.8}$$

Writing in (6.8) $c_i = \alpha_i + \varepsilon\beta_i$ for i=1,2,3, and expanding the left hand side, all terms containing ε vanish. This verifies that ℓ_s is real.

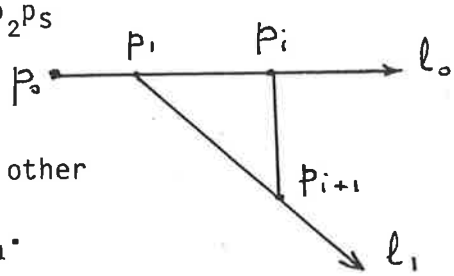
Suppose that p_s is not on ℓ_0, ℓ_1 or on the line p_1p_2. In this case the quadrangle $p_0p_1p_2p_s$ is non-degenerate, and its dual is the quadrilateral found by the lines ℓ_s, ℓ_{s-1}, ℓ_{s-2}, ℓ_0, which are real.

Hence Condition R is satisfied and for this case the proof of the theorem is complete.

The cases where $p_0p_1p_2p_s$ is degenerate, must be considered next.

(ii) <u>Cases when p_s lies on the lines ℓ_0, ℓ_1 or p_1p_2</u>

In all these cases some non-degenerate real quadrangle other than $p_0p_1p_2p_s$ must be found.



Use will be made of real points other than p_0 or p_1 on lines ℓ_0 and ℓ_1.

Let such a point be $p_i = (0, f, g)$ where $f,g \in GF(q)$. Thus $p_{i+1} = (f, g, 0)$. Here $p_i = \sigma_{q^2}^{i}(p_0)$ and $p_{i+1} = \sigma_{q^2}^{i+1}(p_0) = \sigma_{q^2}^{i}(p_1)$.

The transformation $\sigma_{q^2}^{i}$ takes the three consecutive points p_0, p_1, p_2 to the three consecutive points p_i, p_{i+1}, p_{i+2}, where

$$p_{i+2} = \sigma_{q^2}(p_{i+1}),$$

hence by the use of the matrix M

$$p_{i+2} = (c_2 f + g \quad c_1 f \quad c_0 f).$$

(Note: Strictly speaking, the matrix M^i takes p_0 to the vector $\rho(0 \quad f \quad g)$, where $\rho \in GF(q^2)$, hence the points p_1 and p_2 to $\rho(f \quad g \quad 0)$ and $\rho(c_2 f+g \quad c_1 f \quad c_0 f)$, but handling M^i as a matrix of homography, the factor common to all three columns can be disregarded.)

It follows from the above that the transformation

$$\sigma^i_{q^2} \ : \ p_0 \to p_i$$

has the matrix

$$M(i) = \begin{vmatrix} c_2 f+g & f & 0 \\ c_1 f & g & f \\ c_0 f & 0 & g \end{vmatrix} \qquad (6.9)$$

The duals of p_i and p_{i+1} are ℓ_{s-i} and ℓ_{s-i-1} respectively. Rather than showing generally that for $p_s = (\beta_2, \beta_1, \beta_0)$, the dual ℓ_{s-i} and ℓ_{s-i-1} are real, it turns out to be simpler to treat each arising case separately.

Case (a) s=0

Then $p_s = (0 \quad 0 \quad 1)$ hence $\beta_2 = \beta_1 = 0$, thus $c_2, c_1 \in GF(q)$.

The line coordinates of ℓ_{s-i} and ℓ_{s-i-1}, (which in this case are ℓ_{-i} and ℓ_{-i-1}) are evaluated by using the line corodinates of ℓ_0 and ℓ_{-1}, given in (6.3) and the matrix $M^{(i)}$.

For ℓ_{-i}:

$$[1\ \ 0\ \ 0]\begin{vmatrix} c_2f+g & f & 0 \\ c_1f & g & f \\ c_0f & 0 & g \end{vmatrix} = [c_2f+g\ \ \ f\ \ \ 0] \qquad (6.10)$$

For

$$\ell_{-i-1} : [c_2\ 1\ \ 0]M^{(i)} = [c_2^2f + c_2g + c_1f\ \ \ c_2f+g\ \ \ f] \quad (6.11)$$

Since c_2, $c_1 \in GF(q)$, all components in the equations (6.10) and (6.11) are real.

Thus the real non-degenerate quadrangle $p_0\ p_2\ p_{i+1}\ p_i$ has as dual the real quadrilateral $\ell_0\ \ell_{-2}\ \ell_{-i-1}\ \ell_{-i}$.

Case (b) s=1

This time $p_s = (0\ \ 1\ \ 0)$, hence $\beta_2 = \beta_0 = 0$ and so c_2 and c_0 are real.

The duals of p_i and p_{i+1} are now ℓ_{1-i} and ℓ_{-i}.

For ℓ_{-i} (6.10) can be used. Since $c_2 \in GF(q)$, ℓ_{-i} is real.

For ℓ_{1-i}:

$$[0\ \ 0\ \ 1]M^{(i)} = [c_0f\ \ \ 0\ \ \ g]$$

Hence ℓ_{1-i} is real.

The non-degenerate quadrangle and its dual are now $p_0\ p_2\ p_{i+1}\ p_i$ and $\ell_1\ \ell_{-1}\ \ell_{-i}\ \ell_{1-i}$ respectively, hence satisfy the requirements.

Case (c) s=2

$p_s = (1\ \ 0\ \ 0)$ hence $\beta_1 = \beta_0 = 0$ and so c_1 and c_0 are in $GF(q)$.

The dual of the quadrangle $p_0\ p_2\ p_{i+1}\ \ p_i$ is now $\ell_2\ \ell_0\ \ell_{1-i}$ ℓ_{2-i}.

Only ℓ_{2-i} must be calculated. Using (6.3) again for ℓ_{2-i}:

$$[0 \quad c_0 \quad -c_1]M^{(i)} = [0 \quad c_0g \quad c_0f-c_1g]$$

All sides of the dual quadrilateral are real lines.

Case (d) p_s is on ℓ_0, but $s\neq 0$, $s\neq 1$

In this case we taken $i=s$ and use the quadrangle $p_0\ p_2\ p_{s+1}\ p_s$ with its dual $\ell_s\ \ell_{s-2}\ \ell_{-1}\ \ell_0$:

The lines ℓ_s, ℓ_{s-2}, ℓ_0 are always real as shown before. The coordinates of ℓ_{-1} are

$$[c_2 \quad 1 \quad 0].$$

Since p_s is on ℓ_0,

$$p_s = (0 \quad x_2 \quad x_3) \text{ so } \beta_2 = 0,$$

and c_2 is real. So ℓ_{-1} is also real. This case is concluded.

Case (e) p_s is on ℓ_1 and $s\neq 1$, $s\neq 2$.

Now take $i=s-1$, since p_{s-1} is real and is on line ℓ_0. The quadrangle and its dual are now

$$p_0\ p_2\ p_s\ \ p_{s-1}$$

and $\ell_s\ \ell_{s-2}\ \ell_0\ \ell_1$.

All the sides of the quadrilateral are real lines.

Case (f) p_s is on the line p_0p_2, $s\neq 0$, $s\neq 2$.

Note that p_{s-1} is not on ℓ_0, because if it were, then p_s would be on ℓ_1 hence at the intersection of ℓ_1 and p_0p_2, so $p_s = p_2$ which has been excluded. The point p_{s-1} is known to be real, hence, unless p_{s-1} is on the line p_0p_2, we may choose the quadrangle

$$p_0 \; p_1 \; p_s \quad p_{s-1}$$

with dual

$$\ell_s \; \ell_{s-1} \; \ell_0 \; \ell_1$$

and thus settling the case.

The only case left is:

p_s and p_{s-1} are on the line p_0p_2.

Now we choose the quadrangle $p_1 \; p_i \; p_s \; p_{s-1}$ where $p_i \in \ell$, $i \neq 0$ or 1, and p_i is real.

The dual is

$$\ell_{s-1} \; \ell_{s-i} \; \ell_0 \; \ell_1$$

Here $\ell_{s-1} = p_{s-1}p_s$ which is the line p_0p_2, hence ℓ_{s-1} is the line [0 1 0].

So ℓ_s is

$$[0 \quad 1 \quad 0]M^{-1} = [1 \quad 0 \quad -c_2/c_0]$$

But ℓ_s is known to be real, so $c_2/c_0 \in GF(q)$.

The only line to be checked is ℓ_{s-i}. We have for it

$$[1 \quad 0 \quad -c_2/c_0]M^{(i)} = [g \quad f \quad -\frac{c_2}{c_0} g]$$

hence this line is also real.

This completes the proof for all cases. □

(Note: In Chapter 3 this theorem is generalised for higher dimensions.)

Theorem 2.9 is equivalent to stating that the <u>differences of the indices of consecutive real lines are in a cyclic order reverse to the differences of indices of consecutive real points</u>.

Examples of this can be seen in the tables for PG(2,4).

As further illustration, consider lists of real points and lines, calculated by computer for PG(2,9).

Using generating cubic

$$x^3 = \alpha^2 x + \alpha^6$$

over GF(9) where α is a primitive element of GF(9) and is a root of

$$x^2 + x - 1 = 0 \quad \text{over GF(3).}$$

Indices of real points:

0 1 2 3 4 6 17 26 58 63 77 78 80 (mod 91)

Indices of real lines:

0 1 2 3 4 15 17 18 32 37 64 78 89 (mod 91)

Here s=4.

Dual map : $\ell_0 \rightarrow p_4$.

Differences of indices, beginning at p_4 for points and at ℓ_0 for lines:

points	:	2	11	9	32	5	14	1	2	11	1	1	1	1
lines	:	1	1	1	1	11	2	1	14	5	39	9	11	2

2.7 Singer Orbits of Baer-planes

Denote the Singer group acting on the points and lines of $PG(2,q^2)$ by

$$\Xi_{q^2} = \langle \sigma_{q^2} \rangle$$

Let $\overline{B}$ be some Baer-plane in $PG(2,q^2)$. Then for all i, the image

$$\sigma^i_{q^2}(\overline{B})$$

is again a Baer-plane.

The orbit of the Baer-plane $\overline{B}$ under the action of the group Ξ_{q^2}, denoted by $\Xi_{q^2}(\overline{B})$ is the set

$$\{\sigma^i_{q^2}(\overline{B})\},$$

where the elements of the set are distinct.

Since the order of the Singer group is

$$|\Xi_{q^2}| = q^4 + q^2 + 1,$$

$\overline{B}$ can have no more than $q^4 + q^2 + 1$ distinct images under the action of Ξ_{q^2}, in other words the orbit-length of $\overline{B}$ under the action of Ξ_{q^2} is $\leq q^4 + q^2 + 1$.

We investigate conditions under which the length of the orbit is less than $q^4 + q^2 + 1$.

Suppose that for some j and k where

$$0 \leq j < k \leq q^4 + q^2$$

$$\sigma^j(\overline{B}) = \sigma^k(\overline{B}). \qquad (7.1)$$

(Note: here it is understood that the Singer-group is Ξ_{q^2}, so the subscript can be omitted.)

The equality (7.1) means that each side represents the same set of points, differently ordered.

It follows immediately that for all m

$$\sigma^{j+m}(\overline{B}) = \sigma^{k+m}(\overline{B}) \quad \text{and so for } \ell = k-j$$

$$\left.\begin{array}{l} \sigma^{\ell}(\overline{B}) = \overline{B} \\ \text{where} \\ 0 < \ell < q^4 + q^2 + 1 \end{array}\right| \qquad (7.2)$$

Denote by i the <u>least</u> value of ℓ satisfying (7.2). It follows that i is a divisor of $q^4 + q^2 + 1$.

Denote by $\overline{B}_i$ the transform $\sigma^{i}(\overline{B})$. Then by (7.2) $\overline{B}_i = \overline{B}$. So it follows that for all $p_r \in \overline{B}$, $p_{r+i} \in \overline{B}$ and hence the set

$$\{p_{r+ki} | k \text{ integer}\} \text{ is in } \overline{B}.$$

Suppose that the above set has n <u>distinct</u> points. Then

$$p_{r+ni} = p_r \qquad (7.3)$$

It follows that ni is a multiple of $q^4 + q^2 + 1$, and since i divides $q^4 + q^2 + 1$, it follows that

$$ni = q^4 + q^2 + 1 \qquad (7.4)$$

Since (7.3) holds for all points $p_r \in \overline{B}$, it follows that $\overline{B}$ is partitioned into cycles of points, each cycle of length n. Thus n is a divisor of $q^2 + q + 1$, the number of points in $\overline{B}$.

Write

$$n = \frac{q^2 + q + 1}{d}.$$

Then

$$(q^2+q+1)i = d(q^4+q^2+1) = d(q^2+q+1)(q^2-q+1)$$

Hence

$$i = d(q^2-q+1). \tag{7.5}$$

Investigate first the case when $d=1$. Then $n = q^2 + q + 1$ and $i = q^2 - q + 1$.

In this case the transformation σ^i causes a shift of $q^2 - q + 1$ in the Singer index of each of the $q^2 + q + 1$ points of $\overline{B}$. It follows that the indices of the points of $\overline{B}$ are congruent mod(q^2-q+1).

It remains to be shown that such a set of points $\overline{B}$ represents indeed a Baer-plane. This will be stated and proved in the following theorem.

Theorem 2.10 (cf. also [36])

For each Singer ordering of the points of PG$(2,q^2)$ the points which have Singer indices in the same residue class modulo (q^2-q+1), form a Baer-plane of PG$(2,q^2)$. It follows that the points of PG$(2,q^2)$ can be partitioned into $q^2 - q + 1$ disjoint Baer-planes.

Proof

Notation

In the following, points will be simply denoted and referred to by their Singer indices. Correspondingly, elements of the set of congruency classes modulo $q^4 + q^2 + 1$ will be sometimes called "points".

Recall that the Singer indices of the points of any line in PG$(2,q^2)$ form a perfect difference set modulo (q^4+q^2+1). The terms "points of a line" or "elements of a difference set" will be used alternatively.

Choose any line of reference ℓ in PG$(2,q^2)$. Then for any subset S of the points of PG$(2,q^2)$, a subset Δ of the points of the line can be chosen such that each point of S is uniquely represented as a difference of two elements of Δ. If in particular, S is chosen to be the set of points belonging to residue class 0 mod(q^2-q+1) then

$$S = \{k(q^2-q+1)\}$$

and the corresponding subset of differences, Δ has the following property:

for each k mod(q^2+q+1)

$$k(q^2-q+1) = \delta_i - \delta_j \quad (\text{mod } q^4+q+1) \qquad \delta_i,\ \delta_j \in \Delta \tag{7.6}$$

and this representation is unique.

Let $\delta_i \equiv r_i (\text{mod } q^2-q+1)$ for each point $\delta_i \in \ell$.

Then

$$\delta_i = (q^2-q+1)d_i + r_i \ (\text{mod } q^4+q^2+1) \tag{7.7}$$

We then obtain for the points of the subset S, by (7.6)

$$k(q^2-q+1) = (q^2-q+1)(d_i-d_j) + r_i-r_j \ \ \text{mod}(q^4+q^2+1) \tag{7.8}$$

Since $q^4+q^2+1 = (q^2+q+1)(q^2-q+1)$, it follows from (7.8) that

$$\left.\begin{array}{l} r_i - r_j = 0 \mod(q^2-q+1) \\ \text{for each pair } (\delta_i,\delta_j) \text{ satisfying (7.6).} \end{array}\right\} \qquad (7.9)$$

Furthermore, (7.8) can now be simplified to

$$k = d_i - d_j \mod(q^2+q+1) \qquad (7.10)$$

since (q^2-q+1) and (q^2+q+1) are coprime.

The set $\Delta_0 = \{d_i\}$ marks those values of d_i as defined in (7.7) which correspond to the δ_i values in the subset Δ.

Since the representation (7.6) is unique for each point of S, and by (7.9)

$$\delta_i - \delta_j = (q^2-q+1)(d_i-d_j)$$

it follows that (7.10) gives unique representation for each k, where $d_i, d_j \in \Delta_0$.

Thus Δ_0 is a perfect difference set $\mathrm{mod}(q^2+q+1)$ and so

$$|\Delta_0| = |\Delta| = q+1$$

and all elements of Δ are congruent modulo $q^2 - q + 1$.

The line ℓ has q^2+1 points. Those which do not belong to Δ must belong pairwise to different congruency classes (mod q^2-q+1) since their pairwise differences determine points belonging to $PG(2,q^2)\backslash S$. Hence each congruency class $\mathrm{mod}(q^2-q+1)$ is represented by the points of ℓ. Those belonging to Δ, all represent the same class, while each of the remaining points belongs to one of the remaining q^2-q classes.

Suppose that the line of reference ℓ has $q+1$ points belonging to class r (mod q^2-q+1). Thus a shift by r results in a line with q+1 points in the 0 class. There are $(q^4+q^2+1)/(q^2-q+1) = q^2+q+1$ lines in $PG(2,q^2)$ which have q+1 points in the 0 class (mod q^2-q+1). Denote the set of lines with this property by $\mathcal{L}_0$.

Denote the set of points of $PG(2,q^2)$ belonging to the 0 class (mod q^2-q+1) by C_0. The number of points of C_0 is also $q^2 + q + 1$.

The join of any two points of C_0 is a line belonging to $\mathcal{L}_0$, since no other line in $PG(2,q^2)$ has more than one point in the 0 class.

Next it must be shown that the intersection of any two lines of $\mathcal{L}_0$ is a point of C_0.

Let $P \in C_0$. Join P to the remaining $q^2 + q$ points of C_0. Each of these joins is a line of $\mathcal{L}_0$, and each has q points of C_0, other than P. Since $C_0\setminus\{P\}$ has $q^2 + q$ points, it follows that there are exactly $q + 1$ lines of the set $\mathcal{L}_0$ through P, hence through any point of C_0. Let $\ell \in \mathcal{L}_0$. Then through each point of $\ell \cap C_0$, there are q lines of $\mathcal{L}_0$ other than ℓ. This accounts for $q(q+1)$ lines, hence all lines of $\mathcal{L}_0\setminus\ell$. Hence all intersections of ℓ with a line of $\mathcal{L}_0$ belongs to C_0 as claimed.

Thus the points and lines belonging to C_0 and $\mathcal{L}_0$ respectively form a closed configuration of $q^2 + q + 1$ points and lines respectively and hence determine a Baer-plane.

Denote this Baer-plane by $\hat{B}_0$.

A shift σ^k of the points of $\hat{B}_0$, where $k \neq 0$ (mod q^2-q+1) produces another Baer-plane $\hat{B}_k$ with points belonging to class k (mod q^2-q+1). Hence $\hat{B}_k$ is disjoint from $\hat{B}_0$.

Thus we obtain exactly q^2-q+1 Baer-planes, mutually disjoint and covering all the points in $PG(2,q^2)$. This completes the proof. □

Notation

Denote by $S_{\hat{B}}$ the set of Baer-planes

$$\{\hat{B}_0, \hat{B}_1, \ldots, \hat{B}_{q^2-q}\}$$

where $\hat{B}_i$ is the Baer-plane the points of which belong to class $i \pmod{q^2-q+1}$.

Return now to the discussion of the Singer-orbit of a general Baer-plane. Theorem 2.10 establishes that there exists at least one Singer orbit of length less than $q^4 + q^2 + 1$, namely the orbit of any of the Baer-planes belonging to $S_{\hat{B}}$. This orbit is of length $q^2 - q + 1$.

The question arises naturally : are there any other Baer-planes with Singer orbits shorter than $q^4 + q^2 + 1$? The arguments which follow give rise to the conjecture that excepting Baer-planes belonging to the set $S_{\hat{B}}$, all Baer-planes have Singer-orbits of maximal length = $q^4 + q^2 + 1$. However, Theorem 2.11 which summarises the results, leaves the conjecture unproved for certain values of q.

Suppose that $\bar{B}$ is a Baer-plane with an orbit shorter than $q^4 + q^2 + 1$. Then by (7.5) the length of its orbit is

$$i = d(q^2-q+1)$$

where d is a divisor of $q^2 + q + 1$.

Recall now that $\bar{B}$ is partitioned into cycles of length n where

$$ni = q^4 + q^2 + 1 \quad \text{and} \quad nd = q^2 + q + 1.$$

The case $d = 1$, $n = q^2 + q + 1$, $i = q^2 - q + 1$ has been settled, while in the case when $d = q^2 + q + 1$, $n = 1$, $i = q^4 + q^2 + 1$, the orbit is of maximal length.

Hence assume that n is a proper divisor of $q^2 + q + 1$. Since $q^2 + q + 1$ is always odd, n must be odd, thus

$$n \geqslant 3.$$

We distinguish between two cases :

(i) $n > 3$, (ii) $n = 3$.

(i) $\overline{B}$ contains together with some point r, the points $r+i, \ldots, r+(n-1)i$, where

$$i \equiv 0 \pmod{q^2-q+1} \text{ by } (7.5).$$

Thus $\overline{B}$ contains n points belonging to the same congruency class (mod q^2-q+1) and thus shares n points with one of the planes of the set $S_{\hat{B}}$. By assumption

$$n \geqslant 4.$$

Assuming that no three of the common points are collinear, it follows that they determine a unique Baer-plane, and so $\overline{B}$ coincides with one of the Baer-planes of the set $S_{\hat{B}}$.

If, on the other hand, the set of n points contains 3 collinear points, then $\overline{B}$ and the Baer-plane of the set $S_{\hat{B}}$ share at least q+1 points of a line.

However, $n \neq q + 1$ and $n \neq q + 2$ since

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

and thus neither q+1 nor q+2 can be divisors of $q^2 + q + 1$.

Hence $\overline{B}$ and the other Baer-planes share a whole slot of q+1 points and at least two more points and so they coincide. Thus case (i) leads to contradiction.

(ii) This case could only occur if 3 divides $q^2 + q + 1$, that is

$$q \equiv 1 (\mathrm{mod}\ 3).$$

Then by assumption $\overline{B}$ shares 3 points with each Baer-plane of a subset of S_B, and we may assume that exactly 3 points of $\overline{B}$ belong to each subplane of that set, for the alternative has been covered by the arguments used in (i). So the points of $\overline{B}$ belong to $(q^2+q+1)/3$ distinct congruency classes $\mathrm{mod}(q^2-q+1)$.

Without loss of generality, we may assume that 0 belongs to $\overline{B}$, for an appropriate Singer shift can achieve this situation.

Denote

$$\eta = \frac{q^4 + q^2 + 1}{3} = (q^2-q+1) \frac{q^2 + q + 1}{3} .$$

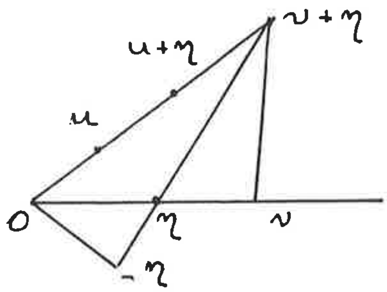
Then $\hat{B}_0 \cap \overline{B}$ consists of the three points:

$$0,\ \eta,\ 2\eta = -\eta.$$

For convenience, we may now index the lines of $PG(2,q^2)$ by beginning with the join of 0 and η, and marking it by ℓ_0. Hence the line ℓ_η goes through η and 2η (or η, $-\eta$), while $\ell_{-\eta}$ is the join of $-\eta$ and 0.

Furthermore, if j, $j+\eta$, $j-\eta$ is another point-triple of $\overline{B}$, shared with B_j, the lines $(j,j+\eta)$, $(j+\eta,j-\eta)$ and $(j-\eta,j)$ have Singer indices j, $j+\eta$, $j-\eta$ respectively, so by this indexing the same set of indices determines the points and lines of $\overline{B}$.

The line ℓ_0 has q+1 points of $\overline{B}$, 0 and η being two of them. Let v be one point of $\overline{B} \cap \ell_0$ different from 0 and η. Let ℓ_u be the line joining 0 and v+η. Then ℓ_u belongs to $\overline{B}$, where u belongs to a congruency class (mod q^2-q+1) different from 0 or v, since it represents a line joining two points of different classes, (i.e. two points lying in different planes of the set $S_{\hat{B}}$, so the line u contains two points u and u+η different from 0 and v+η, and belonging to $\overline{B}$.



We can now list successively some points and lines of $\overline{B}$, beginning with the lines 0, η, $-\eta$, v, v+η, v-η, u, u+η, u-η. On each line we can list 5 points in terms of η, u and v, since the line 0 has the points 0-u, v+η-u in addition to 0, η, and v, and the corresponding points on these other lines are obtained by Singer shifts. Tabulating these, we have:

Line	Points				
0	0	η	v	-u	v-u+η
η	η	-η	v+η	-u+η	v-u-η
-η	-η	0	v-η	-u-η	v-u
v	v	v+η	2v	v-u	2v-u+η
v+η	v+η	v-η	2v+η	v-u+η	2v-u-η
v-η	v-η	v	2v-η	v-u-η	2v-u
u	u	u+η	v+u	0	v+η
u+η	u+η	u-η	v+u+η	η	v-η
u-η	u-η	u	v+u-η	-η	v

Not all points listed above are known to belong to $\overline{B}$. However, v-u is the intersection of the lines v and $-\eta$, hence it belongs to $\overline{B}$, together with u-v+n and u-v-n and these points are in a class different from n and v, being intersections of lines belonging to different classes. A further listing then gives

Line	Points				
v-u	v-u	v-u+n	2v-u	v-2u	2v-2u+n
v-u+n	v-u+n	v-u-n	2v-u+n	v-2u+n	2v-2u-n
v-u-n	v-u-n	v-u	2v-u-n	v-2u-n	2v-2u

It can be seen that 2v-u is the intersection of the lines v-u and v-n, so the points 2v-u, 2v-u+n, 2v-u-n and the corresponding lines give new triples.

We continue by <u>induction</u> and show that the points (and lines) k(v-u) and (k+1)v-ku are in $\overline{B}$:

Assume that kv-ku and kv-(k-1)u belong to $\overline{B}$. Since the line 0 contains v, and v-u+n,the line kv-ku contains (k+1)v-ku, and the line kv-(k-1)u-n also contains (k+1)v-ku. Hence the triple defined by (k+1)v-ku is in $\overline{B}$. A shift from -u on the line 0 to the line (k+1)v-ku shows that (k+1)v-(k+1)u is on the line (k+1)v-ku, while a shift of kv-ku-n from v-u+n on the line 0 shows that (k+1)v-(k+1)u is also on the line kv-ku-n and so is the intersection of two lines of $\overline{B}$. This completes the induction.

For completing the proof, we restrict ourselves to the case when $q^2 - q + 1$ is a prime number. (This is true when $q \equiv 1 \pmod 3$ and q = 4, 7, 13, 16, 25 but not true when q = 19, 31.) In this case the set k(u-v), where u = 0, 1, .., $q^2 - q$ gives a full set of the residue classes mod (q^2-q+1). So $\overline{B}$ has points in <u>all</u> the Baer-planes belonging to $S_{\hat{B}}$. This contradicts the original assumption. This argument does not work in itself when $q^2 - q + 1$ is not a prime. To close the gap, it is necessary to prove some further conjectures. It is easy to show that u-v takes at least (q+3)/2 different values when choosing different points for v on the line 0 where the points u-v+η are on the line 0. So it is a natural conjecture that at least one of these points is coprime to $q^2 - q + 1$. Having failed however to prove this conjecture, the theorem can be stated only in a restricted form.

Theorem 2.11

The orbit of a Baer-plane under the action of the Singer group Ξ_{q^2} is of length $d(q^2-q+1)$, where d is a divisor of q^2+q+1. If the Singer indices of the points of $\overline{B}$ belong to the same residue class mod(q^2-q+1), then d=1. Otherwise, $d = q^2 + q + 1$, hence the orbit length is $q^4 + q^2 + 1$, provided that $q \not\equiv 1 \pmod 3$, or $q \equiv 1 \pmod 3$, but $q^2 - q + 1$ is a prime number.

In the cases when the theorem is valid the Baer-planes may be divided into classes of planes belonging to the same orbit. The number of orbits of length $q^4 + q^2 +1$ (if $q \not\equiv 1$ mod 3, or $q \equiv 1 \pmod 3$) but $q^2 - q + 1$ is a prime is

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

where

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

is the total number of Baer-planes of Π_{q^2}.

Then $N' = (q^4+q^2-1)$, and so the total number of Singer orbits is

$$q^4 + q^2 = q(q^3+1).$$

2.8 On Collineations Fixing One Baer-plane

Denote again by B_0 the real Baer-plane in $PG(2,q^2)$. This time a Singer ordering is given to B_0, by applying Singer's theorem to $PG(2,q)$, the coefficients of the generating cubic and entries of the Singer matrix being elements of $GF(q)$.

Denote the Singer group by

$$\Xi_q = \langle \sigma_q \rangle.$$

The points of B_0 are successively indexed from 0 to $q^2 + q$ (mod q^2+q+1). The components of the vectors in B_0 are elements of $GF(q)$. The projective plane $PG(2,q^2)$ is constructed as an extension of B_0.

Denote by

$$\alpha_1, \alpha_2, \ldots, \alpha_{q^2-q}$$

the elements of $GF(q^2)\setminus GF(q)$.

Theorem 2.12 [24]

Let p, $\overline{p}$ be any two fixed distinct points of the Baer-plane B_0. Consider the set

$$S_{p\overline{p}} = \{p + \alpha_i\overline{p} \mid i=1,2,..,q^2-q\}$$

and let Ξ_q act on each of its points. Then

(i) The orbit of each point corresponding to an element of $S_{p\overline{p}}$ is a Baer-plane in $PG(2,q^2)$. Denote the orbit of $p + \alpha_i\overline{p}$ by B_i.

(ii) For $i\neq j$ the Baer-planes B_i, B_j are disjoint.

(iii) $B_0, B_1, \ldots, B_{q^2-q}$ partition $PG(2,q^2)$.

Proof

(i) Denote by θ the transformation

$$\theta : \sigma^{k} p \to \sigma^{k}(p+\alpha_i\overline{p}) = \sigma^{k} p + \alpha_i \sigma^{k}\overline{p} \qquad (8.1)$$

(The subscript q is omitted from σ_q, since all this section refers to $\Xi_q = \langle\sigma_q\rangle$.)

Then <u>θ is a collineation</u>, which maps the points of B_0 to those of $\Xi(p+\alpha_i\overline{p})$, where α_i is fixed, $\alpha_i \in GF(q^2)\setminus GF(q)$.

