Contents

Chapter 1

André's Theory Of Spreads.

André's theory of spreads is arguably one of the most important events in finite geometry: hardly any finite projective planes were known before André seminal 1954-paper, [2]. André's paper is ultimately responsible for the explosive growth in the discovery of finite non-Desarguesian planes during the last thirty years. Moreover, the theory of spreads, which reduces the study of translation planes to structures that live on vector spaces, has meant that all the machinery of linear algebra, and hence also group repreentation theory, can be brought to bear on the study of translation planes.

The lectures in this chapter will mainly be concerned with developing the André theory of spreads and its computational aspect — spreadsets of matrices. In the next chapter, the associated theory of spreads as structures that live in *projective* spaces will be emphasized.

1.1 Affine Planes with a Transitive Translation Groups.

In this first lecture, we begin our study of projective and affine planes. With the exception of three infinite families of projective planes called the planes of Hughes, Figueroa, and Coulter-Matthews, all finite projective planes are related to a class called 'translation planes.'

In this lecture, we consider a fundamental representation of a translation plane. This is the classical description of translation planes using vector spaces due to André. In a later lecture, we shall consider the Bruck-Bose approach using projective spaces.

Less well known but of increasing importance are what might be called coordinate methods. These include the study of quasifields, spread sets and Oyama coordinates. Professor Jha will be lecturing on some of these topics in the algebraic tract.

We begin with the definition of an affine plane, which we state in terms of an INCIDENCE STRUCTURE $(\mathcal{P}, \mathcal{L}, \mathcal{I})$. This means that $\mathcal{P}$ and $\mathcal{L}$ are disjoint sets of objects called POINTS and LINES resp. and $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$. To facilitate discussion we make extensive use of geometric terminology: any set of points incident with the same line is said to be collinear, two lines are DISJOINT if they are not incident with any common point. Similarly we use notation based on geometry and set theory: we write $P \in p$, or say the point P LIES ON the line P, if $(P, p) \in \mathcal{I}$, and if $P, Q \in \mathcal{P}$ are distinct points that share exactly one line we write PQ to denote the unique line that they share.

Definition 1.1.1 *An affine plane π is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ with the following properties:*

1. *Given two distinct points $P, Q \in \mathcal{P}$, there exists a unique line p such that (P, p) and $(Q, p) \in \mathcal{I}$; thus $PQ = p$.*

2. *Given a point P and a line p such that P is not incident with p, there exists a unique line q disjoint from p such that $P \in q$.'*

3. *There exists at least three noncollinear points.*

Two lines of an affine plane are said to be PARALLEL, if they are disjoint, and the notation $p \parallel q$ means that lines p and q are parallel when $p \neq q$. However, in order to force $\parallel$ to be an equivalence relation, *we continue to write $p \parallel q$ even when $p = q$.*

Remark 1.1.2 *Let $\pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be an affine plane. Then $\parallel$ is an equivalence relation on the set of lines. The equivalence classes are called 'parallel classes'.*

Proof: Routine exercise. ∎

We shall often use variations of the above terminology that often arise in the literature. For example the parallel classes of an affine plane is often called its SLOPESET, or its set of 'infinte points' or its 'ideal points'. Similarly, the class of any line is its SLOPE, or its 'point at infinity', etc.

We shall encounter many incidence structures related to affine planes: projective planes, Desarguesian affine and projective spaces, nets, etc. We

therefore give a general definition of an isomorphism from one incidence structure to another.

Definition 1.1.3 *Let $\pi_i = (\mathcal{P}_i, \mathcal{L}_i, \mathcal{I}_i)$, $i = 1, 2$, be incidence structures. Then an isomorphism from π_1 onto π_2 is an ordered pair of bijections*

$$(\rho : \mathcal{P}_1 \to \mathcal{P}_2, \lambda :: \mathcal{L}_1 \to \mathcal{L}_2),$$

from the points and lines of π_1 onto the points and lines of π_2 (respectively), such that incidence is preserved in both directions:

$$(p, \ell) \in \mathcal{I}_1 \Longleftrightarrow (\rho(p), \lambda(\ell)) \in \mathcal{I}_2.$$

An isomorphism from an incidence structure π to itself is = an AUTOMORPHISM, *and the group of automorphism of π is usually denoted by $Aut(\pi)$.*

An automorphism of an affine plane is completely specified by its action on the points: this is because two points determine a unique line and every line lies on at least two points. Thus we have

Remark 1.1.4 *Let π be an affine plane. Show that if (σ, τ) and (σ, ρ) are collineations of π then $\tau = \rho$.*

The above remark justifies the usage of only the *point*-bijection to refer to the automorphism. This applies to any incidence structure where the *incidence is set-theoretic*: this means that lines may be viewed as sets of points and distinct lines are associated with distinct sets of points. All the incidence structures we encounter may be regarded as being set-theoretic incidence structures. This allows us to freely use set-theoretic language rather than the more cumbersome terminology associated with incidence.

Thus, in any set-theoretic incidence structure, an automorphism $(\phi : P \to P, \psi : L \to L)$ is full determined by the action of the associated point-bijection $\phi : P \to P$; the action on the lines correspond to the usual action induced by ϕ on the powerset 2^P. We shall refer to ϕ as a *collineation*: thus a collineation is the action on the points corresponding to an automorphism of a set-theoretic incidence structure. In particular:

Definition 1.1.5 *A collineation of a set-theoretic incidence structure π is a bijection of its points that extends to an automorphism of π. Autπ will be used to denote the collinetaion group of π and also its automorphism group: both groups are of course isomorphic.*

Thus, the collineation group in the above sense is the faithful representation of the automorphism group on the points. Accordingly, we shall not attempt to seriously distinguish between the two concepts.

Exercise 1.1.6 *Let ϕ be a bijection from the points of an affine plane A onto the points of an incidence structure B such that ϕ maps collinear sets of points onto pairwise incidence sets of points. Is it true in general that ϕ induces an isomorphism from A onto B? Show that ϕ does induce an isomorphism when B is also an affine plane.*

Definition 1.1.7 *A* TRANSLATION *of an affine plane is a collineation which leaves each parallel class invariant and fixes each line of some parallel class.*

Our goal is to verify that the translations of an affine plane form a group and this group acts semiregularly on the affine points, that is, the points other than the parallel classes. The first step is to note that all non-trivial translations are semiregular:

Lemma 1.1.8 *A translation of an affine plane which fixes a point is the identity.*

Proof: Exercise. ∎

The following remark may be taken as an alternative definition of a translation, equivalent to definition 1.1.7 above.

Remark 1.1.9 *Let σ be a non-trivial collineation of an affine plane $\mathcal{A}$.*

Then σ is a translation iff it fixes every parallel classes of $\mathcal{A}$ and does not fix any affine point.

Proof: $\Rightarrow$ follows from lemma 1.1.8 above. Conversely assume σ leaves invariant every parallel class but does not fix any affine point. So choosing any affine point A, we have $B := A\sigma$ is distinct from A, and let m be the parallel class of AB. Let ℓ be any other affine line in the parallel class m. It is sufficient to show that such ℓ are σ-invariant. Choose an affine point $C \in \ell$. By hypothesis $D = C\sigma \neq C$. So CD is in the parallel class of m and, like ℓ, contains C. Hence both ℓ and CD are lines in the class m that contain C, so they coincide. Hence $\ell\sigma = CD = \ell$, since the image of any line is completely determined by the image of any one of itss affine points and the image of its parallel class. Thus all lines in the parallel class m are fixed by σ. ∎

We now consider collineations of the above type that might not fix any parallel class.

Definition 1.1.10 *A collineation fixing all the parallel classes of an affine plane is called a* DILATATION. *Dilations that are not translations are called kern homologies.*

So by remark 1.1.9 above, dilations other than translations fix at least one affine point point. If they fix more than one affine point then the set of fixed points form a subaffine plane which actually coincides with the parent plane. Thus, if π is any affine plane then the dilations other than translations, that is, the kern homologies, fix exactly one affine point Z, called its *center*. Moreover, remark 1.1.9 further implies that a non-trivial translation fixes all the lines of *exactly* one parallel class. This class is called the *center* of the translation. We summarize all this.

Remark 1.1.11 *Every non-trivial dilation of an affine plane is either a translation or a kern homology. Every non-trivial translation fixes all the lines of exactly one parallel class, called its* CENTER, *and no other affine lines or points, while every non-trivial kern homology fixes exactly one affine point, called its* CENTER, *and the other affine line that it fixes are just the lines through its center.*

Thus the set of all dilations of an affine plane form a group: the DILATION group, and it has as subgroups: the TRANSLATION group and the KERN HOMOLOGY group. To discuss these further we recall some standard definitions from permutation groups.

Definition 1.1.12 *Let G denote a permutation group acting on a set Ω. Then the G-orbit of $x \in \Omega$ is denoted by*

$$Orb_G(x) := \{x^g \mid g \in G\},$$

and the STABILIZER *of $x \in \Omega$ in G is denoted by:*

$$G_x = \{g \in G \mid x^g = x\}.$$

In particular, G is transitive on Ω if it has only one orbit, or equivalently:

$$x, y \in \Omega \Rightarrow \exists g \in G \ni x^g = y.$$

G is REGULAR *if additionally G_a is trivial for all $a \in \Omega$. More generally. a permutation group G on Ω is* SEMIREGULAR *if only the identity of G fixes any element in Ω.*

Using the above terminology, remark 1.1.11, yields:

Proposition 1.1.13 *Let $\mathcal{A}$ be an affine plane and G its dilation group. Then the translation subgroup T of G is normal in G and semiregular on all the affine points of $\mathcal{A}$. G is the union of T and all its maximal groups of kern homologies, and any two distinct groups in the union have trivial intersection.*

Proof: Exercise. ∎
The above result is far from optimal, particularly in the finite case, where the finite case where theory of Frobenius may be applied. But the reader is warned that glib generalizations to the infinite case might be dangerous.

We may now define translation planes.

Definition 1.1.14 *A translation plane is an affine plane whose translation group acts transitively on the affine points.*

As an immediate consequence of remark 1.1.9 we have

Remark 1.1.15 *An affine plane is a translation plane iff its translation group is regular on the affine points.*

A Frobenius group is a transitive permutation group in which the stabilser of any two points is trivial. By proposition 1.1.13 we have:

Remark 1.1.16 *The dilation group of an affine plane acts, faithfully, as a Frobenius group on its affine points.*

The point being made is that there is a deep and powerful theory for *finite* Frobenius groups that has been exploited in *finite* translation plane theory.

We now describe a simple construction for translation planes, and eventually we shall demonstrate that the construction is generic. The method is based on the notion of a *spread*, the most important concept in translation plane theory. *A spread is a partition of the non-zero points of a vector space by a collection of subspaces that pairwise direct-sum to the whole space.*

The lines through the origin in the real plane $\Re^2$ is the most familiar example of a spread: the real translation plane consists of the cosets of the components of the spread.

Viewing $\Re^2$ as a vector space over the rational field $\mathcal{Q}$, we have a $\mathcal{Q}$-spread with the same components as before — the lines through the origin — but now these components are infinite-dimensional subspaces. One can of course generalize all this: start with a rank two vector space over a a

skewfield F, then the one-spaces form a spread, and if F is an extension of a subskewfield K then the '1-dimensional spread' F-spread becomes a d-dimensional K-spread, when $dim_K F = d$, and the additive cosets define a translation plane.

Of course, the translation planes described above are the familiar Desarguesian planes, and indeed one could regard this construction as a definition of a Desarguesian spread: thus *a Desarguesian plane is the affine plane consisting of the cosets of the components of a one-dimensional spread over a skewfield F.*

We summarize our terminology for spreads and related items:

Definition 1.1.17 *Let V be a vector space, and let $\mathcal{S}$ be a collection of mutually disjoint additive subgroups of $(V,+)$ such that $V = \cup\mathcal{S}$ and the sum of each distinct pair of additive subgoups of $\mathcal{S}$ is V. Then $\mathcal{S}$ is called a* SPREAD *on V, or with* AMBIENT SPACE *V, and the subspaces on V are its* COMPONENTS. *The associated incidence structure is defined to be*

$$\Pi_{\mathcal{S}} := (V, \mathcal{C}),$$

with pointset V, lineset

$$\mathcal{C} := \{x + S \mid S \in \mathcal{S}, x \in V\},$$

and with set-theoretic incidence.

*If V is a vector space over a specified skewfield K, such that all the components of $\mathcal{S}$ are themselves K-subspaces of V, then $\mathcal{S}$ is called a K-*SPREAD*; this spread is called a d-*DIMENSIONAL *K-spread if each component is K-dimensional as a K-vector space.*

Remarks 1.1.18

1. *It will often be useful to draw attention to the ambient space V, associated with a spread $\mathcal{S}$, by referring to the pair $\pi = (V, \mathcal{S})$ as a spread. Thus,* π is viewed as being synonymous with $\mathcal{S}$.

2. *Every spread on V is a K-spread when K is chosen to be the prime subfield of the skewfields over which V is a vector space.*

3. *The direct-sum condition forces all components of a K-spread to have the same dimension d over K; d has sometimes been called the Ostrom dimension of the spread, to distinguish it from the dimension of the ambient space V which is $2d$, for finite d.*

We now note that the incidence structure of a spread is always a translation plane, and later we shall establish that all translation planes arise in this manner.

Theorem 1.1.19 *Let $\mathcal{S}$ be a spread on an ambient vector space V. Then the associated set-theoretic incidence structure, $\Pi(V,\mathcal{S})$, definition 1.1.17, is a translation plane. The full group of translations of $\Pi(V,\mathcal{S}$ is just the group of translations of V regarded as a vector space:*

$$\Theta := T = \{T_a : x \mapsto x + a \mid a \in V\}.$$

Moreover, if V is a vector space over a skewfield K such that the components are K-subspaces, that is $(V,\mathcal{S})$ is a K-spread, then the scalar action of K^* on V is a group of kern homologies of $\Pi(V,\mathcal{S})$; thus, the group of bijections on V

$$\widehat{K^*} := \{\forall x \in V : x \mapsto (x)k \mid k \in K^*\},$$

where $(x)k$ denotes the image of x under $k \in K$, is a group of kern-homologies, c.f., definition 1.1.10 of the translation plane $\Pi(V,\mathcal{S})$.

Proof: Straightforward exercise. ∎
Of particular importance are the maximal skewfields K over which the components are K-spaces. It will turn out that there is a unique maximal skewfield with this property. This will become clear as we develop the theory more fully.

Exercise 1.1.20 *Let $(V,\mathcal{S})$ be a spread and let T be the full translation group of the associated translation plane. To each component $\sigma \in \mathcal{S}$ assign the subgroup $T_{\{\sigma\}}$, the global stabilser of σ in T. Show that*

$$\cup_{\sigma\in\mathcal{S}} T_{\{\sigma\}} = T,$$

and that $T_\mu \cap T_\nu$ is the trivial group, whenever $\mu,\nu \in \mathcal{S}$ are distinct components.

Thus the full translation group T of a translation plane admits a partition by subgroups and thus appears to be analogous to the ambient space of a spread on a vector space. Our study of group partitions, in the next lecture, will show that such group partitions may be identified with spreads, and, in particular, that any translation group T may be taken to be the additive group of a vector space.

1.2 Group Partitions and André Theory.

In this lecture we develop André's fundamental theory relating translation planes to spreads. Our starting point is concerned with group partitions: a collection of pairwise disjoint subgroups of a group G that union to G.

A partition of a vector space by its set of one-spaces is an example of a group partition. A less trivial example arises when a field F is r-dimensional over a subfield K for then the additive group of F is partitioned by its r-dimensional K-spaces. Note, only the case $r = 2$ corresponds to examples of spreads in the sense of definition 1.1.17.

Definition 1.2.1 *(Group Partition.) Let G be a group. A* PARTITION *of G is a set N of nontrivial pairwise disjoint proper subgroups of G such that $G = \cup N$; the members of N are the* COMPONENTS *of the partition and if all the components in N are normal in G, then N is a* NORMAL PARTITION *of G.*

We have already noted that many normal partitions do not yield spreads, in the sense of definition 1.1.17. However, if the ambient group G of a normal partition is generated by any two of its elements then this is the only possibility, by the following fundamental characterization:

Theorem 1.2.2 *Let G be a group and N a normal partition of G such that*

$$G =< N_1, N_2 > \forall N_1, N_2 \in N, N_1 \neq N_2.$$

Then each of the following is valid:
(1) G is a direct product of any two distinct subgroups of N.
(2) each two distinct subgroups of N are isomorphic and
(3) G is Abelian.

Proof: (1) This is elementary as the elements of disjoint normal subgroups commute.
(2) A group cannot be expressed as the disjoint union of two distinct subgroups. Hence N contains at least three members. So given distinct $N_1, N_2 \in N$, we may choose a third $N_0 \in N$, and now $N = N_1 \oplus N_0$ and also $N = N_2 \oplus N_0$. Hence

$$N_1 \cong \frac{N}{N_0} \cong N_2,$$

as required.
(3) Since G is the direct sum of any two distinct members of N, we see that

elements from distinct subgroups of N commute. So assume $x, y \in A \in N$ and choose a nonidentity $b \in B \in N - \{A\}$, and observe

$$\begin{aligned} xyb &= xby \\ &\Rightarrow xyb = byx \text{ since } by \notin A \\ &\Rightarrow xyb = yxb \\ &\Rightarrow xy = yx, \text{ as required.} \end{aligned}$$

■

In view of the above it is desirable to call a normal partition N of a group G a *generating* normal partition if G is generated by every pair of distinct components $N_1, N_2 \in N$ generate G as a group.

Theorem 1.2.3 *Let N be the components of a spread on a group G. Then the set-theoretic incidence structure whose pointset is G and whose lines are the cosets of the elements of N is an affine translation plane whose translation group consists of the bijections of G, for every $a \in G$ of type:*

$$\begin{aligned} G &\to G \\ g &\mapsto ga \end{aligned}$$

Proof: A straightforward consequence of the theorem above.■

Theorem 1.2.4 *Let G be a group and N a generating normal partition of G. Let $\mathcal{K}$, denote the set of group endomorphisms which leave each component invariant.*

Then $\mathcal{K}$ is a skewfield and G is a vector space over $\mathcal{K}$.

The elements of the skewfield $\mathcal{K}$ are called the "kernel endomorphisms" of the partition. The skewfield $\mathcal{K}$ is called the "kernel of the spread."

Proof: Since G is abelian by the previous result, the endomorphisms in $\mathcal{K}$ clearly form a ring. Hence it is clearly sufficient to show that all the non-zero maps $\phi \in \mathcal{K}$ are bijective. Suppose $a^\phi = 0$ for $a \neq 0$. Now we force $\phi = 0$ by demonstrating that ϕ vanishes on every component $B \neq A$, where $a \in A$. We note that this is more than sufficient to force $\phi = 0$ since any two components of N generate G. As $0 = a^\phi = (a+b)^\phi + (-b)^\phi$ then $(a+b)$ and b are on C and B respectively which are distinct components so that

$b^\phi \in B \cap C = 0$ whenever b is in any component $B \neq A$. Thus all members $\phi \in \mathcal{K}$ are injective homomorphisms of G.

Next we check the elements $\phi \in \mathcal{K}$ are surjective.

Given nonzero $v \in G$, we require $w \in G$ such that $v = w^\phi \exists \phi \in \mathcal{K}$. Let V denote the component containing v and let $u \in U$ be a nonzero element in some other component of N, and define a third component Z that contains $u^\phi - v$. Now we claim that the required w is the unique point in the set $(Z + u) \cap X$. Note that the intersection is unique since it is the intersection of two lines of the affine point associated with the spread N.

It is now sufficient to show that $v - w^\phi = 0$, and we demonstrate this by showing that $v - w^\phi \in V \cap Z$. Since $w \in V$, $v - w^\phi$ certainly lies in V. Thus, it is sufficient to verify that $v - w^\phi \in Z$. But, by definition, $u^\phi - v \in Z$, so it is sufficient to verify that$(v - w^\phi) - (u^\phi - v) = (w - u)^\phi \in Z$. This condition holds because $w \in u + Z$ means that $(w - u) \in Z$, and Z is ϕ-invariant. Thus, ϕ is surjective. ∎

The following standard notation concerning linear groups will be used thoughout our lectures.

Definition 1.2.5 *Let V be a left vector space over a skewfield K. Let σ be an additive mapping on V. We shall say that σ is K-semi-linear if and only if for all α in K and for all x in V then $\sigma(\alpha x) = \alpha^\rho \sigma(x)$ where ρ is an automorphism of K. We shall say that σ is K-linear if and only if $\rho = 1$.*

The group $\Gamma L(V, K)$ of all bijective K-semi-linear mappings is called the general semi-linear group. The subgroup $GL(V, K)$ of linear mappings is called the general linear group.

Let F denote the prime field of K. Then $\Gamma L(V, F) = GL(V, F)$. Since any additive bijection is in $GL(V, F)$, the notation $GL(V, +)$ is always used.

In 1954, André provided the foundation for the theory of translation planes by proving that any translation plane may be identified with a normal partition of a group which actually turns out to be a vector space over a skewfield:

Theorem 1.2.6 *(The Fundamental Theorem Of Translation Planes.)*
Let π be a translation plane with translation group T and let $\mathcal{P}$ denote the set of parallel classes of π.
Let T_p denote the subgroup of T fixing all the lines of p, for $p \in \mathcal{P}$. Then all the following hold.

1. $\Gamma = \cup\{T_p \mid p \in \mathcal{P}\}$ *is a spread on* T *and hence* T *is a vector space over the associated kernel* $\mathcal{K}$.

2. π *is isomorphic to* π_Γ, *the translation plane constructed from the spread of* T.

3. *The full collineation group* G *of* π_Γ *is* TG_O *where* G_O *is the full subgroup of the group* $GL(T,+)$, *that permutes the members of* Γ *among themselves.*

4. *The full collineation group* G *of* π_Γ *is* TG_O *where* G_O *is the full subgroup of the group* $\Gamma L(T,\mathcal{K})$ *that permutes the members of* Γ *among themselves.*

Proof: (1) T_p is the subgroup of T fixing individually all the lines through p, hence it is trivially normalized by T since T fixes p. Since every translation in T has a unique center, T gets partitioned by its normal subgroups of type T_p. It remains to show that $T = T_p \oplus T_q$ whenever p and q are distinct points on the translation axis. Let $t \in T$, and suppose $t : a \mapsto b$, where a is any affine point, and assume $b \neq a$, to avoid trivialities. Since T_p and T_q are normal and disjoint, it is sufficient to verify that $t \in < T_p, T_q >$. Let $pa \cap qb = x$. Since T_p has as its non-trivial orbits all the affine on each line through p, there is a $g \in T_p$ such that $g : a \mapsto x$ and, similarly, there is an $h \in T_q$ such that $h : x \mapsto b$. Now clearly $a^{gh} = b$. But the regularity of T now forces $t = gh$. Thus T is generated by any two distinct T_p and T_q.

(2) Fix an affine point O of π, and to each affine point a of π assign the translation $\tau_a \in T$ that maps O onto a. Consider the bijection $\Theta : a \mapsto \tau_a$, from the affine points of π onto the points of the vector space T.

Consider the affine point $a \in A$, where A is any affine line of π. Let A_m be the unique line parallel to A through O with slope m. Clearly, T_m has A_m as its O-orbit, so $(A_m)\Theta = T_m$.

Next note that the points of A may be expressed as $O^{\tau_a T_m}$, as the group T_m acts transitively on the affine points of each line through m. Now the image $\left(O^{\tau_a T_m}\right)\Theta = \tau_a T_m$, i.e., a coset of T_m. Thus we have shown the bijection Θ maps the lines of π to cosets of the spreads associated with T, which means Θ is a bijection from the affine plane π onto the affine plane associated with the spread on T that sends lines onto lines. Hence, Θ is an isomorphism between the planes.

(3) The translation subgroup of the full collineation group G of π_Γ may, of course, be identified with T itself. Let $H = G_O$, so $G = HT$, by the transitivity of T , and by its regularity we further have $H \cap T = \{1\}$ (the identity element). We next verify that H is in $GL(T, +)$.

We define addition in π as follows: $a + x = \tau_a(x)$. It follows that this makes $(\pi, +)$ isomorphic to T.