To show that θ is indeed a collineation, consider an arbitrary line ℓ_r in B_0. The real points on this line are

$$\sigma^{k_0}p,\ \sigma^{k_1}p,\ \ldots,\ \sigma^{k_q}p,$$

represented as Singer images of p. Suppose that the Singer shift from p to $\overline{p}$ is s, then the points

$$\sigma^{k_0}\overline{p},\ \sigma^{k_1}\overline{p},\ \ldots,\ \sigma^{k_q}\overline{p}$$

are the real points of the line ℓ_{r+s}.

It follows that the points $\sigma^{k_j}p + \alpha_i\sigma^{k_j}\overline{p}(k = 0,1,..,q)$ are collinear. Hence (8.1) represents a collineation, and so the image of B_0 is again a Baer-plane, which has no point in common with B_0. Denote the image by B_i.

(ii) Assume that $\alpha_i \neq \alpha_j$. Suppose that some point P belongs to both Baer-planes B_i and B_j. Then σ takes P again to a common point and this is repeated through the whole cycle of Ξ. Hence B_i and B_j coincide. Since each of these Baer-planes intersects the real line $p\overline{p}$ in one point only, it follows that $\alpha_i = \alpha_j$, which is a contradiction.

(iii) To show that each point in $PG(2,q^2)$ belongs to one of the Baer-planes $B_0, B_1, \ldots, B_{q^2-q}$, it suffices to count the number of points in the union of these Baer-planes. Since they are disjoint, and each contains q^2+q+1 points, the total number of points in the union in $(q^2-q+1)(q^2+q+1) = q^4+q^2+1$, which is the number of points in $PG(2,q^2)$. □

Notation

Denote by S_B the set $\{B_i \mid i=0,1,..,q^2-q\}$. (This is distinct from the notation used for the partitioning set $\hat{S}_B$ in the previous section.)

Remark

The set S_B is defined by the action of Ξ_q on the set

$$\{p+\alpha_i\bar{p} \mid i=1,..,q^2-q\}$$

where p, $\bar{p}$ are arbitrarily chosen, distinct fixed points of B_0. However, the set S_B is independent of the choice of p and $\bar{p}$.

To see this, think first of the Baer-planes generated by choosing

$$\sigma^k p \quad \text{and} \quad \sigma^k \bar{p}$$

instead of p and $\bar{p}$.

This only gives different starting points to the orbits of the original points given by $\{p+\alpha_i\bar{p}\}$, but the orbits, that is the Baer-planes, remain the same.

Next consider the case when p and $\bar{p}$ are replaced by p' and $\bar{p}'$ in B_0 and on the same line as p and $\bar{p}$.

Then the sets

$$\{p' + \alpha_i \overline{p}' \,|\, i=1,2,\ldots,q^2-q\}$$

and

$$\{p + \alpha_i \overline{p} \,|\, i=1,2,\ldots,q^2-q\}$$

are identical, since both represent all the points of the extension of ℓ into $PG(2,q^2)$. The Baer-planes themselves are permuted, but the set remains unchanged.

Finally, given any pair of distinct points p'' and $\overline{p}''$ in B_0, the line determined by these two is the k^{th} Singer image of the line $\ell = p\overline{p}$, for some k. So p'' and $\overline{p}''$ are Singer images of some pair p' and $\overline{p}'$ on ℓ and so determine the same set S_B as p' and $\overline{p}'$, hence the (possibly permuted) set determined by p and $\overline{p}$.

Thus the set S_B depends only on the Singer ordering of B_0.

In Section 2.4 it was found that there is a simple relation between the number of Baer-planes disjoint from a fixed Baer-plane and $\Lambda_0 = |PGL(3,q)|$, the order of the collineation group fixing a Baer-plane. In the following this relation will be interpreted.

Let $\rho \in PGL(3,q)$, hence ρ is a collineation fixing the Baer-plane B_0. Then ρ permutes the points and lines of B_0, hence permutes the extended lines, lines of $PG(2,q^2)$, (belonging to B_0). In general, ρ leaves only B_0 fixed, while it transforms the Baer-planes of the set S_B into other Baer-planes, still mutually disjoint and disjoint from B_0.

Two questions arise:

(i) which collineations in $PG(3,q)$ (if any) fix each $B_i \in S_B$,

(ii) which collineations (if any) fix the set S_B, while permuting amongst themselves the Baer-planes belonging to S_B?

Collineations of type (i) can be found immediately: all transformations belonging to $\Xi_q = \langle\sigma_q\rangle$ cause a mere shift of the points and lines of B_0, thus shifting points on the extensions of the lines into positions within their own Singer orbits, thus leaving the Baer-planes $B_i \in S_B$ unaltered.

Conversely, suppose that B_0 is given a Singer-ordering and θ is a transformation which leaves B_0 and all Baer-planes belonging to S_B unaltered.

Let $B_i \in S_B$. Without loss of generality it can be represented as

$$\{\sigma_q^j(p_0 + \alpha_i p_1)\}$$

$$j \in \{0,1,..,q^2+q (\text{mod } q^2+q+1)\}$$

and

$$\alpha_i \in GF(q^2)\backslash GF(q).$$

The action of θ on a general point

$$p_j + \alpha_i p_{j+1} \in B_i$$

is

$$\theta : p_j + \alpha_i p_{j+1} \to p_k + \alpha_i p_{k+1}$$

also

$$\theta : p_{j+1} + \alpha_i p_{j+2} \to p_\ell + \alpha_i p_{\ell+1}$$

where $k, \ell \in \{0,1,..,q^2+q \ (\text{mod}(q^2+q+1))$, since the images of the two successive points of B_i are still in B_i.

Then $\theta(p_j) = p_k$ and $\theta(p_{j+1}) = p_{k+1} = p_\ell$, hence

$$\ell = k + 1 \ (\text{mod } q^2+q+1).$$

Thus if $j = 0$ and $\theta(p_0) = p_m$ then $\theta(p_1) = p_{m+1}$ and generally $\theta(p_j) = p_{m+j}$. So $\theta \in \Xi_q$.

Hence the only homographies of B_0 which leave $B_i \in S_B$ unaltered (for all i in the range) are those which belong to the Singer group Ξ_q.

Since any homography can be represented as a product of a transformation belonging to Ξ_q and one which leaves a point fixed, it suffices now to find homographies which leave one point of B_0, say p_0, fixed and leave the set S_B unaltered, while permuting the Baer-planes within the set.

Refer again to a given Singer-ordering of B_0, having generating cubic

$$x^3 = d_2x^2 + d_1x + d_0 \tag{D}$$

over GF(q), with associated Singer matrix M.

Since the cubic (D) is irreducible over GF(q), its three roots belong to $GF(q^3)\backslash GF(q)$ and are the conjugate elements:

$$\alpha,\ \alpha^q,\ \alpha^{q^2} = (\alpha^q)^{-1}.$$

The Singer ordering of B_0 is achieved by mapping the successive powers of one of the roots of D onto the vectors representing the points of B_0. Any one of the three roots of (D) can be used equivalently.

Fix for the moment one of the roots α of D and regard the vectors representing the points

$$p_0,\ p_q,\ p_{2q},\ \cdots$$

These are associated with

$$\alpha^0,\ \alpha^q,\ (\alpha^q)^2\ \ldots$$

Since α^q is also a root of (D), the Singer transformation taking α^{jq} to $\alpha^{(j+1)q}$ for any j (mod q^2+q+1), has the same Singer matrix M with respect to new fundamental points associated with α^0, α^q, α^{2q}.

A similar situation holds for the transformation

$$\alpha^{jq^2} \to \alpha^{(j+1)q^2} \text{ for all } j \pmod{q^2+q+1}.$$

Consider now the following permutations of the points of B_0:

$$\left.\begin{array}{l} \tau : p_j \to p_{qj} \\ \tau^2 = \tau^{-1} : p_j \to p_{q^2j} \end{array}\right| j=0,1,..,q^2+q \pmod{q^2+q+1} \qquad (8.2)$$

(Note that p_0 is fixed by τ.)

It follows from the considerations above that the group $\langle\tau\rangle$ of order 3, is a subgroup of the homography-group of PG(2,q), since lines $p_j, p_{j+1}, \ldots$ go to lines $p_{jq}, p_{(j+1)q}, \ldots$ for all j (mod q^2+q+1).

Let T and $T^2 = T^{-1}$ be the matrices associated with τ and τ^2. Then the matrices TMT^{-1} and $T^2MT^{-2} = T^{-1}MT$ are the transformation-matrices which take p_{jq} to $p_{(j+1)q}$ and p_{jq^2} to $p_{(j+1)q^2}$ respectively for all j (mod q^2q+1).

Conversely, suppose that a homography ρ in PG(2,q) with the associated matrix R is such that RMR^{-1} takes p_{jr} to $p_{(j+1)r}$ for some fixed r and all j (mod q^2+q+1).

The matrix RMR^{-1} has the same characteristic equation and roots as as M, hence the only values possible for r are 1, q, q^2.

We have come now to

Lemma 2.13

Let the points of PG(2,q) be ordered by the Singer group

$\Xi = \langle\sigma\rangle$.

Let ρ be a homography in PG(2,q) such that for some fixed r and all j (mod q^2+q+1)

$$\rho\sigma\rho^{-1}(p_{jr}) = p_{(j+1)r} \qquad (8.3)$$

Then

(i) $r = 1$ or q or q^2.

(ii) If in addition ρ leaves p_0 fixed, then ρ is the identity, or the transformation τ or τ^2 respectively, where τ is defined in (8.2).

Proof of (ii).

Let $r = q$. Then from (8.3) $\rho\sigma\rho^{-1}(p_{jq}) = p_{(j+1)q}$ for all j (mod q^2+q+1). Let $j = 0$. Then $\rho p_0 = p_0$, hence $\rho^{-1}p_0 = p_0$ and so

$$\rho\ \sigma\ p_0 = p_q$$

or

$$\rho\ \ p_1 = p_q.$$

By induction on j we obtain $\rho\ p_j = p_{jq}$ as claimed, so $\rho = \tau$. The other cases go similarly. When $r = 1$, ρ is the identity, and when $r = q^2$, $\rho = \tau^2$. □

Let $B_i \in S_B$, hence B_i is a Baer-plane generated by the action of the group Ξ_q on a point on the extension of $\ell_0 = p_0p_1$ into PG(2,q^2). Let this point be

$$p^{(i)} = p_0 + \alpha_i p_1$$

where $\alpha_i \in GF(q^2)\backslash GF(q)$.

Investigate next the action of τ (defined by (8.2) on B_i.

A general point of B_i is

$$\sigma^k(p^{(i)}) = p_k + \alpha_i p_{k+1}.$$

Hence by (8.2)

$$\tau(\sigma^k p^{(i)}) = p_{kq} + \alpha_i p_{kq+q} \tag{8.4}$$

while

$$\tau(p^{(i)}) = p_0 + \alpha_i p_q \tag{8.5}$$

Thus τ takes $p^{(i)}$ to a point on the line

$$p_0 p_q = \ell_s = p_s p_{s+1}$$

(Note: possibly $\ell_s = \ell_0$.)

Since by (8.5), $\tau(p^{(i)})$ is on ℓ_s, we may write

$$\tau(p^{(i)}) = p_s + \alpha_j p_{s+1} \tag{8.6}$$

Here $\alpha_j \in GF(q^2)\backslash GF(q)$, since by (8.5) $\tau(p^{(i)})$ is not in B_0.

Furthermore, $\alpha_j \neq \alpha_i$, otherwise

$$p_s + \alpha_i p_{s+1} = p_0 + \alpha_i p_q,$$

comparing real parts, it follows that $p_s = p_0$, so $p_{s+1} = p_1$.
This leads to contradiction, since $p_1 \neq p_q$.

Comparing (8.4) and (8.5) it is seen that $\tau(\sigma^k(p^{(i)}))$ is obtained from $\tau(p^{(i)})$ by a Singer-shift of kq, while by (8.6), $\tau(p^{(i)})$ represents a Singer shift of s from

$$p^{(j)} = p_0 + \alpha_j p_1.$$

Hence for all k (mod (q^2+q+1)) $\tau(\sigma^k(p^{(i)})$ represents a kq+s Singer-shift from $p^{(j)}$.

This means that the transformation τ turns the Singer orbit of $p^{(i)}$ into the Singer orbit of $p^{(j)}$, hence it permutes the Baer-planes B_i and B_j, leaving the set S_B unaltered.

Conversely, suppose that a homography ρ of B_0 which leaves p_0 fixed, fixes also the set S_B (while possibly permuting the Baer-planes belonging to S_B).

Denote again $p^{(i)} = p_0 + \alpha_i p_1$ $(\alpha_i \in GF(q^2)\backslash GF(q))$. Then

$$\rho\ \sigma^k(p^{(i)}) = \rho(p_k + \alpha_i p_{k+1}).$$

Let $\rho(p_k) = p_u$ and $\rho(p_{k+1}) = p_v$. Then

$$\rho\ \sigma^k(p^{(i)}) = p_u + \alpha_i p_v. \qquad (8.7)$$

Similarly $\rho\ \sigma^{k+1}(p^{(i)}) = \rho(p_{k+1} + \alpha_i p_{k+2})$. Let $\rho p_{k+2} = p_w$, then

$$\rho\ \sigma^{k+1}(p^{(i)}) = p_v + \alpha_i p_w \qquad (8.8)$$

Since by assumption $\rho\ \sigma^k(p^{(i)})$ lies in the same Singer orbit of some point on the extension of ℓ_0 into $PG(2,q^2)$ for all values of k (mod (q^2+q+1)), it follows from (8.7) and (8.8) that

$$v-u = w-v \qquad \text{(for all } k\text{)}.$$

Thus the Singer indices of the ρ-transforms of the points of B_0 form an arithmetic progression.

It follows from Lemma 2.13 that $r = 1$, q or q^2 (referring to the notations in Lemma 2.13) and $\rho = 1$, τ or τ^2 (as defined in (8.2)).

The above results can now be summarised in the following.

Theorem 2.14

Let B_0 be the real Baer-plane in $PG(2,q^2)$ and $\Xi_q = \langle\sigma_q\rangle$ the Singer group acting on it. This ordering induces a partitioning of $PG(2,q^2)\backslash B_0$ into a set of disjoint Baer-planes, denoted by S_B.

The set of homographies acting on B_0 and leaving S_B invariant is a subgroup of $PGL(3,q)$. Each element of this subgroup, denoted by L_B is the product of an element of the group $\langle\tau\rangle$ and a Singer shift:

$$L_B = \{\sigma_q^j \tau^i \mid i=0,1,2,\ j=0,1,..,q^2+q\}$$

where

$$\sigma_q : p_k \to p_{k+1} \text{ and } \tau : p_k \to p_{qk} \text{ for all } k \pmod{q^2+q+1}.$$

The order of L_B is

$$|L_B| = \Lambda_B = 3(q^2+q+1).$$

Corollary

The number of ways in which $PG(2,q^2)$ can be partitioned into disjoint Baer-planes, one of them being fixed (e.g. taking B_0 for the fixed Baer-plane) is

$$N_B = \frac{\Lambda_0}{\Lambda_B},$$

where $\Lambda_0 = |PGL(3,q)|$.

Hence

$$N_B = \frac{q^3(q^3-1)(q^2-1)}{3(q^2+q+1)} = \frac{q^3(q-1)^2(q+1)}{3}. \qquad \square$$

Compare this result with (4.9) in Section 4. This formula gives the number of Baer-planes N_0, in $PG(2,q^2)$ disjoint from a fixed Baer-plane (e.g. B_0). The comparison yields the result

$$N_0 = (q^2-q)N_B \qquad (8.9)$$

Each set S_B, determined by a fixed Singer-ordering contains q^2-q Baer-planes. Since N_B gives the number of partitionings of $PG(2,q^2)\setminus B_0$ into disjoint Baer-planes, the relation (8.9) leads to the conclusion that every Baer-plane, disjoint from B_0 belongs to exactly one partition of $PG(2,q^2)/B_0$ into disjoint Baer-planes.

This may now be stated in a more general form:

Theorem 2.15

(i) If B_1 and B_2 are two disjoint Baer-planes in $PG(2,q^2)$, there exists exactly one set of q^2-q+1 mutually disjoint Baer-planes, including the given Baer-planes B_1 and B_2, which partitions $PG(2,q^2)$.

(ii) The number of ways in which $PG(2,q^2)$ can be partitioned into disjoint Baer-planes is

$$P = \frac{q^6(q^4-1)(q^2-1)}{3}$$

Proof

(i) Transform B_1 into B_0.

(ii) Let N be the total number of Baer-planes in PG(2,q^2), and N_0 the number of Baer-planes disjoint from a fixed Baer-subplane. Then there are

$$\frac{N\ N_0}{2}$$

ways in which a pair of disjoint Baer-planes may be chosen. By (i) such a pair determines uniquely a partition of PG(2,q^2).

On the other hand, each partition contains q^2-q+1 Baer-planes, hence the number of ways a pair may be chosen out of these is

$$\frac{(q^2-q+1)(q^2-q)}{2}.$$

So the nubmer of possible partitions is

$$P = \frac{N\ N_0}{(q^2-q+1)(q^2-q)}.$$

Setting for N and N_0 the formulae given in (1.2) and (4.8) of this chapter, we obtain

$$P = \frac{q^3(q^3+1)(q^2+1)q^4(q-1)^3(q+1)}{3(q^2-q+1)(q^2-q)}$$

which can be simplified to

$$P = \frac{q^6(q^4-1)(q^2-1)}{3}$$

as claimed. □

2.9 The "Singer wreath" of Baer-planes

(Note: In [28] the name given to Singer wreaths was "Singer Merry Go Round".)

In Section 2.2 it has been proved that if two Baer-planes share q+1 points on a line ℓ, then they share also q+1 lines going through the same point, which may or may not be a point of ℓ. Conversely : if two Baer-planes share q+1 lines intersecting in the same point P, then they share also q+1 points of some line, which may or may not contain P.

We shall say in this situation that the two Baer-planes are <u>strongly intersecting</u>.

Configurations of strongly intersecting Baer-planes have been found before. Each pair of Baer-planes belonging to a homology- or elation-cluster is strongly intersecting. These configurations are generated by perspectivity groups.

It is found that a Singer group acting on $PG(2,q^2)$ generates another interesting configuration of strongly intersecting Baer-planes. This configuration will be called a

<u>Singer wreath</u>

and is described in the following theorem.

<u>Theorem 2.16</u>

The orbit of B_0 under the action of the Singer group $\Xi_{q^2} = \langle\sigma_{q^2}\rangle$ contains a set of q(q+1) Baer-planes strongly intersecting B_0 which in <u>two different ways</u> fall into <u>q+1 classes</u>, such that

(a) in each class there are q Baer-planes which share q+1 points of the same line;

(b) in each class there are q Baer-planes which share q+1 lines going through the same point.

<u>Example</u>

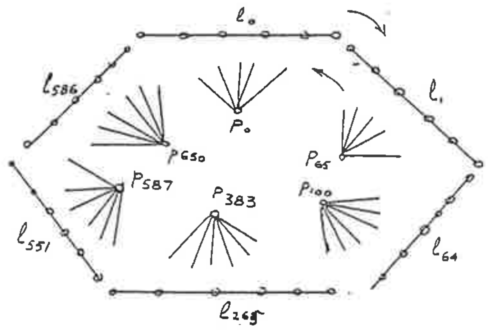
Before proving the theorem, we illustrate it with a diagrammatic sketch of results obtained by a computer survey of PG(2,25).

In this case the generating cubic of the Singer group is

$$x^3 + x + \gamma = 0$$

where γ is a root of $x^2 - 2x - 2 = 0$ over GF(5).

In the computations illustrated by the diagram, 30 Baer-planes were found, such that



(a) they all intersect strongly B_0, in all the real points of one of the following 6 lines:

$$\ell_0,\ \ell_1,\ \ell_{64},\ \ell_{265},\ \ell_{551},\ \ell_{586} \qquad (\pounds^*)$$

and in all the real lines through one of the following 6 points:

$$P_0,\ P_{65},\ P_{100},\ P_{383},\ P_{587},\ P_{650} \qquad (P^*)$$

(b) the 30 planes fall into 6 classes. Each class has 5 Baer-planes which share all the real points of one of the lines in $\pounds^*$.

(c) the 30 Baer-planes fall into 6 classes, 5 Baer-planes in each class, which share all the real lines through one of the points of the set P^*.

Some further observations can be made in this particular case:

The Singer indices of the points belonging to $B_0 \cap \ell_0$ in PG(2,25) under the given Singer ordering are

0, 1, 64, 265, 551, 586,

while the lines belonging to the set $\pounds^*$ have the same indices.

The general case : It was seen before (cf. Section 2.6) that if p_i is a real point on line ℓ_0, then p_{i+1} is also a real point, hence the line

$$\ell_i = p_i p_{i+1}$$

is indeed a real line.

Moreover, if $p_i \in \ell_0 \cap B_0$, then all the real points on ℓ_i are i^{th} Singer images of the real points on ℓ_0.

For consider the point $p_j \in \ell_0 \cap B_0$.

Then $p_j = (0 \quad f \quad g) = fp_1 + g\, p_0$, hence

$$\sigma^i p_j = p_{i+j} = f\, p_{i+1} + g\, p_i, \tag{9.1}$$

where $f, g \in GF(q)$.

So the real points on ℓ_i are

$$p_i, p_{i+1}, \ldots, p_{i+j}, \ldots \qquad (p_j \in \ell_0 \cap B_0).$$

Remark:

(i) It follows that if $\ell_i, \ell_j \in \mathcal{L}^*$, which is the set of lines $p_i\, p_{i+1}$ $(p_i \in \ell_0 \cap B_0)$, then their intersection is the point p_{i+j}

(ii) if $p_i \in \ell_0 \cap B_0$, then p_{2i} is a real point.

Note: In (9.1) the Singer transformation is treated as a linear transformation on a sum. This is justified within the range considered, but not generally. The Singer group $\langle\sigma_q\rangle$ is identified with a cyclic group of linear transformations in GL(3,q) only for σ_q^i where $0 < i < q^2 + q + 1$ (cf. proof of Singer's Theorem in the introductory chapter). The Singer group referred to in (9.1) is $<\sigma_{q^2}>$, hence here the permitted range is $0 \leq i < q^4+q^2+1$. The transformation σ^i takes p_0 and p_1 to p_i and p_{i+1} respectively. where $i+1 < q^4+q^2+1$. This is so, because i represents a point on the line $\ell_0 = p_0p_1$, so $p_{q^4+q^2} = p_{-1}$ cannot be on ℓ_0, otherwise p_0, p_1, p_2 are collinear (contradiction).

Proof of Theorem 2.16

Denote by B_k the transform $\sigma^k_{q^2}(B_0)$. Consider the set

$$W = \{B_{j-i} \mid j \neq i,\ p_i,\ p_j \in \ell_0 \cap B_0\} \qquad (9.2)$$

The set W contains (q+1)q distinct Baer-planes, since there are (q+1)q ordered pairs formed out of the q+1 indices of the real points on ℓ_0. Since these indices form a perfect difference set, the differences j-i are distinct. It is claimed now that the Baer-planes of the set W form a Singer-wreath having the properties stated.

Consider the set of lines

$$\pounds^* = \{\ell_i = p_ip_{i+1} \mid p_i \in \ell_0 \cap B_0\} \qquad (9.3)$$

and for each $\ell_i \in \pounds^*$, consider the Singer-dual $\overline{\ell_i} = p_{s-i}$, where s is defined as in Section 2.6. By the Singer duality theorem (Theorem 2.9) for each $\ell_i \in \pounds^*$, $p_{s-i} \in B_0$.

Define $P^* = \{p_{s-i} \mid \ell_i \in \pounds^*\}$ (9.4)

It was shown in the preliminaries that the transformation $\sigma^j_{q^2}$ takes the real slot on ℓ_0 to the real slot on ℓ_j, where $\ell_j \in \pounds^*$. Since $\sigma^{j-i}_{q^2}(\ell_i) = \ell_j$ ($\ell_i \in \pounds^*$), and the real slot on ℓ_i is the $\sigma^i_{q^2}$ image of the real slot on ℓ_0, it follows that a (j-i)-shift takes the real slot on ℓ_i to the real slot on ℓ_j.

Dually, the bunch of the real lines through p_s, belonging to B_0, is taken by $\sigma_{q^2}^{-i}$ to the bunch through p^{s-i}; the lines through p_s being duals of the points on ℓ_0, their $\sigma_{q^2}^{-i}$ transforms are duals of the $\sigma_{q^2}^{i}$ transforms of the points on ℓ_0, and since it was shown that the $\sigma_{q^2}^{i}$ transform of the real slot on ℓ_0, is again real, so is its dual, the $\sigma_{q^2}^{-i}$ transform of the real bunch through p_s. It follows that if p_{s-i}, $p_{s-j} \varepsilon P^*$, then $\sigma_{q^2}^{j-i}$ takes the real bunch through p_{s-j} to the real bunch through p_{s-i}.

Let W_i and W^j be subsets of W, such that

$$W_i = \{B_{j-i} | j \neq i,\ p_i,\ p_j \ \varepsilon\ \ell_0 \cap B_0 \text{ and } i \text{ is fixed}\}$$

$$W^j = \{B_{j-i} | j \neq i,\ p_i,\ p_j \ \varepsilon\ \ell_0 \cap B_0 \text{ and } j \text{ is fixed}\}$$

Then all the Baer-planes belonging to W^j share the slot ℓ_j B_0 and all the Baer-planes belonging to W^j share the bunch of real lines through p_{s-i}.

In the first case, $B_{j-i} = \sigma_{q^2}^{j-i} B_0$, and the line ℓ_j belongs to it, since $\ell_j = \sigma^{j-i} \ell_i$, where $\ell_i \ \varepsilon\ B_0$. Moreover, it follows from the preceding that B_{j-i} shares with B_0 a slot of q+1 points on the line ℓ_j.

(Note: the line ℓ_j belongs to all Baer-planes B_{j-k}, if $\ell_k \ \varepsilon\ B_0$, but only if ℓ_j, $\ell_k \ \varepsilon\ \mathcal{L}^*$, can it be ascertained that the slot $\ell_j \cap B_{j-k}$ is real.)

Similarly, if $B_{j-i} \ \varepsilon\ W_i$, then $p_{s-i} = \sigma^{j-i} p_{s-j}$ where $p_{s-j} \ \varepsilon\ B_0$.

Hence $p_{s-i} \ \varepsilon\ B_{j-i}$.

Since p_{s-i}, $p_{s-j} \ \varepsilon\ P^*$, it follows also that the bunch through p_{s-i} determined by B_0, belongs to B_{j-i}.

There are q Baer-planes belonging to each set W_i, W^j, and each of the sets W_i and W^j can be chosen in q+1 ways by fixing i or j respectively.

This completes the proof. □

Remark

The two sets $\mathcal{L}^*$, P^* belonging to B_0 determine $(q+1)^2$ clusters, by choosing the slot from one of the lines belonging to $\mathcal{L}^*$, together with a bunch determined by a point belonging to P^*. Each of the q(q+1) Baer-planes belonging to W belongs to one of the clusters together with B_0, but

(i) no Baer-planes of W belongs to a (p_{s-i}, ℓ_i)-cluster (that is a cluster determined by a line of $\mathcal{L}^*$ and its dual).

(ii) no two Baer-planes of W belong to the same (p_{s-i}, ℓ_j)-cluster ($p_{s-i} \in P^*$, $\ell_j \in \mathcal{L}^*$).

This follows from the fact that the Baer-plane W_{j-i} belongs to the (p_{s-i}, ℓ_j)-cluster determined by the bunch and slot in B_0, determined by the point p_{s-i} and the line ℓ_j respectively. Here $i \neq j$ and each Baer plane in W is determined by a different (i,j)-pair ($i \neq j$).

Theorem 2.16 proves that Singer-wreaths of Baer-planes exist in all $PG(2,q^2)$, but at this stage the number of such structures remains an open problem.

To add a further example where Singer-wreaths are produced by calculations not needing computers, tables 1(a) and 1(b) are completed with tables 2(a) and 2(b) which exhibit lists of Baer-planes produced by the action of the respective Singer-cycles acting on the real Baer-plane.

Referring to tables 1(a) and 1(b) for finding the sets $\pounds^*$ and P^*, we have the following data:

I. <u>Tables 1(a) and 2(a)</u>

Here $c_2 = c_1 = 1$, $c_3 = \alpha$ (primitive element of GF(4)).

So $p_s = (0 \quad 0 \quad 1) = p_0$. Hence $s = 0$.

The real points on ℓ_0 are p_0, p_1, p_{14}

Hence $\pounds^* = \{\ell_0, \ell_1, \ell_{14}\}$

Duals : $P^* = \{p_0, p_{20}, p_7\}$

The values for i and j are 0, 1, 14, with differences :

1, 14, 13, 20, 7, 8.

Hence $W = \{B_1, B_{14}, B_{13}, B_{20}, B_7, B_8\}$

Classes:

(a) Sharing q+1 = 3 points of a line

$W^1 = \{B_1, B_8\}$ Common line: ℓ_1 with points: p_1 p_2 p_{15}

$W^{14} = \{B_{13}, B_{14}\}$ Common line: ℓ_{14} with points: p_7 p_{14} p_{15}

$W^0 = \{B_7, B_{20}\}$ Common line: ℓ_0 with points: p_0 p_1 p_{14}

(b) Sharing 3 lines through a point

$W_0 = \{B_1, B_{14}\}$ Common point: p_0 with lines ℓ_0 ℓ_7 ℓ_{20}

$W_1 = \{B_{13}, B_{20}\}$ Common point: p_{20} with lines ℓ_6 ℓ_{19} ℓ_{20}

$W_{14} = \{B_7, B_8\}$ Common point: p_7 with lines ℓ_6 ℓ_7 ℓ_{14}

II. Tables 1(b) and 2(b)

Here $c_2 = c_1 = c_0 = \alpha$

$p_s = (1 \;\; 1 \;\; 1) = p_3$, hence $s = 3$.

Real points on ℓ_0: p_0, p_1, p_8.

So $\mathcal{L}^* = \{\ell_0, \ell_1, \ell_8\}$

Duals: $P^* = \{p_3, p_2, p_{16}\}$.

Differences of set $\{0, 1, 8\}$ are 1, 8, 7, 20, 13, 14.

$W = \{B_1, B_8, B_7, B_{20}, B_{13}, B_{14}\}$

Classes:

(a) $W^1 = \{B_1, B_{14}\}$ Common line: ℓ_1 with points: p_1 p_2 p_9

$W^8 = \{B_7, B_8\}$ Common line: ℓ_8 with points: p_8 p_9 p_{16}

$W^0 = \{B_{13}, B_{20}\}$ Common line: ℓ_0 with points: p_0 p_1 p_8

(b) $W_0 = \{B_1, B_8\}$ Common point: p_3 with lines: ℓ_2 ℓ_3 ℓ_{16}

$W_1 = \{B_7, B_{20}\}$ Common point: p_2 with lines: ℓ_1 ℓ_2 ℓ_{15}

$W_8 = \{B_{13}, B_{14}\}$ Common point: p_{16} with lines: ℓ_8 ℓ_{15} ℓ_{16}

All these results agree with Tables 2(a) and 2(b).

Table 2(a)

Generating cubic : $x^3 = x^2 + x + \alpha$

Plane	Indices of Points p_i							Indices of lines ℓ_i						
B_0	0	1	2	7	14	15	20	0	1	6	7	14	19	20
B_1	1	2	3	8	15	16	0	1	2	7	8	15	20	0
B_2	2	3	4	9	16	17	1	2	3	8	9	16	0	1
B_3	3	4	5	10	17	18	2	3	4	9	10	17	1	2
B_4	4	5	6	11	18	19	3	4	5	10	11	18	2	3
B_5	5	6	7	12	19	20	4	5	6	11	12	19	3	4
B_6	6	7	8	13	20	0	5	6	7	12	13	20	4	5
B_7	7	8	9	14	0	1	6	7	8	13	14	0	5	6
B_8	8	9	10	15	1	2	7	8	9	14	15	1	6	7
B_9	9	10	11	16	2	3	8	9	10	15	16	2	7	8
B_{10}	10	11	12	17	3	4	9	10	11	16	17	3	8	9
B_{11}	11	12	13	18	4	5	10	11	12	17	18	4	9	10
B_{12}	12	13	14	19	5	6	11	12	13	18	19	5	10	11
B_{13}	13	14	15	20	6	7	12	13	14	19	20	6	11	12
B_{14}	14	15	16	0	7	8	13	14	15	20	0	7	12	13
B_{15}	15	16	17	1	8	9	14	15	16	0	1	8	13	14
B_{16}	16	17	18	2	9	10	15	16	17	1	2	9	14	15
B_{17}	17	18	19	3	10	11	16	17	18	2	3	10	15	16
B_{18}	18	19	20	4	11	12	17	18	19	3	4	11	16	17
B_{19}	19	20	0	5	12	13	18	19	20	4	5	12	17	18
B_{20}	20	0	1	6	13	14	19	20	0	5	6	13	18	19

Table 2(b)

Generating cubic : $x^3 = \alpha x^2 + \alpha x + \alpha$

Plane	Indices of Points p_i							Indices of lines ℓ_i						
B_0	0	1	2	3	8	9	16	0	1	2	3	8	15	16
B_1	1	2	3	4	9	10	17	1	2	3	4	9	16	17
B_2	2	3	4	5	10	11	18	2	3	4	5	10	17	18
B_3	3	4	5	6	11	12	19	3	4	5	6	11	18	19
B_4	4	5	6	7	12	13	20	4	5	6	7	12	19	20
B_5	5	6	7	8	13	14	0	5	6	7	8	13	20	0
B_6	6	7	8	9	14	15	1	6	7	8	9	14	0	1
B_7	7	8	9	10	15	16	2	7	8	9	10	15	1	2
B_8	8	9	10	11	16	17	3	8	9	10	11	16	2	3
B_9	9	10	11	12	17	18	4	9	10	11	12	17	3	4
B_{10}	10	11	12	13	18	19	5	10	11	12	13	18	4	5
B_{11}	11	12	13	14	19	20	6	11	12	13	14	19	5	6
B_{12}	12	13	14	15	20	0	7	12	13	14	15	20	6	7
B_{13}	13	14	15	16	0	1	8	13	14	15	16	0	7	8
B_{14}	14	15	16	17	1	2	9	14	15	16	17	1	8	9
B_{15}	15	16	17	18	2	3	10	15	16	17	18	2	9	10
B_{16}	16	17	18	19	3	4	11	16	17	18	19	3	10	11
B_{17}	17	18	19	20	4	5	12	17	18	19	20	4	11	12
B_{18}	18	19	20	0	5	6	13	18	19	20	0	5	12	13
B_{19}	19	20	0	1	6	7	14	19	20	0	1	6	13	14
B_{20}	20	0	1	2	7	8	15	20	0	1	2	7	14	15

CHAPTER THREE

ON THE BAER STRUCTURE OF HIGHER DIMENSIONAL SPACES OF SQUARE ORDER

3.1 Introduction

The intersection properties of Baer-planes studied in Chapter 2 can be generalised for higher dimensions. The introductory chapter deals with the basics of the projective space PG(n,q), of dimension n and order q. In this chapter the space of reference will be

$$S = PG(n,q^2)$$

of dimension $n \geqslant 2$ and of an order which is an even power of some prime number. The points of $PG(n,q^2)$ are (n+1)-tuples of elements belonging to $GF(q^2)$. The subset of points, the coordinates of which are elements of PG(q) (possibly multiplied by some common non-zero element of $PG(q^2)$), determine the subgeometry PG(n,q). As in the two-dimensional case, this subgeometry will be called the real Baer-space B_0, (or more precisely in some instances, the real Baer n-space).

A change of coordinates leads to a different subset of S, with a geometry isomorphic to that of B_0. The coordinates of all the points of S are determined by the choice of n+2 fundamental points:

$$(1\ 0\ ..\ 0),\ (0\ 1\ ..\ 0),\ ..\ (0\ 0\ ..\ 1),\ (1\ 1\ ..\ 1).$$

These serve also as fundamental points of B_0. If any other set of n+2 points of which no n+1 are linearly dependent, is chosen for fundamental points, then (in general) another Baer-space will result. The group of homographies of $PG(n,q^2)$, that is the group

$PGL(n+1,q^2)$, which will be denoted here shortly by Γ, is transitive on ordered sets of n+2 points, no n+1 linearly dependent, as already discussed in the introductory chapter. Thus Γ generates a set of homographical images of B_0, which will be referred to as Baer-spaces (Baer n-spaces) of S and generally denoted by B, with some distinguishing subscripts.

An argument identical to the one used in the two dimensional case (Section 2.1) shows that field-automorphisms of $GF(q^2)$ transform the real Baer-space to itself, and in particular the transformation $\alpha \to \alpha^q$ fixes all the points of B_0 and determines an involution of $PG(n,q^2)$. Since, by the fundamental theorem of projective geometry, all collineations of $PG(n,q^2)$ can be represented as products of a homography and a field automorphism, it follows that all the Baer-spaces of $PG(n,q^2)$ can be represented as homographical images of B_0.

To determine the number of Baer-spaces in S, we proceed similarly to the two-dimensional case. Denoting by Γ the group of homographies of S, and by Γ_0 the subgroup of Γ fixing B_0, we have

$$|\Gamma| = q^{n(n+1)} \prod_{i=2}^{n+1} (q^{2i}-1)$$

while

$$|\Gamma_0| = q^{n(n+1)/2} \prod_{i=2}^{n+1} (q^{i}-1)$$

(by (5.3) in the introductory chapter).

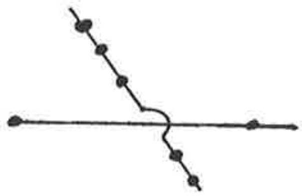
Thus the number of Baer-spaces in S is

$$N = \frac{|\Gamma|}{|\Gamma_0|} = q^{(n+1)n/2} \prod_{i=2}^{n+1} (q^{i}+1) \qquad (1.1)$$

3.2 Computation results in three dimensions

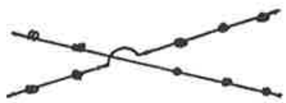
As a preliminary investigation, the computer survey used earlier for finite Galois planes was extended to three dimensions. For $q=2,3,4,5$, Baer 3-spaces of $PG(3,q^2)$ were generated and thus intersections surveyed. The computations yielded, as expected, all the configurations of the two dimensional case listed in Section (2.2), and in addition the following configurations appeared:

(1) $q+3$ points, $q+1$ on one line; the line joining the remaining two points skew to the first line;

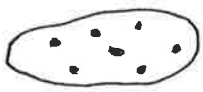


(2) 4 points, not coplanar;

(3) $2q+2$ points of a pair of skew lines;



(4) $q^2 + q + 1$ points of a plane



(5) $q^2 + q + 2$ points, $q^2 + q + 1$ in a plane.

The information given by these results is not as complete as in the two dimensional case, as in this case a full description has to give account of points, lines and planes in a configuration. However, further analysis of the computer survey also showed that the number of planes common to two Baer-spaces is equal to the number of common points. (The exact meaning of the term "common plane" is given in later sections.)

The conjectures which could be made on the basis of these results pointed the way to the general investigations in the n dimensional case, forming the subject of the following sections.

3.3 Basic properties of n-dimensional Baer-spaces

Notations and definitions

Denote shortly by S the space of reference $PG(n,q^2)$, that is a projective space of dimension n and order q^2. It is necessary to distinguish between various types of projective spaces embedded in S.

(i) A subspace, usually denoted by S_k, is a projective space included in the space of reference, having the same order, but smaller dimension. For S_k, we have the dimension k where $0 \leq k < n$ and each S_k is isomorphic to $PG(k,q^2)$.

(ii) A Baer-space, as defined in the Introduction has the same dimension, but different order, namely q instead of q^2. The Baer-space B is a projective space isomorphic to $PG(n,q)$.

(iii) A subspace S_k of S belongs to the Baer-space B if $S_k \cap B$ is a k dimensional subspace of B. Thus a line $S_1 \subset S$ belongs to B if $S_1 \cap B$ has q+1 points. A plane $S_2 \subset S$ belonging to B has $q^2 + q + 1$ points in $S_2 \cap B$, and so on.

Since B is a projective space, it suffices to check that there are k+1 linearly independent points belonging to $S_k \cap B$ for ascertaining that S_k belongs to B.

(iv) Definition

A Baer k-space of S where $0 \leq k \leq n$ is a projective space embedded in S and isomorphic to $PG(k,q)$. Wherever there is no possible ambiguity, a Baer n-space will be called simply a Baer-space of S.

Note: A Baer k-space of S can be thought of alternatively as a k-subspace of some Baer-space, or as a Baer-space of some subspace S_k of S.

The enumeration of projective subspaces

Theorem (1.1) gives the number of k-dimensional subspaces of the n-dimensional linear space LG(n,q) over GF(q) as the Gaussian coefficient:

$$\left[{n \atop k}\right]_q = \frac{(q^n-1)(q^{n-1}-1) \ldots (q^{n-k+1}-1)}{(q-1)(q^2-1) \ldots (q^k-1)}.$$

This formula was already quoted in the introductory chapter, together with its modification for projective spaces. It was found that the number of k-dimensional subspaces of the n-dimensional projective space is equal to the number of k+1-dimensional subspaces of an n+1-dimensional linear space, hence is given by (cf. (4.5) in the Introductory Chapter)

$$\left[{n+1 \atop k+1}\right]_q. \tag{3.1}$$

In particular, the number of points in PG(n,q) is

$$\left[{n+1 \atop 1}\right]_q = \frac{q^{n+1}-1}{q-1} \quad \text{as well known;}$$

the number of lines of PG(n,q) is

$$\left[{n+1 \atop 2}\right]_q = \frac{(q^{n+1}-1)(q^n-1)}{(q-1)(q^2-1)} \tag{3.2}$$

the number of hyperplanes, i.e. subspaces of dimension (n-1) is

$$\left[{n+1 \atop n}\right]_q = \left[{n+1 \atop 1}\right]_q = \frac{q^{n+1}-1}{q-1} \tag{3.3}$$

and so on. These formulae will be frequently used in the following.

The Baer-plane B is known to be dense in $PG(2,q^2)$; each point of $PG(2,q^2)$ lies on a line of B, (on exactly one, if the point is external) and each line of $PG(2,q^2)$ intersects B in 1 or q+1 points. The following two theorems treat the n-dimensional case.

Theorem 3.1

Let P be a point of S, external to the Baer-space B. Then P lies on exactly one line belonging to B.

Proof

P lies on at most one line of B, since two lines belonging to B intersect at a point of B. Hence we must show that through each external point P there exists a line belonging to B.

Equivalently, we show that S has no other points than the ones on the lines belonging to B. We use (3.2) for the number of lines and we count the points external to B on these, since the external points form disjoint sets. Since on each line there are $(q^2+1)-(q+1) = q^2 - q$ external points, the total number of external points on the lines is

$$(q^2-q)\frac{(q^{n+1}-q)(q^n-1)}{(q-1)(q^2-1)} = \frac{q(q^{n+1}-1)(q^n-1)}{q^2-1} \qquad (3.4)$$

On the other hand, the total number of points of S external to B is

$$\begin{bmatrix} n+1 \\ 1 \end{bmatrix}_{q^2} - \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_{q} = \frac{q^{2n+2}-1}{q^2-1} - \frac{q^{n+1}-1}{q-1} \qquad (3.5)$$

Simplification shows that the results in (3.4) and (3.5) are the same.

This completes the proof. □

In the two dimensional case it is also true that each line of the projective plane $PG(2,q^2)$ has at least one point common with any of its Baer-planes. If the line does not belong to the Baer-plane, then it has exactly 1 point in common with the Baer-plane, for a line having 2 points in common with the Baer-plane has $q+1$ points common with it and belongs to it.

In dimensions higher than 2, a line does not necessarily intersect a Baer-space B. In fact we can show that through each point external to B, the <u>number of lines skew to B</u> is

$$L_s = q^3\frac{(q^{n-1}-1)(q^{n-2}-1)}{q^2-1} > 0 \text{ when } n > 2 \qquad (3.6)$$

To prove this, we must find first the number of lines through an external point P intersecting B. Of these, exactly one contains $q+1$ points of B and so the remaining points of B number

$$\frac{q^{n+1}-1}{q-1} - (q+1) = q^2\frac{q^{n-1}-1}{q-1},$$

and each of these, joined to P gives a line not belonging to B, hence containing only one point of B. So the number of lines through P, not skew to B is

$$q^2\frac{q^{n-1}-1}{q-1} + 1.$$

The total number of lines through a point can be found by writing down the numbers of point-line incidences in $PG(n,q^2)$.

Since there are by (3.2), $\left[{n+1 \atop 2}\right]_{q^2}$ lines each with q^2+1 points, the number of incidences is

$$\frac{(q^{2(n+1)}-1)(q^{2n}-1)}{(q^2-1)(q^4-1)}(q^2+1)$$

while on the other hand the $\left[{n+1 \atop 1}\right]_{q^2}$ points in $PG(n,q^2)$ give

$$\ell_p \frac{q^{2(n+1)}-1}{q^2-1}$$

incidences, where ℓ_p is the number of lines through a point. Comparing the two expressions, we obtain

$$\ell_p = \frac{(q^{2(n+1)}-1)(q^{2n}-1)}{(q^2-1)(q^4-1)}(q^2+1) \Big/ \frac{q^{2(n+1)}-1}{q^2-1}$$

$$= \frac{q^{2n}-1}{q^2-1}$$

The result is the same as the number of points in a hyperplane.

Hence L_s is given by the difference

$$\frac{q^{2n}-1}{q^2-1} - (q^2\frac{q^{n-1}-1}{q-1} + 1).$$

Simplifying this expression, result (3.6) is obtained.

In the two dimensional situation the lines of S can be regarded as hyperplanes in $PG(2,q^2)$. Hence it is appropriate to look at the intersections of the hyperplanes of S and B. Here the situation is summarised in the following theorem.

Theorem 3.2

The intersection of a hyperplane of S with a Baer-space B is either a Baer (n-1)-space (a hyperplane of B), or a Baer (n-2)-space.

(Note: This theorem is allied to a result in [9]: If B is a Baer s-space, then an S_{n-t} subspace of S, intersects it in a Baer k-space, where $k \geq S-2t$, a result not seen by the author before publishing this in [29].)

Proof

Any point-pair in the intersection of B and H (the hyperplane of S) determines a line in each H and B, hence H ∩ B is a subspace of B.

It is readily seen that H ∩ B is never empty. Using the dimensional equation for two subspaces S_a and S_b:

$$d(S_a) + d(S_b) = d(S_a \cap S_b) + d(S_a + S_b),$$

we have for the intersection of a line and a hyperplane in S either the line itself, or a point. Hence for each of the lines belonging to B there is at least one intersection point with H. Since the number of points in H is $(q^{2n}-1)/(q^2-1)$ and the number of lines belonging to B is $((q^{n+1}-1)(q^n-1))/((q-1)(q^2-1))$, and the difference

$$\frac{(q^{n+1}-1)(q^n-1)}{(q-1)(q^2-1)} - \frac{q^{2n}-1}{q^2-1} = \frac{q(q^n-1)(q^{n-1}-1)}{(q-1)(q^2-1)} > 0$$

it follows that some points of H are common to at least two lines of B hence belong to B.

In order to determine the possible dimensions of the H ∩ B spaces, we use again the incidence-counting technique, counting incidences of points of H with lines of B.

Let x be the number of points and y the number of lines of H ∩ B.

Then $(q^{2n}-1)/(q^2-1) - x$ points of H do not belong to B and so by Theorem 3.1 each of these points counts for just one incidence.

Similarly $((q^{n+1}-1)(q^n-1))/((q-1)(q^2-1)) - y$ lines of B do not belong to H and so these lines intersect H just in one point each.

For the internal points and lines, (numbering x and y respectively) we have $(q^n-1)/(q-1)$ lines of B on each point, and $q^2 + 1$ points of H on each of the y lines.

So the incidence equation becomes

$$x\frac{q^n-1}{q-1} + \left(\frac{q^{2n}-1}{q^2-1} - x\right) = y(q^2+1) + \left(\frac{(q^{n+1}-1)(q^n-1)}{(q-1)(q^2-1)} - y\right) \qquad (3.7)$$

After some simplification we have

$$x\frac{q^{n-1}-1}{q-1} - qy = \frac{(q^n-1)(q^{n-1}-1)}{(q-1)(q^2-1)} \qquad (3.8)$$

$H \cap B$ is a proper subspace of B, so its dimension d is less than n.

Substitute

$$x = \frac{q^{d+1}-1}{q-1} \quad \text{and} \quad y = \frac{(q^{d+1}-1)(q^d-1)}{(q-1)(q^2-1)}$$

into (3.8) and simplify again to get

$$(q+1)(q^{d+1}-1)(q^{n-1}-1) - (q^{d+1}-1)(q^{d+1}-q) = (q^n-1)(q^{n-1}-1) \qquad (3.9)$$

Let $t = q^{d+1}$. Then (3.8) simplifies to the quadratic

$$t^2 - t(q^n + q^{n-1}) + q^{2n-1} = 0 \qquad (3.10)$$

whence $t = q^n$ or q^{n-1}, that is

$$d = n-1 \quad \text{or} \quad n-2.$$

These are the only possible values for the dimension of $H \cap B$.

Thus if a hyperplane of S does not belong to the Baer-space B, then it shares with it an (n-2)-dimensional subspace of B. In this sense Theorem (3.2) may be interpreted as the dual of Theorem (3.1). □

In the case of two dimensions, Theorem (3.2) says that if a line (a "hyperplane" in $PG(2,q^2)$) does not belong to a Baer-plane, then it intersects it in a 0-dimensional space : a point.

3.4 Intersections of Baer-spaces

The following theorem generalises the result known for Baer-planes and verifies the conjecture based on the computational results in three dimensions.

Note: "Sharing" a subspace S_k between two Baer-spaces B_1 and B_2 does not necessarily mean that $B_1 \cap S_k = B_2 \cap S_k$. It only means that S_k belongs to both B_1 and B_2, that is : both $B_1 \cap S_k$ and $B_2 \cap S_k$ are k-dimensional subspaces of B_1 and B_2 respectively, which may or may not coincide pointwise.

Theorem 3.3

The number of points of intersection of two Baer-spaces of S is equal to the number of hyperplanes shared by them.

Proof

Let B_1 and B_2 be the two Baer-spaces considered and let the number of the points common to them be r where $r \geq 0$.

Denote by h_i the number of hyperplanes belonging to B_1 which share i points with B_2, $h_i \geq 0$. Then we have the following relations:

$$\sum_i h_i = \frac{q^{n+1}-1}{q-1} \tag{4.1}$$

$$\sum_i i\, h_i = r\frac{q^n-1}{q-1} \tag{4.2}$$

where the first relation arises from counting all the hyperplanes of B_1, while the second one counts the incidences of points of $B_1 \cap B_2$ with the hyperplanes of B_1, noting that through each point of B_1 there are $(q^n-1)/(q-1)$ hyperplanes of B_1, (the same number as there are points in a hyperplane, following from the symmetry relation between the number of points and number of hyperplanes in a projective space).

Next count the incidences of the points of $B_2 \backslash B_1$ and the hyperplanes of B_1. By theorem 3.2 these hyperplanes intersect B_2 in an n-1 dimensional or n-2 dimensional subspace of B_2. Assume that out of the set of h_i hyperplanes, defined as above, x_i intersect B_2 in one of its hyperplanes, whence $h_i - x_i$ intersect it in an n-2 dimensional subspace. Thus the number of incidences of this class of hyperplanes of B_1 with $B_2 \backslash B_1$ is

$$x_i\left(\frac{q^n-1}{q-1} - i\right) + (h_i - x_i)\left(\frac{q^{n-1}-1}{q-1} - i\right) = I_i \tag{4.3}$$

Since we are interested in subspaces of dimension n-1 through points external to B_1, fix a point P, not in B_1, and denote the number of hyperplanes through P and belonging to B_1 by h_p. All these hyperplanes intersect in ℓ_p which is the unique line of B_1 through P, because any line of B_1 intersects any hyperplane of B_1 in at least one point and since by assumption ℓ_p also goes through P, it is a line of any particular hyperplane of the set considered. Thus the number of hyperplanes considered is the same as the number of hyperplanes through ℓ_p, a line of B_1, hence h_p is the same for all points external to B_1. Since h_p is given by the number of hyperplanes through a line it may be calculated by the incidence-relation of lines and hyperplanes of B_1, where the number of lines of B_1 is $\left[{n+1 \atop 2}\right]_q$, number of hyperplanes is $\left[{n+1 \atop n}\right]_q$ and the number of lines in a hyperplane is $\left[{n \atop 2}\right]_q$, hence

$$h_p\left[{n+1 \atop 2}\right]_q = \left[{n \atop 2}\right]_q\left[{n+1 \atop n}\right]_q \qquad (4.4)$$

From (4.4) we have

$$h_p = \frac{q^{n-1}-1}{q-1} = \left[{n-1 \atop 1}\right]_q \qquad (4.5)$$

Thus the number of incidences of points of $B_2\backslash B_1$ with the hyperplanes of B_1 is

$$\sum_{P\varepsilon B_2\backslash B_1} h_p = \sum_i I_i,$$

where I_i is expressed in (4.3). Using this together with (4.5), we obtain the required incidence equation:

$$\frac{q^{n-1}-1}{q-1}\left(\frac{q^{n+1}-1}{q-1} - r\right) = \sum_i \left(x_i\left(\frac{q^n-1}{q-1} - i\right) + (h_i-x_i)\left(\frac{q^{n-1}-1}{q-1} - i\right)\right) \qquad (4.6)$$

The right hand side of (4.6) can be written as

$$\left(\frac{q^n-1}{q-1} - \frac{q^{n-1}-1}{q-1}\right)\sum_i x_i - \sum_i h_i\, i + \frac{q^{n-1}-1}{q-1}\sum_i h_i,$$

where $\sum_i x_i = x$ is the number of hyperplanes shared by B_1 and B_2.

By using (4.1) and (4.2), equation (4.6) becomes:

$$\frac{q^{n-1}-1}{q-1}\left(\frac{q^{n+1}-1}{q-1} - r\right) = xq^{n-1} - r\frac{q^{n}-1}{q-1} + \frac{q^{n-1}-1}{q-1}\,\frac{q^{n+1}-1}{q-1},$$

so

$$r\left(\frac{q^{n}-1}{q-1} - \frac{q^{n-1}-1}{q-1}\right) = x\,q^{n-1}$$

whence $r = x$ as claimed. □

Corollary

If two Baer spaces are disjoint (pointwise), there is no hyperplane (of S) belonging to both.

Theorem 3.3 does not say anything about the nature of the intersection configurations. The two dimensional case and the three dimensional computer findings show that in general, the intersections of two Baer-spaces are not Baer k-spaces ($0 \leq k < n$). Intersection structures and restrictions on the possible numbers of intersection points of two Baer-spaces is the subject of the following theorems. The first of these is direct extension of the two dimensional result.

Theorem 3.4

Let P and Q be points common to the Baer-spaces B_1 and B_2. Let $\ell = PQ$. Then

$$(B_1 \cap \ell) \cap (B_2 \cap \ell) = \{P,Q\}$$

or

$$B_1 \cap \ell = B_2 \cap \ell.$$

In other words this theorem means that if two Baer-spaces have three points of a line common, then they share q+1 points, (called earlier a slot).

Proof

As for the two dimensional case (Theorem 2.3), changing appropriately the fundamental points to n+1-tuples and the 3×3 homography matrix to an $(n+1) \times (n+1)$ matrix.

Corollary

A Baer k_1-space and a Baer k_2-space share 0, 1, 2, or q+1 points of any given line.

Proof

Denote the two Baer k-spaces by $B_1^{(k1)}$ and $B_2^{(k2)}$ to indicate their dimensions. Two Baer n-spaces B_1 and B_2 can be chosen such that

$$B_1^{(k1)} \subseteq B_1 \quad \text{and } B_2^{(k2)} \subseteq B_2.$$

Let P and Q be points common to $B_1^{(k1)}$ and $B_2^{(k2)}$. The line $\ell = PQ$ then belongs to $B_1^{(k1)}$, hence to B_1, also to $B_2^{(k2)}$, hence to B_2.

By Theorem (3.4), either

(i) $\quad \ell \setminus \{P_1,P_2\}$ and $B_1 \cap B_2$ are disjoint, or

(ii) $\quad \ell \cap B_1 = \ell \cap B_2$.

In case (i), $\ell\setminus\{P_1,P_2\}$ and $B_1^{(k1)} \cap B_2^{(k2)}$ are disjoint, since

$$B_1^{(k1)} \cap B_2^{(k2)} \subseteq B_1 \cap B_2.$$

In case (ii), we observe that

$$\ell \cap B_1^{(k1)} \subseteq \ell \cap B_1$$

also

$$|\ell \cap B_1(k1)| = |\ell \cap B_1| = q+1$$

hence

$$\ell \cap B_1(k1) = \ell \cap B_1.$$

Similarly $\ell \cap B_2(k2) = \ell \cap B_2$.

Since $\ell \cap B_1 = \ell \cap B_2$ it follows that $\ell \cap B_1(k1) = \ell \cap B_2(k2)$ as claimed.

□

3.5 Baer complexes

In this section the nature of the set of points which can form an intersection of two Baer-spaces is investigated.

Definition

A component of $B_1 \cap B_2$ is a Baer k-space such that

(1) all its points belong to $B_1 \cap B_2$,

(2) it is maximal in the sense that it is not contained in a Baer k'-space (k' > k), which is also included with all its points in $B_1 \cap B_2$.

(A component can be an isolated point.)

Definition

A subspace S_k (that is a k-dimensional subspace of S) is said to belong to $B_1 \cap B_2$ if

(1) S_k belongs to B_1 and belongs to B_2 (that is $S_k \cap B_1$ and $S_k \cap B_2$ are of dimension k),

(2) if $S_k \cap B_1 = S_k \cap B_2$.

Definition

An extended component of $B_1 \cap B_2$ is a subspace S_k (of dimension k) of S, which contains a Baer k-space, a component of $B_1 \cap B_2$.

Notes

(1) A Baer k-space extends uniquely into a subspace S_k of S, hence a component of $B_1 \cap B_2$ determines uniquely an associated extended component.

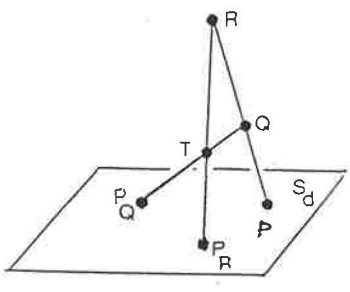
(2) A subspace S_k is an extended component of $B_1 \cap B_2$, if and only if it belongs to $B_1 \cap B_2$ and is not contained in a higher dimensional subspace of S which also belongs to $B_1 \cap B_2$.

(3) If two subspaces of a Baer-space B are skew, then so are their extensions into S, since independent basis vectors of the extensions may be selected out of the vectors belonging to the subspaces of the Baer-space of reference. It follows that if two spaces S_1 and S_2 are known to intersect and each belongs to the Baer-space B, then $S_1 \cap B$ and $S_2 \cap B$ are intersecting spaces.

Lemma 3.5

Let S_d be a d-dimensional subspace of S belonging to $B_1 \cap B_2$, the intersection of the Baer-planes B_1 and B_2. Let ℓ be a line intersecting S_d in P, and containing two points: Q, R distinct from P, in $B_1 \cap B_2$. Then the d+1-dimensional subspace S_{d+1}, spanned by S_d and ℓ belongs to $B_1 \cap B_2$.

Proof



Since S_d belongs to $B_1 \cap B_2$, the intersection $\overline{S}_d = S_d \cap (B_1 \cap B_2)$ is a d-dimensional projective space of order q. It can be regarded as a subspace of say B_1. Since $Q,R \in B_1 \cap B_2$, the line $\ell = QR$ is also in B_1. Thus the space

$\overline{S}_{d+1} = \overline{S}_d + \ell$ is a d+1-dimensional subspace of B_1. Its extension into S is the space $S_{d+1} = \ell + S_d$. It must be shown now that the space $\overline{S}_{d+1}$ is contained in $B_1 \cap B_2$.

Let T be a point in $\overline{S}_{d+1} \backslash (\{Q,R\} \cup \overline{S}_d)$. We consider first the case when T lies on ℓ. Note (3) above implies that $P = \ell \cap S_d$ is in $\overline{S}_d$, hence in $B_1 \cap B_2$. So the line ℓ has 3 points P, Q, R in $B_1 \cap B_2$, hence the slot $\ell \cap \overline{S}_{d+1}$ is in $B_1 \cap B_2$. Assume next that T is not on ℓ. Let P_Q, P_R be the intersections of QT and RT respectively with $\overline{S}_d$. Then the lines QP_Q and RP_R belong to B_2 as well as to B_1, so their intersection T is in $B_1 \cap B_2$. Hence $\overline{S}_{d+1}$ is <u>included</u> in $B_1 \cap B_2$ and so the subspace of S, S_{d+1} <u>belongs</u> to $B_1 \cap B_2$.