Since T is normal in the translation plane π_Γ, we have for every $a \in T$ a unique $a' \in T$ such that

$$h\tau_a = \tau_{a'}h$$

so

$$h\tau_a(x) = \tau_{a'}h(x) \forall x \in T$$

hence

$$h(a + x) = a' + h(x) \forall x \in T.$$

Putting $x = O$, we observe that $a' = h(a)$ and so the above identity yields

$$h(a + x) = h(a) + h(x)$$

so h is additive and hence lies in $GL(T, +)$, and permutes the members of Γ. Conversely, any map with these two properties also permutes the cosets of the components of Γ, and is thus a collineation of π_Γ. Thus (3) is established.

(4) By (3), H is the largest subgroup of $GL(T, +)$ that permutes the members of Γ among themselves, and the kernel of this representation of H on Γ is thus normal in H and coincides with $\mathcal{K}^*$ by definition. The normality of $\mathcal{K}^*$ now forces H to be semilinear over $\mathcal{K}$.

This completes the proof of the theorem. ∎

Since the translation group of any spread (V, S), associated with a translation plane π, is additively isomorphic as an additive group to the translation group of π, all such spreads (V, S) have isomorphic additive groups $(V, +)$. The non-zero kernel endomorphisms of such spreads are permutation isomorphic to the the kern homologies, acting on the plane. This suggests that all such spreads, associated with a fixed translation plane, are related by a spread isomorphism semilinear over their kern, and more generally that any collineation the of the planes associated with the spreads that sends zero to zero must be a semilinear map of the type indicated. This is indeed the case as we shall now verify.

The main problem is to verify that such collineations are additive; we shall verify this directly rather than attempting to derive it from part (3) of the fundamental theorem above.

Theorem 1.2.7 *Let $(V,\mathcal{S})$ and $(W,\mathcal{T})$ be spreads defining isomorphic translation planes, and suppose that $\Psi : W \to V$ is any isomorphism from the translation plane $\Pi_{(W,\mathcal{T})}$ to the translation plane $\Pi_{(V,\mathcal{S})}$ such that $\mathbf{0} \mapsto \mathbf{0}$; ψ exists since the planes admit point-transitive translation groups. Let K and L be respectively the skewfields of kernel endomorphisms of the spreads $(V,\mathcal{S})$ and $(W,\mathcal{T})$. Then there is bijective ring isomorphism $\psi : L \to K$ such that there is a $K-L$-semilinear bijection $\Psi : V \to W$, satisfying $\Psi(aw) = a^{\psi}(w)$, for all $w \in W$, $a \in K$.*

Proof: Since the translation groups of the two planes are isomorphic, V and W are isomorphic additive groups, so $(V,+)$ can be made into a K-vector space such that a K-linear bijection from V to W exists ad this bijection identifies the spread $\mathcal{T}$ with a spread on V, such that the components of $\mathcal{T}$ are K-spaces, and that K is still the full ring of kernel endomorphisms.

Thus we consider $\mathcal{S}$ and $\mathcal{T}$ to be spreads on the same vector space $(V,+)$, over K, such that K is the largest ring leaving the components of $\mathcal{T}$ invariant. Since Ψ is a collineation of the associated planes it must map the components of $\mathcal{T}$ onto the components of $\mathcal{S}$. Since the non-zero kernel endomorphisms of the spreads are subgroups of $GL(V,+)$ that leave its components invariant it is clear that the planar isomorphism Ψ must conjugate the kernel endomorphisms of $\mathcal{T}$ to $\mathcal{S}$, and since the planes are simorphic under Ψ we actualy have a field isomorphism $\psi : K \to L$, $K \mapsto k^{\psi}$, such that $\Psi(av) = a^{\psi}\Psi(v)$, for $a \in K$, $v \in V$, and in particular that $\Psi(-x) = -\Psi(x)$ for all $x \in V$.

It remains to show that Ψ is bijective. It preserves, in the associated affine plane, the parallelogram $\mathbf{0}, a, b, a+b$, whenever a and b are in different components of $\mathcal{T}$, hence in such cases $\Psi(a+b) = \Psi(a) + \Psi(b)$. If they are in same component W then we esatblish this by choosing $u \notin W$ and noting that:

$$\begin{aligned}
\Psi(a+u+b) = \Psi(a+u) + \Psi(b) &= \Psi(a) + \Psi(u) + \Psi(b) \\
\Psi(a+u+b) - \Psi(u) = \Psi(a+u) + \Psi(b) &= \Psi(a) + \Psi(b) \\
\Psi(a+u+b) - \Psi(+u) = \Psi(a+u) + \Psi(b) &= \Psi(a) + \Psi(b) \\
\Psi(a+b) + \Psi(u) - \Psi(+u) = \Psi(a+u) + \Psi(b) &= \Psi(a) + \Psi(b) \\
\Psi(a+b) + \Psi(u) - \Psi(u) = \Psi(a+u) + \Psi(b) &= \Psi(a) + \Psi(b)
\end{aligned}$$

$$\Psi(a+b) = \Psi(a+u) + \Psi(b) \quad = \quad \Psi(a) + \Psi(b)$$

provided u is further restricted not to lie in the component containing $a+b$.
■
As an immediate consequence we have:

Theorem 1.2.8 *Let $(V,\mathcal{S})$ and $(W,\mathcal{T})$ be spreads, with associated translation planes $\pi_{\mathcal{S}}$ and $\pi_(W,\mathcal{T})$. Let L and T denote the kernel endomorphism rings of $(V,\mathcal{S})$ and $(W,\mathcal{T})$ respectively.*
Let $\Psi : W \to V$ be an additive bijection. Then the following are equivalent:

1. *Ψ is an isomorphism from the spread $(W,\mathcal{T})$ onto the spread $(V,\mathcal{T})$.*
2. *There is a bijective kern isomorphism $\psi : K \to L$ such that Ψ is a K-L semilinear isomorphism, with companion isomorphism ψ, that induces a spread isomorphism from $(W,\mathcal{T})$ onto the spread $(V,\mathcal{T})$.*
3. *Ψ is an isomorphism from the plane $\pi_(W,\mathcal{T})$ onto the plane $\pi_(W,\mathcal{T})$.*

In view of the importance of the above reformulate as follows:

Theorem 1.2.9 *(Isomorphism Theorem For Translation Planes.) Let $\Phi := \Pi_{(V,\mathcal{S})}$ be a translation plane defined by a spread $(V,\mathcal{S})$, where the components of $\mathcal{S}$ are K-subspaces of the K-vector space V, where K is any skewfield. Suppose that there is an affine-plane isomorphism:*

$$f : \Phi \longrightarrow \Psi$$

from the translation plane Φ to a translation plane $\Psi := \Pi_{(W,\mathcal{R})}$, defined by a spread $(W,\mathcal{R})$, where the components of $\mathcal{R}$ are L-subspaces of the L-vector space W, where L is any skewfield.

1. *Then L and K are isomorphic skewfields and ϕ may be considered a semi-linear mapping from W onto V.*
2. *If $\Phi = \Psi$ then ϕ is an element of the group $\Gamma L(V,K)$.*
3. *The full automorphism group G of the translation plane π is a semi-direct product of the translation group T by the subgroup G_0 of $\Gamma L(V,K)$ which permutes the components of the spread S.*

The subgroup G_0 of $\Gamma L(V,K)$ is called the 'translation complement' of G or π. $G_0 \cap GL(V,K)$ is called the 'linear translation complement.'

Proof: See above. ∎

We now make some conventions regarding the kernel of a spread, or its *kern*, as we shall usually call it. These relates to the fact that the components of a spread $\mathcal{S}$ may be regarded as being subspaces of the ambient vector space V, over *any* subfield F in the kern of $\mathcal{S}$, in the sense of theorem 1.2.6 above: so in general there is a multitude of dimensions associated with a spread — depending on the field or skewfield over which we choose to *represent* it. If the 'chosen field' is F, in the kern K of the spread $\mathcal{S}$, then we shall sometimes call F the 'chosen kern', the 'component kern' or the 'intended kern'.

Definition 1.2.10 *Let V be a vector space over a skewfield F that contains a spread $\mathcal{S}$), consisting of F-subpaces; so F is the component kern. The* RANK OVER F *of $(V,\mathcal{S})$ is the common dimension of the members of $\mathcal{S}$: so an n-dimensional F-spread $\mathcal{S}$ has ambient space V with* dimension $2n$*; now $\pi := (V,\mathcal{S})$* IS REGARDED AS BEING AN F-SPREAD OF F-RANK n. *The* RANK *of $\mathcal{S}$ is its rank over K, the kern of $\mathcal{S}$.*

Since any rank two vector space, over an arbitrary skewfield K, partitions into a collection of rank one spaces, we conclude that *one dimensional spreads exist over every sfield*! But, as indicated earlier, we may now regard these spreads as being F-spreads of rank > 1 whenever F is a subfield of K. Thus F-spreads of F-rank n exist in abundance. This raises a problem — not too hard but certainly non-trivial — how do we know whether any spread that we construct is not a rank-one spread in disguise? Putting it somewhat more provocatively:

$$\boxed{\text{Are ALL spreads rank ONE!?}} \tag{1.1}$$

So we need to first of all describe all rank one spreads, that is, spreads that are rank one over their *full* kern. We begin by officially adopting the definition:

Definition 1.2.11 *A rank one spread is called a* DESARGUESIAN SPREAD.

A rank one spread is isomorphic to a spread δ on the vector space $V = K^2$, where

1. K is a skewfield acting wlog from the left in the standard way:

$$\forall k, k_1, k_2 \in K : k(k_1, k_2) = (kk_1, kk_2);$$

2. The components of δ are the subspaces of type 'y=xm', $m \in K$, and $x = 0$, as in coordinate geometry.

The proof follows from the fact that any rank two vector space may be regarded as some K^2, with K acting form the left, and *all* the rank-one spaces must be components. The associated affine plane consists of all cosets of the spread components and hence the lines are of form $y = xm + b$ and $y = c$. Thus rank-one spreads correspond to precisely the high-school interpretation of the term. Hence we have justified our terminology by showing that:

Remark 1.2.12 (Desarguesian Spreads.) *The following are equivalent for a spread $\mathcal{S}$:*

1. *$\mathcal{S}$ is rank one over its kern;*

2. *The affine plane $\pi_{\mathcal{S}}$, associated with $\mathcal{S}$, is a Desarguesian plane.*

Note that we have now described all one-dimensional spreads over any skewfield K! In the finite case all finite skewfields are Galois fields, so *all rank one spreads are* REALLY! *known.* So the obvious next step is:

INVESTIGATE THE RANK TWO SPREADS OVER A GALOIS FIELD! (1.2)

During the last twenty years a great deal of attention has been given to this project; there are also associations with other areas of finite geometries, particularly flocks and generalized quadrangles. Note that the existence of rank two spreads obviously settles as a by-product the 'first question' for spreads, see (1.1). The principal tool for such investigations involve *spreadsets*, the main concern of the next lecture.

1.3 Spreadsets and Partial Spreads.

In the previous lecture, we saw that by the fundamental theorem of translation planes, theorem 1.2.6, translation planes may be identified with spreads. Here we introduce tools and concepts that arise inevitably in the study of spreads. The concept of a *partial* spread describes collections of subspaces of a vector space that putatively extend to a spread. The other concept that we introduce aims at 'coordinatizing' spreads and partial spreads by sets of matrices (in the finite-dimensional case), exploiting the fact that spreads

(and hence translation planes) are always associated with some vector space. These sets of matrices, or linear maps in the general case, are called [partial] spreadsets: they provide the most important computational tool in the study of translation planes.

In the motivating case, *a spreadset is a set of q^n matrices $\mathcal{M} \subset GL(n,q) \cup \{\mathbf{O}\}$ such that any two members of $\mathcal{M}$ differ by a non-singular matrix and $\mathbf{O} \in \mathcal{M}$.* Such a set yields a spread $\pi_{\mathcal{M}}$ in $V = GF(q)^n \oplus GF(q)^n$: the components are $y = xM$, $M \in \mathcal{M}$ and $x = 0$, mimicking the the construction of elementary coordinate geometry. The spread $\pi_{\mathcal{M}}$ actually turns out to be a generic form for any $GF(q)$-spread on V: so spreads may be computationally investigated via their spreadsets of matrices.

The complete definition of a spreadset is a routine generalization of the above, assigning to *any* spread a spreadset of linear maps that represents it. As in the finite case, this association enables all the major tools of linear algebra to be brought to bear on the study of spreads. When the underlying field $GF(q)$ is generalized to an arbitrary skewfield K the cardinality and dimensionality condition implicit in $|\mathcal{M}| = |K|^n$ needs to be reformulated. This will be achieved by defining the familiar concepts of semiregularity and transitivity from permutation group theory so as to apply to SETS of possibly infinite bijections.

Accordingly, we begin by explaining what transitivity and regularity mean in the context of a set of permutations on Ω, where Ω may be an infinite set. The definitions here generalize the corresponding definitions for permutation *groups* listed in definition 1.3.1.

Definition 1.3.1 *Let G denote a set of bijections of a set Ω. Then the G-orbit* AT *$x \in \Omega$ is*

$$Orb_G(x) := \{x^g \mid g \in G\}.$$

G is called a TRANSITIVE *set of maps on Ω if $Orb_G(x) = \Omega$ for all $x \in \Omega$. The set G is called semi-regular if:*

$$(x,y) \in \Omega \times \Omega \Longrightarrow \exists! g \in G \ni xg = y,$$

and G is a REGULAR *set of bijections of Ω if it semiregular and transitive on Ω.*

For finite sets, it is straightforward to check that all of the above concepts coincide provided G and Ω have the same size:

Remarks 1.3.2 *If G is a set of bijections on a finite set Ω and $|G| = |\Omega|$ then the following are equivalent:*

(a) G is semiregular;

(b) G is regular;

(c) G is transitive.

Note that condition (b) above implies $|G| = |K|$, even in the infinite case, and hence we shall use it as the basis of our general definition of a spread. However, we begin by introducing spreadsets, not in their most general form, but rather in the form that they are most frequently encountered: as sets of q^n matrices in $\overline{GL(n,q)} := GL(n,q) \cup \{\mathbf{O}\}$ that act regularly on $GF(q)^n - \{\mathbf{0}\}$.

Definition 1.3.3 *An $n \times n$* SPREADSET OF MATRICES *over $GF(q)$ is a set of matrices*

$$\{\mathbf{O}\} \subset \mathcal{M} \subset \overline{GL(n,q)}$$

such that (1) $|\mathcal{M}| = q^n$; (2) Any two distinct member of $\mathcal{M}$ differ by a non-singular matrix.

It is immediate that the action of the above $\mathcal{M}^* := \mathcal{M} - \{\mathbf{O}\}$ on $GF(q)^n - \{\mathbf{0}\}$ is regular and that the regularity of $\mathcal{M}^*$ is actually equivalent to the definition of a finite spreadsets. Thus the concept of a spreadset, as indicated earlier, can be generalized to arbitrary vector spaces over any skewfield as follows:

Definition 1.3.4 *Let K be any skewfield, and V a vector space over K. A* K-SPREADSET *of V is a set $\mathcal{M}$ of linear maps:*

$$\{\mathbf{O}\} \subset \mathcal{M} \subset \overline{GL(V,K)}$$

such that $\mathcal{M}^*$ acts as a regular set of maps on V^*.

Thus, a finite set of matrices over $K = GF(q)$, is a spreadset of matrices in the sense of defintion 1.3.3 iff it is a spreadset of linear maps in the sense of definition 1.3.4 above: just apply remark 1.3.2 above.

It is important to realise that the non-singularity-of-difference condition, in the definition of finite matrix spreadsets, definition 1.3.3, may be used in characterising general spreadsets:

Remark 1.3.5 *Let K be any skewfield, and V a vector space over K. A set $\mathcal{M}$ of linear maps of V satisfying:*

$$\{\mathbf{O}\} \subset \mathcal{M} \subset \overline{GL(V,K)}$$

is a spreadset iff:

1. *$A, B \in \mathcal{M}$ are distinct then $A - B \in GL(V,K)$;*
2. *If $(x,y) \in V^* \times V^*$ then there is an element $M \in \mathcal{M}$ such that $xM = y$.*

In particular, a set $\mathcal{M}$ of $n \times n$ matrices over $GF(q)$ is a spreadset iff they form a matrix spreadset in the sense of definition 1.3.3, that is, $\mathcal{M}$ has q^n elements, including zero, any two of which differ by a non-singular matrix or zero.

Proof: The second condition means that $\mathcal{M}^*$ is transitive on V^*, and the first condition means that $\mathcal{M}^*$ is semiregular on V^*, since otherwise $x(A-B)$ would be zero for some $x \in V^*$. ∎

With every spreadset we shall associate a collection of subspaces which turn out to be spreads. The notation that we use here is suggested by elementary coordinate geometry, and similar notation will be used throughout these notes, sometimes without explicit definition.

Definition 1.3.6 *Let W be a vector space over a skewfield K and let $\mathcal{M}$ be a K-spreadset on W. Then $\pi_{\mathcal{M}}$ is a collection of subsets of $V = W \oplus W$ defined by*

$$\pi_{\mathcal{M}} := \{Y\} \cup \{y = xM \mid M \in \mathcal{M}\},$$

where $Y = \mathbf{O} \oplus W$ and $y = xM$, $m \in \mathcal{M}$, denotes the subset $\{(w, wM) \mid w \in W\}$ of V — so $y = \mathbf{O}$, also called X, is in $\pi_{\mathcal{M}}$. The collection $\pi_{\mathcal{M}}$ is called the SPREAD ASSOCIATED WITH $\mathcal{M}$.

We now justify the terminology by verifying that $\pi_{\mathcal{M}}$ is a genuine K-spread:

Remark 1.3.7 *Let W be a vector space over a skewfield K. Let $\mathcal{M}$ is a K-spreadset on W. Then its associated spread $\pi_{\mathcal{M}}$, definition 1.3.6 above, is a collection of K-subspaces of V that form a K-spread, in the standard sense, with ambient space $V = W \oplus W$.*

Proof: The linearity of M over K ensures that $\{(x, xM) \mid x \in W\}$ is a K-subspace of $V = W \oplus W$ — the linearity means that the K-action on W commutes with the M-action. Next we note that $y = xM$ and $y = xN$, where $M, N \in \mathcal{M}$, are *disjoint* K-subspaces of V, for $M \neq N$: for otherwise $M - N$ would be singular, contradicting $M - N \in GL(n, W)$, c.f., remark 1.3.5. Given $(a, b) \in W^* \oplus W^*$, there is an $M \in \mathcal{M}$ such that $b = aM$, by the transitivity condition on $\mathcal{M}$. Hence, it easily follows that the subspaces in the structure $\pi_{\{}\mathcal{M}\}$ form a pairwise disjoint cover of V^*. It remains to check that V is a direct sum of any two of the 'components' in $\pi_{\{}\mathcal{M}\}$. (This is obvious if W is finite dimensional over K, in particular if $\mathcal{M}$ is finite.) The main case is when the components are $y = xM$ and $y = xN$, where $\mathbf{O} \neq M \neq N \neq \mathbf{O}$, and here we need to show that any $(a, b) \in V$ lies in the sum of $y = xM$ and $y = xN$. Thus, we need to show that

$$(a, b) = (u, uM) + (v, vN) \exists u, v \in W,$$

or, equivalently, for some $u, v \in W$:

$$\begin{aligned} a &= u + v \\ b &= uM + vN \end{aligned}$$

and this means $b - aN = u(M - N)$, which can be solved for u by the non-singularity condition on $M - N$, remark 1.3.5, and the desired result follows easily. ∎

Thus to find a spread, and hence a translation plane of order q^n, it is sufficient to find a set of $q^n - 1$ matrices in $GL(n, q)$ such that any two of them differ by a non-singular matrix. This follows from the above, also c.f. defintion 1.3.3. We illustrate this with an important example, discovered first by Donald Knuth.

Example 1.3.8 *(Knuth's γ-spreads.)* Let $K \cong GF(q)$ be a finite field, where $q = p^r > p$ is odd. Let γ be a fixed nonsquare in K, and $\sigma \in Gal(K)^*$ Then

$$\mathcal{M} = \left\{ \begin{bmatrix} u & \gamma t^\sigma \\ t & u \end{bmatrix} \forall u, t \in K \right\}.$$

Proof: Because γ is non-square, the determinant $u^2 - \gamma t^(\sigma + 1)$ cannot be zero unless $u = t = 0$. Thus we have an additive group of matrices whose non-zero elements are non-singular. This means that the difference between

any two distinct members of $\mathcal{M}$ are non-singular, and since we have $q^n = q^2$ such matrices $\mathcal{M}$ is a spreadset by remark 1.3.5. ∎
This is the first spread of rank 2 that we have displayed, although we have not yet shown that it is not Desarguesian, i.e. a rank-one spread in disguise. Once we have developed some more machinery this will become immediately obvious. At this stage more compuational effort is required: as an exercise the reader is invited to verify that the group of kern-homologies is *not* transitive, as a group of homolgies: this means the spread cannot be Desarguesian and hence must be rank two — thereby answering the 'first question' (1.1), and also contributing to (1.2).

Note also that the argument used in example 1.3.8 above yields a more general result: the proof is left as an exercise, and involves recalling the connection between spreads and translation planes:

Proposition 1.3.9 *An additive group $\mathcal{M}$ of $n \times n$ matrices over $GF(q)$ is a spreadset iff the group has order q^n and its non-zero elements are all nonsingular. Moreover, the associated spread $\pi_{\mathcal{M}}$ corresponds to a translation plane that admits a group of kern homologies of order $q-1$.*

The spreadsets of the above type are called *additive* spreadsets, and will be treated in detail later on. They form a major branch of translation plane theory with their own methodology, related to non-associative divison ring theory.

We now turn to the converse of remark 1.3.7. The eventual goal is to show that every *spread* is associated with a *spreadset*. But we first take the opportunity to work from more general premises, by introducing *partial* spreads and the partial spreadsets that coordinatize them.

Definition 1.3.10 *Let $\mathcal{T}$ be a non-empty collection of subspaces of a vector space V over a skewfield K. Then $\mathcal{T}$ is a* PARTIAL SPREAD *on V, and its members are its* COMPONENTS *if $V = A \oplus B$ for every pair of distinct $A, B \in \mathcal{T}$, and if $|\mathcal{T}| \leq 2$ assume explicitly that $V/A \cong A$ for $A \in \mathcal{T}$.*

Of course, $V/A \cong A$ applies automatically if $\mathcal{T}$ has at least three components. Note also that although subsets of spreads are always partial spreads, there are many partial spreads that cannot be extended to spreads: thus, there are maximal partial spreads that are *not* spreads.

To construct partial spreads, we generalize, in obvious ways, the notation and concepts that relate spreadsets to spreads in definition 1.3.6. We continue

with our convention of applying the language of coordinate geometry to any direct sum $V = W \oplus W$, c.f. definiton 1.3.6.

Definition 1.3.11 *Let W be a vector space over a skewfield K. Then a non-empty set $\tau \subset GL(V,K) \cup \{\mathbf{O}\}$ is a* PARTIAL K-SPREADSET *if*

$$T_1, T_2 \in \tau \Longrightarrow T_1 - T_2 \in \overline{GL(V,K)}.$$

The associated structure of τ is the collection of subspaces of $V = W \oplus W$ given by:

$$\pi_\tau := \{y = xT \mid T \in \tau\} \cup \{Y\}.$$

In general, $\tau \subset GL(V,K) \cup \{\mathbf{O}\}$ is a SPREAD SET *if τ is a K-spread where K is the prime field over which V is a vector space.*

Note that we have included $\{Y\}$, as our earlier convention requires us to do this if τ is a spreadset, c.f., definition 1.3.6. Stating the obvious:

Remark 1.3.12 *If τ is a partial spreadset on a vector space W then π_τ is a partial spread on $V = W \oplus W$, and π_τ is a spread iff τ is a spreadset. Hence π_τ is called the* PARTIAL SPREAD ASSOCIATED WITH THE PARTIAL SPREADSET τ.

It is worth restressing that the above remark assumes that the spread on $W \oplus W$ by a spreadset τ of W always includes $Y := \mathbf{O} \oplus W$, unless the contrary is indicated: without this assumption π_τ fails to be a spread when τ is a spread.

The following easy exercise emphasizes that in the finite case a partial spreadset is just a set of non-singular matrices, possibly augmented by $\mathbf{O}$, such that any two differ by a non-singular matrix.

Remark 1.3.13 *Let V be a vector space over a skewfield K. A non-empty set $\tau \subset \overline{GL(V,K)}$ is a partial spread iff τ^* is semiregular on V^*.*

In particular, if $\tau \subset \overline{GL(n,q)}$ is a non-empty set of matrices then τ is a partial spreadset iff and the difference between any two distinct matrices in τ is non-singular.