□

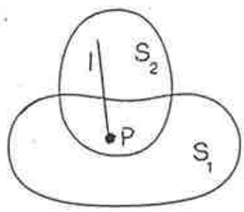
<u>Corollary</u>

If the subspace S_d belongs to $B_1 \cap B_2$ and intersects a line which contains two points of $B_1 \cap B_2$, then S_d is not an extended component of $B_1 \cap B_2$.

<u>Lemma 3.6</u>

If two subspaces, S_1 and S_2 belong to $B_1 \cap B_2$, and $S_1 \cap S_2 \neq \phi$, S_1 or S_2, then each is contained in a higher dimensional subspace of S, belonging to $B_1 \cap B_2$.

<u>Proof</u>



Let the dimensions of S_1, S_2 be d_1 and d_2 respectively. Suppose the point P is in $S_1 \cap S_2$. Let ℓ be a line through P in S_2. Then by Lemma 3.5 the d_1+1 dimensional space in S, spanned by S_1 and ℓ belongs to $B_1 \cap B_2$. Similarly S_2 is a subspace of some d_2+1 dimensional subspace of S, belonging to $B_1 \cap B_2$.

□

Corollary

If S_1 and S_2 are extended components of $B_1 \cap B_2$, then they are skew to each other. It follows that the components of $B_1 \cap B_2$ are mutually skew.

Proof

Suppose that S_1 and S_2 intersect (properly). Then by Lemma 3.6 they are subspaces of higher dimensional subspaces belonging to $B_1 \cap B_2$. Thus S_1 and S_2 cannot be extended components of $B_1 \cap B_2$. □

Lemma 3.7

If S_1 and S_2 are extended components of $B_1 \cap B_2$, then the space spanned by S_1 and S_2 does not contain any point of $B_1 \cap B_2$ other than those in S_1 and S_2.

Proof

Let d_1 and d_2 be the dimensions of S_1 and S_2 respectively. Since by the corollary of Lemma 3.6, S_1 and S_2 are skew, it follows from the dimensional (Grassman) equation that the dimension of $S_1 + S_2 = S_3$ is

$$d_1 + d_2 + 1.$$

Suppose that there exists a point P in S_3 such that

$$P \in B_1 \cap B_2, \text{ but } P \notin S_1 \cup S_2.$$

Let $\overline{S}_1$ and $\overline{S}_2$ be subspaces spanned by S_1 and P, and S_2 and P respectively. Their dimensions are d_1+1, and d_2+1. Comparing these with the dimension of S_3, it follows from the dimensional equation that $\overline{S}_1$ and $\overline{S}_2$ intersect in a line ℓ. It follows again from the dimensional equation applied to $\overline{S}_1$, S_1 and ℓ that ℓ

intersects S_1 in a point Q. Similarly ℓ intersects S_2 in R. The points Q and R are distinct from P, since P is not in S_1 or S_2. Thus ℓ contains three points P, Q, R of $B_1 \cap B_2$ and so by Lemma 3.5, $S_1+\ell$ belongs to $B_1 \cap B_2$, hence S_1 is not an extended component of $B_1 \cap B_2$. The same applies to S_2. This contracdiction concludes the proof. □

Lemma 3.8

The space $\overline{S}$ spanned in S by t components of $B_1 \cap B_2$ contains no point of $B_1 \cap B_2$ other than those in the components. The dimension of $\overline{S}$ is

$$d_1 + d_2 + \dots + d_t + t-1$$

where $d_1, d_2, \dots, d_t$ are the dimensions of the components of $B_1 \cap B_2$.

Proof

The case for two components is settled by Lemma 3.7. We proceed by induction, assuming that the proposition is valid for t components: $\ell_1, \dots, \ell_t$ of dimensions $d_1, \dots, d_t$ respectively. Let the $(t+1)^{th}$ component be C_{t+1}, with dimension d_{t+1}.

Denote by S_t the space spanned by $C_1, C_2, \dots, C_t$ and by S_{t+1} the space spanned by $C_1, C_2, \dots, C_t, C_{t+1}$.

By the inductive hypothesis the dimension of S_t is

$$d' = d_1 + d_2 + \dots + d_t + t-1 \qquad (5.1)$$

By the Corollary of Lemma (3.6), C_{t+1} is skew to $C_1, \dots, C_t$, hence it is skew to the space S_t. Hence the dimension of S_{t+1} is

$$d = d' + d_{t+1} + 1 \tag{5.2}$$

Suppose now that there exists a point P in S_{t+1} such that

$$P \in B_1 \cap B_2, \quad \text{but} \quad P \notin C_1 \cup C_2 \cup .. \cup C_{t+1}.$$

Since P and C_{t+1} are both in S_{t+1}, they span a subspace $\overline{S}$ of S_{t+1}, the dimension of which is

$$\overline{d} = d_{t+1} + 1 \tag{5.3}$$

Apply the dimensional equation to the subspaces $\overline{S}$ and S_t of S_{t+1}. It follows from (5.2) and (5.3) that S_t and $\overline{S}$ intersect in exactly one point : Q.

Since $C_1, C_2, \ldots, C_t$ are subpsaces of B_1 and of B_2, it follows that

$$S_t = C_1 + C_2 + \ldots + C_t$$

is an extended subspace of <u>each</u> B_1 and B_2.

Similarly, $\overline{S} = P + C_{t+1}$ is an extended subspace of <u>each</u> B_1 and B_2.

Since $\overline{S}$ and S_t are intersecting spaces, it follows (Note 3) that their restrictions to B_1 also intersect. Since Q is the only point of intersection of $\overline{S}$ and S_t, it follows that $Q \in B_1$. Similarly $Q \in B_2$.

Hence Q is in $B_1 \cap B_2$.

Q is a point of S_t, which by the inductive hypothesis contains no point of $B_1 \cap B_2$ other than those in one of components. Hence $Q \in C_i$, $(i \in \{1,2,..,t\})$.

However, by Lemma 3.7, the space $\overline{S}$, spanned by two components (P and S_{t+1}) does not contain any point of $B_1 \cap B_2$ other than P or a point of S_{t+1}. so Q cannot belong to $\overline{S}$, since it is not in S_{t+1} (skew to S_i) and it is different from P, since by the inductive hypothesis S_t cannot contain P. This contradiction proves the first part of Lemma 3.8. The dimension of S_{t+1} is now by (5.1) and (5.2)

$$d = d' + d_{t+1} + 1 = d_1 + d_2 + \ldots + d_t + d_{t+1} + t$$

This completes the proof. □

Definition

A Baer complex, denoted by the symbol

$$C_{\{d_1 d_2 \ldots d_t\}}$$

is a collection of t Baer k_i-spaces (i=1,..,t) of dimensions d_1, d_2, ..., d_t respectively in $PG(n,q^2)$, pairwise skew, and such that the span in $PG(n,q^2)$ of any subset of the complex contains no points of the complementary set of the complex. A Baer k-space (k=-1,0,1,..,n) can be regarded as a Baer complex, of singleton type. The case k = -1 representing the null-space is included.

Lemmas 3.5 to 3.8 can now be summarised:

Theorem 3.9

Two Baer n-spaces intersect in a Baer complex.

Corollary

The intersection of a Baer k_1-space and a Baer k_2-space is a Baer complex.

Proof of Corollary

By the corollary of Theorem 3.4, the existence of three collinear points on the intersection of a Baer k_1-space and a Baer k_2-space implies that the Baer k_1-space and the Baer k_2-space share a slot of q+1 points. Keeping this in mind, all the arguments used in the proofs of Lemmas 3.5 to 3.8, leading to Theorem 3.9, are valid for the intersection of a Baer k_1-space and a Baer k_2-space. □

The intersection configurations of Baer planes in Chapter 2, and the computer results for 3 dimensions, listed in the beginning of this chapter provide simple examples of Baer-complexes.

In the next section, Baer-complexes will be given further attention. Before that, however, the possible numbers of points belonging to the intersection of two Baer-spaces will be determined. By Theorem 3.3, these numbers also give the possible number of hyperplanes belonging to the intersection. For obtaining an upper bound for the number of points in the intersection we need the following lemma.

Lemma 3.10

Let q and m be integers greater than 1 and the set $\{r_1, r_2, \ldots, r_k\}$ a nontrivial partition of m, i.e.

$$r_1 + r_2 + \ldots + r_k = m$$

where $1 \leq r_1 \leq r_2 \ldots \leq r_k$ and $k > 1$. Then

$$\sum_{i=1}^{k} q^{r_i} \leq q^m \qquad (5.4)$$

The inequality is strict except for the case

$$q = m = 2.$$

Proof

When m = 2, the only non-trivial partition is

$$r_1 = r_2 = 1.$$

In this case

$$\sum_{i=1}^{2} q^{r_i} = 2q \;\begin{cases} < q^2 & \text{when } q > 2 \\ = q^2 & \text{when } q = 2 \end{cases}$$

We proceed by induction, assuming that (5.4) is valid for all $m < n$.

Let

$$\sum_{i=1}^{k} r_i = n+1.$$

Then

$$\sum_{i=1}^{k} q^{r_i} = q^{r_1} + \sum_{i=2}^{k} q^{r_i}.$$

Here

$$\sum_{i=2}^{k} r_i = n+1 - r_1 \leq n, \text{ since } r_1 \geq 1.$$

By the inductive hypothesis

$$\sum_{i=2}^{k} q^{r_i} \leq q^n$$

and so

$$\sum_{i=1}^{k} q^{r_i} \leq q^{r_1} + q^n$$

where $0 < n - r_1 < n$. We have

$$q^{r_1} + q^n = q^{r_1}(1 + q^{n-r_1}) < q^{r_1}q^{n-r_1+1} = q^{n+1}$$

for all $q > 1$.

Thus for all $q > 1$ and $m > 2$ and $\sum_{i=1}^{k} r_i = m$ $(r_i \geqslant 1, (i=1,..,k))$

$$\sum_{i=1}^{k} q^{r_i} < q^m.$$

□

Theorem 3.11

Let B_1 and B_2 be two Baer n-spaces in $PG(n,q^2)$. Let r denote the number of points common to B_1 and B_2. Then

$$0 \leqslant r = \sum_{i=1}^{t} \frac{q^{d_i+1}-1}{q-1} \leqslant \frac{q^n-1}{q-1} + 1 \tag{5.5}$$

where $\{d_i | (i=1,..,t)\}$ represents a partition of the number $d+1-t$ into t summands. Here $0 \leqslant d \leqslant n$.

Proof

Here t denotes the number of components of the Baer-complex, which is the intersection of the two Baer-spaces, where

$$d_1 + d_2 + \ldots + d_t + t-1 = d \leqslant n$$

Let $d_1 \leqslant d_2 \leqslant \ldots \leqslant d_t$.

Since each component C_{d_i} is a Baer d_i-space, the number of points in it is

$$\frac{q^{d_i+1}-1}{q-1},$$

hence the number of points belonging to the complex is

$$r = \sum_{i=1}^{t} \frac{q^{d_i+1}-1}{q-1}.$$

To prove the inequality in (5.5), we consider three cases first.

(i) The components are a hyperplane B_{n-1} of B_1 and a point P not belonging to B_{n-1}. It will be shown later that such intersections always exist. In this case

$$r = \frac{q^n-1}{q-1} + 1,$$

hence the upper bound of the inequality is reached in this case.

(ii) The components are t linearly independent points where $t \leq n + 1$.

Write

$$1 + \frac{q^n-1}{q-1} = q^{n-1} + q^{n-2} + \ldots + 1 + 1 > n + 1,$$

since $q > 1$ and $n > 1$.

In this case the inequality is strict.

(iii) $t = 1$. Thus the intersection is a single subspace of dimension at most $n - 1$, since we consider the intersection of two distinct Baer n-spaces. The inequality is again strict.

Next deal with the general case when $t > 1$ and $d_t = \max\{d_i | i=1,..,t\} \geq 1$, also $d_t \leq n - 2$, as $d_t = n - 1$ has been settled as case (i).

We have to show that under these conditions

$$\sum_{i=1}^{t} \frac{q^{d_i+1}-1}{q-1} < \frac{q^n-1}{q-1} + 1,$$

(the inequality is strict).

Write $r_i = d_i + 1$ $(i=1,..,t)$. Then the inequality to be proved becomes

$$\sum_{i=1}^{t} q^{r_i} < q^n + q + t - 2.$$

Since $q \geq 2$ and $t > 1$, it suffices to show that

$$\sum_{i=1}^{t} q^{r_i} \leq q^n$$

provided that $\sum_{i=1}^{t} r_i = \sum_{i=1}^{t} d_i + t \leq n+1$ and $2 \leq r_t \leq n-1$.

Write

$$\sum_{i=1}^{t} q^{r_i} = \sum_{i=1}^{t} q^{r_i} + q^{r_t} \qquad (5.6)$$

It follows from the given conditions that

$$\sum_{i=1}^{t-1} r_i = \sum_{i=1}^{t} r_i - r_t \leq n + 1 - 2 = n - 1.$$

From Lemma 3.10

$$\sum_{i=1}^{t-1} q^{r_i} \leq q^{n-1},$$

also $q^{r_t} \leq q^{n-1}$ since $r_t \leq n - 1$. So on the right hand side of (5.6) we have

$$\sum_{i=1}^{t-1} q^{r_i} + q^{r_t} \leq 2q^{n-1} \leq q^n \quad \text{since } q \geq 2.$$

This completes the proof. □

3.6 Baer complexes : basic properties

Regarding Baer complexes as basic elements in the structure of a finite projective space of square order, this section is assigned to their closer study.

Definitions

The dimension d of the Baer complex $\{d_1, .., d_t\}$ is the dimension of the space spanned by its components. Thus

$$d = d_1 + d_2 + \ldots + d_t + t - 1 \qquad (6.1)$$

The fragmentation t of the complex is the number of its components.

The class of the complex is determined by the set $\{d_1, .., d_t\}$, that is the set of dimensions of its components.

Notes

1. The maximal dimension of a complex is n, the dimension of the geometry of reference $PG(n,q^2)$. In particular a Baer n-space is a complex of maximal dimension.

2. The maximal fragmentation of a complex is $t_{max} = n + 1$. This follows immediately from (6.1). In this case the complex is a set of n + 1 linearly independent points.

   More generally, the maximal fragmentation of a complex of dimension d is d + 1.

3. The dimension of any component of a complex cannot exceed d + 1 - t.

4. If two pairs of Baer spaces intersect in Baer complexes of the same class, their intersection configurations are not necessarily isomorphic. As an example, take intersection configuration 2(i) and 2(ii) in Section 2.2. The space of reference is the projective plane $PG(2,q^2)$. Two Baer planes may intersect in a single point, hence the class of the intersection complex is $\{0\}$. But then $B_1 \cap B_2$ has also a common line. The point may or may not be on the line.

Theorem 3.12

The number of classes of Baer complexes in PG(n,q^2) is

$$T_C(n) = 1 + \sum_{d=0}^{n} P(d+1)$$

where P(d+1) is the number of partitions of the integer d + 1.

Proof

The dimension of a Baer complex in PG(n,q^2) can take any integer value in the range [-1,n], where -1 is the dimension of the null-space, treated as a Baer complex.

From (6.1) it follows that

$$d + 1 = \sum_{i=1}^{t} (d_i+1).$$

The set $\{d_1,..,d_t\}$ is fully determined by partitioning the number d + 1 into a set of t values : $\{d_i+1\}$, where $d_i + 1 > 0$, (i=1,..,t), if t is fixed. Since the fragmentation t may take any value from 1 to d+1 (Note 2), then for the fixed dimension d, the number of classes is P(d+1). Thus, summing for all dimensions, 0 to n, and then adding 1 to count as a single class the empty set ∅, for the null-space, we obtain $T_C(n)$.

□

Taking values from tables of partition-numbers of integers [23], numbers of classes of Baer complexes of projective planes PG(n,q^2) up to n=9 are listed in the following.

Partition numbers

n	P(n)	n	P(n)
1	1	6	11
2	2	7	15
3	3	8	22
4	5	9	30
5	7	10	42

Classes of Baer Complexes

Dimension of PG(n,q^2)	No. of Classes	Classes
-1	1	ϕ
0	2	ϕ, {0}
1	4	ϕ, {0} {0,0} {1}
2	7	ϕ, {0} {0,0} {1} {0,0,0} {1,0} {2}
3	12	ϕ, {0} {0,0} {1} {0,0,0} {1,0} {2} {0,0,0,0} {1,0,0} {1,1} {2,0} {3}
4	19	
5	30	
6	45	
7	57	
8	87	
9	129	

The following two theorems deal with relations of Baer complexes to Baer k-spaces.

It has been established in the previous section that a Baer k_1-space and a Baer k_2-space intersect in a Baer-complex. Generally, Baer-complexes inside a Baer n-space, are obtained by splitting up some subspace of the Baer-space into a direct sum of subspaces. It is not obvious however that an arbitrary Baer complex can be embedded in some Baer space. This will be proved next.

Theorem 3.13

A Baer complex of dimension d can be embedded in a Baer d-space. (Note: the embedding is not unique.)

Proof

The proof is based on the facts that d + 1 independent points determine uniquely a d dimensional subspace S_d of $PG(n,q^2)$, while d + 2 points, not d + 1 of which are dependent, determine uniquely a Baer d-space.

For complexes $C\{0,..,0\}$ of d + 1 independent points, or $C\{d\}$ where the complex is a single Baer space, no proof is needed. Two further cases will be considered.

Case (i)

The complex is of type $C\{d-1,0\}$.

This means that the complex has two components : a Baer (d-1)-space and an external point. The dimension of this complex is d.

Denote the Baer space by B and the external point by P. From earlier remarks it follows that the dimension of B can be taken to be more than 0.

Choose a set $A = \{A_0, A_1, .., A_d\} \subset B$, consisting of d + 1 points, no d of them dependent. Let X be a point on A_0P, different from A_0 or P. Then X is not in the extension of B into S, denoted by S_B and of dimension d - 1.

Consider the set $\{P, X, A_1, .., A_d\}$. It consists of d + 2 points, not d + 1 of them dependent. To see this, only sets containing P, X and d-1 points of the set $A\setminus\{A_0\}$ have to be considered. Suppose that X is in a subspace S_X of $PG(n,q^2)$, spanned by P and d-1 points of $A\setminus\{A_0\}$. The dimension of S_X is d-1, and line $PX \subset S_X$. Then the point A_0 is also in S_X. But A_0 together with the d-1 points chosen out of $A\backslash\{A_0\}$ spans S_B. Thus $S_B \subseteq S_X$ and since they are of the same dimension, $S_B = S_X$. Then P and X are in S_X which is a contradiction. Thus the set

$$\{P\} \cup \{X\} \cup A\backslash\{A_0\}$$

determines a unique Baer d-space B'. The line $PX \subset B'$. The subspace of S, spanned by $A\backslash\{A_0\}$ belongs to B', hence its intersection point A_0 with PX, is an internal point of B'. So B' is a Baer d-space containing both P and B.

Case (ii)

Let $C\{d_1,..,d_t\}$ be the complex considered.

We may now assume:

(a) $t > 1$,

(b) at least one component has dimension greater than 0. Let this be the t^{th} component, the Baer d_t-space: B_t, (of dimension d_t).

(c) $C\{d_1,..,d_{t-1}\}$ is not a single point.

(If t=2, the alternative is covered in case (i).)

Proceed by induction on t. For t = 1, theorem 3.13 is trivially true. Assume that the complex $C\{d_1,..,d_{t-1}\}$ of dimension $d_1 + .. + d_{t-1} + t-2 = d'$ is embedded in a Baer d'-space B'.

Choose sets of $d' + 2$ and $d_t + 2$ points

$$A = \{A_0, A_1, .., A_{d'+1}\}$$

and

$$T = \{T_0, T_1, ..., T_{d_t+1}\}$$

in B' and B_t respectively, so that no d' + 1 points of the set A and no $d_t + 1$ points of T are dependent.

Let X be a point on A_0T_0, different from A_0 and T_0.

Consider the set

$$U = \{X\} \cup A\backslash\{A_0\} \cup T\backslash\{T_0\},$$

containing $d' + d_t + 3 = d + 2$ points. No d + 1 of these are linearly dependent. This is clear for the set $U\backslash\{X\}$. Suppose next that the set of d + 1 points contains X, all points of $A\backslash\{A_0\}$ and all but one point of the set $T\backslash\{T_0\}$. Assume that these points are dependent and hence they are the points of some d-1-dimensional space S_{d-1} (of order q^2). Since A_0 is linearly dependent on $A\backslash\{A_0\}$, it is also in S_{d-1}. Hence the line A_0X is in S_{d-1} and so is T_0. Thus S_{d-1} contains all of the set A, in particular d' + 1 linearly independent points of it, and it contains $d_t + 1$ points of T which are independent and independent also of the points of A. Now $d_t + 1 + d' + 1 = d + 1$, hence S_{d-1} contains d + 1 independent points. This is a contradiction. Similar conclusion is reached considering a set containing X, all points of $T\backslash\{T_0\}$ and all but one of $A\backslash\{A_0\}$.

Thus the set U determines uniquely a Baer d-space $\overline{B}$. It remains to be shown that B' and B_t are included in $\overline{B}$.

Let S_A be the space spanned by $A\backslash\{A_0\}$ and X and S_T the sub-space spanned by $T\backslash\{T_0\}$ and X. Their dimensions are d' + 1 and $d_t + 1$ respectively. A_0 and T_0 are in S_A and S_T respectively, hence the line $A_0X\,T_0 \subset S_A \cap S_T$. Both S_A and S_T are subspaces belonging to the Baer space $\overline{B}$, so their intersection-line $A_0X\ T_0$ is also in $\overline{B}$, hence the intersection of $A_0X\ T_0$ and A_0A_i where $A_i \in A\setminus\{A_0\}$ is also in $\overline{B}$. Thus A_0 is in $\overline{B}$. The same applies to T_0. Thus $\overline{B}$ contains the set A and the set T which determine uniquely the Baer-spaces B' and B_t. So $B' \subset \overline{B}$, in particular $C\{d_1,..,d_{t-1}\} \subset \overline{B}$ and $B_t \subset \overline{B}$.

Hence $\overline{B}$ contains the complex $C\{d_1,...,d_t\}$. □

Definition

A k-dimensional subspace of $PG(n,q^2)$ belongs to a Baer complex if k + 1 independent points of the subspace are in the complex.

Note: This does not mean that the points of some Baer-space of the subspace are all in the complex.

Theorem 3.14 (Symmetry)

The number of j-dimensional subspaces belonging to a d-dimensional Baer complex is equal to the number of (d-1-j)-dimensional subspaces belonging to it.

Proof

It is known that the number of j-dimensional subspaces of a projective space of dimension d is equal to the number of its (d+1-j) dimensional subspaces, since

$$\begin{bmatrix} d+1 \\ j+1 \end{bmatrix}_q = \begin{bmatrix} d+1 \\ d+1-(j+1) \end{bmatrix}_q = \begin{bmatrix} d+1 \\ d-j \end{bmatrix}_q = \text{number of (d-j-1)-dimensional subspaces.}$$

Thus the theorem needs no proof for Baer complexes of type $C\{d\}$. Use the symbol $\underline{M}_j^d$ in the following to denote the number of j-dimensional subspaces belonging to a Baer d-space.

Denote by $\overline{M}_j^d$ the number of j-dimensinoal subspaces belonging to some given Baer complex of dimension d. Note that while M_j^d is fixed by the values of d and j, $\overline{M}_j^d$ depends on the structure of the given complex.

Proceed by induction on the fragmentation t, splitting the complex $C\{d_1,\ldots,d_t\}$ of dimension $d = \sum_{i=1}^{t} d_i + t - 1$ into the complex $C\{d_1,\ldots,d_{t-1}\}$ of dimension $d' = \sum_{i=1}^{t-1} d_i + t - 2$ and the Baer-space B_t of dimension d_t, where $t \geqslant 2$. We assume that the symmetry relation holds for the complex $C\{d_1,\ldots,d_{t-1}\}$ of dimension d'.

A subspace of dimension j belonging to $C\{d_1,\ldots,d_t\}$ where $-1 \leqslant j \leqslant d$ may be spanned by some subspace of dimension i' belonging to the complex $C\{d_1,\ldots,d_{t-1}\}$ and a subspace of dimension i_t of the Baer d_t-space B_t.

Here

$$-1 \leqslant i' \leqslant d' \tag{6.2}$$

$$-1 \leqslant i_t \leqslant d_t \tag{6.3}$$

$$i' + i_t = j-1 \tag{6.4}$$

Hence the number of j-dimensional subspaces belonging to $C\{d_1,\ldots,d_t\}$ is

$$\overline{M}_j^d = \sum \overline{M}_{i'}^{d'} M_{i_t}^{d_t} \tag{6.5}$$

where i' and i_t satisfy (6.2), (6.3) and (6.4). Using the symmetry property of B_t and the inductive hypothesis for $C\{d_1,\ldots,d_t\}$ we put

$$\overline{M}_{i'}^{d'} = \overline{M}_{(d'-1)-i'}^{d'} \quad \text{and} \quad M_{i_t}^{d_t} = M_{(d_t-1)-i_t}^{d_t} \tag{6.6}$$

in each term of the sum.

The inequalities (6.2) and (6.3) imply that

$$-1 \leq (d'-1)-i' \leq d'$$

and

$$-1 \leq (d_t-1)-i_t \leq d_t,$$

for all i' and i_t respectively in the range.

The dimension of the subspace spanned by a $(d'-1)-i'$ dimensional subspace belonging to $C\{d\ ,\ldots,d_{t-1}\}$ and a $(d_t-1)-i_t$ dimensional subspace in B_t is

$$(d'-1-i') + (d_t-1-i_t) + 1 = (d-1)-j \qquad (6.7)$$

The result (6.7) is deduced from (6.4). It follows now from (6.5) and (6.6) that

$$\overline{M}^{d}_{j} = \sum \overline{M}^{d'}_{(d'-1)-i'}\, {}^{d_t}M_{(d-1)-i} = \overline{M}^{d}_{d-j}.$$

This completes the proof. □

<u>Theorem 3.15</u>

The intersection of two Baer complexes is a Baer complex.

<u>Proof</u>

Let $C\{d_1,\ldots,d_s\}$ and $C'\{d'_1,\ldots,d'_t\}$ be the complexes. Let

$$C\{d_1,\ldots,d_s\} = \{B_i,\ i=1,\ldots,s\}$$

and

$$C'\{d'_1,\ldots,d'_t\} = \{B'_j,\ j=1,\ldots,t\}$$

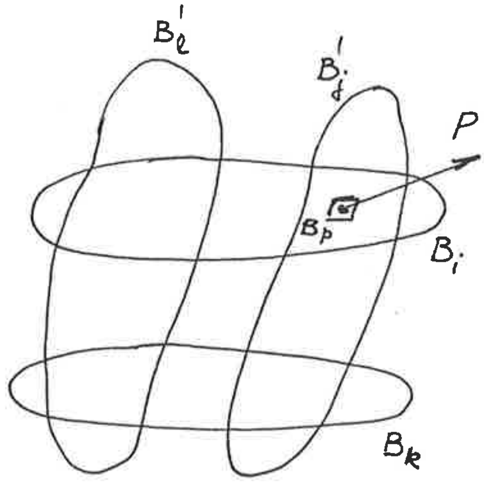
where the component sets $\{B_i\}$ and $\{B_j\}$ satisfy the required conditions.

Then

$$C\{d_1,\ldots,d_s\} \cap C'\{d'_1,\ldots,d'_t\} = \{B_i \cap B'_j \mid i \in \{1,..,s\},\ j \in \{1,..,t\}.$$

For each ordered pair (i,j), where $i \in \{1,..,s\}$, $j \in \{1,..,t\}$, the intersection $B_i \cap B'_j$ is a Baer complex as shown in Section 3.5.

The situation is shown on the diagram. For convenience, we will call the complexes formed by the intersections of the components B_i of the complex $C\{d_1,...,d_s\}$ and B'_j of the complex $C\{d'_1,...,d'_t\}$ <u>mini-complexes</u> (for $i=1,...,s$, $j=1,..,t$). We are going to show that the collection of these mini-complexes is again a Baer-complex.



Let P be a point in the mini-complex $B_i \cap B'_j$ belonging to a component B_p of the mini-complex.

Since $B_i \cap B'_j$ is a Baer-complex, P cannot be in the span of any components of $B_i \cap B'_j$ other than B_p.

The span of components chosen out of the set $B_i \cap B'_j \backslash B_p$ and components belonging to <u>mini-complexes external</u> to $B_i \cap B'_j$ cannot include P either, for the span of P and components belonging to $B_i \cap B'_j \backslash B_p$ belongs to $B_i \cap B_j$, hence cannot contain external points. Consider <u>next the span of components belonging to mini-complexes other than $B_i \cap B'_j$</u>.

(a) If <u>none</u> of the components is included <u>in B_i</u>, then their <u>span</u> cannot contain a <u>point of B_i</u>. This is so, because $C\{d_1,..,d_s\}$ is a Baer complex, hence no point of B_p can belong to such a span. The situation is <u>similar</u> if <u>none</u> of the components is <u>included in B'_j</u>.

(b) Suppose next that <u>some</u> components belong to mini-complexes inside B_i, <u>some not in B_i</u> and their space contains P. This leads to a contradiction similar to the one encountered before, since P together with the components inside B_i spans a subspace of B_i and so cannot contain external components.

(c) The only remaining case is that of all components belonging to B_i B_i B'_j. This however means that no component belongs to B'_j and this case was dismissed in (a).

This completes the proof.

All Baer complexes in $PG(n,q^2)$ are partially ordered by inclusion. Theorem 3.15 implies that the partially ordered set of Baer complexes of $PG(n,q^2)$ is a semi-lattice.

However, it is not generally possible to define a join for two Baer complexes which is itself a Baer complex. A simple counter example is the case of two distinct Baer-planes belonging to the same subplane ($\cong PG(2,q^2)$) of $PG(n,q^2)$. Hence the set of Baer complexes does not form a lattice in $PG(n,q^2)$. However, if the set is restricted to complexes included in the same Baer n-space (or more generally Baer k-space) of $PG(n,q^2)$, then the semi-lattice defined by the restricted set possesses a common upper bound in the semi-lattice, hence it is a lattice.

In [25] a unified theory of partially ordered locally finite sets is established. A variety of combinatorial objects fit into this scheme, amongst them are integers ordered by magnitude or divisibility, sets ordered by inclusion, linear or projective spaces ordered by inclusion, partitions of integers ordered by refinement, and so on. The lattice of complexes of $PG(n,q)$ or more generally the semi-lattice of Baer complexes of $PG(n,q^2)$ combine features of lattices of projective spaces and also features of partitions. A later investigation should produce general results characterising these type of sets. The scope of the work discussed in the next section is more limited, it presents some enumerations and algorithms.

3.7 Baer complexes : numerical relations

It has been proved in Section 3.5 that Baer-spaces intersect in Baer complexes. The question arises naturally : Can any given Baer complex be the intersection of two Baer n-spaces? Also in Section 2, formulae were given for numbers of Baer planes intersecting a given plane in a fixed configuration. The aim is now to extend such numerical relations to spaces of higher dimension. Before establishing such relations it is convenient to tabulate notations for counting numbers of various structures. This is done in the following list.

I.	N^n_k	Number of Baer k-spaces in $PG(n,q^2)$ $0 \leq k \leq n$.
II.	$\left[{n \atop r}\right]_q$	Gaussian binomial coefficient (as defined in Chapter 1, Formula 1.1)
III.	$[k]!(q)$	Gaussian "factorial" notation used here to denote $(q-1)(q^2-1)..(q^k-1)$
IV.	$P^k_{k_1,k_2,\ldots,k_t}(q)$	Number of partitions of $PG(q,k)$ into skew subspaces of dimensions $k_1, k_2,\ldots,k_t$.
V.	$T^n_{d_1,\ldots,d_t}$	Number of $C\{d_1,\ldots,d_t\}$ complexes in $PG(n,q^2)$.
VI.	$t^n_{d_1,\ldots,d_t}$	Number of $C\{d_1,\ldots,d_t\}$ complexes in a fixed Baer n-space.
VII.	$L^{\delta_1,\ldots,\delta_s}_{d_1,\ldots,d_t}$	Number of $C\{d_1,\ldots,d_t\}$ complexes contained in a fixed $C\{\delta_1,\ldots,\delta_t\}$ complex.

VIII. $U^{\delta_1,\ldots,\delta_s}_{d_1,\ldots,d_t}$ — Number of $C\{\delta_1,\ldots,\delta_s\}$ complexes <u>containing a fixed</u> $C\{d_1,\ldots,d_t\}$ complex

IX. $S^{k}_{d_1,\ldots,d_t}$ — Number of Baer k-spaces containing a fixed $C\{d_1,\ldots,d_t\}$ complex.

X. $I_{d_1,\ldots,d_t}$ — Number of Baer n-spaces intersecting a <u>fixed</u> Baer n-space in a fixed $C\{d_1,\ldots,d_t\}$ complex.

<u>Note:</u>

All the notations refer to a fixed projective space of reference. However, in II, III and IV q or q^2 must be displayed as a subscript or variable, because these may refer to subspaces (of order q^2) of $PG(n,q^2)$ or to Baer k-spaces (of order q).

We begin by recalling from Section 3.1 the formula (1.1) counting the total number of Baer n-spaces. This will be denoted here by N^n_n, in accordance with Notation I.

So

$$N^{n}_{n} = q^{n(n+1)/2} \prod_{i=2}^{n+1} (q^i+1) \tag{7.1}$$

As seen in Section 3, the number of subspaces of dimension k in PG(n,q) is given by

$$\left[{n+1 \atop k+1}\right]_q = \frac{(q^{k+1}-1)(q^k-1)\ldots(q^{n-k+1}-1)}{(q-1)(q^2-1)\ldots(q^{k+1}-1)} \tag{7.2}$$

hence the number of subspaces of dimension k in $PG(n,q^2)$ is

$$\left[{n+1 \atop k+1}\right]_{q^2} = \frac{(q^{2k+2}-1)(q^{2k}-1)\ldots(q^{2n-2k+1}-1)}{(q^2-1)(q^4-1)\ldots(q^{2k+2}-1)} \tag{7.3}$$

Using formulae (7.1) and (7.3) together with the fact that a Baer k-space is embedded in a unique k-subspace of $PG(n,q^2)$, we obtain

$$N_k^n = \begin{bmatrix} n+1 \\ k+1 \end{bmatrix}_{q^2} N_k^k =$$

$$= \frac{(q^{2n+2}-1)\ldots(q^{2n-2k+2}-1)}{(q^2-1)\ldots(q^{2k+2}-1)} q^{k(k+1)/2} \prod_{i=2}^{k+1} (q^i+1) \qquad (7.4)$$

The next aim is to determine $T^n_{d_1,\ldots,d_r}$ as defined by V.

Since each d_i-dimensional component $(i=1,..,t)$ determines a unique d_i-dimensional subspace of $PG(n,q^2)$ into which it is embedded, the first task is to determine the number of ways in which a d-subspace of $PG(n,q^2)$ can be partitioned into a set of $d_1, \ldots, d_t$ dimensional subspaces where

$$d = \sum_{i=1}^{t} d_i + t - 1,$$

that is, the dimension of the complex.

The number of subspaces complementary to a given k-dimensional subspace will be needed for the calculations. In the case of linear spaces, this is given as special case (d) of Theorem 1.2 in Chapter 1, as

$$q^{k(n-k)}.$$

Using the modification necessary in projective spaces, we have that the number of subspaces of $PG(n,q)$ complementary to a subspace of dimension k is

$$q^{(k+1)[(n+1)-(k+1)]} = q^{(k+1)(n-k)} \qquad (7.5)$$

We use this relation first to determine the number of ways in which a space P(d,q) can be partitioned into <u>two</u> spaces of dimensions d_1 and d_2 respectively where

$$d = d_1 + d_2 + 1.$$

Setting $f = 1$, when $d_1 \neq d_2$

and $f = 1/2$, when $d_1 = d_2$ gives

$$P^d_{d_1 d_2}(q) = f\left[{d+1 \atop d_1+1}\right]_q q^{(d_1+1)(d-d_1)}.$$

In order to generalise this result for partitions into a set of t skew spaces, we use the "factorial" notation introduced in III. The formula for two components becomes

$$P^d_{d_1 d_2}(q) = f\frac{[d+1]!(q)}{[d_1+1]!(q)[d_2+1]!(q)} q^{d_1 d_2 + d} \qquad (7.6)$$

Next we derive the general partition formula for a d-dimensional space $S_d \simeq PG(d,q)$ divided into t spaces S_{d_1}, S_{d_2}, ..., S_{d_t} of dimensions d_1, d_2, ..., d_t respectively, where

$$d_1 + d_2 + \ldots + d_t + t - 1 = d.$$

The result (7.6) will be generalised to

$$P^d_{d_1,\ldots d_t}(q) = f\frac{[d+1]!(q)}{[d_1+1]!(q)\ \ldots[d_r+1]!(q)} q^{e_t}$$

where

$$e_t = \sum_{1 \leqslant i < j \leqslant t} d_i d_j + (t-1)d - \frac{1}{2}(t-1)(t-2) \qquad (7.7)$$

and $f = \dfrac{1}{s_1!\, s_2!\ \ldots}$ if s_i of the component spaces are of the same dimension (i=1,2,...).

For deriving (7.7) proceed step by step. Denote by $d^{(1)}$ the dimension of a space complementing S_{d_1} in S_d, and generally by $d^{(i)}$ the dimension of a space complementing S_{d_i} in $S_{d^{(i-1)}}$ (where $S_{d^{(0)}} = S_d$).

For i = 1 to t, we have $d^{(i)} + d_i = d^{(i-1)}-1$, (note that $d_t = d^{(t-1)}$ and the number of complementary $S_{d^{(i)}}$ spaces which complement S_{d_i} in $S_{d^{(i-1)}}$ is

$$q^{(d^{(i-1)}-d_i)(d_i+1))}.$$

We obtain then

$$P^{d}_{d_1..d_t}(q) = f\begin{bmatrix} d+1 \\ d_1+1 \end{bmatrix}_q \begin{bmatrix} d^{(1)}+1 \\ d_2+1 \end{bmatrix}_q \cdots \begin{bmatrix} d^{(r-1)}+1 \\ d_r+1 \end{bmatrix} q^{e_t}$$

with

$$e_t = \sum_{i=1}^{t-1} (d^{(i-1)}-d_i)(d_i+1).$$

For simplification we use the factorial notation:

$$\begin{bmatrix} d^{(i-1)}+1 \\ d_i+1 \end{bmatrix}_q = \frac{[d^{(i-1)}+1]!(q)}{[d_i+1]!(q)[d^{(i-1)}-d_i]!(q)}$$

$$= \frac{[d^{(i-1)}+1]!(q)}{[d_i+1]!(q)[d^{(i)}+1]!(q)}$$

while for e_t we write in each term (i=1,...,t-1)

$$(d_i+1)(d^{(i-1)}-d_i) = (d_i+1)(d_{i+1}+\ldots+d_t+t-1).$$

A short calculation brings the formula to the simplfied form (7.7).

Using the partition formula, we can now evaluate $T^{n}_{d_1,..d_t}$.

$$T^{n}_{d_1,..d_t} = \begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_{q^2} P^{d}_{d_1,..d_t}(q^2) \prod_{i=1}^{t} N^{d_i}_{d_i}$$

$$= \frac{[n+1]!_{q^2}}{[n-d]!_{q^2} \prod_{i=1}^{t} [d_i+1]'_{q^2}} \prod_{i=1}^{t} \frac{d_i(d_i+1)}{2} \prod_{j=2}^{d_i+1} (q^j+1) \qquad (7.8)$$

These results are used now to find $S^{n}_{d_1...d_t}$, the number of Baer n-spaces containing a given Baer complex $C\{d_1,..,d_t\}$.

We count the incidences of Baer n-spaces with $C\{d_1,..,d_t\}$ type complexes in two ways. On one hand, we have $T^{n}_{d_1,..d_t}$ complexes of the given type, each contained in $S^{n}_{d_1,..d_t}$ Baer n-spaces, hence

$$T^{n}_{d_1,..d_t} S^{n}_{d_1,..d_t} \text{ incidences.}$$

On the other hand, each Baer n-space contains $\begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q$ Baer d-spaces, and each of these can be partitioned in $P^{d}_{d_1,..d_r}(q)$ ways into $C\{d_1,..,d_r\}$ complexes. Since the number of Baer n-spaces is N^{n}_{n}, the number of incidences obtained in this way is

$$N^{n}_{n}\begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q P^{d}_{d_1,..d_t}(q).$$

Using (7.8), we can write down the incidence equation:

$$S^{n}_{d_1...d_t}\begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_{q^2} P^{d}_{d_1,..,d_t}(q^2) \prod_{i=1}^{t} N^{d_i}_{d_i} =$$

$$= N^{n}_{n}\begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q P^{d}_{d_1,..d_t}(q) \qquad (7.9)$$

From (7.9) we calculate $S^n_{d_1,..d_t}$.

After simplifying, obtain

$$S^n_{d_1,..d_t} = q^{(d+1)+(d+2)+..+n} \; (q+1)^{t-1} \prod_{i=1}^{n-d} (q^i+1)$$

if $d < n$ and

$$S^n_{d_1,..d_t} = (q+1)^{t-1} \text{ if } d = n \qquad (7.10)$$

The remarkable feature of this result is that the number of Baer n-spaces containing a given Baer complex depends only on the dimension d and the fragmentation t of the complex.

Let B be a fixed Baer n-space. An algorithm can be given now to evaluate successively the number of Baer n-spaces which intersect B in a fixed Baer complex. Return to the notations introduced in the beginning of this section:

$$I_{d_1...d_t} = S^n_{d_1...d_t} - \sum I_{\delta_1...\delta_s} U^{\delta_1 \,..\, \delta_s}_{d_1,...,d_t} \qquad (7.11)$$

The summation over the complexes $C\{\delta_1,...,\delta_s\}$ on the right hand side of (7.11) refers to all the complexes which are <u>different</u> from $C\{d_1.....d_t\}$. Beginning with $I_n = S^n_n = 1$, referring to B itself, (7.11) is used successively, proceeding from complexes of higher dimension and smaller fragmentation to those of lower dimension and greater fragmentation.

The calculations have been carried out in the three dimensional case. To carry out these calculations, values of $S^n_{d_1,..d_t}$ are found, for each <u>class</u> of complexes, using (7.10). Next the values of $U^{\delta_1 .. \delta_s}_{d_1,..d_t}$ are listed. These are found for each $\{\delta_1,...,\delta_s\}$,

$\{d_1, \ldots, d_t\}$-pair by inspection. These values are checked by using the incidence equation:

$$t^n_{\delta_1,\ldots,\delta_s} L^{\delta_1,\ldots\delta_s}_{d_1,\ldots,d_t} = t^n_{d_1,\ldots d_t} U^{\delta_1,\ldots\delta_s}_{d_1,\ldots,d_t}$$

(referring to notations VI, VII and VIII).

To find $t^n_{d_1,\ldots,d_t}$ for a given class of complexes, use

$$t^n_{d_1,\ldots d_t} = \left[{n+1 \atop d+1}\right]_a P^d_{d_1,\ldots,d_t}(q)$$

where $d = \sum_{i=1}^{t} d_i + t - 1.$

Results for $PG(3,q^2)$ are shown in the following tables.

T(1). Values of $S^d_{d_1,\ldots,d_t}$

Class $\{d_1,\ldots,d_t\}$	Dimension d	$S^n_{d_1,\ldots,d_t}$
$\{3\}$	3	1
$\{2,0\}$	3	$q+1$
$\{1,1\}$	3	$q+1$
$\{1,0,0\}$	3	$(q+1)^2$
$\{0,0,0,0\}$	3	$(q+1)^3$
$\{2\}$	2	$q^3(q+1)$
$\{1,0\}$	2	$q^3(q+1)^2$
$\{0,0,0\}$	2	$q^3(q+1)^3$
$\{1\}$	1	$q^5(q+1)(q^2+1)$
$\{0,0\}$	1	$q^5(q+1)^2(q^2+1)$
$\{0\}$	0	$q^6(q+1)(q^2+1)(q^3+1)$
Null space ϕ	-1	$q^6(q^2+1)(q^3+1)(q^4+1) = N^3_3$

T(2). Values of $U^{\delta_1,\ldots\delta_s}_{d_1,\ldots,d_r}$

$\{d_1,\ldots,d_r\}$	$\{\delta_1,\ldots,\delta_s\}$ containing $\{d_1,\ldots,d_r\}$	$U^{\delta_1,\ldots,\delta_s}_{d_1,\ldots,d_r}$
{2,0}	{3}	1
{1,1}	{3}	1
{1,0,0}	{3} {2,0} {1,1}	1 2 1
{0,0,0,0}	{3} {2,0} {1,1} {1,0,0}	1 4 3 6
{2}	{3} {2,0}	1 q^3
{1,0}	{3} {2,0} {1,1} {1,0,0} {2}	1 $q(q^2+1)$ q^2 q^3 1
{0,0,0}	{3} {2,0} {1,1} {1,0,0} {0,0,0,0} {2} {1,0}	1 $q(q^2+3)$ $3q^2$ $3q^2(q+1)$ q^3 1 3
{1}	{3} {2,0} {1,1} {1,0,0} {2} {1,0}	1 $q^3(q+1)$ q^4 $1/2\ q^5(q+1)$ $q+1$ $q^2(q+1)$

$\{d_1,\ldots,d_r\}$	$\{\delta_1,\ldots,\delta_s\}$ containing $\{d_1,\ldots,d_r\}$	$U^{\delta_1,\ldots,\delta_s}_{d_1,\ldots,d_r}$
$\{0,0\}$	$\{3\}$	1
	$\{2,0\}$	$q^2(q^2+q+2)$
	$\{1,1\}$	$q^3(2q+1)$
	$\{1,0,0\}$	$1/2\ q^4(q+2)(q+3)$
	$\{0,0,0,0\}$	$1/2\ q^5(q+1)$
	$\{2\}$	$q+1$
	$\{1,0\}$	$q(q+1)(q+2)$
	$\{0,0,0\}$	$q^2(q+1)$
	$\{1\}$	1
$\{0\}$	$\{3\}$	1
	$\{2,0\}$	$q^3(q^2+q+2)$
	$\{1,1\}$	$q^4(q^2+q+1)$
	$\{1,0,0\}$	$1/2\ q^5(q^2+q+1)(q+3)$
	$\{0,0,0,0\}$	$1/6\ q^6(q^2+q+1)(q+1)$
	$\{2\}$	q^2+q+1
	$\{1,0\}$	$q^2(q^2+q+1)(q+2)$
	$\{0,0,0\}$	$1/2\ q^3(q^2+q+1)(q+1)$
	$\{1\}$	q^2+q+1
	$\{0,0\}$	$q(q^2+q+1)$
ϕ	$\{3\}$	1
	$\{2,0\}$	$q^3(q+1)(q^2+1)$
	$\{1,1\}$	$1/2\ q^4(q^2+1)(q^2+q+1)$
	$\{1,0,0\}$	$1/2\ q^5(q^2+1)(q+1)(q^2+q+1)$
	$\{0,0,0,0\}$	$1/24\ q^6(q+1)^2(q^2+1)(q^2+q+1)$
	$\{2\}$	$(q+1)(q^2+1)$
	$\{1,0\}$	$q^2(q+1)(q^2+1)(q^2+q+1)$
	$\{0,0,0\}$	$1/6\ q^3(q+1)^2(q^2+1)(q^2+q+1)$
	$\{1\}$	$(q^2+1)(q^2+q+1)$
	$\{0,0\}$	$1/2\ q(q+1)(q^2+1)(q^2+q+1)$
	$\{0\}$	$(q+1)(q^2+1)$

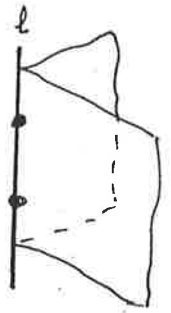
T(3). Values of $I_{d_1,\ldots,d_t}$

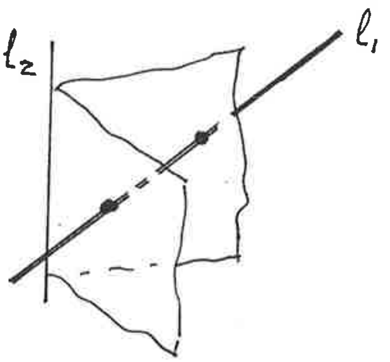
$\{d_1,\ldots,d_t\}$	$I_{d_1,\ldots,d_t}$
$\{2,0\}$	q
$\{1,1\}$	q
$\{1,0,0\}$	$q(q-1)$
$\{0,0,0,0\}$	$q(q-1)(q-2)$
$\{2\}$	q^3-1
$\{1,0\}$	$q^2(2q+1)(q-1)$
$\{0,0,0\}$	$3q^3(q-1)^2$
$\{1\}$	$1/2\ q(q^2\ 1)(q^5-2q^4+2q^3-2)$
$\{0,0\}$	$1/2\ q^4(q^2-1)(q^3-2q^2+6q-6)$
$\{0\}$	$1/6\ q^3(q-1)^2(q+1)(2q^6+3q^5-5q^4+3q^3-6q^2-6)$
ϕ	$1/8\ q^6(q-1)^2(q+1)(q^2+q+1)(3q^4-8q^3-9q^2-10q+8)$

The last tabulated results give the answer for one question posed in the beginning of the section for the three dimension case. All Baer complexes can occur as intersections of two Baer 3-spaces of $PG(3,q^2)$ with one exception. The exceptional case is the set of four independent points in PG(3,4), since when q=2, $I_{0,0,0,0} = 0$. It is easy to see that in all the other cases, the $I_{d_1,\ldots,d_t}$ polynomials have no roots greater or equal to 2, hence take positive values for q=2,3....

As pointed out earlier, the intersection of two Baer n-spaces is not fully characterised by the class to which the intersection complex belongs. From Theorem 3.3 it follows that the number of hyperplanes belonging to the intersection of two Baer spaces is fixed, because it is equal to the number of points in the Baer complex of intersection. Furthermore, Bruen in [11] proved that the dual structure of the intersection, that is the set of spaces determined by the intersection structure of the common hyperplanes is isomorphic to the structure of the spaces spanned by the points of intersection. Hence the intersection of two Baer spaces can be regarded as a pair of two isomorphic complexes; the Baer complex as introduced before and its dual. In the two dimensional case the configurations listed were point-complexes coupled with their duals. The situation there is simple, because the only subspaces to be considered are points and lines.

The list shown in the three-dimensional case gives only the possible complexes without their duals. Though the complex fully determines the geometry of its dual, their dual is not fully determined. As an example, regard the simple case when the intersection complex consists of two points, hence is one dimensional. Its dual consists of two planes. The complex and its dual, each determine a line. However, the two lines may coincide as in Figure (a) or may be distinct as in Figure (b).





(If the two intersection lines do not coincide, they must be skew.)

Thus, even in the three dimensional case, there is a greater variety of possible configurations for the intersection of two Baer spaces than shown in the list of possible complexes.

However, if two Baer n-spaces intersect in a complex of dimension n, then it follows from the symmetry theorem (Theorem 3.14) that the class of the complex determines fully the configuration.

The next section will offer more insight into the relation of a Baer complex and its dual.

3.8 Singer Duality : The General Case

In Section 2.6 Singer duality was treated in the two dimensional case. The duality map ν_s as defined by (6.1) in that section, mapped the points of the plane $PG(2,q^2)$ into its lines and its lines into its points by

$$\nu_s(p_i) = \ell_{s-i} = \overline{p_i(s)}$$
$$\nu_s(\ell_i) = p_{s-i} = \overline{\ell_i(s)}.$$

The important result which is summarised in Theorem 2.9 is that there exists a unique number s such that ν_s maps the real Baer-plane B_0 in $PG(2,q^2)$ into the real Baer-plane of the dual of $PG(2,q^2)$. In other words, the correlation established for the points and lines of $PG(n,q^2)$ restricts naturally to a correlation between the points and lines of B_0, the real Baer-plane is $PG(2,q^2)$. Section 2.9 deals with the structure of Singer wreaths, and uses Theorem 2.9 to establish their existence. In this section it will be shown that the duality theorem can be generalised for n dimensions, and some of the consequences of this will be considered.

Let S be again the n-dimensional projective space $PG(n,q^2)$ and B_0 the real Baer-space in S. The coordinates of the points in $PG(n,q^2)$ can be successively generated by a Singer cycle determined by a suitable polynomial equation of degree n + 1 over $GF(q^2)$ (cf. Introduction):

$$x^{n+1} = c_n x^n + c_{n-1} x^{n-1} + \dots + c_0,$$

which is the characteristic equation of the (n+1) × (n+1) Singer matrix

$$M = \begin{vmatrix} c_n & 1 & 0 & 0 \\ c_{n-1} & 0 & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ c_0 & 0 & 0 & 0 \end{vmatrix} \tag{8.1}$$

The coefficients $\{c_i\}$ $(i=0,1,..,n)$ may be written in the form

$$c_i = \alpha_i + \varepsilon\gamma_i \tag{8.2}$$

where α_i, γ_i ε GF(q) and ε is a root of an irreducible quadratic equation over GF(q).

We write the matrix M as

$$M = A + \varepsilon D \tag{8.3}$$

where

$$A = \begin{vmatrix} \alpha_n & 1 & 0 & .. & 0 \\ \alpha_{n-1} & 0 & 1 & .. & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_0 & 0 & 0 & .. & 0 \end{vmatrix} \tag{8.4}$$

and

$$D = \begin{vmatrix} \gamma_n & 0 & .. & 0 \\ \gamma_{n-1} & 0 & .. & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_0 & 0 & .. & 0 \end{vmatrix} \tag{8.5}$$

Both matrices A and D belong to GF(q). Define the point p_s by

$$p_s = (\gamma_n, \gamma_{n-1}, \ldots, \gamma_0) \tag{8.6}$$

Thus $p_s \; \varepsilon \; B_0$.

Next we note that the action of the (singular) matrix D (or εD) on a column-vector representing a point $p = (x_1, .., x_{n+1})$ in $PG(n,q^2)$

results in P_s, that is the column-vector representing p_s, if $x_1 \neq 0$, or the zero-vector if $x_1 = 0$.

For, if

$$P = \begin{vmatrix} x_1 \\ \vdots \\ x_{n+1} \end{vmatrix} \qquad \text{and } P_s = \begin{vmatrix} \gamma_n \\ \vdots \\ \gamma_0 \end{vmatrix}$$

we have

$$\varepsilon DP = \varepsilon x_1 P_s.$$

The Singer cycle $\Xi = \langle\sigma\rangle$ determined by the matrix M orders the points of $PG(n,q^2)$ as follows:

$$\left.\begin{array}{l} p_0 = (0 \;\; 0 \;\; . \;\; . \;\; 0 \;\; 1) \\ p_1 = (0 \;\; 0 \;\; . \;\; . \;\; 1 \;\; 0) \\ \vdots \\ p_n = (1 \;\; 0 \;\; . \;\; . \;\; 0) \\ p_{n+1} = (c_n, c_{n-1}, \ldots, c_0) \\ \vdots \\ p_i = (x_1^{(i)} \ldots x_{n+1}^{(i)}) \\ \vdots \\ \text{(where } P_i = \begin{vmatrix} x_1^{(i)} \\ \vdots \\ x_{n+1}^{(i)} \end{vmatrix}\text{)} \\ P_{i+1} = \begin{vmatrix} x_1^{(i+1)} \\ \vdots \\ x_{n+1}^{(I+1)} \end{vmatrix} = MP_i \end{array}\right| \qquad (8.7)$$

By Singer's theorem, the <u>hyperplanes</u> of $PG(n,q^2)$, $(q^{2n+2}-1)/(q^2-1)$ in number, same as the number of points, are also ordered by the Singer cycle $PG(n,q^2)$. We may write down an ordering of the hyperplanes of $PG(n,q^2)$ in a manner similar to the ordering of the lines $PG(n,q^2)$:

h_0 is the hyperplane spanned by $p_0, p_1, \ldots, p_{n-1}$

h_1 is the hyperplane spanned by $p_1, p_2, \ldots, p_n$

and generally h_i is the hyperplane through the points $p_i, p_{i+1}, \ldots, p_{i+n-1}$.

(Since σ is a non-singular transformation, it follows that for all i, the points $p_i, p_{i+1}, \ldots, p_{i+n-1}$ are independent.)

We now define the dual Singer map ν_s by

$$\left.\begin{aligned} \nu_s(p_i) &= h_{s-i} = \overline{p_i(s)} \\ \nu_s(h_i) &= p_{s-i} = \overline{h_i(s)} \end{aligned}\right\} \tag{8.8}$$

By reasoning similarly as before, (hyperplanes taking the role of lines of the two dimensional case), we conclude that

$\overline{p_i(s)}$ is incident with $\overline{h_j(s)}$, if and only if
p_i is incident with h_j,

so the map is a correlation, Baer spaces go into dual Baer spaces.

In aiming to generalise Theorem 2.9, we prove first that if s is the Singer index of p_s as defined by (8.6), then the hyperplane h_s is real.

By the ordering of hyperplanes as in (8.7), the hyperplane h_s is determined by the points $p_s, p_{s+1}, \ldots, p_{s+n-1}$. Of these, the point p_s is real by its definition (8.6). The other points $p_{s+1}, p_{s+2}, \ldots, p_{s+n-1}$ are not necessarily real. However, we show by proceeding step by step, that the subspaces $p_s, p_{s+1}, \ldots, p_{s+n-\ell}$ where $\ell \leqslant n-1$ are all real. We begin with the line $p_s\, p_{s+1}$:

Since $p_{s+1} = \sigma p_s$, we can write

$$P_{s+1} = MP_s$$

(adapting the convention of denoting by P the column-matrix formed by the coordinates of p_s).

Using (8.3), we have

$$P_{s+1} = (A + \varepsilon D)P_s = AP_s + \varepsilon DP_s = AP_s + k_1 P_s \qquad (8.9)$$

where $k_1 \in GF(q^2)$.

Here AP_s is a column matrix with all its entries in GF(q), since the matrix A is real. Furthermore, we observe that while A is not necessarily non-singular, $AP_s \neq 0$, otherwise $P_{s+1} = P_s$ or $P_s = 0$, neither of which is possible, for no point of $PG(n,q^2)$ has all its coordinates equal to 0, and no consecutive points are equal.

We distinguish between two cases :

(i) $\gamma_n \neq 0$, that is, p_s is not in the hyperplane $x_1 = 0$. Then, by (8.9), p_{s+1} is on the line $p'p_s$, where p' is the point defined by the column-matrix AP_s, hence it is real. So the line $p'p_sp_{s+1}$ is real.

(ii) $\gamma_n = 0$. In this case, $p_{s+1} = p' \neq p_s$ and so the line p_sp_{s+1} is again real.

We proceed by induction, assuming that the space spanned by the points p_s, p_{s+1}, $p_{s+\ell-1}$ is real, where $\ell < n-1$.

We want to show that the ℓ-dimensional space determined by the $\ell+1$ points p_s, p_{s+1}, ..., $p_{s+\ell}$ (known to be independent) is again a real space.

Write again

$$P_{s+\ell} = MP_{s+\ell-1} = AP_{s+\ell-1} + \varepsilon DP_{s+\ell-1} \tag{8.10}$$

By the inductive hypothesis, $p_{s+\ell-1}$ belongs to a real, $(\ell-1)$-dimensional subspace, hence the associate column-vector is a linear combination of ℓ real vectors, denoted by

$$p^1,\ p^2,\ \ldots,\ p^\ell.$$

(Superscripts are used here instead of subscripts, which have been reserved for Singer ordering.)

Thus

$$AP_{s+\ell-1} = A\sum_{j=1}^{\ell} k_j p^j \qquad \text{where } k_j \in GF(q^2) \text{ for } j=1,\ldots,\ell.$$

Hence

$$AP_{s+\ell-1} = \sum_{j=1}^{\ell} k_j (AP^j),$$

where the column-matrices are real for $j=1,\ldots,\ell$.

So $P' = AP_{s+\ell-1}$ determines a point in a real subspace spanned by the set $\{APj \mid j=1,\ldots,\ell\}$.

(It is not necessary to ascertain here that the set $\{APj\}$ represents independent points.)