Proof: Exercise. ∎

We now introduce the notion of isomorphic partial spreads, generalising the corresponding notion for a spread.

Definition 1.3.14 *Let $\pi_i = (V_i, \tau_i)$, $i = 1, 2$, be partial spreads, where V_1 and V_2 are the underlying vector spaces over a common skewfield K. Then a K-linear bijection $\Psi : V_1 \to V_2$ is* A K-LINEAR ISOMORPHISM *from π_1 to π_2, or τ_1 to τ_2, iff it bijectively maps the components τ_1 onto those of τ_2.*

More generally, an ISOMORPHISM *from π_1 onto π_2 is an additive isomorphism from V_1 onto V_2 that maps components onto components.*

There are of course a number of equivalent ways of defining isomorphisms among partial spreads, for example an additive isomorphism from V_1 onto V_2 is an isomorphism of the associated spreads iff it maps components onto components. The usual terminology associated with isomorphism, automorphism etc. will be used without further comment.

The following theorem implies that all spreads arise from spreadsets: there is an isomorphism from any K-spread (or partial spread) to the spread arising from a spreadset (or partial spreadset). This is one of the most important connections in translation plane theory.

Theorem 1.3.15 (Equivalence Of (Partial) Spreads and Spreadsets *Let V be a vector space over a skewfield K, and let $\mathcal{T}$ a partial spread of subspaces, with at least three components X, Y, W,.... Choose a K-linear bijection* IDENTIFYING *Y with X:*

$$\Psi : Y \longrightarrow X.$$

Then relative to (X, Y, Ψ):

1. *For every $W \in \mathcal{T} \setminus \{Y\}$ the map $\tau_W : X \to Y$ specified by:*

$$\begin{array}{rcl} \tau_W : X & \longrightarrow & Y \\ x & \longmapsto & y \Leftrightarrow x \oplus y \in W \end{array}$$

   is a linear bijection from X onto Y when $W \neq X$ ($\tau_X = \mathbf{O}$) and hence $\Psi\tau_W : X \to X$, WRITTEN *σ_W, is an element of $GL(V, K)$; σ_W is called the* SLOPE MAP, *or the* SLOPE ENDOMORPHISM, *of W, relative to* AXES *(X, Y) (via the identification $\Psi : Y \to X$).*

2. *For fixed X and Y and* any *choice of $W \in \mathcal{T} \setminus \{X, Y\}$, Ψ can be chosen so that $\sigma_W = \mathbf{1}$; in fact $\Psi = {\tau_W}^{-1}$.*

3. *The set of all endomorphisms of* $\mathcal{T}$*:*

$$\sigma_{\mathcal{T}} := \{\sigma_W \mid W \in \mathcal{T} \setminus \{Y\}\}$$

corresponds, after deleting the zero map, to a semiregular subset of $GL(X, K)$ *on* X^**.*

4. *The partial spread determined by* $\sigma_{\mathcal{T}}$*, viz.* $\pi_{\sigma_{\mathcal{T}}}$*, c.f., definition 1.3.11 and remark 1.3.12, is isomorphic to the given spread* $\mathcal{T}$*. In fact, the linear bijection* $\mathbf{1}_X \oplus \Psi^{-1}$*:*

$$\begin{array}{rcl} X \oplus X & \longrightarrow & X \oplus Y \\ a \oplus b & \longmapsto & a \oplus (b)\Psi^{-1} \end{array}$$

is a linear isomorphism from the [partial] spread $\pi_{\sigma_{\mathcal{T}}}$ *onto the [partial] spread* $\mathcal{T}$ *that maps* $X \oplus \mathbf{O}$ *and* $\mathbf{O} \oplus X$ *onto* X *and* Y *respectively, that is, the isomorphism can be chosen so that the* X *and* Y *'axes' are preserved.*

Moreover, if the 'axes-identifying' linear bijection $\Psi : X \to Y$ *is specified by* $\Psi := {\tau_W}^{-1}$*, where* $\tau_W : X \to Y$ *is the linear bijection associated with* $W \in \tau \setminus \{X, Y\}$*, then the 'unit component'* $Z := \{(x, x) \mid x \in X\}$ *is assigned, by the partial spread isomorphism* $\mathbf{1}_X \oplus \Psi^{-1}$*, to the chosen component* $W \in \mathcal{T}$*.*

To summarize, $\mathcal{T}$ *may be identified, via a linear bijection* $\Lambda : V \to X \oplus X$*, with a partial spread* π_τ *on* $X \oplus X$*, corresponding to a spreadset* τ *on* X*, such that the identification sends respectively the components* X *and* Y *of* $\mathcal{T}$ *onto respectively the* x*-axis, i.e.* $X \oplus \mathbf{O}$*, and the* y*-axis, i.e.* $\mathbf{O} \oplus X$*. Morever, the map* $\Phi : Y \to X$ *that* Λ *induces naturally from* Y *to* X*, defined by restrictiing it to* Y*:*

$$\Phi := \Lambda | Y \to \mathbf{O} \oplus X \overset{\text{natural}}{\longrightarrow} X$$

can be chosen, for appropriate $\Lambda := \Lambda_\Phi$*, so that* $\Phi = \Psi^{-1}$*, where* $\Psi : Y \to X$ *is the given identification; and if now* Ψ *is taken as* ${\tau_W}^{-1}$ *then* Λ *additionally maps the component* W*, distinct from* X*,* Y*, onto the unit line* Z *defined above.*

5. *If* $\mathcal{T}$ *is a spread then the following are equivalent:*

(a) The set of slope endomorphisms σ_T is a spreadset on X.

(b) σ_T^* is regular on X^*.

(c) σ_T^* is transitive on X^*.

Proof: (1) We first show that τ_W is a map. Consider $\tau_W(x)$. If y_1 and y_2 are distinct elements of Y such that $x + y_1 \in W$ and $x + y_2 \in W$, then $y_1 - y_2 \in W$, and this is a contradiction because the components of a partial spread do not overlap. Since $X \oplus Y$ is the whole space we certainly have $x + y \in W$, for some $y \in Y$. Hence $\tau_W : X \to Y$ is a map, and it is equally straightforward to check that this map is linear and injective, for $W \notin \{X, Y\}$.

To verify that τ_W is bijective, for W distinct from X and Y, consider $y \in Y$. If $y \neq \tau_W(u)$ for all $u \in X$ then $u + y \notin W$ for all $u \in X$, so $y \notin X \oplus W$, contradicting the fact that any two components must direct-sum to the whole space V. Hence (1) holds, since it is trivial that $\tau_X = \mathbf{O}$.
(2) This case is immediate.
(3) Now consider τ_A and τ_B, where A and B are distinct components, other than X and Y. If $\tau_A - \tau_B(x) = \mathbf{0}$, for $x \neq \mathbf{0}$, then $x \oplus \tau_A(x) \in A \cap B$, contradicting the fact that distinct components do not over lap. Thus $\Psi\tau_A(x) \neq \Psi\tau_B(x)$, for $x \neq \mathbf{0}$, which means $\sigma_A(x) \neq \sigma_B(x)$, and hence σ_T is a semiregular spreadset in $\overline{GL(V,K)}$.
(4) The partial spread π_{σ_T} associated with σ_T, in the sense of remark 1.3.12, has components $\{(x, x\tau_W\Psi) \mid x \in X\}$, for $W \in \tau$ The linear bijection $\mathbf{1}_X \oplus \Psi^{-1}$ defined by

$$\begin{array}{rcl} X \oplus X & \longrightarrow & X \oplus Y \\ a \oplus b & \longmapsto & a \oplus (b)\Psi^{-1} \end{array}$$

maps $(x, x\sigma_W) = (x, x\tau_W\Psi)$ onto the component $(x, x\tau_W)$ and $\mathbf{O} \oplus X$ onto $\mathbf{O} \oplus Y$.

The 'summary' is just a restatement of the facts established about $\mathbf{1}_X \oplus \Psi^{-1} : X \oplus X \to X \oplus Y$, in terms of its inverse map $\Lambda : X \oplus Y \to X \oplus X$.
(5) The equivalence of the conditions follows from remark 1.3.2, giving the corresponding equivalences for arbitrary sets of permutations, together with the fact that a partial spreadset is a spread iff it is regular on X^*, c.f. definition 1.3.4. ∎

Thus, the fundamental identification of partial spreads with partial spreadsets corresponds to a generalization of the situation in elementary coordinate

geometry: sets of lines through the origin are identifed with the set of their gradients, the subspace y=xm being identified with its slope m. Moreover, we have shown, as in elementary geometry, that any two lines may be taken as the x and y axis, and that by rescaling (recall the identification $\Phi : Y \to X$) on the y axis we can further force any chosen third line through the origin to be the unit line.

Note however that in our case the 'points' of the x-axis are used as coordinate values, whereas in elementary geometry a distinct set, viz. the reals, are used as coordinate values. It is often convenient to mimic this setup in our situation by allowing the chosen components, X and Y, to be coordinatized by an arbitrary vector space R, isomorphic to the components of the given spread.

For example, the natural choice for R, when the components are n-dimensional over a field K, is to take $R = K^n$, and now X and Y are identified with W by specifying bases $(e_1, e_2, \ldots, e_n$ and $(f_1, f_2, \ldots, f_n$ respectively; in this setup the 'axes-identifying' linear bijection $\Psi : Y \to X$ is tacitly taken to be the linear map sending $f_i \mapsto e_i$, for $1 \leq i \leq n$. Now the associated [partial] spreadset becomes a set of matrices $\mathcal{M}$ and the 'canonical' form of the given [partial] spread is in $K^n \oplus K^n$, and the components are $y = xM$, $M \in \mathcal{M}$, plus the Y-axis.

Recall that to also force a component W, of the given spread, to become the unit line under the chosen coordinatization, it becomes necessary to fix the axes identifier map $\Psi : Y \to X$ — $\Psi = {\tau_W}^{-1}$, in the sense of the theorem. However, since by our convention Ψ is *fixed* by the chosen basis of X and Y we can specify the required Ψ by taking an appropriate basis $(f_1, f_2, \ldots, f_n)$ of B so that the unique linear bijection specified by the basis image $e_i \mapsto f_i$, for all i, coincides with Ψ.

The above, analysis can be repeated for arbitrary vector spaces over a skewfield K. The basis for X and Y are then families $(e_i)_{i\in\lambda}$ and $(f_i)_{i\in\lambda}$ (respectively), indexed by a possibly infinite set λ. As before, a component W can be forced to be the identity by choosing an *appropriate* $(f_i)_{i\in\lambda}$. Note that if K is a non-commutative skewfield and the chosen space R is taken to be the space K^λ, the 'λ-tuples' over K, then it might be necessary to specify whether K^λ is regarded as a left a right K-space.

We summarize our conclusions as follows:

Corollary 1.3.16 (Basis Decomposition Theorem.) *Let V be a vector space over a skewfield K, and suppose $\mathcal{T}$ is a partial spread on V with at*

least three distinct components $X, Y, W \ldots$. Let Z be any vector space that is isomorphic to the components of $\mathcal{T}$. Then

1. *There is a partial spreadset τ on Z that contains the identity map $\mathbf{1}_Z$ and a K-linear isomorphism*

$$\Lambda : V \Longrightarrow Z \oplus Z$$

such that Λ is a K-linear partial spread isomorphism from $\mathcal{T}$ to π_τ satisfying:

$$\Lambda(X) = Z \oplus \mathbf{O}, \quad \Lambda(Y) = \mathbf{O} \oplus Z \quad \text{and } \Lambda(W) = \{(z \oplus z \mid z \in Z\}.$$

In fact, to each K-linear bijection $\alpha : X \to Z$ there corresponds a K-linear bijection $\beta : Y \to Z$ such that

$$\Lambda = \alpha \oplus \beta : V \Longrightarrow Z \oplus Z.$$

2. *Let $B_X := (e_i)_{i\in\lambda}$ be a basis of X and for any basis $B_Y := (f_i)_{i\in\lambda}$; so the juxtapostion $B_V := (B_X; B_Y)$ is a basis of V. Define the canonical K-linear isomorphism $\beta_X : X \to K^\lambda$, $\beta_Y : Y \to K^\lambda$, and $\beta_X \oplus \beta_Y \to X \oplus Y \to K^\lambda \oplus K^\lambda$. (N.B. If K is non-commutative, K^λ is made into a left or a right vector space, depending on whichever guarantees the required K-linear isomorphisms with X and Y.)*

Then there is a partial spreadset τ on K^λ such that the K-linear bijection

$$\beta_X \oplus \beta_Y : V \to X \oplus Y \to K^\lambda \oplus K^\lambda$$

defines an isomorphism from $\mathcal{T}$ to π_τ, the partial spread on $K^\lambda \oplus K^\lambda$ associated with τ.

Moreover, any component $W \in \mathcal{T} \setminus \{X, Y\}$ can be mapped to the unit line $x = y$ of $K^\lambda \oplus K^\lambda$, thus ensuring $\mathbf{1} \in \tau$, for any choice of the basis B_X, and for some choice of B_Y (depending on the B_X selected.

Proof: By the preceding remarks. ∎

For emphasis we restate what this means for finite-dimensional spreads.

Proposition 1.3.17 *Let V be a vector space of dimension $2n$, n a positive integer, over a field K, and that τ is a partial spread of K-subspaces of V with at least three distinct components $X, Y, Z \ldots$. Choose a K-basis $B_X :=$*

$(e_1, e_2, \ldots, e_n)$ of X and K-basis $B_Y := (f_1, f_2, \ldots, f_n)$ of Y, and let $B_V := [B_X, B_Y]$ denote the associated K-basis of V, obtained by juxtaposition, thus:

$$B_V =< B_X, B_Y >:= (e_1, e_2, \ldots, e_n, f_1, f_2, \ldots, f_n).$$

Then there is a basis B_Y of Y such that relative to the basis $[B_X, B_Y]$ of V the canonical linear bijection:

$$\beta : V \longrightarrow K^n \oplus K^n,$$

maps X onto $K^n \oplus \mathbf{O}$, Y onto $\mathbf{O} \oplus K^n$, and Z onto the UNIT LINE

$$\{(x, x) \mid x \in K^n\}.$$

Proof: The proposition is a special case of the result above, corollary 1.3.16. ∎

We conclude with a basic isomorphism result.

Theorem 1.3.18 *Let π be a translation plane with spread S_π of $X \oplus X = V$ where X is a left K-vector space and let ρ be a translation plane with spread S_ρ of $Y \oplus Y = W$ where Y is a left L-vector space. Assume that K and L are the component kernels of π and ρ respectively.*

Let ρ and π be isomorphic by a bijective incidence presering mapping ϕ.

(1) Then L and K are isomorphic skewfields and ϕ may be considered a semi-linear mapping from W onto K.

(2) If $\pi = \rho$ then ϕ is an element of the group $\Gamma L(V, K)$.

Furthermore, the full automorphism group G of the translation plane π is a semi-direct product of the translation group T by the subgroup G_0 of $\Gamma L(V, K)$ which permutes the components of the spread S.

The subgroup G_0 of $\Gamma L(V, K)$ is called the 'translation complement' of G or π. $G_0 \cap GL(V, K)$ is called the 'linear translation complement.'

Proof: We have seen (2) previously. We note that if g is in the kernel endomorphism skewfield $\mathcal{K}$ of π then $g^{-1}\phi g$ is in the kernel endomorphism skewfield $\mathcal{L}$ of ρ. Hence,

$$K \cong \mathcal{K} \cong \mathcal{L} \cong \mathcal{L}.$$

1.4 Tutorial On Spreadsets.

This tutorial discusses important aspects of the above theory: low rank spreads; reguli. The latter suggests the need for introducing a projective-space version of the theory of spreads and partial spreads. This Bruck-Bose theory will be systemaically introduced later on. The focus in the tutorial is on the motivating cases rather than the general case. The reader is invited to tidy up the sketchy treatment presented and to anticipate developments.

Rank-Two Spreads.

We have mentioned on several occasions that all rank-one spreads have been described. It is thus natural to turn to rank two spreads. The literature concerned with this area of translation planes is enormous; part of the interest stems form its connection with the theory of flocks, generalized quadrangles and packing problems that are themselves associated with highly interesting higher rank spreads.

By specialising the above we can reduce the study of rank two spreads to spreadsets indicated in the following theorem. This theorem underpins the enormous literature concerning two-dimensional spreads; the theorem also provides a pathway to the theory of flocks and certain types of generalized quadrangles.

Theorem 1.4.1 *Let $\pi := (V, \mathcal{S})$ be a spread of rank ≤ 2 over a skewfield K. Then there are functions g and f from $K \times K$ to K such that*

$$\mathcal{M}_{(g,f)} \left[\begin{array}{cc} g(t,u) & f(t,u) \\ t & u \end{array} \right] \forall t, u \text{ in } K$$

is a spreadset, and there is a K-linear spread isomorphism Ψ from π onto the spread $\pi_{\mathcal{M}_{(g,f)}}$, vewed as a K-spread such that any ordered triple (X, Y, Z), consisting of three distinct components of π, get mapped under Ψ onto the triple $(y = 0, x = 0, y = x)$: that is, the image under Ψ of X, Y and Z are resp. the x-axis, the y-axis and the the unit line of Ψ.

Proof: By the above we know that an isomorphism form π to $\pi_{\mathcal{M}}$ exists for some two-dimensional spreadset. So the only question is whether it has the given form. Since the difference between distinct members in $\mathcal{M}$ are to be non-singular, distinct members of $\mathcal{M}$ have different first rows and

also distinct second rows. (For *skew*fields consider the image of $(1,0)$ under distinct members of $\mathcal{M}$ to get distinct first rows, and similarly use $(0,1)$ for the second row). Moreover, the regularity condition on a spreadset means that the image of $(0,1)$ must range over K^2, so the second row ranges over all of K^2. Moreover, for any given value of the second row $(u,v) \in K^2$ we must have unique values $g(u,v)$ and $f(u,v)$ in positions $(1,1)$ and $(1,2)$ resp., for otherwise the fact that distinct components have distinct *second* rows gets violated. Hence g and f are single-valued, which is the desired result. ∎
The identification above may be expressed by interchanging the two rows of $\mathcal{M}$. One way to establish this is to appropriately modify the proof of the above. This is left as exercise. Note that the 'new' spreadset is the *same* one as before but expressed differently.

Remark 1.4.2 *The spreadset $\mathcal{M}$, for the given (X,Y,Z), can be alternatively writen as $\mathcal{M}$*

$$\mathcal{M}_{(g,f)} = \begin{bmatrix} t & u \\ g(t,u) & f(t,u) \end{bmatrix} \forall t,u \text{ in } K$$

We end with some simple, but important, exercises on *finite* rank two spreads, or rather on spreads that have a rank two representation — so as not exclude the Desarguesian case. The reader is encouraged to consider how far the results generalize: (1) to finite spreads of arbitrary rank; (2) spreads of rank two over commuative fields and skewfields, etc.

Exercise 1.4.3 *Let $K = GF(q)$, $q = p^r$. Let $\mathcal{M}$ be a 2×2 spreadset with entries in K. Then:*

1. *Let A and B be non-singular matrices in $GL(2,q)$. Then $\mathcal{N} := A^{-1}\mathcal{M}B$ is a spreadset and there is a K-linear spread-isomorphism from $\pi_{\mathcal{M}}$ to $\pi_{\mathcal{N}}$. In fact the mapping*

$$A \oplus B : K^2 \oplus K^2 \longrightarrow K^2 \oplus K^2$$

   is the required isomorphism.

2. *Suppose $\mathcal{M}$ and $\mathcal{N}$ are spreadsets such that one is obtained from the other by a sequence of row and/or column transformations (so each transform θ in the sequence must be applied to every member of the spreadset being considered). Then there is a K-linear spread isomorphism from $\pi_{\mathcal{M}}$ to $\pi_{\mathcal{N}}$ such that the x-axis and the y-axis are both preserved.*

3. *If $\mathcal{M}$ is a spreadset then so is $\mathcal{M}^t$, obtaned by transposing every member of $\mathcal{M}$.*

The Regulus

In the following exercises on partial spreads and partial spreadsets, we introduce the regulus. They provide one of the most important tools for the construction and analysis of spreads, and hence translation planes. A systematic treatment of reguli will follow later, based on the projective space approach to [partial] spreads. The treatment provided here clearly indicates the desirability for introducing projective language instead of always working directly with vector spaces. This approach, the Bruck-Bose version of André's theory, will be introduced systematically in section 2.2.

Exercise 1.4.4 *Let $\mathcal{K}$ denote the scalar regulus in $K^n \oplus K^n$, K a field; thus $\mathcal{K}$ has the scalar field $K \leq GL(n, K)$ as its partial spreadset; $\mathcal{K} = \pi_K$. Here K is identifed with the $n \times n$ scalar matrix field with entries in K.*

1. *Show that for $A \in GL(n, K)$, $\{kA \mid k \in K\}$ is the partial spreadset of a regulus $\mathcal{R}_A$ that contains $y = xA$, and shares $x = 0$ and $y = 0$ with the scalar regulus $\mathcal{K}$. Conversely, every regulus in $K^n \oplus K^n$, that contains the x-axis and y-axis, is of the form $\mathcal{R}_A$, for some $A \in GL(n, K)$.*
   (Apply the linear bijection $Diag\,[\mathbf{1}, A]$ to the scalar regulus; also remember that a regulus is determined by any three of its components.)

2. *For A, B non-singular,*

$$\mathcal{R}_A \cap \mathcal{R}_B = \{x = 0, y = 0\} \quad or \quad \mathcal{R}_A = \mathcal{R}_B$$

3. *In $PG(2n-1, K)$, let $\mathcal{R}_{X,Y}$ be tthe set of all reguli $\mathcal{R}_{X,Y}$ that share two fixed components, X and Y. Then $\mathcal{R}_{X,Y}$ induces a partition on all the subspaces of $PG(2n-1, K)$, that have projective dimension $n-1$, and are distinct from X and Y, and the subgroup G of $PGL(n, K)$ that fixes X identically and leaves Y invariant induces a transitive group on $\mathcal{R}_{X,Y}$, and the global stabilizer in G of any $R \in \mathcal{R}_{X,Y}$ acts sharply transitively [i.e. regularly] on $R \setminus \{X, Y\}$.*
   (Interpret the earlier parts projectively; observe that G is sharply transitive on $\mathcal{K} \setminus \{X, Y\}$.)

We can now establish that our definition of regulus coincides with the classical definition, used in finite geometry.

Exercise 1.4.5 *A regulus in $PG(2n-1,q)$ is a partial spread with $q+1$ components such that a line meeting three of the components meets all of them.*

We note in passing that when $n=1$, then the regulus coincides with a ruling class of a hyperbolic quadric.

Exercise 1.4.6 *A spread $\mathcal{S}$ is called regular iff $\mathcal{R} \subset \mathcal{S}$, whenever $\mathcal{R}$ is the regulus containing three distinct components of $\mathcal{S}$. In $PG(2n-1,2)$ every spread is regular.*

Reguli In Projective Spaces.

Any vector space V over a skewfield K may be viewed as projective spcae $PG(V,K)$ whose points are the rank one K subspaces of V and whose lines are the rank two subspaces; in general the projective dimension of a rank k-subspace W of V is $k-1$ by definition. Using this terminology the fundamental theorem of spreads and partial spreads may be expressed in terms of projective spaces, which is the Bruck-Bose model. All this will be developed in the next section on the basis of a systematic review of projective spaces.

The goal here is to consider certain aspects of partial spreads called reguli: these are the most important partial spreads arising in translation plane theory.

Exercise 1.4.7 *A regulus in $PG(2n-1,K)$, K a field, is a partial spread $\mathcal{S}$, of the associated vector space V, such the set of projective lines meeting three distinct components of $\mathcal{S}$ cover the same projective points as are covered by the members of $\mathcal{S}$. Show that when $V = X \oplus X$ then $y = xk$, $k \in K$, together with $x = 0$, form a regulus called the* scalar regulus *on $X \oplus X$.*

What if K is a non-commutative skewfield?

Proof: The rank two space ℓ_u, $u \in K$, spanned by $\{u \oplus 0, 0 \oplus u\}$ meets ever component in a rank one space, and the totality of points covered are all the projective point of type $[(u, uk)]$, $u, k \in K$ and the points on the y-axis. If K is not commutative then $y = xk$ is additive but not a K-space if K operates from the right as (xa, xka) is not on $y = xk$ if a is not centralized by K. So, although the covering is there and the spread $y = xk$ are both there, the

components of the spreads are not always K-spaces: they are spaces over fields in the center of K. ∎
Thus the scalar regulus is a genuine regulus iff the scalar field K is a *commutative* fields!

Now consider any regulus $\mathcal{S}$ in $PG(2n-1, K)$, the underlying vector space being V, K any field. So we have a K-linear isomorphism Ψ onto a regulus in $K^n \oplus K^n$ such that a triad of distinct components (X, Y, Z) of $\mathcal{S}$ get mapped onto the triad $(y = 0, x = 0, y = x)$; also a line cover of $\mathcal{S}$ gets mapped onto a line cover of the image $\Psi(\mathcal{S})$. But any line meeting all three members of the triad $(y = 0, x = 0, y = x)$ must meet every set $y = xk$, for $k \in K$, and lies in the totality of such subspaces. Thus the regulus $\Psi(\mathcal{S})$ must concide with the scalar regulus. Hence we have established several facts: (1) every regulus over a field may be viewed as a scalar regulus and three components of a partail spread over a field lie in a unique regulus (which may not be in the partial spread).

Thus we have established

Remark 1.4.8 *In $PG(2n-1, K)$, for K a commutative field, there is a linear bijection from any regulus onto the scalar regulus and this bijection can be chosen so that any three components may be mapped respectively onto the x-axis, the y-axis, and the unit ine of the scalar regulus. Moreover, three components of a partial spread lie in a unique regulus and hence the subgroup of $PGL(2n-1, K)$ fixing a regulus is triply transitive on its components.*

We shall eventually deal with the most general case associated with the above result: K any skewfield with infinite dimensions allowed. This is essentially a repeat of the above but with more attention to some details.

Chapter 2

The Bruck-Bose Projective Representation Of Spreads.

In this chapter, we shall be discussing a model of translation planes, due to Bruck and Bose, which mainly uses projective spaces, rather than vector spaces, so we obtain what amounts to a projective version of the results of André discussed above. However, the Bruck-Bose model and the André model are 'equivalent' only in the sense that vector spaces and projective spaces are 'equivalent'.

2.1 Foundational Structures In Finite Geometries: A Review.

In the first chapter, see page 2, we introduced the basic notion of an incidence structure, although so far the only incidence structures we have considered explicitly have been affine planes. To consider projective versions of spread theory, we shall need to consider Desarguesian spaces — affine and projective — and also arbitrary projective planes because they correspond to the 'closure' of arbitrary affine planes. In this lecture, we shall review these concepts and introduce some notational devices useful for the study of translation planes.

All these concepts are closely related to generalizations of affine planes called nets: later we shall study these too.

Definition 2.1.1 *Let $\mathcal{N} := (P, L, C, I)$ be a quadruple, where P, L, C, and I are pairwise disjoint sets consisting of* POINTS, LINES, PARALLEL CLASSES, *and* INCIDENCE, *respectively, and where $I \subset P \times L$; so (P, L, I) is an incidence structure in the usual sense. Then $\mathcal{N}$ is a* NET *if*

1. *C is a partition of the lineset L, based on an equivalence relation called* PARALLELISM, *and the members of C are called* PARALLEL CLASSES.
2. *Each point is incident with exactly one line of each parallel class.*
3. *Given a point p and a line A such that p and A are not incident, there is a unique line B parallel to A which is incident with p.*
4. *Two lines from distinct parallel classes have a unique common incident point.*

If there are n points per line and $k = |C|$ parallel classes, the net is said to have ORDER n *and* DEGREE k

It follows immediately:

Remark 2.1.2

1. *Every affine plane $\mathcal{A}$ is a net.*
2. *Let $D \subset C$, where C is the set of parallel classes of any net $\mathcal{A}$. Then the points of $\mathcal{A}$ and the lines covered by the members of D form a net — a subnet of $\mathcal{A}$ — provided D is appropriately non-degenerate, e.g. $|D| \geq 3$.*
3. *An affine plane of order n is a net of order n with degree $n + 1$, and every net with these parameters is an affne plane of order n.*
4. *Let $\mathcal{M}$ be a partial spread on a vector space V. Then the net with pointset V whose lines are additive cosets of the members of $\mathcal{M}$ form a net; this net is called the net of the partial spread $\mathcal{M}$, and which we denote by $\Pi_{\mathcal{M}}$: the parallel classes may be identified with the members of $\mathcal{M}$: so if $\mathcal{M}$ is a spread then the net $\Pi_{\mathcal{M}}$ coincides with the translation plane $\Pi_{\mathcal{M}}$. (See exercise 2.1.5 for details).*

The PROJECTIVE CLOSURE $\overline{\mathcal{N}}$ of a net $\mathcal{N} = (P, L, C, I)$ is the *incidence structure* obtained by adjoining to its pointset the set of its parallel classes C and lineset $L \cup \{\ell_\infty\}$ as its lineset and with natural incidence, i.e., the new line ℓ_∞ is adjacent to all the parallel classes only and every line in L is incident with its parallel class. When $\mathcal{N}$ is an affine plane then its projective closure is defined to be a projective plane. We adopt a more explicit and homogenious version of this defintion.

Definition 2.1.3 *A projective plane π is an incidence sructure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ with the following properties:*

1. *Given two distinct points P, Q of $\mathcal{P}$, there exists a unique line p such that (P, p) and $(Q, p) \in \mathcal{I}$;*
2. *Given two distinct lines p, q of $\mathcal{L}$, there exists a unique point P such that (P, p) and $(P, q) \in \mathcal{I}$;*
3. *There exist four points no three of which are incident with the same line.*

Incidence is clearly set-theoretic, so we continue with the notational devices for projective planes that were introduced earlier for set-theoretic incidence structure, see page 2. The notion of a central collineation differs slightly for projective planes from the corresponding definition for an affine plane.

Definition 2.1.4 *Let g be a collineation of a projective plane π that fixes all the points of a line ℓ and all the lines through a point P. Then g is a* CENTRAL COLLINEATION *with* AXIS ℓ *and* CENTER P; *g is a* TRANSLATION *(resp.* HOMOLOGY *) if $P \in \ell$ (resp. $P \notin \ell$).*

Exploiting the point-line duality for projective planes it is clear that a central collineation may be equivalently be defined to be one that fixes all the points (lines) on a line (point). Note also that only the trivial collineation is a both an elation and a homology.

We have already indicated, remark 2.1.2, how the 'closure' of a net when applied to an affine plane yields a projective plane. For a projective plane the reverse also holds. The details of all this discussed in the following exercise.

Exercise 2.1.5 *Let π be a projective plane. Choose any line ℓ_∞ and form the incidence structure π^{ℓ_∞} of 'points' those points of π which are not on ℓ_∞ and lines of π not equal to ℓ_∞. Incidence is defined as inherited from the incidence of π. π^{ℓ_∞} is called the affine restriction of π with respect to ℓ_∞.*

1. *Show that π^{ℓ_∞} is an affine plane.*

2. *Conversely, if α is an affine plane we may define a projective plane α^+ as follows: The points of α^+ are the points of α and the parallel classes of α and the lines of α^+ are the lines of α and the set of parallel classes of α. The 'points' of α^+ which are parallel classes of α are called the set of 'infinite points' and the line of α^+ which is the set of parallel classes of α is called the 'line at infinity ℓ_∞' of α^+. (We shall also refer to ℓ_∞ as the 'line at infinity' of the affine plane α).*

   Show that α^+ is a projective plane. α^+ is called the projective closure of α.

3. *Let α be an affine plane and π and ρ two projective planes extending α with respect to the adjoinment of lines p and q of π and ρ respectively.*

   (a) *Show that there is an isomorphism from ρ to π which carries q to p.*

   (b) *Show that $\pi^p \cong \rho^q \cong \alpha$.*

4. *Let α be an affine plane with collineation group G. Let α^+ denote the projective closure of α, and let ℓ_∞ be the line at infinity. Let G^+ denote the collineation group of α^+. Show that G is isomorphic to the subgroup $G^+_{\ell_\infty}$, the global stabilizer of ℓ_∞*

We shall normally consider translation planes π as affine planes although, occasionally , we shall refer to the line at infinity of π to mean the line adjoined to π to produce the projective closure π^+. Similarly, we will use interchangeably the terms 'infinite point' and parallel class.

In the remainder of our review of foundational matters, we consider some of the fundamental concepts related to affine and projective spaces.

Definition 2.1.6 *Let V be a vector space over a skewfield K. The corresponding* AFFINE SPACE *$AG(V,K)$ is the collection of all the K-subspaces $W \leq V$ together with their translates:*

$$AG(V,K) := \{c + W \mid c \in V, W \leq V\}.$$

The members of $AG(V,K)$ are called the affine subspaces of V, and an affine subspace $c+W$ is regarded as having same dimension as W, when viewed as a vector subspace of V. The zero-dimensional subspaces are called points, so

V itself is the set of all affine points, the one-dimensional subspaces are the affine lines and the two dimensional subspaces are the affine planes, etc.

The translation group of $AG(V,K)$ consists of all the bijections of V that hae the form $\tau_v : x \mapsto x+v$, for $v \in V$, and two subspaces are called parallel if they lie in the same orbit of the translation group.

An incidence structure is CONSIDERED *an affine space if it is isomorphic to the subincidence structure corresponding to the points and lines of $AG(V,K)$, for some vector space V over a skewfield K.*

It is not hard to characterise the subspaces of an affine space $AG(V,K)$ in terms of its point-line incidence structure (and its collineation group), and also to determine completely the K vector space V. Thus an incidence structure cannot be isomorphic to the incidence structure of more than one affine space. Hence we shall let the context determine whether we are considering a 'standard' affine plane $AG(V,K)$, or an incidence structure isomorphic to that of an affine space.

The fundamental connections between affine and projective planes, developed in exercise 2.1.5, have straightforward analogues relating affine and projective spaces. For example, projective spaces could be introduced by adding on the equivalence classes of affine spaces as 'infinite' subspaces. However, as in the planar case, we choose to introduce this 'closure' of an affine space by giving a more homogeneous version of the definition.

Definition 2.1.7 *Let W be any K-vector space where K is a skewfield. The* PROJECTIVE SPACE *$PG(W,K)$ is the lattice of vector spaces where incidence is inherited from that of W.*

Let A be any K-vector subspace of W. Then A and $PG(A,K)$ are both regarded as being the 'same' projective subspaces of $PG(W,K)$, and the [projective] dimension of A is $a-1$ where a is the rank of A as a K-vector space; so $PG(W,K)$ has dimension $dim_K W - 1$.

The [projective] POINTS *of $PG(W,K)$ are the subspaces with projective dimension zero, the* LINES *are the subspaces that have projective dimension one, the* PLANES *have projective dimension two and the* HYPERPLANES *H are the subspaces of $PG(W,K)$ that are maximal in W: so hyperplanes H are vector subspaces of W that have codimension one in W.*

An incidence structure is CONSIDERED *a projective space if it is isomorphic to the subincidence structure corresponding to the points and lines of $PG(W,K)$, for some vector space V over a skewfield K.*

Remarks 2.1.8 *A projective space $PG(W, K)$ has all it subspaces determined by the incidence structure of its points and lines: a set S of projective points is a subspace iff S contains the points of every lines that meets it in at least two points.*

However, it still remains to exclude the possibility that projective spaces that are isomorphic as incidence structures arise from non-isomorphic vector spaces, possibly even defined over different fields. We do this by first constructing the associated affine planes.

Definition 2.1.9 *Let $PG(W, K)$ be a projective space associated with a vector space W defined over a skewfield K. Let V be any hyperplane of W. Then $PG(W, K)^V$ is the incidence structure whose points are the projective points in $PG(W, K) - PG(V, K)$ and whose lines are all the sets of points of type $\ell^* = \ell \setminus \{L\}$, where ℓ is any line not in V that meets V in the projective point L.*

We now establish the equivalence between affine and projective spaces, generalising the corresponding result for planes.

One approach to this would be to follow the procedure of exercise 2.1.5: define parallel classes for the lines of $AG(V, K)$, and show that the associated projective closure is the incidence structure of a projective space. But the latter incidence structure needs to be axiomatically recognisable, as in the planar case. Since at this stage these axioms are not available (for dimension > 2), we shall follow an alternative approach based on the method of homogeneous coordinates, but adapted for the infinite-dimensional case.

This method has the advantage of providing a concrete link $\Lambda : AG(V, K)^+ \to PG(V^+, K)$ between the projective closure (which we shall define) of the affine space $AG(V, K)$ and the projective space defined over $V^+ = V \times K$ a rank one extension of V. Basically Λ is the unique extension of the affine-space isomorphism $v \mapsto (v, 1)$, from $AG(V, K)$ to $PG(V^+, K)^{H_\infty}$, where $H_\infty = V \times 0$, such that the 'slope' (W) of a coset $c + W$ maps under Λ to $W \times 0$, in the hyperplane H_∞. We now summarize all this and a few related properties:

Theorem 2.1.10 (Homogeneous Coordinates.) *Let V be a vector space over a skewfield K; so the direct product $V^+ := V \times K$, viewed as a K-space, contains hyperplane*

$$H_\infty := (V) := \{(v, 0) \mid v \in V\} \cong PG(V, K).$$

Define the copies $(V) := \{(v) \mid v \in V\}$ *and* $V_0 := \{(v,0) \mid v \in V\} (= H_\infty)$ *of* V, *and let* (W) *and* W_0 *be the natural image of any subspace* $W \leq V$ *in* (V) *and* V_0 *respectively.*

Let $AG(V,K)^\circ := AG(V,K) \setminus V$ *denote set the set of all the affine subspaces of* $AG(V,K)$ *with* the affine points excluded. *Define the* GRADIENT *or* SLOPE MAP*:*

$$\begin{aligned} \nabla : AG(V,K)^\circ &\rightarrow PG((V),K) \\ c+W &\mapsto (W). \end{aligned}$$

Then the following hold.

1. $\nabla(AG(V,K)^\circ) = PG((V),K)$*; the image* $\nabla(c+W) = (W)$ *is called the* SLOPE *of the affine subspace* $c+W$, *for* $c \in V$, $\mathbf{0} \neq W \leq V$. *The projective space* $PG((V),K)$ *is the* HYPERPLANE AT INFINITY *for* $AG(V,K)$.

2. *Define the structure* $AG(V,K)^+$ *consisting of* POINTS *and* SUBSPACES *where, the point set is defined by*

$$\mathbf{P} := [AG(V,K)] \cup [\nabla(AG(V,K)^\circ)],$$

and the subspaces of $AG(V,K)^+$ *are (1) the members of* $\mathbf{P}$*; (2) the subspaces of the projective space* $PG((V),K)$*; and (3) subsets of* $\mathbf{P}$ *that may be expressed in the form:*

$$(c+W)^+ := (c+W) \cup \{(W)\},$$

where W *is any non-trivial vector subspace of* V *and* $c \in V$. *The subspace* $(c+W)^+$ *is called the (projective)* CLOSURE *of* $c+W$ *(and does not depend on the choice of the coset representitive* c*);* (W) *is the* SLOPE *or* GRADIENT *of* $c+W$.

Then $AG(V,K)^+$ *is a lattice, relative to containment, and the closure of any affine subspace* $c+W$ *is the smallest lattice element containing all the points in it.*

3. *There is a unique lattice isomorphism*

$$\Lambda : AG(V,K)^+ \rightarrow PG(V^+,K),$$

such that its restriction to the points *of* $AG(V,K)$ *defines the following isomorphism* λ *of* affine *spaces:*

$$\begin{aligned} \lambda : AG(V,K) &\rightarrow PG(V^+,K)^{H_\infty} \\ v &\mapsto (v,1). \end{aligned}$$

Λ *maps the closure of every affine subspace* $c+W$ *of* $AG(V,K)$, $W \neq \mathbf{0}$, *into the subspace of* $PG(V^+,K)$ *that meets* H_∞ *in* W_0*: that is,* Λ *maps the slope* (W) *of any affine subspace of* $AG(V,K)$ *into its 'copy'* $W \times 0$ *in the hyperplane* $H_\infty \leq PG(V^+,K)$.

4. *Explicitly,* Λ *is an isomorphism from the projective space* $AG(V,K)^+$ *onto the projective space* $PG(V^+,K)$ *given by:*

$$\begin{aligned} AG(V,K)^+ &\rightarrow PG(V^+,K) \\ (W+c)^+ &\mapsto (W,0) \oplus (c,1) \\ (W) &\mapsto W \times 0. \end{aligned}$$

Proof: For convenience assume all vector spaces are taken as right K spaces. (1) is trivial, it is really only concerned with introducing definitions. (2) is a straightforward verification. (3) is essentially part of the next case: (4). Here the main point is to realise that if $W + c$ is a coset of a subspace of W of V then in the lattice $PG(V^+,K)$:

$$[(W,0) \oplus (c,1)K] = (c+W,1) \cup (W \times 0),$$

where $[X]$ denotes the set of projective points in $X \in PG(V^+,K)$, and that Λ maps the the affine subspace $c+W$ of $AG(V,K)$ onto $(c+W,1)$, and its closure (W) onto $W \times 0 \leq H_\infty$. The proof follows easily. ∎

The above theorem contains within it the equivalence between projective and affine spaces, specifically, that $PG(V^+,K)^V \cong AG(V,K)$ whenever V has codimension one in V:

Corollary 2.1.11 (The Theorem of Veblen, [39].) *Suppose* V^+ *is a vector space over a skewfield* K *of rank* > 1*; thus* $V^+ = V \oplus < c >$*, for subspaces* V *and* $< c >$ *that have resp. codimension and dimension one in* V.

Form the projective space $AG(V,K)^+$*, the closure of* $AG(V,K)$*, obtained by defining points at infinity to be the parallel classes of the lines and with*

each line assigned an extra point, viz., its parallel class. Let $PG(V^+, K)$ be the incidence structure associated with the lattice of K-subspaces of V^+. Then we have the following incidence structure isomorphisms:

1. $AG(V,K)^+ \cong PG(V^+,K)$;
2. $AG(V,K) \cong PG(V^+,K)^\infty$.

It is worth stressing:

Remark 2.1.12 *The affine space $AG(V,K)$ has the same dimension as V whereas $PG(W,K)$ has dimension the dimension of a hyperplane $H(W)$ of W; there is an affine space isomorphism:*

$$PG(W,K)^\infty \cong AG(H(W),K).$$

2.2 Projective Space Representations: Bruck-Bose Theory.

In this lecture, we shall be discussing a model of translation planes, due to Bruck and Bose, which mainly uses projective spaces, rather than vector spaces, so we obtain what amounts to a projective version of the results of André discussed above. However, the Bruck-Bose model and the André model are 'equivalent' only in the sense that vector spaces and projective spaces are 'equivalent'.

We first introduce the projective space version of an André-type spread; this is essentially a restatement of the usual definition of a spread in projective space terminology.

Definition 2.2.1 *Let $\Sigma = PG(V,K)$ be an arbitrary projective space, associated a vector space V over a skewfield K, and let $\mathcal{P}$ denote a collection of [at least two] mutually skew subspaces of Σ. Then $\mathcal{P}$ is called a* PROJECTIVE PARTIAL SPREAD *such that given any two distinct subspaces $L, M \in \mathcal{P}$ and any point $p \in \Sigma$ not on L or M, there is a unique line ℓ which contains p and intersects both L and M.*

If furthermore the points of $\mathcal{P}$ form a cover of the points of Σ then $\mathcal{P}$ is called a PROJECTIVE SPREAD.

It is immediate that a projective [partial] spread in $PG(V, K)$ is just a vector space [partial] spread of K-subspaces of the K-vector space V, and conversely that every space [partial] spread consisting of K-subspaces of V is a [partial] [projective] spread in $PG(V, K)$: the existence of 'ℓ' ensures that two distinct subspaces always direct-sum to the whole space, and hence when at least three components are present, all the components have 'half' the dimension of the associated vector space.

Thus 'ordinary' and 'projective' [partial] spreads are essentially the same objects but viewed from different perspectives; we normally do not distinguish between them. Hence, a spread is defined by its context either vectorially or projectively. Accordingly, we shall not repeat for projective spaces all the terminology that we introduced for ordinary spreads; when interpreting spreads in projective spaces, we shall sometimes use the term '*projective* spread'.

Before moving on, we consider as an exercise a more general, but putatively equivalent form, for the definition of a [partial] spread: instead of requiring the direct sum condition could we replace it by the weaker-to-state condition that if $V = X \oplus X$ then a collection of pairwise skew subspaces isomorphic to X, as projective K-space, form a partial spread?

The following example shows that the indicated generalization does not characterise partial spreads, satisfying the standard definition.

Example 2.2.2 *Let W be a vector space over any skewfield K, with an infinite K-basis $(e_1, e_2, \ldots)$. Now on $V = W \oplus W$ take any spread $\mathcal{S}$ that includes $X := W \oplus \mathbf{0}$, $Y := \mathbf{0} \oplus W$ and $Z := \{w \oplus w \mid w \in W\}$. Now let H_1, H_2 and H_3 be hyperplanes of the three components X, Y and Z, respectively, obtained when $(0, e_1)$, $(e_1, 0)$ and e_1 are deleted. Then*

$$\mathcal{H} := (\mathcal{S} \setminus \{X, Y, Z\}) \cup \{H_1, H_2, H_3\}$$

is a collection of pairwise disjoint K-subspaces of V each of which are isomorphic to W, and $V = W \oplus W$. However, V CANNOT *always be expressed as the direct sum of any two members of $\mathcal{H}$.*

The example shows that $\mathcal{H}$ is a partial spread on $V = W \oplus W$, in the sense that all its members are pairwise disjoint and 'half-dimensional'; however $\mathcal{H}$ is not a partial spread, according to the standard meaning, since the direct sum condition is required to hold.

However, the example does not settle the question when $\mathcal{H}$ is a 'spread' in the sense that all its components form a covering of $PG(V, K)$. We leave this matter for the reader to resolve:

Exercise 2.2.3 *Let be $V = W \oplus W$ a vector space, over a skewfield, such that every point is covered by exactly one K-subspace from a family of such subspaces $\mathcal{H}$, such that every $H \in \mathcal{H}$ is $\cong W$ as a K-space. Is it the case that $\mathcal{H}$ is a spread, i.e., is V the direct sum of every pair of distinct members of $\mathcal{S}$.?!*

Note that the answer is clearly in the affirmative if the projective space being considered is finite-dimensional.

We now turn to the Bruck-Bose model of a spread: it is closely related to the projective version of André's defintion 12.4.12 above, but it enables the *projective plane* associated with a translation plane to be viewed as an incidence substructure of a projective space.

If $\mathcal{S}$ is a spread of K-subspaces, of a vector space V over a skewfield K, then the affine translation plane $\Pi_{\mathcal{S}}$ has V as its points and the lines of $\Pi_{\mathcal{S}}$ are the additive cosets of the components of $\mathcal{S}$. Thus the lines of the translation planes are the set of all the affine subspaces of $AG(V, K)$ that are parallel to the members of $\mathcal{S}$. Thus in $AG(V, K)^+$ the subspaces of $AG(V, K)$ that are the lines of the translation plane $\Pi_{\mathcal{S}}$ have as their closure the set of subspaces

$$(\mathcal{S}) := \{(S) \mid S \in \mathcal{S}\},$$

on the hyperplane at infinity (V).

But each $(S) \in (\mathcal{S})$ may also be regarded as the point at infinity of the lines of $\Pi_{\mathcal{S}}$ that are parallel to (S), and $(\mathcal{S})$ as the line at infinity, c.f., exercise 2.1.5. Thus we have established:

Theorem 2.2.4 (Embedding Translation Planes in Projective Spaces.) *Let V be a vector space over a skewfield K and $\mathcal{S}$ a spread of K-subspace of V. Then the projective closure of the translation plane $\Pi_{\mathcal{S}}$, with pointset V and lines the cosets of $S \in \mathcal{S}$, is just the projective closure Π^+ of $\Pi_{\mathcal{S}}$ in $AG(V, K)^+$, when the points and lines of $\Pi_{\mathcal{S}}$ are regarded as affine subspaces of $AG(V, K)$.*

More explictly, the hyperplane at infinity of $\Pi_{\mathcal{S}}$ in Π^+ is the subspace (V), a 'copy' of V, associated with the projective space $PG((V), K) \cong PG(V, K)$; the infinite points are the members $(S) \in (\mathcal{S})$, the finite points are members of V and the closure of the line $c + S$ is $(c + S) \cup S$.