As in the case where $\ell = 2$, the second term on the right hand side of (8.10) is either zero, or a column-matrix of form $k_\ell P_s$ ($k_\ell \in GF(q^2)$. In either case $P_{s+\ell}$ is the linear combination of column-vectors belonging to B_0, hence it represents a point of an ℓ-dimensional real subspace in $PG(n,q^2)$, possibly in its extension into $PG(n,q^2)$. Since by the inductive hypothesis this applies to all P_{s+i} $(i=0,\ldots,(\ell-1))$, it follows that for all $\ell < n$, hence in particular for

ℓ = n-1, the subspace spanned by p_s, p_{s+1}, ..., $p_{s+\ell}$ is real. Thus we have proved

Lemma 3.16

Let the generating polynomial equation of the Singer cycle for $PG(n,q^2)$ be

$$x^{n+1} = c_n x^n + c_{n-1} \gamma^{n-1} + \ldots + c_0$$

Let

$$c_i = \alpha_i + \varepsilon\, \gamma_i \text{ for } i=0,1,..,n,$$

where α_i, γ_i ε GF(q) and ε ε $GF(q^2)$, being a root of an irreducible quadratic equation over GF(q).

Let s be Singer index of the point $(\gamma_n, \gamma_{n-1}, .., \gamma_0)$, and let the hyperplane h_s be determined by the points

$$p_s, p_{s+1}, \ldots, p_{s+n-1}.$$

Then h_s belongs to the real Baer space B_0. □

The hyperplane h_s is the Singer dual of the point p_0. The points p_0, p_1, ..., p_n are real and independent. We will show in the following that this is also true for their duals. We first prove the following more general lemma.

Lemma 3.17

Let h_j be a real hyperplane containing the point p_s (defined in Lemma 3.16). Then the hyperplane h_{j-1} is also real and passes through the point p_{s-1}.

Proof

Since h_j is real, the coordinates of each of its points satisfy the linear equation

$$a_1x_1 + a_2x_2 \dots + a_{n+1}x_{n+1} = 0.$$

$$a_i \in GF(q) \ (i=1,..,n+1)$$

We may represent h_j by the row-matrix

$$H_j = [a_1, a_2, \dots, a_{n+1}]$$

Similarly, represent the hyperplane h_{j-1} by the row matrix

$$H_{j-1} = [b_1, b_2, \dots, b_{n+1}]$$

The transformation σ carries all the points of H_{j-1} into points of H_j, so if $p = (x, .., x_{n+1})$ is in h_{j-1}, then $p' = \sigma p$ is in h_j. Denoting the column-vectors representing p and p' by P and P' respectively, we have

$$P' = MP,$$

so we may write in matrix form the equation of H_j:

$$H_j(MP) = 0$$

Hence for all points of H_{j-1} we have

$$(H_jM)P = 0 \qquad (8.11)$$

Thus the equation (8.11) represents the hyperplane h_{j-1}, hence

$$H_{j-1} = H_jM,$$

or

$$[b_1, b_2, \dots, b_{n+1}] = [a_1, a_2, \dots, a_{n+1}] \begin{vmatrix} c_n & 1 & 0 & 0 \\ c_{n-1} & 0 & 1 & . \\ \vdots & \vdots & \vdots & \vdots \\ c_0 & 0 & 0 & 0 \end{vmatrix}$$

It follows that

$$[b_1, b_2, \ldots, b_{n+1}] =$$
$$[c_n a_1 + c_{n-1}a_2 + \ldots + c_0 a_{n+1}, a_1, a_2, \ldots, a_n] \qquad (8.12)$$

Writing again $c_i = \alpha_i + \varepsilon\gamma_i$ $(i=0,1,\ldots,n)$ as in (8.2), the first component on the right hand side of (8.12) becomes

$$(\alpha_n a_1 + \alpha_{n-1}a_2 + \ldots + \alpha_0 a_{n+1})$$
$$+ \varepsilon(\gamma_n a_1 + \gamma_{n-1}a_2 + \ldots + \gamma_0 a_n).$$

The second term of the above expression vanishes since by assumption $p_s = (\gamma_n, \ldots, \gamma_0) \varepsilon h_j$, while the first term belongs to GF(q). The remaining components are also real, since h_j is real. From applying the Singer shift -1, it also follows that $p_{s-1} \varepsilon h_{j-1}$, since $p_s \varepsilon h_j$.

□

We apply now this lemma to the hyperplane h_s. Since it is real and contains p_s, it follows that h_{s-1} is also real. Furthermore, by applying the Singer shift,

$$h_{s-1} = p_{s-1} \quad p_s \quad \ldots, p_{s+n-2} \quad \ldots$$

so h_{s-1} also contains p_s.

We proceed in this manner until arriving to $h_{s-(n-1)} = p_{s-n+1}\ p_{s-n+2}\ \ldots, p_s\ \ldots$, still real and containing p_s, hence h_{s-n} is also real (though not containing p_s, only p_{s-1}).

We have thus found that the duals of $p_0, p_1, \ldots, p_n$ are real.

To generalise Theorem 2.9, we have to find n+2 points in B_0, not n+1 of them dependent and with real duals. This is easy, if p_s is not in any of the hyperplanes determined by any n of the n+1 points $p_0, p_1, \ldots, p_n$. Then the points $p_0, p_1, \ldots, p_n, p_s$ satisfy the condition and their duals are $h_s, h_{s-1}, \ldots, h_{s-n}$ and h_0, all real.

However, the above restrictive condition does not generally hold, so other sets of suitable real points must be considered. For this purpose we take the following set of n consecutive (hence independent) points

$$p_i,\ p_{i+1},\ \ldots,\ p_{i+n-1}$$

where

$$\left.\begin{array}{ll} p_i = (0\ \ 0\ \ .\ \ .\ \ 0\ \ a\ \ b), & \\ \text{hence} & \\ p_{i+1} = (0\ \ 0\ \ .\ \ .\ \ a\ \ b\ \ 0) & \\ \vdots & \\ p_{i+n-1} = (a\ \ b\ \ 0\ \ .\ \ .\ \ 0) & \end{array}\right| \begin{array}{l} a,b \neq 0 \\ \\ a,b \in GF(q) \\ \\ \\ \end{array} \qquad (8.13)$$

For all q we can always find at least one such set. (When q=2, there is exactly one set : $p_i = (0\ 0\ .\ 0\ 1\ 1)$ and so on.)

These points determine the hyperplane h_i, the equation of which is

$$b^n x_1 - b^{n-1} a x_2 + \ldots + (-1)^n a^n x_{n+1} = 0 \qquad (8.14)$$

To these n points we add two points: p_0 and p_n and show that any choice of (n+1) points out of this set of n+2 points forms an independent set and that their duals are real.

Equation (8.14) implies immediately that p_0 and p_n are not in h_i. Thus it is not possible to select n+1 points, consisting of the n points of h_i listed and one of p_0 or p_n so that they should be dependent. It must be shown now that we cannot select n+1 dependent points consisting of both p_0 and p_n and n-1 of the set $\{p_j\}$ (j=i,..,i+n-1).

Assume that there exists a hyperplane containing these n+1 points, its equation being

$$k_1x_1 + k_2x_2 + \ldots + k_{n+1}x_{n+1} = 0$$

Since $p_0 = (0 \ 0 \ . \ . \ 0 \ 1)$ and $p_n = (1 \ 0 \ . \ . \ 0)$ belong to the hyperplane, it follows that

$$k_1 = k_{n+1} = 0.$$

Since n-1 points of the set $\{p_j\}$ (j=1,...,i+n-1) are selected, it follows that either p_i or p_{i+n-1} is in the selected set. Since $a \neq 0$, $b \neq 0$, it follows in the first case that $k_n = 0$ and in the second case $k_2 = 0$. Continue in this manner and assume that the equation is of the form

$$k_jx_j + \ldots + k_\ell x_\ell = 0$$

where $j,\ldots,\ell$ are consecutive indices, and coefficients from k_1 to k_{j-1}, also from k_ℓ to k_{n+1} are zero. Since at least one of the points $p_{i+\ell}$ and $p_{i+n-(j-1)}$ is amongst those selected, it follows in the first case that $k_\ell = 0$ and in the second case that $k_j = 0$.

In the beginning the left hand side of the equation of the hyperplane had coefficients from k_2 to k_n, hence n-1 in number. In n-1 steps as above all (n-1) coefficients are found to be equal to zero. This shows that a hyperplane containing p_0, p_n and n-1 points of the set $\{p_i, \ldots, p_{i+n-1}\}$ cannot exist. Thus the set $\{p_0, p_n, p_i, \ldots, p_{i+n-1}\}$ satisfies the required condition.

It remains to be shown that the duals h_s, h_{s-n}, h_{s-i}, ..., $h_{s-i-n+1}$ are real.

The first two of this set of hyperplanes are already known to be real. We have to consider now the hyperplane h_{s-i}.

We find now the form of M^i, the matrix of the transformation taking p_0 to p_i.

Since

$$p_0 = (0 \quad 0 \quad . \quad . \quad 1) \text{ goes to } p_i = (0 \quad 0 \quad . \quad . \quad a \quad b)$$

$$p_1 = (0 \quad . \quad . \quad 1 \quad 0) \text{ goes to } p_{i+1} = (0 \quad . \quad . \quad a \quad b \quad 0)$$

$$\vdots$$

$$p_{n-1} = (0 \quad 1 \quad . \quad . \quad 0) \text{ goes to } p_{i+n-1} = (a \quad b \quad . \quad . \quad 0)$$

the matrix M^i has for its last n columns

$$\begin{vmatrix} a \\ b \\ \vdots \\ 0 \end{vmatrix}, \begin{vmatrix} 0 \\ a \\ b \\ 0 \end{vmatrix}, \ldots, \begin{vmatrix} 0 \\ 0 \\ a \\ b \end{vmatrix}$$

respectively. (Each column may be multiplied by some constant.)

To find the first column, consider

$$M^i P_n, \quad \text{where } P_n = \begin{vmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{vmatrix}$$

and

$$\sigma^i p_n = \sigma\, p^{i-1} p_n = \sigma p_{n+i-1}$$
$$= \sigma(a,\ b,\ \ldots,\ 0).$$

So,

$$M^i P_n = M \begin{vmatrix} a \\ b \\ \vdots \\ 0 \end{vmatrix} = (A+\varepsilon D) \begin{vmatrix} a \\ b \\ \vdots \\ 0 \end{vmatrix},$$

making use of (8.3).

$A \begin{vmatrix} a \\ b \\ 0 \\ \vdots \\ 0 \end{vmatrix}$ is a real column vector, while $\varepsilon D \begin{vmatrix} a \\ b \\ 0 \\ \vdots \\ 0 \end{vmatrix} = kP_s$, where P_s is the column vector determined by the coordinates of p_s, and $k \in GF(q^2)$.

To find h_{s-i}, write

$$H_{s-i} = H_s M^i, \tag{8.15}$$

where H_s and H_{s-1} are row vectors representing the coefficients in the linear equations of h_s and h_{s-1}.

From the calculations above it follows that

$$M^i = A' + kD$$

where A' is a matrix transforming p_0, p_1, ..., p_{n-1} inter p_i, p_{i+1}, ..., p_{i+n-1} respectively, while transforming p_n into the point represented by the real column

$$A\begin{vmatrix} a \\ b \\ 0 \\ \vdots \\ 0 \end{vmatrix}.$$

Thus A' is a real matrix, D is the matrix defined before, having p_s as its first column and 0 for all the other entries. H_s is the real row-vector $[d_1, d_2, \ldots, d_{n+1}]$, and since h_s contains the point p_s, it follows that

$$d_1\gamma_n + d_2\gamma_{n-1} + \ldots + d_{n+1}\gamma_0 = 0,$$

So (8.15) becomes

$$H_{s-i} = H_s(A'+kD) = H_sA',$$

which is a row-vector belonging to GF(q), since H_s and A' are both real.

Hence h_{s-i} is a real hyperplane, as claimed. Moreover, it follows from the duality mapping that

$p_s \varepsilon h_{s-i}$,

since $p_i \varepsilon h_0$, and p_s is the dual of h_0, while $p_i = p_{s-(s-i)}$ is the dual of h_{s-i}.

We apply now Lemma 3.17 (n-1) times; since by (8.13) the points p_i, p_{i+1}, ..., p_{i+n-2} all belong to h_0, so their duals h_{s-i}, h_{s-i-1}, ..., $h_{s-i-n+1}$ all contain p_s.

Thus the hyperplanes h_{s-i}, h_{s-i-1}, .., $h_{s-i-n+1}$, are all real.

This completes the generalisation of Theorem 2.9 for n dimensions. We may also note that the choice of the point p_s is unique by the same argument as used in Section 2.6.

We summarise this now as the General Duality Theorem:

Theorem 3.18

Let B_0 be the real Baer space in $PG(n,q^2)$. Define the duality map v_s between the points and hyperplanes of $PG(n,q^2)$ as in (8.8). A unique number s can be found such that v_s maps n+2 points of B_0, no n+1 of them dependent, into n+2 hyperplanes belonging to B_0.

Corollary

A unique number s exists such that the duality map v_s maps the real Baer space of $PG(2,q^2)$ into itself.

3.9 Applications of the Singer Duality Theorem

a. The Singer Wreath

Note: The Singer group $\Xi = \langle\sigma\rangle$ is here, as in the previous section $\Xi = \langle\sigma_{q^2}\rangle$, the cyclic group acting regularly on the points of $PG(n,q^2)$, so the subscript q^2 is dropped in the following discussions. We consider the action of Ξ on B_0. Each Singer image of B_0 is a Baer space.

Theorem 3.19

The set of Singer images of B_0 contains a subset of q(q+1) Baer spaces, called the Singer Wreath : W_Ξ (belonging to Ξ). It has the following properties:

(i) each Baer space belonging to W_Ξ intersects B_0 in $(q^n-1)/(q-1)$ points of a hyperplane of $PG(q^2)$ and possibly another point outside this hyperplane.

(ii) the set W_Ξ falls into q+1 classes, each containing q Baer-spaces, such that the Baer-spaces belonging to one class have $(q^n-1)/(q-1)$ points of a hyperplane common with B_0.

(iii) the set W_Ξ falls into q+1 classes, each containing q Baer-spaces belonging to one class intersect in a point P of B_0, and each of the $(q^n-1)/(q-1)$ real hyperplanes through P belongs to all the Baer-spaces of the class, that is: each hyperplane through P containing $(q^n-1)/(q-1)$ points of B_0, has also $(q^n-1)/(q-1)$ points in common with each Baer-space of the class.
(Note: the intersections of each of the above hyperplanes with the above Baer-spaces of the class are different sets.)

Proof

Recall that in the previous section hyperplanes of the following type were considered:

$$h_i = p_i, p_{i+1}, \dots, p_{i+n-1}, \dots$$

where

$$\left.\begin{array}{l} p_i = (0 \quad 0 \quad . \quad . \quad t \quad 1) \\ p_{i+1} = (0 \quad 0 \quad . \quad . \quad t \quad 1 \quad 0) \\ \quad \vdots \\ p_{i+n-1} = (t \quad 1 \quad 0 \quad . \quad . \quad 0 \quad 0) \end{array}\right| \qquad (9.1)$$

where

$$t \in GF(q).$$

Each of the hyperplanes of this type has equation:

$$x_1 - tx_2 + \ldots + (-1)^n t^n x_n = 0.$$

Since there are q choices for t, we obtain q hyperplanes of this type. In particular, for t = 0 we have

$$h_0 = p_0, p_1, \ldots, p_{n-1}, \ldots$$

with equation $x_1 = 0$.

Let $H^* = \{h_i\}$ where the h_i hyperplanes are defined by (9.1), together with

$$h_1 = p_1, p_2, \ldots, p_n, \ldots$$

where $p_1 = (0 \quad 0 \quad . \quad . \quad 1 \quad 0)$.

Each of the hyperplanes of H^* is real, hence it has $(q^n-1)/(q-1)$ points belonging to B_0. Furthermore, by Theorem 3.18, the Singer dual of h_i, the point p_{s-i} is also real, where s is defined by (8.6).

Let $h_i \in H^*$ and let $p \in h_i \cap B_0$. Then, using (9.1), we have

$$\left.\begin{array}{l} p = \sum_{k=0}^{n-1} a_k p_{i+k} = (a_{n-1}, a_{n-i}, \ldots, a_0, 0) \text{ for } i = 1 \\ \text{and} \\ \quad = (a_{n-1}t, a_{n-2}t + a_{n-1}) \ldots (a_0 t + a_1), a_0) \end{array}\right| \qquad (9.2)$$

otherwise.

Let a_ℓ be the first non-zero coefficient on the left hand side of (9.2), i.e.

$$0 \leq \ell \leq n-1,\ a_\ell \neq 0, \text{ and for } 0 \leq k < \ell,\ a_k = 0.$$

Then a_ℓ can be chosen arbitrarily, ($a_\ell \neq 0$), but once the choice is made for some fixed point p, the remaining coefficients are uniquely defined. Choosing $a_\ell = 1$, the remaining coefficients must belong to GF(q) as $p \in B_0$.

Let $h_j \in H^*$, $j \neq i$. Then

$$\sigma^{j-i} p_i = p_j$$

$$\vdots$$

$$\sigma^{j-i} p_{i+n-1} = p_{j+n-1},$$

hence h_j is the $(j-i)^{th}$ Singer image of h_i. Moreover, all the points in $h_i \cap B_0$ are transformed into points of $h_j \cap B_0$ by σ^{j-i}. This is so, because

$$\sigma^{j-1}(a_0 p_i + a_1 p_{i+1} + \dots + a_{n-1} p_{i+n-1})$$

$$= a_0 p_j + a_1 p_{j+1} + \dots + a_{n-1} p_{j+n-1}.$$

(Note: Here σ^{j-i} has been treated as a linear transformation. This is justified within the range considered here.)

Define also

$$P^* = \{p_{s-i}\} \text{ where } h_i \in H^*.$$

Through each point $p_{s-i} \in P^*$ there is a set of $(q^n-1)/(q-1)$ hyperplanes, which are the duals of the points of $h_i \cap B_0$, hence they are hyperplanes of B_0. If p_{s-i} and p_{s-j} both belong to P^*, they can be treated as dual hyperplanes $\overline{h_i(s)}$ and $\overline{h_j(s)}$, with the hyperplanes through p_{s-i} and p_{s-j} as dual points $\overline{p(s)}$. So the conclusion reached earlier for the hyperplanes of H^* implies also that

all the hyperplanes containing p_{s-i} and belonging to B_0 go by the transformation σ^{i-j} into hyperplanes through $\sigma_{i-j}p_{s-i} = p_{s-j}$ and belonging to B_0.

Next apply the transformation σ_{j-i} to the entire Baer space B_0, where i and j are as defined above.

Let $B_{ij} = \sigma_{j-i}B_0$. Then B_{ij} is a Baer space. Since $h_i \in B_0$, it follows that $\sigma_{j-i}h_i = h_j$ is in B_{ij}. Moreover, the transformation σ^{j-i} takes all the points of $B_0 \cap h_i$ into points of $B_0 \cap h_j$ by the previous result. On the other hand,
$\sigma^{j-i}(B_0 \cap h_i) = \sigma^{j-i}B_0 \cap \sigma^{j-i}h_i = B_{ij} \cap h_j$. Hence it follows that B_{ij} shares with B_0 all the points of $B_0 \cap h_j$.

The transformation σ^{j-i} takes also the point p_{s-j} of B_0 together with all the hyperplanes through that point, belonging to B_0 into the point p_{s-i} in B_{ij} together with the hyperplanes through p_{s-i} and belonging to B_{ij}. From dual considerations, this point together with the above set of hyperplanes through it belongs also to B_0. Thus

B_{ij} shares with B_0 the point p_{s-i} and $(q^n-1)/(q-1)$ hyperplanes through p_{s-i}.

Since the set H^* consists of q+1 hyperplanes, there are (q+1)q ordered pairs of indices which determine (q+1)q Baer spaces of type B_{ij}, where $i \neq j$.

Fix first j and let i run through all the indices in $H = \{h_i\}$ and diffent from j. There are q Baer spaces of type B_{ij}, all sharing pointwise with B_0 the hyperplane h_j. Since there are q+1 choices for j, we obtain q+1 classes of Baer spaces, q in each class, sharing with B_0 $(q^n-1)/(q-1)$ points of a hyperplane.

Next fix i and let j run through all values of j in $P^* = \{p_{s-j}\}$ so that $j \neq i$. There are again q Baer spaces of type B_{ij}, all intersecting B_0 in the point p_{s-i} and also sharing with B_0 $(q^n-1)/(q-1)$ hyperplanes through p_{s-i}. With q+1 choices for i we obtain q+1 classes of Baer spaces, q in each class, sharing with B_0 a point and $(q^n-1)/(q-1)$ hyperplanes through the point.

This completes the proof of Theorem 3.19. □

b. An interpretation of Theorem 3.3

This theorem states that the number of points belonging to the intersection of two Baer spaces is the same as the number of hyperplanes. In [11] Bruen has also proved that the structures of the point-set and the hyperplane-set of the intersection are "isomorphic". In the terms used earlier in this chapter, this means that the dual of the set of hyperplanes belonging to the intersection of two Baer spaces forms a Baer-complex isomorphic to the complex determined by the set of points of intersection (that is), a structure preserving map can be found from one complex to the other. The Singer duality theorem provides a simple, natural interpretation of this result in the case when the two Baer spaces belong to the same Singer orbit.

Without loss of generality, we may then assume that the two Baer spaces are B_0 and B_t, the real Baer space and its σ^t transform. Denote by

$P = \{p_i\}$

the set of points of $B_0 \cap B_t$. Then for each $p_i \in P$, hence in B_t,

$p_{i-t} \in B_0$.

By the duality theorem $h_{s+t-i} \in B_0$, where s is defined by (8.6). Since p_i is also in B_0, it follows from the duality theorem that $h_{s-i} \in B_0$, hence by applying the transformation σ^t, $h_{s+t-i} \in B_t$.

Thus for each $p_i \in B_0 \cap B_t$, we have $h_{s+t-i} \in B_0 \cap B_t$.

The reasoning can also be carried out conversely : for each $h_j \in B_0 \cap B_t$, $p_{s+t-j} \in B_0 \cap B_t$.

Thus the number of points and number of hyperplanes belonging to the intersection of B_0 and B_t is the same.

Furthermore, the isomorphism of the two structures also follows. For let again

$P = \{p_i\}$.

Denote $P' = \{p_{i-t}\}$.

Then $P \cong P'$, since the Singer transformation is a homography.

Let $H = \{h_{s+t-i}\}$.

Then there is a correlation between P' and H, since the Singer duality preserves incidences.

Thus $H \cong P' \cong P$.

Since H represents by the above the hyperplane set belonging to $B_0 \cap B_t$, it follows that the point-structure and the hyperplane structure are isomorphic. This simple interpretation of the isomorphism of the point and hyperplane-structures of the intersection of two Baer-spaces can be extended to any pair of Baer-spaces, if the following conjecture holds.

Conjecture

For each pair of Baer-spaces B_1 and B_2 in $S = PG(n,q^2)$ some Singer group

$$\Xi_{q^2} = \langle\sigma\rangle_{q^2}$$

can be found such that

$$B_2 = \langle\sigma\rangle^i B_1$$

Facts supporting this conjecture:

Without loss of generality one of the spaces can be taken to be B_0.

The following can be established:

(i) A Singer group Ξ is its own centraliser : $Z(\Xi)$.

Proof

Let $\Xi = \langle\sigma\rangle$ act regularly on the points of S, inducing an ordering

$$p_0, p_1, \ldots, p_i, \ldots, p_\ell$$

where $\ell = |S| - 1 = (q^{2n+2}-1)/(q^2-1) - 1$.

Let $\tau \in Z(\Xi)$. Then $\tau\sigma = \sigma\tau$.

For the point p_i

$$\tau\sigma(p_i) = \tau(\sigma p_i) = \tau p_{i+1} = p_j,$$

then $\sigma(\tau p_i) = p_j$, so $\tau p_i = \sigma^{-1} p_i = p_{j-1}$.

Hence for two consecutive points p_i, p_{i-1},

$$\tau p_i = p_{j-i}, \quad \tau p_{i+1} = p_j$$

for an arbitrary point p_i.

Hence the action of τ causes a uniform shift in the Singer indices of the points of S

$$k = j - (i-1)$$

so $\tau = \sigma^k \in \Xi$.

(ii) The index of the centraliser of Σ in the normaliser of Ξ is n+1.

<u>Proof</u>

The result is a straight generalisation of Lemma 2.13 in Chapter 2. Denote the normaliser of Ξ:

$$N(\Xi) = N(Z).$$

Let $\rho \in N$, then $\rho^{-1} \sigma\rho = \sigma^r$.

By reasoning identical to that in Chapter 2 (Lemma 2.13), we obtain that

$$r = 1, q, q^2, .., q^n.$$

Hence r takes n+1 possible values. Furthermore, suppose that

$$(\rho')^{-1}\sigma\rho' = \sigma^r,$$

that is

$$(\rho')^{-1}\sigma\rho' = \rho^{-1}\sigma\rho$$

or

$$(\rho'\rho^{-1})^{-1}\ \sigma\rho'\rho^{-1} = \sigma$$

So $\rho'\rho^{-1} \in Z(\Xi)$ or ρ, ρ' belong to the same coset of Z in N. Hence the choice of r fixes the coset. Thus the index of $Z(\Xi)$ or of Ξ in N is n+1.

(iii) It follows from here that the number of conjugates of Ξ in the group of homographies Γ of $PG(n,q^2)$ is

$$\frac{|\Gamma|}{(n+1)|\Xi|}.$$

(iv) The intersection of two conjugate, distinct Singer groups cannot contain a primitive element of either group, since a primitive element determines the whole group.

As the number of primitive elements of the cyclic group is $\phi(|\Xi|)$, (where ϕ is the Euler-function giving the number of positive integers less than $|\Xi|$ and co-prime to it), it follows that there are at least

$$\phi(|\Xi|)\frac{|\Gamma|}{(n+1)|\Xi|}$$

distinct homographies, each belonging to some Singer group, which take B_0 to some Baer-space $|B|$.

Since the number of Baer-spaces is

$$N = \frac{|\Gamma|}{|\Gamma_0|},$$

where Γ_0 is the group of homographies of PG(n,q) it follows that

<u>on the average</u> there are <u>at least</u>

$$\frac{\phi(|\Xi|)}{|\Xi|}\,\frac{|\Gamma|}{n+1} \Big/ \frac{|\Gamma|}{|\Gamma_0|}$$

$$= \frac{\phi(|\Xi|)|\Gamma_0|}{|\Xi|(n+1)}$$

homographies taking B_0 to some Baer-space B and belonging to some Singer cycle.

However, this cannot be taken to be a proof of the conjecture, since at this stage it is not shown that these homographies are distributed with some measure of uniformity amongst the various Baer-spaces in $PG(n,q^2)$.

APPENDIX

COMPUTER WORK ON FINITE PROJECTIVE GEOMETRY

In elementary geometry or number theory theorems can be found by experimentation. Calculations or drawings point to some facts which are first conjectured and then established by formal proofs. Similarly, most results proved in this work were first conjectured through computer aided experimentation. Some of the results turned out to be known ones and can be found in the literature published somewhat earlier, others were found simultaneously by other researchers, while some results are believed to be still new. The significance of the computer programs evolved and to be described in the following is, that they give "visibility" to finite projective spaces, by listing and surveying their elements: points, lines, subspaces, Baer spaces with their intersection properties. They should be useful for further research in finding new facts or eliminating false conjectures.

The cyclic structure of projective spaces of dimension greater than two and of projective planes over Galois fields provides the main tool for the survey to be described. Singer's theorem, discussed in the introduction, is used to generate, in succession, the coordinates of the points of PG(n,q), finding at the same time the hyperplanes (or, alternatively, perfect difference sets in GF(q)). In particular, since this present research has focused on Baer spaces, q was chosen to be a perfect square.

To achieve results in limited computing time, small values of n and q^2 were used. In the case of projective planes, the value of q ranged from 2 to 8, that is, planes over GF(4), GF(9), GF(16), GF(25), GF(49) and GF(64) were surveyed. The programs were dimensioned for the above range, but results in PG(2,9) and PG(2,16) already give sufficient insight, the higher values of q were used only in the beginning to confirm the findings. For $n=3$, $q^2=4$, 9, 16, and 25 were used, while for $n=4$ and 5 the only value of q^2 was 4.

The first step in the procedure was to find the generating polynomial equation

$$x^{n+1} = c_n x^n + c_{n-1} x^{n-1} + \dots + c_0 \qquad (n=2,3,4,5) \tag{1.1}$$

as described in [19], (pp.130). The equation used must be irreducible over $GF(q^2)$. It is suitable for our purpose if its roots are primitive elements of $GF(q^{2(n+1)})$, though this condition is not necessary.

The coefficients c_i $(i=0,1,..,n)$ in (1.1) are of the form

$$c_i = \alpha^{\gamma_i} \tag{1.2}$$

where α is a root of an irreducible quadratic equation over $GF(q)$ and γ_i is a natural number belonging to the set $\{1,2,..,(q^2-1)\}$, or $c_i = 0$.

(We will refer to γ_i as the logarithm of c_i.) Thus the numbers c_i are elements of $GF(q^2)$, where $\alpha^{q^2-1} = 1$.

For the low values of q used, it is easy to find an irreducible equation over $GF(q)$, but finding a suitable generating polynomial equation (1.1) is left to the computer: a set of $n+1$ integers is used in determining the coefficients c_i, reading in 0 for $c_i = 0$, or the logarithm γ_i in (1.2) if c_i is non-zero. If the vector $(0, 0, .., 0, t)$ where $t \neq 0$, is reached by the program in less than $(q^{2(n+1)}-1)/(q^2-1)$ steps, then the calculation is aborted, and another set of $(n+1)$ integers is read in to define the equation (1.1).

A few simple rules are obeyed to avoid some unnecessary computations:

(i) $c_0 \neq 0$, otherwise the polynomial in (1.1) is reducible.

(ii) c_0 cannot be the <u>only</u> non-zero coefficient on the right hand side of (1.1), (0, 0, .., t) in n+1 steps.

(iii) To obtain preferably a primitive root, γ_0, the logarithm of c_0 in (1.2) must not be a multiple of q+1.

For then c_0 belongs to the subfield GF(q). In that case equation (1.1) cannot have a primitive element of $GF(q^{2(n+1)})$ for a root. (Suppose ζ is a root, then the product of ζ and its conjugates over $GF(q^2)$ gives $\zeta^{1+q^2+\ldots+q^{2n}} = (-1)^n c_0$. since $((-1)^n c_0)^{2(q-1)} = 1$, it follow that $\zeta^{2(1+q^2+\ldots+q^{2n})(q-1)} = 1$, so ζ is not primitive.)

Even if rules (i), (ii) and (iii) are adhered to, there is no guarantee that the polynomial thus defined yields the set of points of $PG(n,q^2)$. However, polynomials were eliminated in negligibly small computing time.