Since $AG(V,K)^+$ is isomorphic to a projective space $PG(V^+,K)$, where V^+ as a hyperplane, the theorem implies that *any translation plane associated with a spread is a subincidence structure of a projective space*; here a SUBINCIDENCE STRUCTURE $\mathcal{J}$ of a projective space $\mathcal{P}$ means that points and lines of $\mathcal{J}$ are selected from $\mathcal{P}$, viewed as a lattice, and incidence is containment (treated symmetrically). More explicitly

Corollary 2.2.5 *Every projective translation plane $\Pi_{\mathcal{S}}$ is isomorphic to an incidence substructure of $PG(V,K)$,such that the affine points of $\Pi_{\mathcal{S}}$ are the points of the affine space $PG(V^+,K)^H$, H a hyperplane is the line at infinity, the points at infinity are the components of a projective spread $\mathcal{S}_0 \cong \mathcal{S}$ in H, and all the other lines are the subspaces meeting H in a member of $\mathcal{S}$.*

We summarize what we have done. Any spread $(V,\mathcal{S})$ defines a translation plane Π in $AG(V,K)$ whose lines are the cosets of the members of $\mathcal{S}$. The projective closure Π^+ of Π lies in the projective closure space $AG(V,K)^+$, the closure of $AG(V,K)$, and the line at infinity H_∞ of Π^+ is the hyperplane at infinity of $AG(V,K)$; H_∞ has a copy $\mathcal{S}_0$ of $\mathcal{S}$ such that all the lines parallel to $S \in \mathcal{S}$ have as there slope the corresponding $S_0 \in \mathcal{S}_0$. Hence, since every translation plane arises from a spread we conclude that *every translation plane is a subincidence structure of a projective space.*

We have seen that there is a natural isomorphism between the closure of affine spaces $AG(V,K)^+$ and the associated projective space lattice $PG(V^+,K)$, $V^+/V \cong K$, based on homogeneous coordinates. Thus theorem 2.2.4 above, that embeds an affine plane π into its projective closure $AG(V,K)^+$, may be used to define a generic embedding of a projective translation plane in $PG(V^+,K)$ in terms of a projective spread $\mathcal{S}$ in $PG(V,K)$ that defines the plane π. This is the Bruck-Bose model, and it follows immediately from theorem 2.2.4.

Theorem 2.2.6 (The Bruck-Bose Construction.) *Let $\mathcal{S}$ be a projective spread in $\Sigma \cong PG(W,K)$ where W is a K-vector space. Embed $PG(W,K)$ in a projective space Σ^+ so that $PG(W,K)$ is a hyperplane of Σ^+.*
Define the incidence structure, defined by inclusion, whose point-set $\mathcal{P}$ is the set of projective points $\mathcal{P} := \Sigma^+ \setminus \Sigma$ and whose line-set $\mathcal{L}$ includes the hyperplane Σ, the 'infinite line', and the other members of $\mathcal{L}$, the 'finite lines', are the projective subspaces of Σ^+ that contain some component of $\mathcal{S}$ as a hyperplane.

Then the incidence structure with points ($\mathcal{P}$), and lines ($\mathcal{L}$) and with incidence defined by inclusion is a projective translation plane π. The translation axis is Σ and π is isomorphic to the affine translation plane on the ambient vector space V of $\mathcal{S}$, whose lines are the cosets of the members of S.

The isomorphism may be chosen so that the lines parallel to $S \in \mathcal{S}$ maps to the point $S \in \mathcal{S}$, i.e. itself when regarded as a point on the 'line' $\Sigma \in \mathcal{L}$.
π

The above theorem, due to Bruck and Bose, may be regarded as the projective version of André's fundamental theorem of translation plane. Although, the original Bruck-Bose version considered only finite dimensional projective spaces, it was their intent to represent a translation plane projectively and within a projective space. It will become apparent that this viewpoint is extremely useful when considering construction processes within projective planes. Moreover, objects which might be considered "geometric" in some sense might be more conveniently visualized within a projective space as opposed to within a vector space where the projective line is essentially missing. For example, the notion of duality cannot easily be expressed using vector space spreads whereas a dual translation plane has an elegant representation using the projective space projective spreads.

Chapter 3

Combinatorics Of Spreads: Nets and Packings.

In this chapter, we introduce some packing problems related to translation planes, via their spreads, so what we are concerned with might be called the combinatorics of spreads. The process of derivation, a powerful tool for constructing new affine and projective planes, is essentially a packing problem: points covered by certain sets of lines are replaced by sets of subplanes covering the same points, to yield a new plane. In the context of spreads in projective spaces, derivations are closely associated with reguli, and Desarguesian spreads may be combinatorially characterised in terms of the reguli they contain. Reguli and other partial spreads are also closely related to nets and combinatorial structures called packings that are associated with the construction of exceptionally interesting translation planes. The aim of this chapter is to explore these combinatorial tools, particularly in the context of translation planes.

3.1 Reguli and Regular Spreads.

We begin this lecture with a brief review of the classical concept of a regulus in $PG(3, K)$; these reguli provide the most important tool for constructing linespreads and hence two-dimensional translation planes. The overall aim of the lecture is to extend the theory of reguli in $PG(3, q)$ to reguli in arbitrary projective spaces $\Sigma = PG(V, K)$. The section ends with the Bruck-Bose characterization of Desarguesian spreads in terms of reguli.

A line t is called a transversal to a set of pairwise skew lines Λ, in any projective space, if t meets every line of Λ. In $PG(3,K)$, K a field, the points of a hyperbolic quadric can be written as a union of a set of mutually skew lines Λ and also as the union of all the lines in Λ', the set of transversals to the lineset Λ. In fact, it turns out that Λ and Λ' are linesets such that each is precisely the the set of transversals of the other; moreover every line of each set is covered by every line of the other. The line complexes Λ and Λ' are said to be mutually opposite reguli.

Notice that if Σ is a linespread in $PG(3,q)$ that contains a regulus Λ then replacing Λ in Σ by its opposite regulus

$$\Sigma' = (\Sigma \setminus \Lambda) \cup \Lambda',$$

yields a new spread, said to be *derived* from Λ. One can go further: look for a set of k pairwise disjoint reguli in a spread and replace some or all of them yielding in all 2^k distinct spreads, although some of them may be isomorphic. All of this reflects the fact that reguli play an indispensible rôle in the construction and analysis of translation planes. For the rest of the lecture our discussion of reguli includes not just arbitrary odd-dimensional projective spaces $PG(2n-1,K)$, but also the infinite-dimensional case — arguably, these are always odd (and even!) dimensional.

We begin by defining a transveral to a collection of *subspaces* Θ to be any line that meets all the lines of Θ, but we shall also insist that any transversal is *covered* by Θ, modifying our earlier usage of the term:

Definition 3.1.1 *Let Θ be a collection of pairwise skew subspaces of any projective space Σ. A line ℓ of Σ is called a* TRANSVERSAL *to Θ if ℓ meets every subspace in the collection Θ and every point of ℓ lies in some member of Θ.*

Note that this is still not the most general useful form of a transversal. We could have introduced the notion of a pseudo-transversal to take care of the case when Σ consists of additive subspaces of $\Sigma = PG(V,K)$, rather than K-subspaces. However, to focus on the essentials, we shall stick with the above definition.

We now turn to the general definition of a regulus. The motivating example, as indicated above, is a collection R of pairwise skew lines, in some $PG(3,K)$, that are covered by the set of all lines that are transversals to R. In the general case R is still required to be a partial spread of the given

projective space $\Sigma = PG(V, K)$. So we need to reslove what a partial spread is to mean in the context of infinite-dimensional spaces.

There are two reasonable ways of defining R, a pairwise skew collection of subspaces of Σ, to be a partial spread: both are motivated by the need to make the components have 'half' the dimension of V, in the infinite-dimensional case. The more general method is to assume that all the members are isomorphic to some X, where $V = X \oplus X$; the alternative is to regard R as a partial spread if Σ is a direct sum of any two distinct members of R, for $|R| > 2$. We shall follow the latter path since it leads to tidier and less technical-sounding results; we shall leave it to the interested reader to develop more general results that apply to 'X-partial spreads'.

Definition 3.1.2 *Let Σ be a projective space and Γ any collection of at least three pairwise-skew subspaces. Then Γ is a called a partial spread if to each triple (x, U, V), where $U, V \in \Gamma$ are distinct and do not contain x, there corresponds a unique line ell of Σ such that $x \in \ell$ and ℓ meets X and Y*

We can define a regulus in the general case.

Definition 3.1.3 *Let Σ be any projective space and suppose R is a partial spread in Σ that has at least three components. Then R is a* REGULUS *of Σ if the following hold:*

1. *If a line t of Σ meets three members of R then t is a transversal of R, see definition 3.1.1 above;*

2. *the points covered by R coincide with the points covered by the transversals to R.*

We now provide the alternative definition of a regulus, indicated above, based on the possibility of the alternative definition of a partial spread.

Definition 3.1.4 *Let Σ be a projective space associated with a direct sum vector space $W = X \oplus X$, where X is any vector space over a skewfield K. Suppose R is a collection of pairwise skew subspaces of Σ each of which is K-isomorphic to X. Then R is an X-*REGULUS *of Σ if the following hold:*

1. *If a line t of Σ meets three members of R then t is a transversal to R, see definition 3.1.1 above;*

2. *the points of R are covered by the transversals to R.*

Exercise 3.1.5 *If R is an X-regulus in Σ, in the notation of definition 3.1.4, is W always the direct sum of every pair of distinct members of R, that is, is every X-regulus a regulus in the 'standard' sense of definition 3.1.3?*

As already mentioned, we shall work with reguli, in the sense of definition 3.1.3, rather than wih X-reguli; extending results concerning reguli to X-reguli is left to the interested reader.

Exercise 3.1.6 *Suppose R is a collection of $q+1$ distinct subspaces $PG(2n-1,q)$ such that every member of R has projective dimension $n-1$ and that R is covered by all transversal across it. (1) Are the members of R pairwise skew? (2) Is R a regulus?*

We now proceed to a complete description of all reguli in an arbitrary projective space $PG(V,K)$, K a field. The prototype for all such reguli is the *scalar regulus*, and $V = W \oplus W$, W any K-space; the components of the scalar regulus are $y = xk$, $k \in K$, together with $Y = \mathbf{O} \oplus W$. It will turn out that all reguli are essentially of this type. If K above is permitted to be non-commutative skewfield then, as we shall see, a regulus cannot exist in $PG(V,K)$.

However, the absence of reguli, when K is a non-commutative skew field, is true only in a technical sense: in this case all the '$y = xk$' still turn out to be additive subgroups of $V = W \oplus W$, and although they are not always K-spaces they still define a partial spread (when V is veiwed as a vector space over the prime field) that are covered by pairwise skew lines of $PG(V,K)$ that one might call transversals. We shall refer to such structures as (scalar) pseudo-reguli and incorporate them in our analysis; they arise in the classification of subplane covered nets, a fundamental result in the theory of nets and derivation.

To provide a uniform treatment of left and right vector spaces, and also to take into account that skewfields become unavoidable in our analysis, we express '$y = xk$' as $y = (x)k$, $(x)k$ indicating the action induced by $k \in K$ on $x \in V$.

Definition 3.1.7 *Let $\Sigma := PG(V,K)$ be a projective space over a skewfield K such that $V = W \oplus W$, where W is a K-space.*
Then for any $w \in W$, $(w)k$ denotes wk (resp kw) depending on whether W is taken to be a right (resp. left) K-space and $y = (x)k$, for $k \in K$ denotes the additive subgroup $\{(w,(w)\kappa \mid \kappa \in K\}$ of $V = W \oplus W$

The collection S of subspaces of the K-space V given by:

$$S = \{Y\} \cup \{`y = (x)k' \mid k \in K\},$$

where $Y = \mathbf{O} \oplus W$, is called the W-coordinatized SCALAR PSEUDO-REGULUS *in $PG(V, K)$. The members of S are called its* COMPONENTS. *S is called a* SCALAR *regulus if it turns out to be regulus in Σ.*

For all $w \in W^*$, the lines of Σ of form let

$$T_w := \{(wk_1, wk_2) \mid k_1, k_2 \in K\},$$

and define the STANDARD COVER *of the scalar pseudo-regulus S, by*

$$\tau = \{T_w \mid w \in W\}.$$

Note that from our point of view it turns out to be quite harmless to ignore the dependence of some of the above notation on W; we assume a fixed W as our starting point: we avoid references to 'W-defined' objects.

We now show that in projective spaces over a skewfield K, the scalar pseudo-regulus is a regulus iff K is a field, and when this is case, the standard cover, definition 3.1.7, turns out to be the set of its transversals. In the more general situation, when K is non-commutative, virtually the same conclusions would apply if the definition of a transversal were to be appropriately relaxed.

Theorem 3.1.8 *(Scalar Pseudo-Reguli.) Let S be the scalar pseudo-regulus associated with $V = W \oplus W$, where W is a vector space over a skewfield K. Then*

1. *S is an additive partial spread, with ambient space $(V, +)$.*
2. *The components of S are K-subspaces iff K is field.*
3. *The standard cover τ is a collection of pairwise-skew lines of $PG(V, K)$ such that $\cup\tau = \cup S$, with both sides viewed as subspaces of V.*
4. *K is a field iff the pseudo-regulus S is a regulus and the standard cover, definition 3.1.7, is its set of transversals.*

Proof: (1) Let A and B denote any two distinct components of S; the main case is when they are, respectively, $y = (x)a$ and $y = (x)b$, for distinct $a, b \in K^*$. Now these two spaces have trivial intersection, so we have a

partial spread provided $A + B = V$. For convenience, write (x, y), $x, y \in W$ to denote $x \oplus y$. Now $(x, y) \in A \oplus B$ holds iff

$$\exists u, v \in W \ni: (x, y) = (u, (u)a) + ((v, (v)b),$$

and this can easily be solved for u and v. Thus S is an additive spreadset.
(2) Consider a non-zero $w \oplus (w)k \in y = (x)k$. Now for $l \in K$,

$$(w \oplus (w)k)l = ((w)l \oplus ((w)k)l = (w)l \oplus ((w)l)l^{-1}kl,$$

thus $y = (x)k$ is left invariant under K iff k is centralized by K.
(3) Since $T_w = T_{w'}$ holds iff w and w' generate the same rank-one K-space it follows that τ is a collection of pairwise-skew lines of Σ.

The subspace

$$T_w := \{((w)k_1, (w)k_2) \mid k_1, k_2 \in K\}$$

meets Y when $k_2 = 0$, and meets $X := W \oplus vecO$ when $k_1 = 0$. It meets every other component $y = (x)k$ of S at $(w, (w)k)$. Moreover T_w is covered by the components of S because $((w)k_1, (w)k_2)$, for $k_1 \neq 0$, may be expressed as $(wk_1, wk_1\frac{k_2}{k1})$, for $k_1 \neq 0$, meets the component $y = (x)k$, $k := \frac{k_2}{k1}$, and it of course meets Y as well. If $s \in V^*$ is in some $y = (x)k$ then $s = w \oplus (w)k$, $w \in W^*$, and this lies in T_w. So $\cup\tau$ and $\cup S$ coincide as subsets of V.
(4) This follows from the above cases. ∎
We now proceed towards showing that all reguli may be identified with the scalar reguli, that is, scalar pseudo-reguli over a commutative field. We shall not consider here the more general problem of providing a geometric characterization of all pseudoreguli.

Lemma 3.1.9 *Let S be the scalar regulus in $PG(V = W \oplus W, K)$, K a field. Suppose R is any regulus that shares the components $Y = \mathbf{O} \oplus W$, $X = \mathbf{O} \oplus W$ and at least one other component. Then $R = S$.*

Proof: Let $\rho \in R - \{X, Y\}$. So V is a direct sum of any two distinct members of the triad $\{X, Y, \rho\}$, hence, by linear algebra, there is a unique linear bijection $M_\rho : W \to W$ such that

$$\rho := \{(w, wM_\rho) \mid w \in W\}.$$

Since every transversal t of S meets at least three components of R, t must also be a transversal of R, by definition 3.1.3(def:reg1). But, by theorem 3.1.8, the transversals of S are of form

$$T_w := \{(wk_1, wk_2) \mid k_1, k_2 \in K\},$$

and this meets ρ non-trivially iff for some $k_1 \in K^*$ there corresponds a $k_2 \in K$ such that $wk_1M = wk_2$, and this implies that M leaves invariant the rank-one space wK, and this to holds for all $w \in W$ iff M is projectively trivial and hence of form $y = (x)m$, for some $m \in K^*$. Thus R includes all the components of S and hence must coincide with S: if R had more components then the transversals of S would fail to be transversals of R. ∎
The following theorem asserts that any regulus R over a field may be identified with the scalar regulus S; in fact R may be coordinatized by S so that any three components of R may be identifed with the three standard components of S, viz., X, Y and the unit line.

Theorem 3.1.10 *(Standard Coordinates For Reguli.) Let $V = W \oplus W$, where W is a vector space over a field K, and let Σ be the associated projective space $PG(V, K)$. Let S denote the scalar regulus in Σ, relative to W. Then given any regulus R of Σ, and an ordered triple of three distinct components (A, B, C) of R, there is a nonsingular bijection $g \in GL(V, K)$ that maps the triple (A, B, C) onto (X, Y, Z), and the regulus R onto the scalar regulus S; here X, Y and Z are the 'standard components' of S in the usual sense:*

$$X = W \oplus \mathbf{O}, \quad Y = \mathbf{O} \oplus W, \quad \text{and} \quad Z = \{(w, w) \mid w \in W\}.$$

Proof: It is a simple exercise in linear algebra to see that the group $GL(V, K)$ is transitive on the set of all ordered triples (A, B, C) such that V is a direct sum of any two members of the triple. Thus choosing (A, B, C) to be three distinct components of R there is a linear bijection g of V such that g maps (A, B, C) onto (X, Y, Z), and now the regulus $g(R)$ satisfies the conditions of lemma 3.1.9 above, hence $g(R)$ is the scalar regulus. ∎
The following corollary is immediate:

Corollary 3.1.11 *If a projective space Σ, over a field K, contains three mutually skew K-subspaces A, B and C such that any two sum to Σ, then the three subpaces are components of a unique regulus in Σ.*

In the context of a projective space $\Sigma = PG(V, K)$, the concept of a spread and partial spreads only make sense if $V = W \oplus W$ for some K-space W. Hence we shall tacitly assume that Σ has this form, when we refer to its partial spreads.

Definition 3.1.12 *Let Σ be a projective space over a field. A spread of Σ is called* REGULAR *if the unique regulus containing any three mutually distinct spread components is contained within the spread.*

Every spread over $GF(2)$ is regular:

Remark 3.1.13 *Let $K = GF(2)$ and suppose V is any vector space over K. Then every spread S in $PG(V, K)$ is regular.*

Proof: Since, c.f. corollary 3.1.11, the regulus R determined by any three distinct components $a, b, c \in S$ coincides with $R \subset S$. ∎
It will become evident that there are many non-isomorphic translation planes of even order $2^n > 8$, and these may be identified with mutually non-isomorphic spreads in $PG(2n-1, 2)$.

The following theorem, due to Bruck and Bose [5], implies that in every other case all finite regular spreads of the same order are isomorphic. The proof introduces powerful computational techniques that will be systematically conisdered in later chapters. The theorem may be stated more generally, with appropriate modifications, so as to include the infinite case.

Theorem 3.1.14 *A finite spread in $PG(2k-1, q)$ and $q \neq 2$ is regular if and only if the associated translation plane is Desarguesian.*

Proof: We will prove this only in the case $PG(3, K)$, $K = GF(q)$, but the proof remains valid in general.

Let S be a spread in $PG(3, q)$. Choose any three lines of S and write the plane vectorially with points (x, y) where x and y are 2-vectors over K and $x = 0, y = 0, y = x$ are components. Then the regulus defined by the three components has as its components $x = 0$ and $y = xu$ for all u in K. Let

$$y = x \begin{bmatrix} g(t,u) & f(t,u) \\ t & u \end{bmatrix} := M_{t,u} := M$$

be any component of the spread with the choice of three components as $x = 0, y = 0, y = x$. Change bases by

$$\begin{bmatrix} I_2 & 0 \\ 0 & M^{-1} \end{bmatrix}$$

and note that the unique regulus containing $x = 0, y = 0$ and $y = xM$ after the basis change also contains $y = x$ and hence must have the form $x = 0, y = 0, y = xk$ for all k in K. Hence, we have that $y = xMk$ must be in the spread, whenever $y = xM$ is in the spread. This implies that $g(tw, uw) = g(t, u)w$ and $f(tw, uw) = f(t, u)w$ for all $u, t, w \in K$.

Now choose $x = 0$, $y = xM_{s,v}$ and $y = xM_{t,u}$ and determine the regulus containing these three components. Change bases by $\begin{bmatrix} I_2 & -M_{s,v} \\ 0 & I_2 \end{bmatrix}$ to rewrite the spread in the form $x = 0, y = x(M_{k,w} - M_{s,v}) = N$. Use the previous basis change with $\begin{bmatrix} I_2 & 0 \\ 0 & N^{-1} \end{bmatrix}$ to realize the standard form of the regulus containing the three indicated components. Now reverse the basis changes to obtain that $x = 0$ and $y = x\left((M_{t,u} - M_{s,v})w + M_{s,v}\right)$ are components for all $t, u, s, v, w \in K$, provided $(t, u) \neq (s, v)$. In particular, if $t = s$ but $u \neq v$ then this implies that the matrix

$$\begin{bmatrix} 1 & 0 & u & 0 \\ 0 & 1 & 0 & u \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

defines a collineation for all u in K. Similarly, the previous argument shows that

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & w & 0 \\ 0 & 0 & 0 & w \end{bmatrix}$$

defines a collineation for all $w \neq 0$ of K. Hence, we obtain $g(t, u) + w = g(t, u + w)$ for all u, t, w in K so that if follows that $g(t, u) = tg(1, 0) + u$ and similarly $f(t, u) = f(t, u + w)$ so that $f(t, u) = f(t, 0) = tf(1, 0)$. Hence, the spread has the following form, for some constants f and g in K:

$$x = 0, y = x \begin{bmatrix} tg + u & uf \\ t & u \end{bmatrix} \forall t, u \in K.$$

■

Exercise 3.1.15 *Show that the matrices in the spread define a field isomorphic to $GF(q^2)$.*

Hence, the spread consists of all 1-dimensional $GF(q^2)$-spaces within a 2-dimensional $GF(q^2)$-vector space. That is, the spread is Desarguesian. ■

3.2 Derivation.

We have seen that a regulus R in $PG(3,K)$, K a field, is covered by its opposite regulus R'. If S is a spread of $PG(3,K)$ that contains R then $(S \setminus R) \cup R' = S'$ is also a spread called the spread 'derived' from S.

We consider this more generally, but only for finite spreads.

Definition 3.2.1 *If S is a spread in a projective space $\Sigma \simeq PG(2k-1,q)$ and R is a partial spread of S such that R is a regulus in some $PG(3,h)$ where $h^2 = q^k$ then we shall say that R is a 'derivable partial spread' of S. The corresponding affine structure in the associated translation plane is called a 'derivable net'.*

Exercise 3.2.2 *Let π be a translation plane with an associated spread in $PG(3,K)$, $K \equiv GF(q)$. Show that a basis for the vector space can be chosen so that any derivable net D has the spread set*

$$x = 0, y = x \begin{bmatrix} u^\sigma & 0 \\ 0 & u \end{bmatrix} \text{ for all } u \text{ in } K \text{ and } \sigma \text{ in } Gal(K).$$

Exercise 3.2.3 *Consider the spread $x = 0, y = x \begin{bmatrix} u^\sigma & \gamma t^\rho \\ t & u \end{bmatrix}$ for all u, t in $K \simeq GF(q)$, q odd and σ, ρ in $Gal(K)$ and γ is a nonsquare in $K - \{0\}$. Find at least $2q$ derivable nets in the associated translation plane. Show that if neither σ nor ρ is 1 that none of the derivable nets is a regulus in $PG(3,K)$. For each derivable net D, find a field K_D isomorphic to K such that D defines a regulus in $PG(3,K_D)$.*

Theorem 3.2.4 *The number of regular spreads in $PG(3,q)$ is*

$$q^4(q^3-1)(q-1)/2.$$

Proof: Each regular spread defines a field extension of K, $K[t] \cong GF(q^2)$. By the theorem of André, each two Desarguesian affine planes are isomorphic by an element of $\Gamma L(4,K)$. The full collineation group which fixes the zero vector of a given Desarguesian affine plane is clearly $\Gamma L(2,K[t])$, $K[t] \cong GF(q^2))$. Hence, the number of regular spreads is

$$N := \frac{|\Gamma L(4,q)|}{|\Gamma L(2,q)|} = q^4(q^3-1)(q-1)/2,$$

and now it is a simple exercise to verify that $N = q^4(q^3-1)(q-1)/2$. ∎

Remark 3.2.5 *The number of reguli in any regular spread, contained $PG(3,q)$, is given by*

$$\frac{\binom{q^2+1}{3}}{\binom{q+1}{3}} = q(q^2+1).$$

Proof: Exercise.■

Theorem 3.2.6 *Let R be any regulus in $PG(3,q)$ and let N_R denote the corresponding net of order q^2 and degree $q+1$. Let ℓ be any line of $PG(3,q)$ so that $R \cup \{\ell\}$ is a partial spread. Then there exists a unique regular spread containing $R \cup \{\ell\}$.*

Proof: Let $K = GF(q)$ Represent R is standard form:

$$x = 0, \quad y = x \begin{bmatrix} u & 0 \\ 0 & u \end{bmatrix} \forall u \in K.$$

Let ℓ be represented in the form

$$y = x \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

It is immediate that $bc \neq 0$. Furthermore, the difference of these matrices must be non-singular so that

$$\det \begin{bmatrix} a-u & b \\ c & d-u \end{bmatrix} = (a-u)(d-u) - bc = u^2 - (a+d)u - bc \neq 0 \forall u \in K.$$

Hence, the polynomial $x^2 - (a+d)x - bc$ is irreducible over K. Write $d-u = v, b = gt_0$ and then $e = a - d = ft_0$. Now consider the set of matrices

$$\left\{ \begin{bmatrix} ft+v & gt \\ t & v \end{bmatrix} \mid v,t \in K \right\}.$$

We have noted previously that this set forms a field isomorphic to $GF(q^2)$ so that there is a unique Desarguesian (regular) spread defined by this field of matrices. Hence, there is a unique regular spread containing $R \cup \{\ell\}$. ■
In the next theorem, we shall need to appeal to the following elementary fact:

Remark 3.2.7 *The number of polynomials x^2+fx+g for g and f in $GF(q)$ which are $GF(q)$-irreducible is $q(q-1)/2$.*

Proof: Exercise. ∎

Theorem 3.2.8 *Any regulus R in $PG(3,q)$ can be embedded in exactly $q(q-1)/2$ regular spreads.*

Proof: Represent R in the standard form $x = 0, y = x \begin{bmatrix} u & 0 \\ 0 & u \end{bmatrix}$ for all u in $GF(q)$. Any regular spread containing R corresponds to a Desarguesian affine plane and hence a corresponding quadratic field extension of $GF(q)$. The theorem follows by remark 3.2.7.∎

∎

Corollary 3.2.9 *There are exactly $q^4(q^3-1)(q^2+1)$ reguli in $PG(3,q)$.*

Proof: Consider the incidence structure of reguli and regular spreads and count the incidence pairs (flags). Let k denote the number of reguli in $PG(3,q)$. Then the number of Desarguesian spreads times the number of reguli in each Desarguesian spread is equal to the number of reguli times the number of Desarguesian spreads containing a given regulus.

Hence,

$$k = \frac{(q^4(q^3-1)(q-1)/2)q(q^2+1)}{(q(q-1)/2)} = q^4(q^3-1)(q^2+1).$$

∎

Corollary 3.2.10 *Let R be a regulus in $PG(3,q)$. Then, the order of the collineation group of the corresponding regulus net N_R which fixes an affine point is $(q(q^2-1))^2(q-1)r$ where $q = p^r$ and p is a prime.*

Proof: Since any two Desarguesian spreads are isomorphic and since any Desarguesian affine plane admits a collineation group which fixes the zero vector and acts triply transitive on the line at infinity, it follows that

$$|\Gamma L(4,q)_{N_R}| = \frac{q^6(q^4-1)(q^3-1)(q^2-1)(q-1)r}{q^4(q^3-1)(q^2+1)) = (q(q^2-1))^2(q-1)r}.$$

■

We shall see shortly that the collineation group of a regulus net which fixes an affine point is isomorphic to $GL(2,q)\Gamma L(2,q)$ where the product is a central product of intersection the subgroup of order $q-1$ of scalar matrices.

3.3 Direct Products of Affine Planes and Packings.

In $PG(3,q)$ linespreads have size (q^2+1), and the total number of lines is exactly $(q^2+1)(q^2+q+1)$. Thus one might ask for a collection $\mathcal{C}$ of (q^2+q+1) spreads such that every line belongs to (exactly) one spread in the collection $\mathcal{C}$; one might even ask that all the members in $\mathcal{C}$ be regular. Such packings will be used in this section to construct perhaps the two most intriguing translation planes: the Lorimer-Rahilly plane of order 16 and its transpose the Johnson-Walker plane: these are the only known translation planes admitting $GL(3,2)$. The concept of a net product will be introduced partly as an aid to the above, and also because of potential aplications in wider contexts; net products are helpful in constructing nets with interesting properties.

Definition 3.3.1 *Let Σ be a projective space relative to a left K-vector space $X \oplus X$.*

A PACKING (PARALLELISM) *of Σ is a set of spreads which are disjoint with respect to subspaces K-isomorphic to X and such that the union of subspaces isomorphic to X of the set of spreads is the set of all K-subspaces isomorphic to X. The packing Σ is* REGULAR *if the psreads in it are all regular spreads.*

For example, a packing of $PG(3,q)$ is a set of $1+q+q^2$ spreads of q^2+1 lines each. In particular, a regular packing in $PG(3,q)$ gives rise to a set of $1+q+q^2$ *Desarguesian* spreads of order q^2.

In the following, we shall require the concept of the direct product of nets and affine planes. The notion of net was introduced in definition 2.1.1.

Definition 3.3.2 *Let $\pi_1 = (P_1, L_1, C_1, I_1)$ and $\pi_2 = (P_2, L_2, C_1, I_2)$ be two translation planes. Let σ be a $1-1$ correspondence from the set C_1 of parallel classes of π_1 and the set C_2 of parallel classes of π_1. We form the direct product $\pi_1 \times_\sigma \pi_2$ as follows:*

The 'points' are the elements of the cross product $P_1 \times P_2$.

Let ℓ_1 be a line of L_1 so that $\ell_1\sigma$ is a line of L_2. If ℓ_2 is any line parallel to $\ell_1\sigma$, then the set of points of $P_1 \times P_2$ incident with $\ell_1 \times \ell_2$ is a 'line' of the direct product incidence structure.

Note that the construction does not use finiteness. If σ is an isomorphism, we use the term 'regular direct product'.

Exercise 3.3.3 *Show that if the planes are of order n then $\pi_1 \times_\sigma \pi_2$ is a net of order n^2 and degree $n+1$.*

Theorem 3.3.4 *Let T_1 and T_2 denote the translation groups of π_1 and π_2 respectively. Then $T_1 \times T_2$ is a translation group of $\pi_1 \times_\sigma \pi_2$.*

Proof: Define the action of (g_1, g_2) on (a_1, a_2) for a_i in P_i for $i = 1, 2$ by $(a_1, a_2)(g_1, g_2) = (a_1 g_1, a_2 g_2)$. Let ℓ_1 be a line of L_1 and ℓ_2 a line parallel to $\ell_1\sigma$. Then $\ell_1 g_1$ is parallel to ℓ_1 and $\ell_2 g_2$ is parallel to ℓ_2 and to $\ell_1\sigma$. Then $\ell_1 g_1 \times \ell_2\, g_2$ is a line of $\pi_1 \times_\sigma \pi_2$. To show that (g_1, g_2) is a translation, simply note that (g_1, g_2) fixes each parallel class but fixes no affine point.

Definition 3.3.5 *Let $\Sigma \cong PG(2k-1, q)$. A $(k-1)$-regulus $R_{(k-1)}$ is a set of $q+1$ $(k-1)$-dimensional projective subspaces which are mutually skew such that any line of Σ which intersects any three necessarily intersects all elements of $R_{(k-1)}$.*

Note that a regulus in $PG(3, q)$ is a 1-regulus.

Theorem 3.3.6 *If π_1 and π_2 are Desarguesian affine planes of order q and σ is an isomorphism of π_1 onto π_2 then*

(1) there is a collineation group isomorphic to $GL(2, q)\Gamma L(2, q)$ acting on $\pi_1 \times_\sigma \pi_2$ and

(2) $\pi_1 \times_\sigma \pi_2$ is a derivable net.

(3) If π_1 is a Desarguesian affine plane whose spread S_1 is in $PG(3, q)$ then $\pi_1 \times \pi_1$ is a derivable net with partial spread in $PG(7, q)$ which contains a 2-regulus.

Proof: We identify π_1 and π_2 and without loss of generality, we let $\sigma = 1$. We note that $\Gamma L(2, q)$ is a collineation group of π_1.

Exercise 3.3.7 *For h in $\Gamma L(2, q)$ show that (h, h) is a collineation group of $\pi_1 \times \pi_1$.*

Now for $\alpha, \beta, \gamma, \delta \in GF(q)$ such that $\alpha\delta - \beta\gamma \neq 0$, we define $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ acting on (a_1, a_2) to be $(a_1\alpha + a_2\gamma, a_1\beta + a_2)$ where the indicated multiplication is scalar multiplication. Let L_1 is a line represented in the form $y_1 = x_1\sigma + \rho$, it is easy to verify that $L_1\alpha$ is $y_1 = x_1\sigma + \alpha\rho$. It follows that $L_1 \times L_2$ maps to $(L_1\alpha + L_2\gamma) \times (L_1\beta + L_2\delta)$ and $(L_1\alpha + L_2\gamma)$ is parallel to $(L_1\beta + L_2\delta)$. Note that it follows that there is a group isomorphic to $GL(2, q)$ which fixes each line of the net incident with $(0, 0)$. Hence, $GL(2, q)\Gamma L(2, q)$ is a collineation group of the net. This proves (1).

Now $(p, 0)$ for all points p of π_1 is a subplane isomorphic to π_1. Furthermore, $GL(2, q)$ acts transitively on the points of each line thru $(0, 0)$. Hence, the net is covered by subplanes isomorphic to π_1. This is enough to ensure that the net is a derivable net. However, if we represent π_1 by the components $y_1 = x_1\alpha$ and $x_1 = 0$ and π_2 as $y_2 = x_2\alpha$ and $x_2 = 0$ then the points of the direct product have the form $((x_1, y_1), (x_2, y_2))$. Rerepresenting the points in the form (x_1, x_2, y_1, y_2) takes the lines $(y_1 = x_1\alpha) \times (y_2 = x_2\alpha)$ to the form $y = x\alpha$ where (x_1, x_2) and $y = (y_1, y_2)$.

Thus, the direct product net may be coordinatized by a net defined by $y = x\alpha$, $x = 0$ which is clearly a regulus in $PG(3, q)$. This proves (1).

Now assume that π_1 is defined by a regular spread in $PG(3, q)$ so that the order of π_1 is q^2. Then if the associated field if $GF(q)[t] \cong GF(q^2)$, the previous argument shows that there is a net of the form $y = x\alpha$, $x = 0$ for all α in $GF(q)$. Hence, this defines a 2-regulus in $PG(7, q)$. This proves (2) and (3).

We now consider the direct product of two Desarguesian affine planes whose corresponding regular spreads are in the same $PG(3, q)$.

Proposition 3.3.8 *Let S_1 and S_2 be distinct regular spreads in $PG(3, q)$, let π_1 and π_2 denote the Desarguesian affine planes corresponding to S_1 and S_2 respectively.*

Form $\pi_1 \times \pi_1 = D_1$ and $\pi_2 \times \pi_2 = D_2$.

Then $D_1 \cap D_2$ (the intersection of components) is a 2-regulus R_2 and $D_1 \cup D_2$ is a partial spread in $PG(7, q)$ of $2(q^2 - q) + 1 + q$ components. Hence, $N_{(D_1 \cup D_2)}$ is a translation net (admits a translation group transitive on its points) of order q^4 and degree $2(q^2 - q) + 1 + q$.

Proof: We note that D_1 may be coordinatized by a quadratic field extension of $K \cong GF(q)$ say $K[t_1]$. Similarly, D_2 may be coordinatized by a

quadratic field extension $K[t_2]$ of K. If S_1 and S_2 are distinct, it follows that $K[t_1] \cap K[t_2] = K$. Each derivable net has exactly $1 + q^2$ components as π_i is a Desarguesian affine plane of order q^2 for $i = 1, 2$.

Theorem 3.3.9 *Let $\mathcal{P}$ be a regular packing of $1+q+q^2$ spreads in $PG(3,q)$. Let the corresponding Desarguesian translation planes be denoted by π_i for $i = 1, 2, ..., 1 + q + q^2$.*

(1) Then $\cup_{i=1}^{(1+q+q^2)} \pi_i \times \pi_i$ is a translation plane of order q^4 whose spread is in $PG(7,q)$.

(2) The spread consists of $1 + q + q^2$ derivable nets each containing a 2-regulus R_2.

(3) The collineation group of the translation plane contains $GL(2,q)$ in its translation complement . Furthermore, $GL(2,q)$ is generated by central collineations and leaves each derivable net invariant.

Proof: From the preceding, it remains to show that $GL(2,q)$ is a collineation group of the translation plane.

We note that the full group of each derivable net that stabilizes the zero vector is $GL(2, K[t_i])\Gamma L(2, K[t_i])$ where $K[t_i]$ is the quadratic field extension of $K \cong GF(q)$ which coordinatizes π_i and $\pi_i \times \pi_i$.

Clearly, $\cap_1^{1+q+q^2} GL(2, K[t_i])\Gamma L(2, K[t_i]) \cong GL(2,q)\Gamma L(2,q)$. However, only the group isomorphic to $GL(2,q)$ generated by the scalar mappings as noted above are collineations of the translation plane (with the possible exception of the collineations induced by field automorphisms).

3.3.1 A regular parallelism in $PG(3,2)$.

Let S_1 be any regular spread in $PG(3,2)$ we shall construct a parallelism as follows: let C be a cyclic group of order $2^3 - 1 = 1 + 2 + 2^2 = 7$ in $PG(4,2)$ which fixes three components of S_1 then $\cup_C S_1\sigma$ is a regular parallelism.

Choose any point X of $PG(3,2)$. There are exactly seven lines containing X and the seven involutions fixing the lines pointwise respectively generate an elementary Abelian group of order 3 (a 3-dimensional $GF(2)$-vector space) A which is a normal subgroup of $PGL(3,2)_X$. The group induced on A turns out to be isomorphic to $SL(3,2)$ (see e.g. Walker [40]) which is also isomorphic to $PSL(2,7)$.

The stabilizer of each line L_i containing X is isomorphic to S_{4i} and the alternating group A_{4i} fixing L_i fixes it pointwise. For each each element σ of

order three in A_{4i}, there is a unique line M_i skew to L_i which is σ invariant. It turns out that

$$\{L_i \cap M_i S_{4i} \mid i = 1, 2, ..., 7\}$$

is a spread and

$$\cup_1^7 \{L_i \cap M_i S_{4i} \mid i = 1, 2, ..., 7\}$$

is a regular parallelism of $PG(3, 2)$.

Corollary 3.3.10 *Corresponding to the regular parallelism of $PG(3, 2)$ is a translation plane of order 16 with kernel $GF(2)$. The plane admits a collineation group isomorphic to $SL(2, 2) \times Z_7$. The full collineation group is $PSL(2, 7) \times S_3$.*

Now essentially the same construction on the dual space of V_4 produces another translation plane of order 16 from a corresponding regular parallelism. Actually, this may be given a more general construction.

3.3.2 Transpose.

Let $V_{2k} = V$ be a $2k$-dimensional left vector space over a skew field K and let V^* denote the dual space of linear functionals. Choose a basis $\{e_i | i = 1, 2, ..., 2k\}$ of V and let $\{f_i | i = 1, 2, ...2k\}$ denote the dual basis of V^*, so

$$f_j(e_i) = \delta_{ij} \text{ for all } i, j = 1, 2, ..., 2k.$$

Define

$$f\alpha(x) := f(x)\alpha \forall f \in V^*, \alpha \in K,$$

so now V^* becomes a $2k$-dimensional right vector space over K.

Represent vectors of V by

$$(x, y) \equiv (x_1, x_2, ..., x_k, y_1, y_2, ...y_k) \equiv \sum_1^k x_i e_i + \sum_{k+1}^{2k} y_i e_i$$

and represent vectors of V^* by

$$(z, w) \equiv (z_1, z_2, ..., z_k, w_1, w_2, ..., w_k) \equiv \sum_1^k f_i z_i + \sum_{k+1}^{2k} f_i w_i.$$

Define the annihilator mapping $\perp$ as follows:

$$W^{\perp} = \{f \in V^* \mid f(w) = 0 \forall w \in W\},$$

where W is a subspace of V. In terms of the basis then $(z_1, z_2, ..., z_k, w_1, w_2, ..., w_k)$ annihilates $(x_1, x_2, ..., x_k, y_1, y_2, ...y_k)$ if and only if

$$(x_1, x_2, ..., x_k, y_1, y_2, ...y_k) = (z_1, z_2, ..., z_k, w_1, w_2, ..., w_k)^t = 0,$$

where t denotes the transpose matrix.

Now let S be a spread in $PG(V, K)$ then $\{T^{\perp}; T \in S\} = S^*$ is a set of $k-1$-dimensional projective subspaces of $PG(V^*, K)$ such that each hyperplane of the projective space contains exactly one element of S^*.

Definition 3.3.11 *Let $W = Z \oplus Z$ be a L-vector space where L is a skewfield. A dual spread of $PG(W, L)$ is a set S of mutually skew subspaces each L-isomorphic to Z such that every hyperplane contains exactly one subspace of S.*

Hence, S^* is a dual spread of $PG(V^*, K)$ if and only if S is a spread in $PG(V, K)$.

Exercise 3.3.12 *Show that if $\{(x, xA)\}$ is a spread component of S then $\{(x, xA)^{\perp}\} = \{(z, -zA^{-t})$.*

Exercise 3.3.13 *Show that interchanging $x = 0$ and $y = 0$ by a basis change $(x, y) \longmapsto (-y, x)$ maps a partial spread set $\{A \mid A \in \mathcal{M}\}$ onto the partial spread set $\{-A^{-1} \mid A \in \mathcal{M}\}$.*

Hence, we obtain:

Theorem 3.3.14 *Let S be a spread in $PG(V, K)$ for V a $2k$-dimensional left vector space over a skewfield K. Then there is a dual spread S^* in $PG(V^*, K)$ where V^* denotes the dual space of V such that if $\{(x, xA)$ for $A \in \mathcal{M}\}$ is a spread set for S then $\{(x, xA^t)$ for $A \in \mathcal{M}\}$ is a dual spread set for S^*.*

Exercise 3.3.15 *Show that any spread in $PG(2k-1, q)$ is also a dual spread and conversely any dual spread is a spread.*

Given any infinite skewfield K, there is a spread which is not a dual spread due to the work of Bruen and Fisher [6] and Bernardi [4].

Corollary 3.3.16 *Let S be a spread in $PG(2k-1, K)$ for K a field which is a dual spread.*

If $\{x = 0, y = xA$ for $A \in \mathcal{M}\}$ is a spread representation in the associated vector space then $\{\ x = 0, y = xA^t$ for $A \in \mathcal{M}\}$ is also a spread called the transposed spread S^t.

Exercise 3.3.17 *Show that the full collineation group of a transposed spread is isomorphic to the group of the transposed spread.*

Exercise 3.3.18 *Show that the transposed partial spread of a derivable net is a derivable net.*

Previously, p 63, we have given an example of a regular parallelism in $PG(3,2)$ and hence an associated translation plane π. There is a corresponding transposed plane π^t with the property that the spread for π^t still consists of seven derivable nets sharing a 2- regulus in $PG(7,2)$. It follows that there is a corresponding regular parallelism which we might called the transposed parallelism.

The plane corresponding to the original parallelism is called the *Lorimer-Rahilly* plane of order 16 as it was initially found independently by Lorimer and Rahilly. Similarly, the transposed plane is called the *Johnson-Walker* plane of order 16 as it was determined by Walker using group theory and by Johnson using derivation of the semifield planes of order 16.

Remark 3.3.19 *There are exactly three regular parallelisms of even order; two in $PG(3,2)$ and one in $PG(3,8)$. The corresponding translation planes of order q^4 with spreads in $PG(7,q)$ all admit the collineation group $SL(2,q) \times Z_{1+q+q^2}$. Jha and Johnson [20] have shown that translation planes with such collineation groups must correspond to regular packings in $PG(3,q)$.*

There is exactly one known regular parallelism of odd order which is in $PG(3,5)$ and is due to A. Prince ([36]). The collineation group has not yet been fully determined.

3.4 Introduction to Quadrics and Unitals.

In this section we introduce some standard concepts and tools from linear algebra and projective spaces that have proven to be useful in translation plane

theory. As an application, a theorem of Buekenhout, establishing the existence of unitals in translation planes associated with linespreads, is proved using the Bruck-Bose representation of translation planes. The reader might consider skipping this section as nothing in the sequel depends upon it.

Definition 3.4.1 *A correlation of any vector space is an incidence reversing bijection. Let V_n denote a correlation of a n-dimensional K-vector space where K is a field. So, a correlation will map a vector to a hyperplane.*

We represent a vector as a n-tuple $(x_1, x_2, ..., x_n)$ and since a hyperplane is given in terms of a linear equation, $a_1x_1+a_2x_2+...+a_nx_n = 0$, we represent a hyperplane by $(a_1, a_2, ..., a_k)^t$ where t denotes the transpose matrix operation. Hence, a vector X is incident with a hyperplane Y^t if and only if $XY^t = 0$.

We define the following mapping: Let A be any nonsingular $k \times k$ matrix over K and σ any automorphism of K. If $X = (x_1, x_2, ..., x_n)$ define $X^\sigma = (x_1^\sigma, x_2^\sigma, ..., x_n^\sigma)$.

Define $\delta_{A,\sigma}$ as follows: $\delta_A(X) = AX^{t\sigma}$. Furthermore, the induced mapping on Y^t is $\delta_{A,\sigma}(Y^t) = Y^\sigma A^{-1}$.

We shall be interested in 'polarities' which are defined as correlations of order 2 acting on the corresponding projective space.

Exercise 3.4.2 *Show that δ_A is a correlation.*

Remark 3.4.3 *It can be shown that all correlations on a finite dimensional vector space over a field K can be represented in the form $\delta_{A,\sigma}$ for some matrix A and automorphism σ .*

Proposition 3.4.4 *A correlation $\delta_{A,\sigma}$ is a polarity if and only if $\sigma^2 = 1$ and $A^{\sigma t} = kA$ for some k in K such that $k^{\sigma+1} = 1$.*

Proof: $\delta_{A,\sigma}^2(X) = \delta(AX^{\sigma t}) = (AX^{\sigma t})^{t\sigma}A^{-1}$. In order to induce the identity mapping on the projective space, if follows that this latter equation is kX for some nonzero k of F. Hence, a polarity is obtained if and only if $X^{\sigma^2} = X$ for all X and $A^{\sigma t} = kA$.∎

Exercise 3.4.5 *Show that $k^{\sigma+1} = 1$.*

Definition 3.4.6 *A polarity δ is said to be 'orthogonal', 'symplectic', or 'unitary' accordingly as $(\sigma, k) = (1, 1), (1, -1)$ and $(\neq 1, k)$.*

A subspace W of V_n is said to 'totally isotropic', 'isotropic', or 'non-isotropic' if and only if $W \cap W^\delta = W, \neq 0$, or 0 respectively. If W is a 1-dimensional subspace (point in the projective space) then a totally isotropic 1-space is said to be 'absolute'.

Correlations are related to sesquilinear forms:

Definition 3.4.7 *Let V be a vector space over a skewfield K. A mapping s from $V \times V$ into K is called a sesquilinear form if and only if*

$$s(x+x', y+y') = s(x,y) + s(x',y) + s(x,y') + s(x',y')$$

and

$$s(\alpha x, \beta y) = \alpha s(x,y)\beta^\sigma$$

where σ is an automorphism of K. A sesquilinear form is said to be non-degenerate if and only if $s(x,y) = 0$ for all y in V implies that $x = 0$ and $s(x,y) = 0$ for all x in V implies that $y = 0$.