At the time when the programs were developed, there were no packages of Galois-field calculations known to the author, so the next step in the program was to establish a Galois-field addition table, (multiplication table is not needed, as it is done simply by adding $\bmod(q^2-1)$ the logarithms of the non-zero elements of $GF(q^2)$).

To construct the addition table, the elements of $GF(q^2)$ are represented by their logarithms. One thing to be watched in the field calculations is the role of the element 0, which is not represented as a power of the primitive element. The number 0 is not used as an exponent. Instead, the logarithm representing 1 is written as (q^2-1). Hence in the entries of the addition table, the number 0 represents the 0 element of the field, while the non-zero entries stand for the logarithms of the other field elements.

The first row of the addition table is obtained by hand-calculation and read in to the computer. The primitive element α used is a root of the quadratic

$$\alpha^2 = kd + \ell \qquad (1.3)$$

where k, $\ell \in GF(q)$ and the equation is irreducible over GF(q). The powers of α are evaluated in the form:

$$\alpha^i = h'\alpha + \ell' \quad (h', \ell' \in GF(q))$$

and so all sums $\alpha + \alpha^i$ are expressed in the form α^γ. Illustrate this procedure in GF(9)

$\alpha^2 = -\alpha + 1$ is irreducible over GF(3).

Then

$$\alpha^3 = -\alpha^2 + \alpha = -\alpha - 1$$

$$\alpha^4 = -\alpha^2 - \alpha = -1$$

$$\alpha^5 = -\alpha$$

$$\alpha^6 = -\alpha^2 = \alpha - 1$$

$$\alpha^7 = \alpha^2 - \alpha = \alpha + 1$$

$$\alpha^8 = \alpha^2 + \alpha = 1$$

Thus we have:

$$\alpha + 0 = \alpha = \alpha'$$

$$\alpha + \alpha' = -\alpha = \alpha^5$$

$$\alpha + \alpha^2 = 1 = \alpha^8$$

$$\alpha + \alpha^3 = -1 = \alpha^4$$

$$\alpha + \alpha^4 = \alpha - 1 = \alpha^6$$

$$\alpha + \alpha^5 = 0$$

$$\alpha + \alpha^6 = -\alpha - 1 = \alpha^3$$

$$\alpha + \alpha^7 = -\alpha + 1 = \alpha^2$$

$$\alpha + \alpha^8 = \alpha + 1 = \alpha^7$$

So the numbers in the first row of the Galois addition table for GF(q) are:

1 5 8 4 6 0 3 2 7

The rest of the addition table is established by the computer using

(i) symmetry, i.e. $\alpha^i + \alpha^j = \alpha^j + \alpha^i$

(ii) $0 + \alpha^i = \alpha^i + 0 = \alpha^i$

(iii) $\alpha^i + \alpha^i = 0$ if q is even, and

$\alpha^i + \alpha^{i+\frac{1}{2}(q-1)} = 0$ if q is odd.

(iv) $\alpha^{i+1} + \alpha^{j+1} = \alpha(\alpha^i + \alpha^j)$

(Property iv means that entries read diagonally in the table, (excluding the 0 diagonal) follow the natural (cyclic) order.)

The introductory part of each program used can then be described as follows:

Step (i) The value of q is read in.
(The field used is generally $GF(q^2)$).

Step (ii) The Galois addition table of the field is established.
(This table depends on the original irreducible quadratic over $GF(q^2)$.)

Step (iii) The Singer algorithm is used

(a) to find successively the coordinates of the points of $PG(n,q^2)$.

(b) to determine the hyperplane $x_1 = 0$.

Whenever the first coordinate of the point found is 0, the Singer index of the point is stored. The set of Singer indices thus obtained gives a perfect difference set. In terms of block-designs, this is a (v,k,λ)-difference set where

$$v = \frac{(q^2)^{n+1}-1}{q^2-1}, \quad k = \frac{(q^2)^n-1}{q^2-1}, \quad \lambda = \frac{(q^2)^{n-1}-1}{q^2-1}.$$

(c) to determine the real points of PG(n,q^2), that is, the points of which the coordinates belong to the subfield GF(q). This is done by testing whether the ratios of the non-zero coordinates belong to GF(q). This is the case, if the differences of their logarithms are multiples of q+1. The indices of the real points are also stored. The set of real points determines the real Baer-space of PG(n,q^2).

As mentioned before, results are printed out and the program is used for further survey only if the full Singer cycle of $(q^{2n+2}-1)/(q^2-1)$ steps is completed.

Two programs together with outputs are attached to the work to give a sample. The language used is Pascal and the programs were executed on the VAX/VMS of the University of Adelaide.

The first of the two programs is used for finding either the real hyperplanes of PG(n,q^2) (that is, all those hyperplanes which share $(q^n-1)/(q-1)$ points with the real Baer-space), or all the Baer spaces strongly intersecting the real Baer space, that is sharing a hyperplane (and possibly another point) with the real Baer space. This program is dimensioned as high as PG(4,9) or PG(5,4).

The second program is used in three dimensions only, and has three alternative uses :

(i) determining real planes,

(ii) strongly intersecting spaces,

(iii) the real lines in PG($3,q^2$).

The listing of real lines is useful for survey work, but the program is not as straightforward as the listing of the planes, which can be obtained by using successively the Singer transformation on the plane $x_1 = 0$, or the listing of the Baer spaces belonging to the same Singer orbit.

An ordering of the real lines is obtained by listing first those lines which contain 2 points with difference 1 in their Singer indices, next those where the minimum difference is 2, and so on. The lines are obtained as intersections of two planes passing through the two fixed points investigated.

An important step in the program is checking that no repetition of the lines occurs. Full listings were done in PG(3,4), PG(3,9) and PG(3,16). For higher values of q the computing time becomes excessive.

In the outputs, points and hyperplanes are listed by their Singer indices. However, for some purposes the listing of the coordinates of the points is also desirable, in particular, for the points of the real subspace. The listing is done in a condensed form: non-zero coordinates are given by their logarithms and the zero coordinates by the number zero. The whole information about the coordinate of a point is then written in the form of a positive integer in the decimal system. Two examples show then how to read the information.

Example 1 : 2 0 2 0 6 0 6 in PG(3,9)

represents $P = (\alpha^2, \alpha^2, \alpha^6, \alpha^6)$

equivalent to $(\alpha^8, \alpha^8, \alpha^4, \alpha^4) = (1, 1, -1, -1)$ over GF(9).

The point belongs to PG(3,3).

Example 2 : 1 3 0 8 0 0 0 8 in PG(3,16)

represents $P = (\alpha^{13}, \alpha^8, 0, \alpha^8)$

$= (\alpha^{15}, \alpha^{10}, 0, \alpha^{10}) = (1, \alpha^{10}, 0, \alpha^{10})$

where $\alpha^{10} \varepsilon$ GF(4). Here $\alpha^2 = \alpha + \delta$ (where $\delta^2 = \delta + 1$ (over GF(2)).

REFERENCES

[1] Andre, J. 1954
"Uber nicht-Desargessche Ebenen mit transitiver Translationsgruppe
Math. Zeitschr. 60, pp.158-186.

[2] Andrews, G.E. 1976
The Theory of Partitions.
Enc. of Mathematics and its Applications.

[3] Baer, R. 1942
Homogeneity of projective planes.
Amer.J.Math. 64, pp.137-152.

[4] Baer, R. 1947
Projectivities in finite projective planes.
Amer.J.Math. 69, pp.653-684.

[5] Baer, R. 1952
Linear Algebra and Projective Geometry.
Academic Press, New York.

[6] Barnabei, M., Searby, D. and Zucchini, C. 1976
On small (k;q)-arcs in Planes of order q^2.
pp.241-246.

[7] Bender, E.A. 1971
A Generalized q-binomial Van der Monde Convolution.
Discrete Mathematics 1. pp.115-119.

[8] Bender, E.A. - Goldman, J.R. 1975
On the Applications of Mobius Inversion in Combinatorial Analysis.
Amer.Math.Monthly 82. pp.789-802.

[9] Beutelspacher, A. 1983
On Baer Subspaces of Finite Projectice Spaces
Math. Zeitschrift 184, pp.301-319.

[10] Bose, R.C. - Freeman, J.W. - Glynn, D.G. 1980.
On the Intersection of two Baer Subplanes in a Finite Projective Plane.
Utilitas Mathematica 17. pp.65-77.

[11] Bruen, A.A. 1982
Intersection of Baer Subgeometries.
Arch.Math. 39.

[12] Bruck, R.M. 1960
Quadratic Extensions of Cyclic Planes
Proc. Symp.Appl.Math.10, pp.15-44.

[13] Carmichael, R.D. 1937
Introduction to the Theory of Groups of Finite Order.
Reprint Dover, New York, 1956.

[14] Cofman, J. 1972
Baer Subplanes in Finite Projective and Affine Planes.
Can.J.Math. 24, pp.90-97.

[15] Dembowski, P. 1968
Finite Geometries.
Springer-Verlag. Ergebnisse 44.

[16] Goldman, J. - Rota, G.C. 1970
On the Foundations of Combinatorial Theory iv. Finite Vector Spaces and Eulerian Generating Functions (Studies in App.Math. 49, pp.239-258).

[17] Hall, M. 1943
Projective Planes.
Trans.Amer.Math.Soc. 54, pp.229-277.

[18] Hall, M. 1947
Cyclic Projective Planes
Duke Math.J. 14, pp.1079-1090.

[19] Hall, M. 1967
Combinatorial Theory, Blaisdell.

[20] Hirschfeld, J.W.D. 1979
Projective Geometries over Finite Fields.
Oxford Mathematical Monographs.

[21] Hughes, D.R. - Piper, F.C. 1973
Projective Planes.
Springer-Verlag, Graduate Texts.

[22] Ostrom, T.G. 1971
Finite Translation Planes
Springer-Verlag. Lecture notes in mathematics.

[23] Riordan, J. 1958
An Introduction to Combinatorial Analysis
John Wiley.

[24] Room, T.G. - Kirkpatrick, P.G. 1971
Miniquaternion Geometry.
Cambridge U.P.

[25] Rota, G.C. 1964
On the Foundations of Combinatorial Theory 1
(Z.Wahrscheinlichkeitslehre)

[26] Segre, B. 1960
Lectures on Modern Geometry
Ed. Cremonese (Mon.Mat.)

[27] Singer, J. 1938
A theorem in finite projective geometry and some applications to number theory.
Trans.Amer.Math.Soc. 43, pp.377-385.

[28] Sved, M. 1981
On configurations of Baer subplanes of the projective plane over GF(q^2).
Combinatorial Math.Proc. Brisbane, Australia, pp.423-443.

[29] Sved, M. 1982
Baer subspaces in the n dimensional projective space.
Combinatorial Math.Proc., Adelaide, pp.375-391.

[30] Sved, M. 1984
Gaussians and Binomials.
Ars Combinatorica 17A, pp.325-351.

[31] Van der Waerden, B.L.
Modern Algebra (1964 printing)
Vol.1, Fred. Ungar, New York.

[32] Veblen, O. - Wedderburn, J.H.M. 1907
Non-Desarquesian and non-Pascalian Geometries.
Trans.Amer.Math.Soc. 8, pp.379-388.

[33] Vedder, K. 1981
A note on the intersection of two Baer subplanes.
Arch.Math. 37, pp.287-288.

[34] Wedderburn, J.H.M. 1905
A theorem on finite algebras.
Trans.Amer.Math.Soc. 6, pp.349-352.

[35] Yaqub, J.C.D.S. 1967
The Lenz-Barlotti Classification.
Proc.App.Geom. Cont. Illinois, pp.129-160.

[36] Yff, P. 1974
On Subplane Partitions of a Finite Projective Plane.
Journal of Comb.Theory A (22), pp.118-122.

[37] B. Huppert - Blackburn, N. 1982
Finite Groups.
Springer.

A D D E N D U M

COMPUTER PRINTOUTS

PROGRAM HIDIM

OUTPUT 1

PG (3, 16)

GENERATING POLYNOMIAL 15 15 0 1

$(x^4 = x^3 + x^2 + \alpha$

where $\alpha^4 + \alpha + 1 = 0$ over GF(2).)

BAER - SPACES STRONGLY INTERSECTING B_o

(SINGER WREATH)

OUTPUT 2

PG (5, 4)

GENERATING POLYNOMIAL 1 0 0 0 1 1

$x^6 = \alpha (x^5 x + 1)$

where $\alpha^2 + \alpha + 1 = 0$ over GF(2)

SINGER WREATH

```
PROGRAM  HIDIM   (input,output);
         {GENERATION OF POINTS IN PG( n, qs }
var      i,q,salw,j,jp,qs,j1,temp,qfh,lot,k,l,m,n,r,h,
         dim,dip,dhy,lea,ir,nob,nop,com,zrc : integer;
         ind: array[0..5] of integer;
         diff,pla,sta: array[1..821] of integer;
         grof,rel: array[1..156] of integer;
         cof,term,vect,v: array[1..6] of integer;
         saladd: array[0..24,0..24] of integer;
begin
       writeln('        SURVEY OF POINTS,HYPERPLANES, BAER SPACES')
       for i:=1 to 6 do
         begin
          writeln('  ')
         end;
      {Establishing addition table for the Galois field}
       saladd[0,0]:=0;
       read(q,dim);
       qs:=sqr(q);
       writeln(' PROJECTIVE SPACE: PG(',dim,qs,')');
       salw:=qs-1;
       for j:=1 to salw do
        begin
         read(saladd[1,j])
        end;
       if q mod 2 =0 then
        begin
         l:=salw-1;
          for j:=2 to l do
           begin
            saladd[j,j]:=0;
            jp:=j+1;
            for k:=jp to salw do
             begin
              temp:=saladd[j-1,k-1]+1;
              if temp=qs then
              saladd[j,k]:=1 else
              saladd[j,k]:=temp
             end;
            end;
            saladd[salw,salw]:=0;
          end                else
          begin
           qfh:=salw div 2;
           for j:=2 to salw do
            begin
             for k:=j to salw do
              begin
               if (k-j)=qfh then
               saladd[j,k]:=0   else
                begin
                 temp:=saladd[j-1,k-1]+1;
                 if temp=qs then
                 saladd[j,k]:=1 else
                 saladd[j,k]:=temp
                end;
              end;
             end;
           end;
           for j:=2 to salw do
            begin
             j1:=j-1;
             for k:=1 to j1 do
```

```
            begin
             saladd[j,k]:=saladd[k,j]
            end;
           end;
         for j:=1 to salw do
          begin
           saladd[0,j]:=j;
           saladd[j,0]:=j
          end;
      read(ir);
      if ir=1 then
       begin
     writeln('                  ADDITION TABLES IN GF(',q, ')');
     for j:=0 to salw do
      begin
       for k:=0 to salw do
        begin
         write(saladd[j,k]:3);
        end;
       writeln('  ')
      end;
      for j:=1 to 4 do
       begin
        writeln('  ');
       end;
      end;
 {Addition table established }
     dip:=dim+1;
     dhy:=dim-1;
     lot:=1;
     for n:=1 to dim do
      begin
       lot:=qs*lot+1
      end;
     for n:=1 to dip do
      begin
       read (cof[n])
      end;
       writeln('  ');
     writeln(' COEFFICIENTS OF GENERATING EQUATION DEFINED BY');
     for n:=1 to dip do
      begin
       write (cof[n]:6);
      end;
     writeln;
     for j:=1 to 4 do
      begin
       writeln(' ')
      end;
 {Initial values}
      m:=1;
      diff[1]:=1;
      grof[1]:=1;
      n:=1;
      for j:=1 to dip do
       begin
        if j=dim then
         vect[j]:=salw else
         vect[j]:=0
        end;
      b:=q+1;
      i:=1;
{Beginning of cycle}
```

```
{Finding coordinates of points in succession by Singer transformatio
     repeat
      i:=i+1;
      for j:=1 to dip do
       begin
        if (vect[1]=0) or (cof[j]=0) then
       term[j]:=0 else
        begin
         temp:=(cof[j]+vect[1]) mod galw;
         if temp=0 then
         temp:=galw;
         term[j]:=temp
        end;
      end;
     for j:=1 to dim do
      begin
       vect[j]:=galadd[term[j],vect[j+1]]
      end;
     vect[dip]:=term[dip];
 {Coordinates found}
 {Test for realness, zrc=no. of zero-components,jp=no. of non-zeros}
     zrc:=0;
     jp:=0;
     for j:=1 to dip do
      begin
       if vect[j]=0 then zrc:=zrc+1 else
        begin
         jp:=jp+1;
         v[jp]:=(vect[j]) mod b
        end;
       end;
      ind[dim]:=0;
      for j:= dim downto 1 do
       begin
        ind[j-1]:=ind[j]+abs(v[dip-j]-v[dip-j+1])
       end;
 {Registering real points}
      if ind[zrc]=0 then
      begin
       n:=n+1;
       grof[n]:=i;
      end;
  {Obtaining difference set}
     if vect[1]=0 then
      begin
       m:=m+1;
       diff[m]:=i;
      end;
     lea:=1;
     while vect[lea]=0 do
      begin
       lea:=lea+1
      end;
     until lea=dip;
 {Cycle completed}
       writeln(' TOTAL NO OF POINTS IS   ',lot,'   i=  ',i);
 {This print-out checks generating equation for primitivity of root}
  if i=lot then
   begin
  { Display of basic results}
  {nob=no. of points in Baer space,nop=no of points in hyperplanes}
    nob:=1;
    for j:=1 to dim do
```

```
 begin
  nob:=q*nob+1
 end;
for k:=nob downto 2 do
 begin
  grof[k]:=grof[k-1]
 end;
grof[1]:=0;
b:=nob div 7 ;
   writeln;
   writeln;
   writeln;
   writeln;
   writeln('   INDICES OF REAL POINTS ');
   writeln;
   n:=0;
   while n<=b do
    begin
     j:=1;
     m:=7*n;
     while ((j<=7) and ((m+j)<=nob)) do
      begin
       write (grof[m+j]:10);
       j:=j+1
      end;
     writeln('  ');
     n:=n+1
    end;
   for j:=1 to 5 do
    begin
     writeln
    end;
   nop:=1;
   for j:=1 to dhy do
    begin
     nop:=qs*nop+1
    end;
   for k:=nop downto 2 do
    begin
     diff[k]:=diff[k-1]
    end;
   diff[1]:=0;
   b:=nop div 10;
   writeln('  DIFFERENCE SET IS ');
   writeln;
   n:=0;
   while n<=b do
    begin
     j:=1;
     m:=10*n;
     while ((j<=10) and  ((m+j)<=nop)) do
      begin
       write (diff[m+j]:8);
       j:=j+1
      end;
     writeln;
     n:=n+1
    end;
  { Listing planes and scanning for real points in the planes}
  {Alternatively listing strongly intersecting Baer planes}
   for j:=1 to 6 do
    begin
     writeln
```

```
end;
if ir=1 then
 begin
  r:=nop;
  for j:=1 to nop do
   begin
    sta[j]:=diff[j]
   end;
  end      else
  begin
   r:=nob;
   for j:=1 to nob do
    begin
     sta[j]:=grof[j]
    end;
  end;
i:=0;
while i<lot do
 begin
  for j:=1 to r do
   begin
    if i=0 then
     pla[j]:=sta[j] else
     pla[j]:=pla[j]+1
   end;
   j1:=r-1;
   if pla[r]=lot then
    begin
     for j:=j1 downto 1 do
      begin
       pla[j+1]:=pla[j]
      end;
     pla[1]:=0
    end;
  {Scan for real intersections}
   com:=0;
   for j:=1 to nob do
    begin
     k:=1;
     while ((pla[k]<grof[j]) and (k<r)) do
      begin
       k:=k+1
      end;
     if pla[k]=grof[j] then
      begin
       com:=com+1;
       rel[com]:=grof[j];
      end;
     end;
     qfh:=1;
     for j:=1 to dhy do
      begin
       qfh:=q*qfh+1
      end;
    if com>(qfh-1) then
     begin
      writeln;
      if ir=1 then
      writeln(' REAL POINTS OF HYPERPLANE  ',i,'     ARE')
     else
      writeln('  SPACE   ', i,'    MEETS REAL SPACE IN');
      writeln;
      n:=0;
```

```
  while n<=8 do
   begin
    j:=1;
    m:=10*n;
    while ((j<=10) and ((m+j)<=com)) do
     begin
      write (rel[m+j]:8);
      j:=j+1
     end;
    writeln;
    n:=n+1
   end;
  end;
  i:=i+1;
  end;
 end;
end.
```

SURVEY OF POINTS,PLANES,SPACES IN PG(3,SQ)

FIELD: GF(16)

ADDITION TABLES IN GF(4)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	5	9	15	2	11	14	10	3	8	6	13	12	7	4
2	5	0	6	10	1	3	12	15	11	4	9	7	14	13	8
3	9	6	0	7	11	2	4	13	1	12	5	10	8	15	14
4	15	10	7	0	8	12	3	5	14	2	13	6	11	9	1
5	2	1	11	8	0	9	13	4	6	15	3	14	7	12	10
6	11	3	2	12	9	0	10	14	5	7	1	4	15	8	13
7	14	12	4	3	13	10	0	11	15	6	8	2	5	1	9
8	10	15	13	5	4	14	11	0	12	1	7	9	3	6	2
9	3	11	1	14	6	5	15	12	0	13	2	8	10	4	7
10	8	4	12	2	15	7	6	1	13	0	14	3	9	11	5
11	6	9	5	13	3	1	8	7	2	14	0	15	4	10	12
12	13	7	10	6	14	4	2	9	8	3	15	0	1	5	11
13	12	14	8	11	7	15	5	3	10	9	4	1	0	2	6
14	7	13	15	9	12	8	1	6	4	11	10	5	2	0	3
15	4	8	14	1	10	13	9	2	7	5	12	11	6	3	0

EQUATION DEFINED BY 15 15 0 1

TOTAL NO OF POINTS IS 4369 i= 4369

INDICES OF REAL POINTS

0	1	2	3	86	135	136
156	191	193	194	195	328	386
387	469	571	579	766	767	837
891	910	959	1042	1144	1289	1419
1442	1691	1744	1776	1942	1971	1972
1995	2076	2129	2164	2166	2167	2168
2203	2301	2359	2360	2467	2477	2552
2672	2673	2865	2932	3152	3297	3347
3348	3448	3464	3492	3493	3540	3685
3746	3784	3935	3950	3979	3980	4080
4137	4145	4146	4151	4172	4174	4175
4176	4291	4309	4332	4333	4338	4367
4368						

LIST OF REAL POINTS

1	1500	150000	15000000	4090414	40414	4041400
3080308	2121207	308	30800	3080000	7020707	60001
6000100	2001207	1010011	9140409	51005	5100500	6010101
1110106	14040404	8001313	5150005	2120007	14040009	10150505

14040904	2001202	13130308	15150505	5101005	40914	4091400
2120712	15151510	8080808	7000007	808	80800	8080000
4000404	12000207	110601	11060100	14140904	6110606	14140909
101015	10101500	13080008	13080813	6060106	3000308	101515
10151500	11000111	1060001	70202	7020200	13001308	10101510
1010106	4140904	1000006	9000404	80013	8001300	1110606
12071207	130813	13081300	1010001	11010106	1207	120700
12070000	14000009	1060006	10001	1000100	1010006	151515
15151500						

DIFFERENCE SET IS

0	1	2	5	8	14	26	50	98	135
137	169	193	194	237	259	268	272	275	287
336	347	384	386	457	472	491	501	516	521
534	542	543	548	565	569	572	605	613	619
670	692	715	735	755	766	770	773	819	839
855	867	899	912	923	942	973	977	980	1000
1030	1040	1045	1066	1082	1084	1094	1095	1128	1136
1142	1153	1208	1219	1224	1235	1236	1245	1247	1287
1337	1338	1355	1382	1405	1428	1445	1455	1468	1497
1508	1530	1538	1544	1613	1631	1636	1657	1676	1708
1732	1745	1747	1777	1796	1801	1822	1844	1875	1879
1882	1911	1935	1944	1952	1958	1971	1998	2058	2077
2078	2088	2130	2131	2149	2162	2166	2167	2169	2186
2188	2253	2254	2270	2282	2304	2315	2323	2329	2359
2414	2431	2436	2446	2457	2468	2470	2488	2492	2495
2543	2553	2563	2572	2595	2605	2613	2619	2635	2647
2672	2674	2708	2733	2762	2795	2803	2808	2809	2829
2854	2863	2888	2908	2913	2934	2992	3001	3014	3058
3059	3074	3086	3123	3125	3141	3153	3171	3224	3251
3260	3269	3270	3312	3343	3347	3350	3365	3401	3414
3433	3457	3462	3467	3483	3488	3492	3495	3503	3509
3552	3583	3587	3590	3600	3617	3642	3686	3715	3747
3748	3756	3762	3771	3811	3820	3857	3859	3868	3886
3902	3914	3919	3927	3933	3937	3940	3977	3979	3994
4043	4059	4071	4091	4114	4115	4145	4149	4152	4154
4174	4175	4207	4215	4221	4231	4243	4258	4260	4273
4289	4293	4296	4301	4307	4322	4330	4332	4336	4339
4355	4363	4367							

SPACE 0 MEETS REAL SPACE IN

0	1	2	3	86	135	136	156	191	193
194	195	328	386	387	469	571	579	766	767
837	891	910	959	1042	1144	1289	1419	1442	1691
1744	1776	1942	1971	1972	1995	2076	2129	2164	2166

SPACE 1 MEETS REAL SPACE IN

0	1	2	3	136	194	195	387	767	1972
2167	2168	2360	2673	3348	3493	3980	4146	4175	4176
4333	4368								

SPACE 192 MEETS REAL SPACE IN

156	191	193	194	195	328	386	387	579	959
2164	2359	2360	2552	2865	3540	3685	4172	4338	4367
4368									

SPACE 193 MEETS REAL SPACE IN

0	156	191	193	194	195	328	386	387	579
959	2164	2359	2360	2552	2865	3540	3685	4172	4338
4367	4368								

SPACE 195 MEETS REAL SPACE IN

0	1	2	135	193	194	195	386	766	1971
2166	2167	2359	2672	3347	3492	3979	4145	4174	4175
4332	4367								

SPACE 196 MEETS REAL SPACE IN

1	2	3	136	194	195	387	767	1972	2167
2168	2360	2673	3348	3493	3980	4146	4175	4176	4333
4368									

SPACE 388 MEETS REAL SPACE IN

156	191	193	194	195	328	386	387	579	959
2164	2359	2360	2552	2865	3540	3685	4172	4338	4367
4368									

SPACE 1973 MEETS REAL SPACE IN

156	469	1144	1289	1776	1942	1971	1972	2129	2164
2166	2167	2168	2301	2359	2360	2552	2932	4137	4176
4332	4333								

SPACE 2008 MEETS REAL SPACE IN

191	571	1776	1971	1972	2164	2203	2477	3152	3297
3784	3950	3979	3980	4137	4172	4174	4175	4176	4309
4367	4368								

SPACE 2165 MEETS REAL SPACE IN

156	469	1144	1289	1776	1942	1971	1972	2129	2164
2166	2167	2168	2301	2359	2360	2552	2932	4137	4332
4333	4368								

SPACE 2166 MEETS REAL SPACE IN

0	156	469	1144	1289	1776	1942	1971	1972	2129
2164	2166	2167	2168	2301	2359	2360	2552	2932	4137
4332	4333								

```
SPACE          2203     MEETS REAL SPACE IN

     0       1       2     135     193     194     386     766    1971    2166
  2167    2203    2359    2672    3347    3492    3979    4145    4174    4175
  4332    4367

SPACE          2204     MEETS REAL SPACE IN

     1       2       3     136     194     195     387     767    1972    2167
  2168    2203    2360    2673    3348    3493    3980    4146    4175    4176
  4333    4368

SPACE          2361     MEETS REAL SPACE IN

   156     195     469    1144    1289    1776    1942    1971    1972    2129
  2164    2166    2167    2168    2301    2359    2360    2552    2932    4137
  4332    4333

SPACE          2396     MEETS REAL SPACE IN

   156     191     193     194     195     328     386     387     579     959
  2164    2203    2359    2360    2552    2865    3540    3685    4172    4338
  4367    4368

SPACE          3981     MEETS REAL SPACE IN

   191     571    1776    1971    1972    2164    2477    3152    3297    3784
  3950    3979    3980    4137    4172    4174    4175    4176    4309    4367
  4368

SPACE          4173     MEETS REAL SPACE IN

   191     571    1776    1971    1972    2164    2477    3152    3297    3784
  3950    3979    3980    4137    4172    4174    4175    4176    4309    4367
  4368

SPACE          4174     MEETS REAL SPACE IN

     0     191     571    1776    1971    1972    2164    2477    3152    3297
  3784    3950    3979    3980    4137    4172    4174    4175    4176    4309
  4367    4368

SPACE          4176     MEETS REAL SPACE IN

     0       1       2     135     193     194     386     766    1971    2166
  2167    2359    2672    3347    3492    3979    4145    4174    4175    4176
  4332    4367

SPACE          4177     MEETS REAL SPACE IN

     1       2       3     136     194     195     387     767    1972    2167
  2168    2360    2673    3348    3493    3980    4146    4175    4176    4333
  4368
```

SPACE 4368 MEETS REAL SPACE IN

0	1	2	135	193	194	386	766	1971	2166
2167	2359	2672	3347	3492	3979	4145	4174	4175	4332
4367	4368								

SURVEY OF POINTS,HYPERPLANES, BAER SPACES

PROJECTIVE SPACE: PG(5 4)

COEFFICIENTS OF GENERATING EQUATION DEFINED BY

1 0 0 0 1 1

TOTAL NO OF POINTS IS 1365 i= 1365

INDICES OF REAL POINTS

0	1	2	3	4	5	6
19	31	49	50	91	175	234
244	257	258	287	288	289	337
370	395	413	414	472	473	482
483	525	526	527	528	608	609
633	634	651	652	653	671	774
812	846	847	848	871	872	873
889	890	891	892	945	1050	1051
1127	1128	1129	1130	1131	1160	1176

DIFFERENCE SET IS

0	1	2	3	4	16	17	23	25	26
37	39	44	46	47	49	54	56	60	62
68	74	85	86	88	89	93	94	100	101
102	108	120	126	129	130	134	135	138	142
151	152	153	161	163	171	172	173	180	190
191	194	200	207	208	215	218	219	225	226
230	231	249	251	253	257	271	274	282	283
287	288	292	293	302	310	314	316	319	322
331	332	333	335	342	348	350	353	366	372
373	374	383	393	398	403	408	413	420	422
427	431	441	449	466	468	469	470	472	476
478	480	482	485	498	502	504	508	516	519
523	525	526	527	530	531	532	534	539	543
547	551	557	558	568	583	591	592	595	603
606	608	619	625	628	630	633	636	637	639
641	642	646	647	649	651	652	655	662	665
666	668	673	676	678	681	689	694	696	701
703	723	724	730	734	738	744	753	756	768
769	770	771	777	778	780	784	793	799	803
808	810	814	818	820	825	832	837	840	843
846	847	853	856	859	861	865	868	869	871
872	879	880	881	884	885	886	889	890	891
897	902	911	912	916	917	919	920	923	926
932	933	936	939	940	943	949	952	954	956

958	960	965	975	979	984	986	989	993	998
1002	1004	1026	1030	1033	1035	1040	1044	1046	1047
1050	1055	1060	1063	1064	1072	1075	1076	1088	1093
1099	1100	1122	1123	1124	1125	1127	1128	1129	1130
1138	1140	1141	1143	1147	1152	1154	1155	1156	1168
1173	1185	1192	1193	1203	1204	1207	1210	1212	1215
1220	1222	1223	1227	1228	1236	1237	1251	1254	1256
1258	1261	1267	1273	1274	1278	1279	1281	1293	1294
1296	1298	1299	1305	1309	1312	1317	1323	1325	1329
1331	1332	1334	1340	1345	1347	1349	1352	1355	1357
1359									

SPACE 0 MEETS REAL SPACE IN

0	1	2	3	4	5	6	19	31	49
50	91	175	234	244	257	258	287	288	289
337	370	395	413	414	472	473	482	483	525
526	527	528	608	609	633	634	651	652	653
671	774	812	846	847	848	871	872	873	889
890	891	892	945	1050	1051	1127	1128	1129	1130
1131	1160	1176							

SPACE 1 MEETS REAL SPACE IN

1	2	3	4	5	6	50	258	288	289
414	473	483	526	527	528	609	634	652	653
847	848	872	873	890	891	892	1051	1128	1129
1130	1131								

SPACE 238 MEETS REAL SPACE IN

0	1	2	3	4	49	244	257	287	288
413	472	482	525	526	527	608	633	651	652
846	847	871	872	889	890	891	1050	1127	1128
1129	1130								

SPACE 239 MEETS REAL SPACE IN

1	2	3	4	5	50	244	258	288	289
414	473	483	526	527	528	609	634	652	653
847	848	872	873	890	891	892	1051	1128	1129
1130	1131								

SPACE 1126 MEETS REAL SPACE IN

5	19	49	50	175	234	244	287	288	289
370	395	413	414	608	609	633	634	651	652
653	812	889	890	891	892	1127	1128	1129	1130
1131	1176								

SPACE 1127 MEETS REAL SPACE IN

6	19	49	50	175	234	244	287	288	289
370	395	413	414	608	609	633	634	651	652
653	812	889	890	891	892	1127	1128	1129	1130
1131	1176								

SPACE 1364 MEETS REAL SPACE IN

0	1	2	3	4	5	49	257	287	288
413	472	482	525	526	527	608	633	651	652
846	847	871	872	889	890	891	1050	1127	1128
1129	1130								

PROGRAM BEARSP

OUTPUT 1

PG (3,9)

GENERATING POLYNOMIAL 1 1 4 1

($x^4 = \alpha x^3 + \alpha x^2 + 2x + \alpha$

where $\alpha^2 + \alpha + 2 = 0$ over GF(3).)