It turns out that correlations may always be defined from nondegenerate sesquilinear forms as follows:

$$W^\delta = \{x \in V \mid s(x,w) = 0 \forall w \in W\}.$$

Conversely, given any correlation, there is an associated non-degenerate sesquilinear form which gives rise to it as above.

An orthogonal polarity corresponds to a symmetric, bilinear form ($\sigma = 1$) and $s(x,y) = s(y,x)$. A symplectic polarity corresponds to a skew-symmetric bilinear form where $s(x,y) = -s(x,y)$ (for characteristic two, $s(x,x) \neq 0$ for some x is required), and a unitary polarity corresponds to a Hermitian form where $s(x,y) = s(y,x)^\sigma$ for some automorhism σ of order two.

Definition 3.4.8 *A quadratic form Q is a mapping of V into K such that $Q(\alpha x) = \alpha^2 Q(x)$ and $Q(x+y) = Q(x)+Q(y)+s(x,y)$ where s is a symmetric bilinear form. A quadric is the set of points x in the associated projective space such that $Q(x) = 0$. If the characteristic is not two then the form is nondegenerate if and only if $s(x,y) = 0$ for all y in V if and only if $x = 0$. If the characteristic is two then Q is nondegenerate if and only if $Q(w) \neq 0$ when $s(w,x) = 0$ for all x.*

The set $\{v;\ Q(v) = 0$ and $s(v,y) = 0$ for all y in $V\}$ is the set of singular points.

It turns out that when K is not of characteristic two then the set of absolute points of the associated symmetric bilinear form is the set of points of the quadric.

Moreover, in any case, all maximal subspaces contained in a nondegenerate quadric have the same rank (as do all maximal totally isotropic subspaces of a polarity) which is called the index.

Definition 3.4.9 *An ovoid in $PG(3,q)$ is a set of q^2+1 points such that no three are collinear and for any point P the set of tangent lines forms a plane (hyperplane).*

If Q is a nondegenerate quadric in $PG(3,q)$ of rank 1 then the quadric is an ovoid.

Now let π be a Desarguesian projective plane of order q^2 considered as $PG(2,q^2)$. Let σ denote the involutory automorphism of the associated field $F \cong GF(q^2)$ coordinatizing π and defined by $z^\sigma = z^q$ for all z in F.

Let V_3 denote the associated 3-dimensional vector space whose lattice of subspaces define $PG(2,q^2)$. Let $A = I_3$ and consider the unitary polarity $\delta_{I,\sigma}$.

The major facts about unitary polarities in V_3 are as follows: Let $\Sigma = PG(2,q^2)$.

Theorem 3.4.10 *A unitary polarity of V_3 over $GF(q^2)$ has q^3+1 absolute points and $q^4-q^3+q^2$ non-isotropic lines in Σ.*

Assuming that the polarity is $\delta_{I,\sigma}$, a point represented by (x,y,z) is absolute if and only if $x^{\sigma+1}+y^{\sigma+1}+z^{\sigma+1}=0$.

Exercise 3.4.11 *Prove part (1) assuming $\delta_{I,\sigma}$ represents the polarity.*

Theorem 3.4.12 *(1) Each non-isotropic line contains $q+1$ absolute points and every two absolute points are incident with a unique non-isotropic line.*

(2) There are exactly q^2 non-absolute lines on any absolute point. Hence, there is a unique absolute line incident with any point.

Definition 3.4.13 *A $t-(v,k,\lambda)$-design is an incidence structure of 'points', 'blocks', and 'incidence' where there are v points, k points per block and any set of t distinct points is incident with exactly λ blocks.*

A 'unital' is defined to be a $2-(q^3+1,q+1,1)$-design.

Hence, we see that the absolute points and non-absolute lines in $\Sigma \cong PG(2, q^2)$ *form a unital called the classical unital. However, there are unitals which are not classical some of which cannot be embedded into projective planes. But, if unitals are embedded into projective planes where the blocks are lines, they share the regularity conditions exhibited in the previous theorem.*

Theorem 3.4.14 *Let* π^+ *denote a projective plane of order* q. *Assume that* π^+ *contains a unital* $\mathcal{U}$ *as a* $2-(q^3+1, q+1, 1)$*-design.*

Then

(1) each point P *of* $\mathcal{U}$ *lies on exactly* q^2 *lines of* $\mathcal{U}$ *which we call 'secant lines'. The remaining line incident with* P *intersects* $\mathcal{U}$ *in exactly* P *and is called a 'tangent line'.*

(2) Each line of π^+ *is either a secant line of a tangent line. That is, each line of the plane either intersects* $\mathcal{U}$ *in one of* $q+1$ *points and ,in the latter case, is a line of the design.*

(3) Each point Q *of* $\pi^+ - \mathcal{U}$ *is incident with exactly* $q+1$ *tangent lines and* q^2-q *secant lines. The* $q+1$ *intersections of the tangents of* Q *with* $\mathcal{U}$ *are called the feet of* Q. *When the unital is classical, the line (hyperplane)* $\delta_{I,\sigma}(Q)$ *is non-isotropic so intersects* $\mathcal{U}$ *in exactly* $q+1$ *points which implies that the feet of* Q *are collinear in the classical situation.*

Proof: We count the flags (point of $\mathcal{U}$, line (block) of $\mathcal{U}$) and note that the number of points of $\mathcal{U}$ times the number B of blocks per point $= (q^3+1)B =$ the number U of lines of $\mathcal{U}$ times the number of points of $\mathcal{U}$ per line $= U(q+1)$. Given any point P and any of the q^3 remaining points Q of $\mathcal{U}$, there is a unique line of the unital containing P and Q. Hence, there are exactly q^3/q lines incident with P which are lines of the unital. Hence, it follows that $B = q^3$ so that $U = q^4 - q^3 + q^2$. Since there are exactly $q^4 + q^2 + 1$ lines of the projective plane and there are $q^3 + 1$ tangent lines by the above argument, this accounts for all of the lines of the plane and proves (1) and (2).

Exercise 3.4.15 *Prove part (3).*

The motivation for inducing unitals at this time is to employ the Bruck-Bose representation to show there exist unitals in any translation plane of order q^2 with spread in $PG(3, q)$.

The reader is referred to Buekenhout [7] for further and more complete details.

Proposition 3.4.16 *Let π be an affine Desarguesian translation plane of order q^2 with spread S in $PG(3,q)$. and let $\mathcal{U}$ be a classical unital embedded in the projective plane π^+.*

Realize π and π^+ in $PG(4,q)$ using the Bruck-Bose representation.

We note that the points on ℓ_∞ are represented as the lines of S in the hyperplane $PG(3,q)$.

Let $A(\mathcal{U}) = \mathcal{U} \cap \pi$. Futhermore, let

$\Delta(\mathcal{U}) := A(\mathcal{U}) \cup \{$*points on lines of S corresponding to infinite points of π*$\}$.

1. *If ℓ_∞ is a tangent line to the unital then,in $PG(4,q)$, $\mid \Delta(\mathcal{U}) \mid = q^3+q+1$ and*

2. *if ℓ_∞ is a secant line to the unital then, in $PG(3,q)$, $|\Delta(\mathcal{U})| = q^3 - q + (q+1)^2$.*

Exercise 3.4.17 *Prove the above proposition.*

Definition 3.4.18 *In situation (1), the unital is said to be 'parabolic' and in situation (2), 'hyperbolic'.*

The main theorem of Buekenhout is

Theorem 3.4.19 *$\Delta(\mathcal{U})$ is a quadric in $PG(4,q)$.*

(1) If $\mathcal{U}$ is parabolic then $\Delta(\mathcal{U})$ has one singular point p and is the union of all lines joining p to the points of some 3-dimensional ovoid of $AG(4,q)$ with one point at infinity.

(2) If $\mathcal{U}$ is hyperbolic then $\Delta(\mathcal{U})$ is non-singular.

Proof: We shall sketch the proof of (1). The proof of (2) is similar. Consider the regular spread

$$x = 0, y = x \begin{bmatrix} u+tg & tf \\ t & u \end{bmatrix} \forall u, t \in K \cong GF(q),$$

in $PG(3,q)$. Note that $x^2 - xg + f$ is a K-irreducible polynomial. By results from the algebraic tract, we extend K to a field $K[e]$ such that $e^2 = eg - f$ and multiplication in $K[e] \cong GF(q^2)$ is given as follows:

$$(t^*e + u^*)(te + u) = (t^*, u^*) \begin{bmatrix} u+tg & tf \\ t & u \end{bmatrix}$$

written over $\{e, 1\}$ for all t^*, u^*, t, u of K.

Let σ denote the automorphism of $K[e]$ given by $x^\sigma = x^q$.

We consider the classical unital $\mathcal{U}$ in the associated Desarguesian projective plane $PG(2, K[e] = F \cong GF(q^2))$ whose points are given homogeneously by (x, y, z) for x, y, z in F and $(x, y, z) \neq (0, 0, 0)$.

We choose $z = 0$ to be the line at infinity ℓ_∞ and $z = 1$ to denote the affine point of π. Furthermore, we identify $(x, y, 1)$ and (x, y). We choose $(x, 1, 0) = (x)$ and $(0, 1, 0) = (\infty)$ on the line at infinity. We choose the unique point on ℓ_∞ of $\mathcal{U}$ as $(\infty) = (0, 1, 0)$. We choose a matrix for the unitary polarity so that $(0, 1, 0)$ is an absolute point. In particular, the matrix $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ provides the form as $\{(x, y, z); x^{\sigma+1} + zy^\sigma + yz^\sigma = 0\}$.

Hence, with our notation, we have $\{(x, y); x^{\sigma+1} + y^\sigma + y = 0\} \cup \{(\infty)\} = \mathcal{U}$.

Now to form $\Delta(\mathcal{U})$. We note that using the Bruck-Bose model, $x = 0 = (x_1, x_2)$ is a set of $q + 1$ points of $\Delta(\mathcal{U})$. Since $x^2 - xg + f$ is irreducible, it follows that $x_1^2 f - x_1 x_2 g + x_2^2 = 0$ is equivalent to $(x_1, x_2) = 0$.

Exercise 3.4.20 *Show that* $e^\sigma = -e+g$ *and* $e^{\sigma+1} = -f$. *Letting* $x = x_1 e + x_2$ *and* $y = y_1 e + y_2$ *show that*

$$x^{\sigma+1} + y^\sigma + y = 0 = -(x_1^2 f - x_1 x_2 g + x_2^2 + y_1 g + 2y_2).$$

Exercise 3.4.21 Embed the affine space $AG(4, q)$ into $PG(4, q)$ as follows:

$$(x_1, x_2, y_1, y_2) \longmapsto (x_1, x_2, y_1, y_2, z)$$

and consider the points of $PG(4, q)$ as the 1-dimensional subspaces of a 5-dimensional K-vector space. Show that

$$x_1^2 f - x_1 x_2 g + x_2^2 + y_1 g + 2y_2 = 0$$

if and only if

$$x_1^2 f - x_1 x_2 g + x_2^2 + z y_1 g + 2z y_2 = 0.$$

Note that the intersection with the infinite points when $z = 0$ is $(x_1, x_2) = 0$ which is $\{(0, 0, 1, \alpha), (0, 0, 0, 1, 0); \alpha \in GF(q)\}$.

Hence, the above equation defines a quadric defining $\Delta(\mathcal{U})$.

Exercise 3.4.22 *Show the quadric above is degenerate. Show the unique singular point is* $(0,0,-2,g,0) = p$.

Now choose the hyperplane defined by $y_2 = 0$ and note that intersection with $\Delta(\mathcal{U})$ is given by

$$\{(x_1, x_2, y_1, z); x_1^2 f - x_1 x_2 g + x_2^2 + z y_1 g = 0.$$

Exercise 3.4.23 *The above quadric in the hyperplane isomorphic to* $PG(3,q)$ *is nondegenerate and of index* 1. *Show this when* q *is odd.*

Hence, all points of $\Delta(\mathcal{U})$ lie on lines of p, there are exactly q^2+1 points of an ovoid of H in $AG(4,q)$ and exactly one infinite point $(0,0,1,0,0)$ of H. Since each line is a 2-dimensional K-vector space and $\Delta(\mathcal{U})$ is a quadric, it follows that there are exactly $q+1$ points of $\Delta(\mathcal{U})$ on each line thru p. Hence, this accounts for the q^3+q+1 points as $(q^2+1)q+1$ points on lines thru p. Hence, there is an ovoid $\mathcal{O}$ in $PG(3,K)$ such that $\Delta(\mathcal{U})$ lies on $p\mathcal{O}$.

Now, it turns out that $\Delta(\mathcal{U})$ induces a unital in any translation plane with spread in $PG(3,K)$.

Theorem 3.4.24 *Let* ρ *be any translation plane of order* q^2 *with spread in* $PG(3,q)$ *then* ρ *contains a parabolic unital.*

Proof: The idea of the proof is to show that $\Delta(\mathcal{U})$ remains a unital in ρ.

If (∞) is the tangency point, we may assume that $x = 0$ (L) is a line common to ρ and the Desarguesian affine plane π. We identify the points of π and ρ so that we may consider $\Delta(\mathcal{U})$ as a set of points in ρ^+ (the projective extension of ρ). We assert that the lines of ρ^+ which join pairs of points of $\Delta(\mathcal{U})$ is a $2-(q^3+1, q+1, 1)$-design ; a unital. It remains only to show that the lines of ρ^+ joining pairs of such points intersect $\Delta(\mathcal{U})$ in exactly $q+1$ points.

First consider a line of ρ incident with (∞). Any such line becomes a 2-dimensional projective subspace which intersects the hyperplane at infinity in $x = 0$ which consists of $q+1$ points of $\Delta(\mathcal{U})$.

Suppose a, b are points of $\Delta(\mathcal{U})$ which are in π so in ρ. The line ab is a plane of $AG(4,K)$ and $\Delta(\mathcal{U})$ is a quadric. Assume that ab is not on (∞). Hence, the projective extension $ab^+ \cap \Delta(\mathcal{U}) = C$ is a quadric possibily degenerate. In the former case, a nondegenerate quadric in a projective plane $PG(2,q)$ is a conic of $q+1$ points. In the latter case, it is possible that C is

the union of two lines of $PG(4,K)$. If C contains a line of $PG(4,K)$ then it contains a line ℓ of $AG(4,K)$ which is contained in a line ρ_ℓ of the translation plane ρ. But, the projective extension of ℓ contains a point of $\Delta(\mathcal{U})$ so that ρ_ℓ must be incident with (∞). This completes the proof.

We have noted that any regulus in $PG(3,K)$ can be embedded in a regular spread. The same idea as above shows that any translation plane with spread S in $PG(3,K)$ such that S contains a regulus in $PG(3,K)$ forces the existence of a hyperbolic unital in such translation planes.

Theorem 3.4.25 *Let ρ be a translation plane with spread S in $PG(3,K)$. If S contains a regulus then ρ^+ contains a hyperbolic unital (ℓ_∞ is a secant line to the unital).*

There are many questions and problems that might be mentioned with regard to translation planes admitting unitals. However, here is a general problem.

Let π denote a translation plane with spread in $PG(3,q)$ that admits a unital. When is the unital a Buekenhout unital?

Finally, we point out that the construction given can be generalized and need not depend upon a classical unital.

Chapter 4

Quasifields And Their Variants.

Quasifields coordinatize translation planes. In the finite case, these are basically non-associative division rings but possibly missing a distributive law and a multiplicative identity. Here we consider, alternative approaches to the definition, and the problems that arise in the infinite case.

4.1 Quasigroups and Loops.

A binary system $(X, \circ)$ is a *quasigroup* if:

$$a, b, c \in X \Longrightarrow \exists! x, y \in X \ni a \circ x = c \wedge y \circ b = c,$$

or

"Two in $x \circ y = z$ fixes Third."

If a two-sided multiplicative identity exists in a quasigroup then it is a *loop*, thus, loops additionally satisfy:

$$\exists e \in X \ni \forall x \in X : x \circ e = e = e \circ x.$$

Exercise 4.1.1 *Let $(X, \circ)$ denote a quasigroup.*

1. *A loop has a unique identity e, and every one-sided identity is two-sided and hence must coincide with e.*

2. *If $(X, \circ)$ is a finite loop with identity e and $Y \subset X$ is a non-empty set closed under $\circ$, then $(Y, \circ)$ is a loop iff $e \in Y$.*

3. *Show that the finiteness hypothesis is essential above: consider the case when X is a group.*

4. *Let Y be a set and suppose $C : X \to Y$, $A : X \to Y$ and $B : X \to Y$ denote bijections. Then define $(Y, *)$ by:*

$$\forall x, y \in X : (x \circ y)C = (xA) * (yB).$$

Show that $(Y, *)$ is a loop.

5. *Define the cartesian product of a family of quasigroups and hence demonstrate the ubiquity of quasigroups and non-associative loops. In particular resolve the following question:*
Is there a non-associative loop of order n for all integers $n > 2$?

Now if $(X, \circ)$ and $(Y, \circ)$ are related by a triple of bijections $\mu = (A, B, C)$ then the triple is called an *isotopism* from $(X, \circ)$ to $(Y, \circ)$; the latter is called an isotope of the former: isotopism is an equivalence relation. The set of isotopisms from $(X, \circ)$ to itself are called its autotopisms. Compostion of isotopisms are defined in the natural way, and under this defintion the autotopisms of a quasigroup $(X, \circ)$ form a group: its *autotopism group*. The *automorphism* group of $(X, \circ)$, in the usual sense, are just the autotopisms satisfying $A = B = C$; similarly the isomorphisms from one quasigroup to another are just the isotopisms with all three components in agreement.

Exercise 4.1.2

1. *Assume $(X, \circ)$ is a quasigroup. Choose $e \in X$ and define the binary operation $*$ on X by:*

$$\forall x, y \in X : x * y = (x \circ e) * (e \circ y).$$

Show that $(X, *)$ is a loop with identity $e \circ e$.

2. *Show that every quasigroup is isotopic to a loop.*

3. *Show that every loop admits autotopisms that are not automorphisms.*

4. *Show that every quasigroup $(X, \circ)$ is isotopic to a quasigroup $(X, *)$ such that the two quasigroups are* non-*isomorphic.*

5. *Every finite group G is the automorphism group of a finite abelian group, e.g., G lies in infinitely many $GL(n,q)$. The question arises: Is every finite group an autotopism/automorphism group of at least one non-associative loop? [What if the non-associative requirement is dropped?]*
Suggestion: G can be viewed as a planar group of some free plane, and this can easily be chosen so that the fixed plane can be coordinatized by a ternary ring with non-associative multiplication.

4.2 Translation Algebras and Quasifields.

In this section, we consider certain choices for the definition of a quasifield — the systems coordinatizing affine translation planes. For example, some translation planes have simpler representations when they are coordinatized by certain 'quasifields' with the multiplicative identity missing — prequasifields. Also, the simple axioms that characterise finite quasifields and prequasifields, do not yield translation planes in the infinite case — so the structures that satisfy the natural axioms for finite quasifields have sometimes been called 'weak' quasifields [18]. To put things in perspective we shall make a brief examination of the most general such systems in this section: these are 'weak-pre-quasifields', but we prefer to call them simply translation algebras, and we define [pre]-quasifields as the translation algebras that coordinatize translation *planes*, rather than more general *combinatorial* structures. The reader is invited to complete the 'André theory' for translation structures that is hinted at here.

If $(K,+,\circ)$ is a skewfield then the associated incidence structure is an affine Desarguesian plane $\Pi(K)$, whose points are the members of $K \oplus K$ and whose lines are all sets of points that are of form $y = x \circ m + c$ or $x = k$, for $m, c, k \in K$. More generally, one might consider structures of type $(Q,+,\circ)$ such that the associated incidence structures $\Pi(Q)$, obtained as above, are non-Desarguesian affine planes. Affine planes coordinatized by *cartesian groups* are of the form $\Pi(Q)$, where $(Q,+)$ is a group.

Our interest in such systems is restricted to the case when $(Q,+)$ is an abelian group: this will allow us to deal simultaneously with the notions of prequasifields, weak quasifields, pre-weak quasifields..., which become unavoidable in the study of translation planes: many translation planes have their simplest forms when they are expressed in terms of *pre*-quasifields, and

the associated objects in the infinite case are 'weak'.

Now if $(Q,+)$ is an abelian group then the additive group $Q \oplus Q$ admits a natural translation group τ, consisting of all bijections

$$\begin{aligned} \tau_{(a,b)} : Q \oplus Q &\rightarrow Q \oplus Q \\ (x,y) &\mapsto (x,y)+(a,b), \end{aligned}$$

for $a,b \in Q$. Thus τ is regular on the points of $\Pi(Q)$, when $(Q,+,\circ)$ is such that the additive group $(Q,+)$ is abelian. Our interest in $(Q,+,\circ)$ is restricted to the case when τ is, additionally, a collineation group of the incidence structure, and $x \circ 0 = 0 \circ x = 0$, where 0 is the identity of the additive group $(Q,+)$.

In the finite case, this simply turns out to mean that $\Pi(Q)$ is a translation plane, and eventually it will be shown that all finite translation planes are of this type. In the infinite case, $(Q,+,\circ)$ becomes a 'weak' pre-quasifield: the incidence structure $\Pi(Q)$ may fall short of being an affine plane, although still admitting the transitive translation group τ.

Definition 4.2.1 *$Q = (V,+,\circ)$ is called a zero-linked system if:*

1. *$(V,+)$ is an abelian group with neutral element 0;*
2. *$V^* = V - \{0\}$ is a quasigroup;*
3. *$0 \circ x = 0 = x \circ 0 \forall x \in V$,*

The set-theoretic incidence structure $\Pi(Q)$, coordinatized by Q, is defined to have $V \oplus V$ as its points, and its lines are the subsets of $V \oplus V$ that may be expressed in the form

$$\forall m,b \in K : y = x \circ m + b := \{(x, x \circ m + b) \mid x \in V\},$$

or

$$\forall k \in K : x = k := \{(k,y) \mid y \in V\}.$$

The zero-linked system $Q = (V,+,\circ)$ is called a translation algebra *if additionally the translation group of the additive group $V \oplus V$, viz:*

$$\tau := \{\tau_{a,b} : (x,y) \mapsto (x+a, y+b) \mid (a,b) \in V \oplus V\}$$

is a collineation group of $\Pi(Q)$.

A translation algebra is called a pre-quasifield *if $\Pi(Q)$ is an affine plane (and hence an affine translation plane).*

Exercise 4.2.2 *Let $(Q,+,\circ)$ be any zero-linked structure.*

1. *Show that the group*

$$\Theta := \{(x,y) \mapsto (x, y+b) \mid b \in Q\}$$

is a translation group of $\Pi(Q)$.

2. *Give examples of finite $(Q,+,\circ)$ such that $\Pi(Q)$ is not a translation plane.* Consider coordinatizing a dual translation plane.

3. *Are all zero-linked systems translation algebras?*

The following proposition means that a *finite* translation algebra is the same things as a *finite* prequasifield.In the infinite case a translation algebra is the same thing as a 'weak (pre)quasifield' in the sense of Hughes and Piper. Thus, translation algebras are introduced (temporarily) to refer to the same objects that have been given different names in the finite and infinite situations.

Proposition 4.2.3 *Let $(Q,+,\circ)$ be a zero-linked system. Then it is a translation algebra iff the right distributive law holds:*

$$\forall a,b,c \in Q : (a+b)\circ c = a\circ c + b\circ c.$$

Proof: Assume the translations $\tau_{a,b} : (x,y) \mapsto (x+a, y+b)$, of $Q \oplus Q$, permute the lines of $\Pi(Q)$. So

$$\begin{aligned}
y = x\circ m + c &\mapsto y = x\circ m' + c' \\
\Rightarrow \{(x+a, x\circ m + c + b) \mid x \in Q\} &= \{(x+a, (x+a)m' + c') \mid x \in Q\} \\
\Rightarrow x\circ m + c + b &= (x+a)\circ m' + c' \\
\text{So by } x \leftarrow 0 : -a\circ m' + c + b &= c' \\
\text{So} : x\circ m + c + b &= (x+a)\circ m' + (-a\circ m' + c + b) \\
\Rightarrow x\circ m + a\circ m' &= (x+a)\circ m'
\end{aligned}$$

and the result follows because all translations must be permitted. The converse, that the right distributive law implies that τ is a collineation group of $\Pi(Q)$, is just as easy. ∎

The following proposition gives the standard condition for a translation algebra, finite or infinite, to be a prequasifield in the usual sense of the term.