LIST OF REAL PLANES

OUTPUT 2

PG (3,4)

GENERATING POLYNOMIAL 0 1 1 1

($x^4 = \alpha (x^2 + x + 1)$

where $\alpha^2 + \alpha + 1 = 0$ over GF(2) .)

LIST OF REAL LINES

```
PROGRAM  BAERSP  (inPut,outPut);
        {GENERATION OF POINTS IN THREE DIMENSIONS}
var     i,q,salw,j,jP,qs,j1,temP,qfh,lot,k,l,m,n,r,b,
        js,a,d,qss,lino,ir,nob,noP,com,zrc : inteser;
        st,li,sP: array[1..26] of inteser;
        reP: array[1..32] of inteser;
        diff,Pla,sta,tem: array[1..651] of inteser;
        srof,aP,rel: array[1..156] of inteser;
        Plc: array[1..2,1..651] of inteser;
        cof,term,vect,v: array[1..4] of inteser;
        saladd: array[0..24,0..24] of inteser;
besin
       writeln(' SURVEY OF POINTS,LINES,PLANES,SPACES in 3D');
       for i:=1 to 6 do
         besin
          writeln('  ')
         end;
      {Establishins addition table for the Galois field}
       saladd[0,0]:=0;
       read(q);
       qs:=sqr(q);
       writeln('         FIELD: GF(',qs ,')');
       salw:=qs-1;
       for j:=1 to salw do
        besin
         read(saladd[1,j])
        end;
       if q mod 2 =0 then
        besin
         l:=salw-1;
          for j:=2 to l do
           besin
            saladd[j,j]:=0;
            jP:=j+1;
            for k:=jP to salw do
             besin
              temP:=saladd[j-1,k-1]+1;
              if temP=qs then
              saladd[j,k]:=1 else
              saladd[j,k]:=temP
             end;
            end;
            saladd[salw,salw]:=0;
          end                else
          besin
           qfh:=salw div 2;
           for j:=2 to salw do
            besin
             for k:=j to salw do
              besin
               if (k-j)=qfh then
               saladd[j,k]:=0   else
                besin
                 temP:=saladd[j-1,k-1]+1;
                 if temP=qs then
                 saladd[j,k]:=1 else
                 saladd[j,k]:=temP
                end;
               end;
              end;
            end;
           for j:=2 to salw do
            besin
```

```
          j1:=j-1;
          for k:=1 to j1 do
           begin
            saladd[j,k]:=saladd[k,j]
           end;
          end;
        for j:=1 to salw do
         begin
          saladd[0,j]:=j;
          saladd[j,0]:=j
         end;
   writeln('                ADDITION TABLES IN GF(',qs, ')');
   for j:=0 to salw do
    begin
     for k:=0 to salw do
      begin
       write(saladd[j,k]:3);
      end;
     writeln('  ')
    end;
    for j:=1 to 4 do
     begin
      writeln('  ');
     end;
 {Addition table established and exhibited}
   lot:=qs*(sqr(qs)+qs+1)+1;
   read(cof[1],cof[2],cof[3],cof[4]);
     writeln('  ');
   writeln(' EQUATION DEFINED BY  ',cof[1],cof[2],cof[3],cof[4]);
   for j:=1 to 4 do
    begin
     writeln(' ')
    end;
    read(ir);
{Initial values}
    m:=1;
    diff[1]:=1;
    sprof[1]:=1;
    n:=1;
    ap[1]:=100*salw;
    vect[1]:=0;
    vect[2]:=0;
    vect[3]:=salw;
    vect[4]:=0;
    b:=q+1;
    i:=1;
{Beginning of cycle}
{Finding coordinates of points in succession by Singer transformation}
   repeat
    i:=i+1;
    for j:=1 to 4 do
     begin
      if (vect[1]=0) or (cof[j]=0) then
     term[j]:=0 else
      begin
       temp:=(cof[j]+vect[1]) mod salw;
       if temp=0 then
       temp:=salw;
       term[j]:=temp
      end;
    end;
   for j:=1 to 3 do
    begin
```

```
      vect[j]:=saladd[term[j],vect[j+1]]
     end;
    vect[4]:=term[4];
{Coordinates found}
{Test for realness, zrc=no. of zero-components,jp=no. of non-zeros}
    zrc:=0;
    jp:=0;
    for j:=1 to 4 do
     begin
      if vect[j]=0 then zrc:=zrc+1 else
       begin
        jp:=jp+1;
        v[jp]:=(vect[j]) mod b
       end;
      end;
     case zrc of
     0: afh:=abs(v[1]-v[2])+abs(v[2]-v[3])+abs(v[3]-v[4]);
     1: afh:=abs(v[1]-v[2])+abs(v[2]-v[3]);
     2: afh:=v[1]-v[2];
     3: afh:=0;
     end;
{Registering real points}
    if afh=0 then
     begin
      n:=n+1;
      grof[n]:=i;
      ap[n]:=1000*1000*vect[1]+10000*vect[2]+100*vect[3]+vect[4];
     end;
 {Obtaining difference set}
    if vect[1]=0 then
     begin
      m:=m+1;
      diff[m]:=i
     end;
    until((vect[1]=0) and (vect[2]=0) and (vect[3]=0));
{Cycle completed}
      writeln(' TOTAL NO OF POINTS IS   ',lot,'   i=  ',i);
{This print-out checks generating equation for primitivity of root}
 { Display of basic results}
 {nob=no. of points in Baer space,nop=no of points in planes}
  if i =lot then
   begin
   nob:=q*qs+qs+q+1;
   r:=ap[nob];
   for k:=nob downto 2 do
    begin
     grof[k]:=grof[k-1];
     ap[k]:=ap[k-1]
    end;
   ap[1]:=r;
   grof[1]:=0;
   b:=nob div 7 ;
      writeln;
      writeln;
      writeln;
      writeln;
      writeln('   INDICES OF REAL POINTS ');
      writeln;
      n:=0;
      while n<=b do
       begin
        j:=1;
        m:=7*n;
```

```
  while ((j<=7) and ((m+j)<=nob)) do
   begin
    write (grof[m+j]:10);
    j:=j+1
   end;
  writeln('  ');
  n:=n+1
 end;
writeln;
writeln;
writeln('   LIST OF REAL POINTS  ');
writeln;
n:=0;
while n<=b do
 begin
  j:=1;
  m:=7*n;
  while ((j<=7) and ((m+j)<=nob)) do
   begin
    write (ap[m+j]:10);
    j:=j+1
   end;
  writeln;
  n:=n+1
 end;
for j:=1 to 5 do
 begin
  writeln
 end;
nop:=qs*qs +qs +1;
for k:=nop downto 2 do
 begin
  diff[k]:=diff[k-1]
 end;
diff[1]:=0;
b:=nop div 10;
writeln('  DIFFERENCE SET IS ');
writeln;
n:=0;
while n<=b do
 begin
  j:=1;
  m:=10*n;
  while ((j<=10) and  ((m+j)<=nop)) do
   begin
    write (diff[m+j]:8);
    j:=j+1
   end;
  writeln;
  n:=n+1
 end;
{ Listing planes and scanning for real points in the planes}
{Alternatively listing strongly intersecting Baer planes}
 for j:=1 to 6 do
  begin
   writeln
  end;
  if ir=1 then
   begin
    r:=nop;
    for j:=1 to nop do
     begin
      sta[j]:=diff[j]
```

```
   end;
  end       else
  begin
   if ir=2 then
    begin
     r:=nob;
     for j:=1 to nob do
      begin
       sta[j]:=grof[j]
      end;
   end;
  end;
if ir<>3 then
 begin
i:=0;
while i<lot do
 begin
  for j:=1 to r do
   begin
    if i=0 then
     pla[j]:=sta[j] else
     pla[j]:=pla[j]+1
   end;
   j1:=r-1;
   if pla[r]=lot then
    begin
     for j:=j1 downto 1 do
      begin
       pla[j+1]:=pla[j]
      end;
     pla[1]:=0
    end;
  {Scan for real intersections}
   com:=0;
   for j:=1 to nob do
    begin
     k:=1;
     while ((pla[k]<grof[j]) and (k<r)) do
      begin
       k:=k+1
      end;
     if pla[k]=grof[j] then
      begin
       com:=com+1;
       rel[com]:=grof[j];
      end;
     end;
    if ir=1 then
     afh:=a+1   else
     afh:=as+a;
    if com>afh then
     begin
      writeln;
      if ir=1 then
      writeln(' REAL POINTS OF PLANE  ',i,'     ARE')
     else
      writeln('  SPACE   ', i,'    MEETS REAL SPACE IN');
      writeln;
      n:=0;
      while n<=3 do
       begin
        j:=1;
        m:=10*n;
```

```
                    while ((j<=10) and ((m+j)<=com)) do
                     begin
                      write (rel[m+j]:8);
                      j:=j+1
                     end;
                    writeln;
                    n:=n+1
                   end;
                  end;
                  i:=i+1;
                  end;
                  end               else
          {Scan for real lines begins}
                   begin
                    ass:=as+1;
                    afh:=(as+a) div 2;
                    lino:=ass*(as+a+1); {expected number of lines}
                    a:=0;
                    d:=0; {beginning of main d-loop}
    {Lines are classified by the minimal difference d between the
     indices of their points.}
                    while ((a<lino) and (d<=lot)) do
                     begin
                      m:=0;
             {m will be the number of iterations of the same
              difference value in the difference-set, here m=as+1}
                      j:=1;
            {Beginning of j-loop,where j is the position of point
            temporarily fixed within difference-set to locate point
            (if any) differing from it by d}
              while j<=nop do
               begin
                jp:=nop-j;
                if jp>0 then
                 begin
                  for k:=1 to jp do
                   begin
                    tem[k]:=diff[j+k]
                   end;
                  end;
                 l:=jp+1;
                 for k:=1 to nop do
                  begin
                   tem[k]:=diff[k-jp]+lot
                  end;
 {Difference set (0-plane) shifted by j positions.}
                  temp:=d-1;
                  k:=0;
                  while ((temp<d) and (k<nop)) do
                   begin
                    k:=k+1;
                    temp:=tem[k]-diff[j]
                   end;
                  if temp=d then
                   begin
                    m:=m+1;
                    st[m]:=diff[j]
                   end;
                  j:=j+1;
                 end;
                      {end of small j-loop and beginning of a
                 large j-loop, scanning the points of the real
                 Baer-space.}
```

```
                    j:=1;
                    while j<=nob do
                     begin
                      jp:=nob-j;
                      if jp>0 then
                       begin
                        for k:=1 to jp do
                         begin
                          tem[k]:=grof[j+k]
                         end;
                        end;
                       l:=jp+1;
                       for k:=1 to nob do
                        begin
                         tem[k]:=grof[k-jp]+lot
                        end;
                       temp:=d-1;
                       k:=0;
                       while ((temp<d) and (k<nob))do
                        begin
                         k:=k+1;
                         temp:=tem[k]-grof[j]
                        end;
                       if temp=d then
                        begin
                         for l:=1 to m do
                          begin
                           sp[l]:=grof[j]-st[l];
{sp[l] is the shift of the fixed point grof[j] of the real space from the
lower index in the difference set having the difference d in question.It
represents the index of one of the planes containing the point and its
follower by difference d.}
                           if sp[l]<0 then
                           sp[l]:=sp[l]+lot;
                          end;
                         js:=j;
                         for n:=1 to 2 do
                          begin
                           for i:=1 to nop do
                            begin
                             tem[i]:=(diff[i]+sp[n]) mod lot
                            end;
    {tem[i] is a real point followed by another real point with difference d}
                           i:=1;
                           while (((tem[i+1]-tem[i])>0) and (i<nop)) do
                            begin
                             i:=i+1
                            end;
                           if i<nop then
                            begin
                             j1:=nop-i;
                             for k:=1 to j1 do
                              begin
                               plc[n,k]:=tem[i+k]
                              end;
                             end;
                             jp:=nop-i+1;
                             for k:=jp to nop do
                              begin
                               plc[n,k]:=tem[k-jp+1]
                              end;
                            end;
     {two planes generating line found}
```

```
                    for i:=1 to nop do
                     begin
                      tem[i]:=plc[1,i]
                     end;
  {finding intersections of the two planes}
                     com:=0;
                      for i:=1 to nop do
                       begin
                        k:=1;
                        while  ((plc[2,k]<plc[1,i]) and (k<nop)) do
                         begin
                          k:=k+1
                         end;
                        if plc[2,k]=plc[1,i] then
                         begin
                          com:=com+1;
                          li[com]:=plc[1,i]
                         end;
                        end;
 {Next,find real points of line}
                      zrc:=0;
                      for i:=1 to com do
                       begin
                        k:=1;
                        while ((li[i]>grof[k]) and (k<nob)) do
                         begin
                          k:=k+1
                         end;
                        if li[i]=grof[k] then
                         begin
                          zrc:=zrc+1;
                          rep[zrc]:=li[i]
                         end;
                        end;
{check for smaller difference}
                 b:=0;
                 j1:=d+1;
                 jp:=d+1;
                 i:=0;
                 r:=0;
                 while ((j1>=d) and (jp>=d) and (i<zrc) and (r=0))
                 do
                  begin
                   i:=i+1;
                   k:=0;
                   while ((j1>=d) and (jp>=d) and ((i+k)<zrc) and (r=0)
                   ) do
                    begin
                     k:=k+1;
                     b:=b+1;
                     j1:=rep[i+k]-rep[i];
                     jp:=rep[i]-rep[i+k]+lot;
                     if ((j1=d) and (rep[i]<grof[j])) then
                     r:=r+1
                    end;
                   end;
                  if ((j1>=d) and (jp>=d) and (b=gfh) and (r=0)) then
                   begin
                    a:=a+1;
                    for i:=1 to 4 do
                     begin
                      writeln
                     end;
```

```
              writeln( 'LINE  ',a, '    HAS POINTS');
              for i:=1 to ass do
               besin
                write (li[i]:6)
               end;
               writeln;
               writeln( '              REAL POINTS ARE');
               for i:=1 to zrc do
                besin
                 write (rep[i]:6)
                end;
               writeln;
               writeln( 'PLANES CONTAINING LINE ARE');
               for i:=1 to ass do
                besin
                 write (sp[i]:6)
                end;
               writeln;
              end;
             j:=js+1
            end                else
           j:=j+1
          end;    {end of larse j-loop}
         d:=d+1
        end;    {end of d-loop}
        end; {end of line-scanning}
       end;
     end.
```

FIELD: GF(9)

ADDITION TABLES IN GF(9)

0	1	2	3	4	5	6	7	8
1	5	8	4	6	0	3	2	7
2	8	6	1	5	7	0	4	3
3	4	1	7	2	6	8	0	5
4	6	5	2	8	3	7	1	0
5	0	7	6	3	1	4	8	2
6	3	0	8	7	4	2	5	1
7	2	4	0	1	8	5	3	6
8	7	3	5	0	2	1	6	4

EQUATION DEFINED BY 1 1 4 1

TOTAL NO OF POINTS IS 820 i= 820

INDICES OF REAL POINTS

0	1	2	3	6	7	26
73	96	97	98	102	153	154
192	193	214	249	288	314	324
325	366	374	390	413	414	415
419	420	509	510	566	577	605
644	737	795	797	790		

LIST OF REAL POINTS

5	800	80000	8000000	10501	1050100	6060602
2060206	105	10500	1050000	2020606	40408	4040800
20202	2020200	6020202	5000505	3000007	7070307	80404
8040400	4080004	4040008	8080808	707	70700	7070000
8000008	1010001	80004	8000400	3070007	3000707	1050501
5010505	7000703	4000804	60006	6000600		

DIFFERENCE SET IS

0	1	2	6	19	21	34	43	48	78
90	93	96	97	108	127	146	147	153	160
163	187	192	208	219	226	230	234	242	244
292	320	324	350	360	369	377	378	381	401
403	404	406	413	414	448	471	473	479	482

||

488	499	509	512	517	523	528	531	549	559
570	571	579	586	592	598	614	651	652	666
683	689	691	703	707	712	714	716	734	747
751	754	767	768	775	780	790	792	797	806
816									

REAL POINTS OF PLANE 0 ARE

0	1	2	6	96	97	153	192	324	413
414	509	797							

REAL POINTS OF PLANE 1 ARE

1	2	3	7	97	98	154	193	325	414
415	510	798							

REAL POINTS OF PLANE 5 ARE

1	6	7	26	98	102	192	249	325	374
419	795	797							

REAL POINTS OF PLANE 6 ARE

2	6	7	96	102	153	193	214	366	419
420	577	798							

REAL POINTS OF PLANE 7 ARE

3	7	26	97	153	154	249	413	420	566
577	605	797							

REAL POINTS OF PLANE 30 ARE

0	2	7	26	73	193	249	390	509	644
737	797	798							

REAL POINTS OF PLANE 46 ARE

1	6	154	192	193	288	366	415	577	605
644	737	797							

REAL POINTS OF PLANE 54 ARE

1 2 26 73 97 102 214 288 374 414
566 577 737

REAL POINTS OF PLANE 95 ARE

26 96 97 192 314 325 415 419 509 566
577 644 798

REAL POINTS OF PLANE 96 ARE

73 96 97 98 102 192 193 249 288 420
509 510 605

REAL POINTS OF PLANE 106 ARE

0 2 102 154 214 314 325 509 510 577
605 795 797

REAL POINTS OF PLANE 132 ARE

1 3 26 102 153 324 366 374 509 510
605 644 798

REAL POINTS OF PLANE 171 ARE

2 3 98 102 192 214 249 324 390 413
415 577 644

REAL POINTS OF PLANE 206 ARE

0 98 102 153 154 192 249 314 366 414
566 737 798

REAL POINTS OF PLANE 227 ARE

73 96 98 154 324 374 390 414 419 577
605 797 798

REAL POINTS OF PLANE 228 ARE

0 6 97 214 249 324 325 374 415 420
605 737 798

REAL POINTS OF PLANE 266 ARE

```
   97     98    153    193    214    314    374    413    419    510
  644    737    797

REAL POINTS OF PLANE        267      ARE

    6     26     98    154    214    288    413    414    420    509
  644    795    798

REAL POINTS OF PLANE        318      ARE

    7     26     96    214    249    288    314    324    366    414
  415    510    797

REAL POINTS OF PLANE        322      ARE

    1     73    153    154    193    214    249    324    415    419
  509    566    795

REAL POINTS OF PLANE        323      ARE

    2     26     73    154    192    324    325    366    413    419
  420    510    737

REAL POINTS OF PLANE        324      ARE

    3     96    102    193    324    325    414    420    566    644
  737    795    797

REAL POINTS OF PLANE        347      ARE

    0      6     26     97     98    193    324    366    390    510
  566    577    795

REAL POINTS OF PLANE        394      ARE

   73     97    102    153    288    325    366    390    413    415
  795    797    798

REAL POINTS OF PLANE        413      ARE

    6      7    102    390    413    414    415    419    509    510
  566    605    737

REAL POINTS OF PLANE        414      ARE
```

0 7 73 153 192 374 414 415 420 510
577 644 795

REAL POINTS OF PLANE 417 ARE

0 1 3 96 249 288 413 419 510 577
737 795 798

REAL POINTS OF PLANE 418 ARE

1 2 97 249 314 366 390 414 419 420
605 644 795

REAL POINTS OF PLANE 419 ARE

0 2 3 98 288 366 374 415 419 420
509 566 797

REAL POINTS OF PLANE 420 ARE

1 3 6 73 192 214 314 390 420 510
566 797 798

REAL POINTS OF PLANE 442 ARE

0 3 26 153 192 193 214 288 325 390
414 419 605

REAL POINTS OF PLANE 443 ARE

0 1 26 96 102 154 193 314 374 390
413 415 420

REAL POINTS OF PLANE 445 ARE

2 3 6 26 73 96 98 153 314 415
605 737 795

REAL POINTS OF PLANE 503 ARE

3 7 96 97 154 192 214 366 374 390
509 737 795

REAL POINTS OF PLANE 596 ARE

2	6	96	153	154	249	288	325	374	390
510	566	644							

REAL POINTS OF PLANE 635 ARE

2	7	192	193	288	314	324	374	413	566
605	795	798							

REAL POINTS OF PLANE 663 ARE

3	6	73	193	249	314	325	366	374	413
414	509	577							

REAL POINTS OF PLANE 674 ARE

0	1	7	73	96	98	214	325	366	413
566	605	644							

REAL POINTS OF PLANE 730 ARE

0	3	6	7	73	97	102	154	288	314
324	419	644							

REAL POINTS OF PLANE 731 ARE

1	7	98	153	288	314	324	325	390	420
509	577	737							

FIELD: GF(4)

ADDITION TABLES IN GF(2)

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

EQUATION DEFINED BY 0 1 1 1

TOTAL NO OF POINTS IS 85 i= 85

INDICES OF REAL POINTS

0	1	2	3	4	5	19
26	36	41	42	63	64	65
67						

LIST OF REAL POINTS

1	300	30000	3000000	10101	1010100	1010101
2020002	1000101	10001	1000100	101	10100	1010000
2000002						

DIFFERENCE SET IS

0	1	2	4	8	16	17	32	34	37
41	43	51	61	63	64	68	73	74	79
82									

LINE 1 HAS POINTS

0 1 16 63 73

REAL POINTS ARE

```
     0      1     63
PLANES CONTAINING LINE ARE
     0     84     69     22     12


LINE            2    HAS POINTS
     1      2     17     64     74
            REAL POINTS ARE
     1      2     64
PLANES CONTAINING LINE ARE
     1      0     70     23     13


LINE            3    HAS POINTS
     2      3     18     65     75
            REAL POINTS ARE
     2      3     65
PLANES CONTAINING LINE ARE
     2      1     71     24     14


LINE            4    HAS POINTS
     3      4     19     66     76
            REAL POINTS ARE
     3      4     19
PLANES CONTAINING LINE ARE
     3      2     72     25     15


LINE            5    HAS POINTS
     4      5     20     67     77
            REAL POINTS ARE
     4      5     67
PLANES CONTAINING LINE ARE
     4      3     73     26     16


LINE            6    HAS POINTS
    19     29     41     42     57
            REAL POINTS ARE
    19     41     42
PLANES CONTAINING LINE ARE
    41     40     25     63     53


LINE            7    HAS POINTS
    41     51     63     64     79
            REAL POINTS ARE
    41     63     64
PLANES CONTAINING LINE ARE
    63     62     47      0     75
```

```
LINE            8    HAS POINTS
     42     52     64     65     80
               REAL POINTS ARE
     42     64     65
PLANES CONTAINING LINE ARE
     64     63     48      1     76


LINE            9    HAS POINTS
      0      2     32     41     61
               REAL POINTS ARE
      0      2     41
PLANES CONTAINING LINE ARE
      0     83     53     44     24


LINE           10    HAS POINTS
      1      3     33     42     62
               REAL POINTS ARE
      1      3     42
PLANES CONTAINING LINE ARE
      1     84     54     45     25


LINE           11    HAS POINTS
      2      4     34     43     63
               REAL POINTS ARE
      2      4     63
PLANES CONTAINING LINE ARE
      2      0     55     46     26


LINE           12    HAS POINTS
      3      5     35     44     64
               REAL POINTS ARE
      3      5     64
PLANES CONTAINING LINE ARE
      3      1     56     47     27


LINE           13    HAS POINTS
     10     19     39     63     65
               REAL POINTS ARE
     19     63     65
PLANES CONTAINING LINE ARE
     63     61     31     22      2
```

```
LINE            14    HAS POINTS
    12     21     41     65     67
             REAL POINTS ARE
    41     65     67
PLANES CONTAINING LINE ARE
    65     63     33     24      4


LINE            15    HAS POINTS
     0      3      7     40     67
             REAL POINTS ARE
     0      3     67
PLANES CONTAINING LINE ARE
    84     51     24      6      3


LINE            16    HAS POINTS
     1      4      8     41     68
             REAL POINTS ARE
     1      4     41
PLANES CONTAINING LINE ARE
     0     52     25      7      4


LINE            17    HAS POINTS
     2      5      9     42     69
             REAL POINTS ARE
     2      5     42
PLANES CONTAINING LINE ARE
     1     53     26      8      5


LINE            18    HAS POINTS
    19     46     64     67     71
             REAL POINTS ARE
    19     64     67
PLANES CONTAINING LINE ARE
    63     30      3     70     67


LINE            19    HAS POINTS
     0      4     37     64     82
             REAL POINTS ARE
     0      4     64
PLANES CONTAINING LINE ARE
     0     81     48     21      3


LINE            20    HAS POINTS
     1      5     38     65     83
```

```
            REAL POINTS ARE
     1     5     65
 PLANES CONTAINING LINE ARE
     1     82    49    22     4


 LINE            21   HAS POINTS
    15    42    60    63    67
            REAL POINTS ARE
    42    63    67
 PLANES CONTAINING LINE ARE
    63    59    26    84    66


 LINE            22   HAS POINTS
     0     5    11    19    54
            REAL POINTS ARE
     0     5    19
 PLANES CONTAINING LINE ARE
    53    22    17    11     3


 LINE            23   HAS POINTS
     5    36    41    47    55
            REAL POINTS ARE
     5    36    41
 PLANES CONTAINING LINE ARE
     4    58    53    47    39


 LINE            24   HAS POINTS
     0    31    36    42    50
            REAL POINTS ARE
     0    36    42
 PLANES CONTAINING LINE ARE
    34    84    53    48    42


 LINE            25   HAS POINTS
     1    19    22    26    59
            REAL POINTS ARE
     1    19    26
 PLANES CONTAINING LINE ARE
    18    70    43    25    22


 LINE            26   HAS POINTS
    26    36    48    49    64
            REAL POINTS ARE
    26    36    64
 PLANES CONTAINING LINE ARE
```

```
    70      60      48      47      32

LINE            27    HAS POINTS
     3     13     25     26     41
          REAL POINTS ARE
     3     26     41
PLANES CONTAINING LINE ARE
    25     24      9     47     37

LINE            28    HAS POINTS
     4     14     26     27     42
          REAL POINTS ARE
     4     26     42
PLANES CONTAINING LINE ARE
    26     25     10     48     38

LINE            29    HAS POINTS
     2     19     36     53     70
          REAL POINTS ARE
     2     19     36
PLANES CONTAINING LINE ARE
     2     70     53     36     19

LINE            30    HAS POINTS
     1     36     67     72     78
          REAL POINTS ARE
     1     36     67
PLANES CONTAINING LINE ARE
    35      4     84     78     70

LINE            31    HAS POINTS
     0     24     26     56     65
          REAL POINTS ARE
     0     26     65
PLANES CONTAINING LINE ARE
    48     24     22     77     68

LINE            32    HAS POINTS
     2     26     28     58     67
          REAL POINTS ARE
     2     26     67
PLANES CONTAINING LINE ARE
    50     26     24     79     70
```

```
LINE            33   HAS POINTS
      5      23      26      30      63
             REAL POINTS ARE
      5      26      63
PLANES CONTAINING LINE ARE
     74      47      29      26      22


LINE            34   HAS POINTS
      4       6      36      45      65
             REAL POINTS ARE
      4      36      65
PLANES CONTAINING LINE ARE
     57      48      28       4       2


LINE            35   HAS POINTS
      3      36      63      81      84
             REAL POINTS ARE
      3      36      63
PLANES CONTAINING LINE ARE
     47      20       2      84      80
```