Proposition 4.2.4 *Let $(Q, +, \circ)$ be a translation algebra. Then $\Pi(Q)$ is a translation plane if and only if:*

$$\forall a, c, d \in Q, a \neq c(\exists! x \ni x \circ a - x \circ c = d)$$

Proof: We need to check that the incidence structure $\Pi(Q)$ is an affine plane iff the condition holds. We verify that for any translation algebra, distinct points (a, b) and (c, d) of $\Pi(Q)$ lie on a unique line. When $a \neq c$, then the equations:

$$\begin{aligned} a \circ m + b &= n \\ c \circ m + d &= n, \end{aligned}$$

together with the right distributive law and the quasigroup property of Q^*, enable m and n to be uniquely determined since we have: $(a - c) * m = -(b - d)$. And if $a = c$ then '$x = c$' is the only common line. So two points meet, and clearly parallel lines, meaning those with the 'same slope', do not meet. Hence for $\Pi(Q)$ to be an affine plane everything clearly depends on whether or not the lines '$y = x \circ a + b$' and '$y = x \circ c + d$' meet for $a \neq c$. But these lines meet at points whose X-coordinates x satisfy:

$$x \circ a + b = x \circ c + d$$

and this equation has a unique solution iff:

$$x \circ a - x \circ c = d - b,$$

and this is the given condition. The result follows. ∎

Corollary 4.2.5 *Finite translation algebras and distributive translation algebras always coordinatize translation planes.*

Proof: Using the notation of proposition 4.2.4 above, the map $\theta : x \mapsto x \circ a - x \circ c$ is an additive map, and its kernel corresponds to x satisfying $x \circ a = x \circ c$, contradicting the quasigroup hypothesis on $W^*, \circ)$, unless θ is injective. So in the finite case θ is certainly bijective. In the general case, when $\circ$ is distributive, the distributive law yields the identity $-u \circ v = u \circ (-v)$ and hence also $\theta(x) = x \circ (a - c)$. So distributivity implies that θ is bijective since $(W^*, \circ)$ is a multiplicative loop. Thus in both cases, finite or distributive, θ

is bijective whenever $a \neq c$. Hence proposition 4.2.4 yields the desired result. ∎

Thus the concept of a translation algebra coincides with that of a pre-quasifield (structures that coordinatize affine translation planes) in the *finite case* or when *both the distributive law* holds.

4.3 Schur's Lemma, Slope Maps and Kern.

In this lecture we introduce some tools and concepts essential for the study of spreads and translation planes. We begin by recalling Schur's lemma, a result that plays a central part in spread theory. We shall use it in a moment to show that all translation algebras are built on vector spaces.

Result 4.3.1 *[Schur's Lemma.] If V and W are irreducible modules and $\Phi : V \to W$ is a non-trivial linear map from V to W then Φ is a bijective isomorphism.*

Proof: The kernel of Φ is trivial because V is irreducible and Φ is surjective because its image is a submodule of W. ∎

We have met the concept of slopesets (or slope maps) of a spread. We now turn to slope maps of a translation algebra. We shall eventually see that slope maps associated with a translation algebra and those associated with a spread are essentially identical concepts.

Definition 4.3.2 (Slope Maps) *Let $Q = (W, +, \circ)$ be a translation algebra. Then the endomorphisms of $(W, +)$ of form: $\tau_a : x \mapsto x \circ a$ are its* slope maps. *$\tau = \{\tau_a \mid a \in W\}$ is the* slope-set *of the translation algebra Q.*

We can now apply Schur's lemma to show that translation algebras, of all types, are built on vector spaces and that their non-zero slope maps are *non-singular* relative to the vector structure.

Lemma 4.3.3 (Kern Endomorphisms.) *Let $Q = (V, +, \circ)$ be a translation algebra; so its slopeset τ consists of a subset of $Hom(V, +)$ such that τ_a, for all $a \in V^*$, are bijective members of $Hom(V, +)$. Let K be the centralizer of τ in $Hom(V, +)$. Then the following apply:*

1. *K is a skewfield whose non-zero elements are all bijections in $Hom(V, +)$;*

2. *τ consists of K-linear maps of V when V is viewed as a vector space over K: thus, $\theta \in \tau$ implies:*

$$vk\theta = v\theta k \forall k \in K, \theta \in \tau.$$

Proof: The quasigroup condition on V^* shows that τ^* generate a group acting transitively on V^*, and so the group $< \tau^* >$ is irreducible. Now apply Schur, lemma 4.3.1. ∎
The skewfield K of the lemma will be called the external *kern* of the translation algebra:

Definition 4.3.4 (External Kern.) *Let τ be the set of slope maps of a translation algebra $Q = (V, +, \circ)$. Then the the centralizer of τ in $Hom(V, +)$ is the [external]* KERN *of Q, and also of τ; these are denoted by $kern(Q)$ and $kern(\tau)$ resp.*

The following remarks follow from lemma 4.3.3 and the definition of the kern of a translation algebra. It might be helpful to remind the reader that all prequasifields are translation algebras and in the finite case both concepts coincide.

Remarks 4.3.5 *Let K be the kern of a translation algebra $(Q, +, \circ)$. Then the following hold.*

1. *The additive group $Q \oplus Q$ becomes a vector space relative to the operation:*

$$k(x, y) := (x^k, y^k) \forall k \in K, x, y \in Q.$$

This is always taken as the STANDARD *kern action on $Q \oplus Q$.*

2. *The standard action of K^* on $Q \oplus Q$ induces faithfully a group of collineations of $\Pi(Q)$ that fixes $(0, 0)$ and all the lines through it. Conversely every additive bijection of $Q \oplus Q$ that fixes every line through the origin $(0, 0)$ is of form $(x, y) \mapsto (x^k, y^k)$, $k \in K^*$.*

Thus the above remark shows that the concept of kern homolgies, associated with a translation plane, carries over to a considerable extent to $\Pi(Q)$, where Q is a translation algebra.

Exercise 4.3.6 *To what extent does the André theory of spreads and translation planes carry over to $\Pi(Q)$, the incidence structure associated with translation structures? For example, resolve the following questions:*

1. *Is the full group of 'dilations' of* $\Pi(Q)$ *just the group* τK^**?*
2. *Does every collineation* σ *fixing the origin an element of* $\Gamma L(Q \oplus Q, K^*)$*, the group of non-singular semilinear maps of the* K*-space* $Q \oplus Q$*.*

The obvious approach to the above exercise is to try and imitate the André theory. However, since we only deal with translation structures that are quasifields, and thus by *definition* $\Pi(Q)$ is a translation plane, we already have available the complete answer to such questions by André theory.

We now establish a simple result of fundamental importance: the kern of any quasifield $(Q, +, \circ)$, as opposed to a *pre*-quasifield, may be defined in two equivalent ways — as the centralizer of the slope maps of $(Q, +, \circ)$ in $Hom(Q, +)$, as done earlier, definition 4.3.4, and as the sub[skew] field of $(Q, +, \circ)$ consisting of the elements in the left nucleus $N_\ell(Q)$ that distribute from the left — the internal kern.

Definition 4.3.7 (Internal Kern.) *Let* $Q = (V, , +, \circ)$ *be a translation algebra with multiplicative identity* e*. Then the* INTERNAL *kern* $\kappa(Q)$ *of* Q *is:*

$$\{k \in Q \mid \forall x, y \in V : (k \circ (x + y) = k \circ x + k \circ y) \wedge (k \circ x) \circ y = k(\circ x \circ y)\}.$$

The following result establishes the equivalence of the external and the internal kern, c.f., definition4.3.4 and definition 4.3.7.

Proposition 4.3.8 *Let* $(Q, +, \circ)$ *be a translation algebra that has a multiplicative identity* e *and let* $\kappa(Q)$ *be its internal kern, c.f., definition 4.3.7. To each* $k \in \kappa(K)$ *assign the map:* $\overline{k} : x \mapsto k \circ x$*. Then*

$$End(Q, +) \geq \overline{\kappa(Q)} = kern(Q),$$

where the RHS is the [external] kern, c.f., definition 4.3.4.

Proof: It is straightforward to verify that the elements of $\kappa(Q)$ are additive maps of Q and that they centralize the slopemaps of the quasifield Q and hence, by definition, $\kappa(Q)$ is contained in $kern(Q)$. We verify the converse. Suppose $\alpha \in kern(Q)$ and let $e^\alpha = a$. We must demonstrate that a satisfies the defining identities for $\kappa(Q)$. Since α centralizes the slope maps of Q we have:

$$\forall x, m \in Q : (x \circ m)^\alpha = (x^\alpha) \circ m,$$

so

$$\forall x, m \in Q : (x \circ m)^\alpha = (x^\alpha) \circ m,$$

and choosing $x = e$ yields:

$$\forall m \in Q : m^\alpha = a \circ m$$

so

$$\forall x, m \in Q : a \circ (x \circ m) = (a \circ x) \circ m,$$

so $a \in N_\ell(Q, \circ)$. Moreover, the requirement that $\alpha \in Hom(Q, +)$, now easily yields the required distributive law:
$a \circ (x + y) = a \circ x + a \circ y$. ■
In view of the above theorem, we shall eventually cease to distinguish between the internal and external kern. Note that by lemma 4.3.3, and definition 4.3.4, the external kern is always a skewfield and hence by the proposition above the same holds for the internal kern. Thus we have established:

Remark 4.3.9 *Let $(Q, +, \circ)$ be any translation algebra with a multiplicative identity. Then internal and external kern of $(Q, +, \circ)$, are isomorphic skewfields.*

Appendix: Quasi-Quasifields

We pause to mention another system, distinct from a translation algebra, that in the finite case reduces to a pre-quasifield, as does translation algebras. These structures are called quasi quasifields, and in the infinite case, quasifibrations are either spreads or maximal partial spreads, see [19]; thus they arise naturally in investigations involving transation nets.

The essential difference between the two structures, translation algebras and quasi-quasifields, lies in the fact that the one-half of quasigroup condition, '$a \circ \boxed{x} = b$' need not hold for quasi-quasifields, but holds for translation algebras, while the distributive-equation

$$(a + b) \circ \boxed{x} = a \circ \boxed{x} + b \circ \boxed{x},$$

has a unique solution for x in quasi-quasifields but may fail for infinite translation algebras.

Definition 4.3.10 *A triple $(Q, +.\circ)$ is called a quasi-quasifield if:*

1. *$(Q, +)$ is an abelian group: so 0 denotes the additive identity;*

2. *$\forall x : x \circ 0 = 0 \circ x = 0$;*

3. *$(Q, \circ)$ has a left identity e: so $e \circ x = x$ for $x \in Q$;*

4. *The right distributive law holds:*

$$\forall x, a, b \in Q : (a + b) \circ x = a \circ x + b \circ x;$$

5. *For $a, b, c \in Q$, $a \neq c$, the equation $x \circ a = x \circ b + c$ has a unique solution for x.*

The maps $T_a : x \mapsto xa$, for $a \in Q$. are called the slope maps of the quasi qausifield, and τ_Q, the set of all slope maps, is called the slope set: it is clearly a subset of $Hom(Q, +)$. The centralizer of τ in $Hom(Q, +)$ is a ring K called the [outer] kern of the quasi-quasifield.

Remark 4.3.11

1. *The slopeset τ is a sharply one-transitive set on Q, equivalently, in $(Q^*, \circ)$ every equation $x \circ a = b$ has a unique solution for $x \in Q^*$, when $a, b \in Q^*$: so the 'right-loop law' holds.*

2. *The outer kern K of a quasi-quasifield Q is a skew field, and the slopemaps of Q are linear maps of $(Q, +)$, when this additive group is regarded as a vector space over K under its standard action.*

3. *The difference $T_a - T_b$ is non-singular when $a, b \in \tau$ are distinct.*

4. *A finite quasi-quasifield is a quasifield.*

Proof: Case (1): Apply condition 4.3.10(5) with $b = 0$. Case (2): the previous case enables a Schur argument to be applied, see lemma 4.3.3. Now applying the condition 4.3.10(5) again yields Case (3). Case (4) follows by noting that if for $a \neq 0$: $a \circ x = a \circ y$ then for $x \neq y$ we have $T_x - T_y$ is singular, contrary to case (3); hence $x \mapsto a \circ x$ is injective and thus in the finite case it is bijective. ∎

Thus a finite translation algebra and a finite quasi-quasifield are just pre-quasifields. In the infinite case they lead to different structures: a translation algebra may have the condition 4.3.10(5) missing, but the multiplication is required to yield a quasigroup, so $a \circ x = c$ has a solution for x when $a \neq 0$: this need not hold in an infinite quasi-quasifield. The structure associated with quasi-quasifields are called quasifibrations.

Chapter 5

Coordinatization.

The theme of this chapter is coordinatization of structures that are associated with translation planes. In particular, we emphasize how spreads are coordinatized by spreadsets and (pre)quasifields, and also on how spreadsets may themselves be coordinatized by (pre)quasifields.

5.1 Spreads and Quasifields.

Recall that, by definition 1.1.17, a spread $\pi = (V, \mathcal{S})$ is a collection of additive subspaces $\mathcal{S}$, of an additive group V, such that every $x \in V$ lies in some *component* $\sigma \in \mathcal{S}$, and

$$\alpha, \beta \in \mathcal{S} \Longrightarrow V = \alpha \oplus \beta \vee \alpha = \beta.$$

We now assign to each prequasifield Q an associated spread $\pi(Q)$, said to be *coordinatized* by Q. We summarize some related notation which will be very extensively used: the notation is essentially that of elementary coordinate geometry in the context of quasifields; it is kept sufficiently flexible to consider the classification of quasifields among zero-linked structures, defintion 4.2.1; variants of the notation are useful in studying partial spreads and nets.

Notation 5.1.1 *Let $Q = (W, +, \circ)$, where $(W, +)$ is the additive group of a vector space and $\circ$ is a binary operation on W. Then on the vector space $W \oplus W$ we define the following subsets.*

1. *The X-axis and the Y-axis are respectively $X := W \oplus \mathbf{O}$ and $Y := \mathbf{O} \oplus W$.*

2. *The unit line is the set* $\{(x,x) \mid x \in W\}$, *and denoted by* Z *or* $vecI$.

3. *The* non-vertical lines *are the sets of type*

$$\forall m, b \in W : \text{`}y = x \circ m + b\text{'} := \{(x, x \circ m + b \mid x \in W\}.$$

4. *The vertical lines are all sets of type:*

$$\forall b \in W : \text{`}x = b\text{'} := \{(b,y) \mid y \in W\}.$$

The quotation marks above are often dropped. Also note that, in the context of a translation algebra $(Q,+,\circ)$, the collection of all lines whether or not they are vertical, coincides with $\Pi(Q)$, the incidence structure associated with $(Q,+,\circ)$. As $\Pi(Q)$ is determined by the lines through zero, we shall introduce a special notation for this structure: we write $\pi(Q)$ for the lines $\Pi(Q)$ through the origin:

Definition 5.1.2 *If* $Q = (W,+,\circ)$ *is any zero-linked structure, see definition 4.2.1 structure,then* $\pi(Q) := (V,\mathcal{S})$, *where* $V = W \oplus W$ *and*

$$\mathcal{S} = Y = \{\mathbf{O} \oplus W\} \cup \{\text{`}y = x \circ m\text{'} \mid m \in Q\};$$

the members of $\mathcal{S}$ *are the components of* $\pi(Q)$*; thus the components are the lines of* $\Pi(Q)$ *through the origin.*

A fundamental but elementary result is that $\pi(Q)$ is a spread iff the given zero-linked structure Q is at least a pre-quasifield.

Remark 5.1.3 *Let* $Q = (W,+,\circ)$ *be a zero-linked structure, definition 4.2.1, and the sfield* K *its kern: thus* K *is the centralizer of the slopeset of* Q *in the ring* $Hom(W,+)$. *Then* $\pi(Q)$, *is a spread iff* Q *is a pre-quasifield;* $\pi(Q)$ *is said to be* coordinatized by *the prequasifield* Q.

Proof: $\Leftarrow$ is straightforward. To establish the converse we assume that Q is a zero-linked structure and that π_Q is a spread on V; we must deduce that Q is a prequasifield. Consider $\Pi(Q)$, c.f., definition 4.2.1, the incidence structure associated with $Q = (W,+,\circ)$; so the pointset of $\Pi(Q)$ is $V := W \oplus W$ and the lines of $\Pi(Q)$ are all the subspaces and cosets of $(V,+)$ that are of form '$x = c$' or '$y = x \circ m + c$', for $m, c \in W$. Hence, the lines of $\Pi(Q)$ through the 'origin' $\mathbf{O} = \mathbf{0} \oplus \mathbf{0}$ consists of the components of the spread π_Q.

So every subspace of type '$x = c$' or '$y = x \circ m + c$' is a translate of a component of π_Q. Hence $\Pi(Q)$ is the translation plane associated with the spread π_Q, and $W \oplus W$ may be identified with its translation group in the obvious way. Thus Q is a translation algebra, as defined in 4.2.1, that coordinatizes a translation plane, and hence must be a pre-quasifield by proposition 4.2.3. ∎

5.2 Quasifields and Spreadsets.

We introduced in an earlier chapter, see definitions 1.3.4 and 1.3.11, the notion of a [partial] spreadset, and we described how they give rise to [partial] spreads. In this lecture, we similarly explore the connection between spreadsets and quasifields.

Although in some theoretical sense, spreadsets, quasifelds and spreads all turn out to be 'equivalent', the correspondence is not one-one: for example, many non-isomorphic quasifields are associated with the same spread and most spreadsets are associated with several non-isomorphic quasifields that they 'coordinatize'. Thus, spreadset and [pre]quasfields provide essentially distinct approaches to the study of spreads and translation planes.

To keep this lecture self-contained, we review the definition of a partial spreadset in the following exercise: it provides a characterization of the concept as given in our earlier definition 1.3.11. For the convenience of the reader, the rest of this lecture tacitly treats this exercise as defining a [partial] spreadset.

Exercise 5.2.1 *Let τ be a set of homomorphisms of the additive group $(W, +)$ of a vector space. Then τ is a partial spreadset on W iff*

$$\alpha, \beta \in \tau \Rightarrow \alpha - \beta \in \overline{GL(W, +)}.$$

A partial spreadset τ is a spreadset iff $\mathbf{O} \in \tau$ and τ is a transitive set of maps on W, which means:

$$\forall x, y \in W : \exists t \in \tau \ni y = x^t.$$

If W is a vector space over a [skew]field K then τ is a [K-linear] spreadset if the members of τ are K-linear.

Much of the following remark amounts to restating the meaning of a spreadset, in terms of its characterization in the exercise above, and also reviews the connection between spreads and spreadsets as discussed in section 1.3. However, the main point of the remark is to establish the theoretical equivalence between spreadsets and [pre]quasifields.

Remarks 5.2.2 *Let $(W,+)$ be the additive group of a vector space and suppose τ is a set of additive maps of W such that $\mathbf{O} \in \tau$ and $\tau^* \subset GL(V,+)$. Then:*

1. *τ is a spreadset iff τ^* is regular on W^*, that is:*

$$\forall x, y \in W^* : \exists! t \in \tau \ni y = x^t.$$

2. *If $|W|$ is finite then τ is a partial spread iff $\tau^* \subset GL(W,+)$ is such that $A-B$ is also non-singular, whenever A and B are distinct members of τ.*

3. *If $|W|$ is finite then τ is a spread iff $\mathbf{O} \in \tau$ and τ contains $|W|$ elements any two of which differ by a non-singular map or zero.*

4. *Let $Q = (W,+,\circ)$ be a [pre]quasifield. Then the set of its slope maps, see definition 4.3.2, τ_Q form a spreadset, called the spreadset* associated *or* coordinatized *by Q.*

Proof: We only consider case (4), as this is the least trivial case. The slope maps $T_m : x \mapsto x \circ m$, $m \in Q^*$, are bijections because Q^* is a quasigroup, and the distributive law for Q means that every such $T_m \in GL(W,+)$. Next we must show that the additive map $T_a - T_b$, for $a, b \in W$ is bijective, assuming $a \neq b$. If $x(T_a - T_b) = \mathbf{0}$ then $x \circ a = x \circ b$, contradicting the quasigroup property for multiplication. Thus $T_a - T_b$ is injective. To show this map is surjective, consider $w \in W^*$. Now $w = x(T_a - T_b)$ for some $x \in W$ iff

$$w = x \circ a - x \circ b \exists x \in W,$$

and this holds by proposition 4.2.4. It only remains to check that if x and y are non-zero then $y = x^t$, for a unique $t \in \tau$. This equivalent to checking that $y = x \circ t$ has a unique solution for t, and this again follows from the quasigroup property. ∎

We now associate with any spreadset, in the sense of definition 5.2.1, several

related algebraic systems that turn out to be at least prequasifields: this will lead to the correspondence between spreadsets and [pre]quasifields mentioned earlier.

Definition 5.2.3 (Sytems Coordinatizing Spreadsets.) *Let τ be a spreac set on $(W,+)$, the additive group of a vector space. To each $e \in W^*$ assign the system $Q_e := (W,+,\circ)$, where $\circ$ is defined by:*

$$x \circ y = x^{t(e\mapsto y)},$$

where $t(e \mapsto y)$ denotes the unique element of τ that maps e to y. The system Q_e is said to coordinatize τ at e.

It is immediately obvious that $e \circ y = y$, so Q_e has e as a left identity. Moreover, when $\mathbf{1} \in \tau$ then e actually becomes a two-sided identity. Now consider whether Q_e is a [pre]quasifield. The non-singularity of the non-zero members in τ shows that $x \circ a = c$ has a unique solution for x when $a \neq 0$. The additive property of linear maps provides the right distributive law. Also, the condition

$$x \circ a - x \circ b = x(\tau_a - \tau_b), \tag{5.1}$$

shows the LHS, as a function of x, is bijective on W because, by definition, any two distinct members of a spreadset differ by a non-singular W-bijection. Finally an equation of type $a \circ x = b$ has a unique solution for x because of the 'regularity hypothesis'. Thus we conclude:

Remark 5.2.4 (The Quasifields Coordinatizing A Spreadset.) *Let τ be a spreadset on some some $(W,+)$, the additive group of a vector space. Then for each $e \in W^*$ the system Q_e coordinatizing τ, as in definition 5.2.3, is a [pre]quasifield, which we call the [pre]quasifield* coordinatizing τ *at e. The [pre]quasifield has e as a left identity, and hence Q_e is a quasifield (with identity e) iff τ includes the identity map.*

Corollary 5.2.5 (The centralizer of a spreadset is the kern.) *The centralizer of τ in $Hom(W,+)$ is a [skew]field K, and K is the external kern of all the [pre]quasifields Q_e, $e \in W^*$, coordinatizing τ. In particular, if W is a vector space over a [skew]field F and if τ is a spread set of F-linear maps then F is in the external kern of the [pre]quasifield Q_e.*

We shall gradually get less pedantic with kern terminology: for instance, we shall usually not specify whether the kern considered is 'internal' or 'external'.

In the finite case, spreadsets have a particularly simple characterization:

Remark 5.2.6 *Let $\tau \subset \overline{GL(n,q)}$ such that $\mathbf{O} \in \tau$. Then τ is a spread iff $|\tau| = q^n$ and any two members of τ differ by an element of $GL(n,q)$. More $GF(q)$, associated with the scalar maps, is in the kern of the quasifields associated with π_τ.*

Proof: This is just a restatement of remark 5.2.2(4), bearing in mind that, by the corollary above, the centralizer of a spreadset corresponds to the kern of all the quasifields associated it. ∎

We now verify that every spreadset τ determines a spread π_τ and this coincides with all spread as $\pi(Q_e)$, as Q_e ranges over the quasifields coordinatizing τ. We first fix our notation in the context of *partial* spreadsets $\tau \subset Hom(W,+)$.

Definition 5.2.7 *Let $(W,+)$ be an additive group of a vector space and $\tau \subset Hom(V,+)$ such that:*

$$A, B \in \tau \Longrightarrow A - B \in \overline{GL(W,+)}.$$

The τ is a PARTIAL SPREADSET *and the associated partial spread is the collection of additive subspaces of $V = W \oplus W$ given by:*

$$\pi_\tau := \{[y = xT] \mid T \in \tau\} \cup \{Y\},$$

and we define

$$\pi_{\underline{\tau}} := \{[y = xT] \mid T \in \tau\}.$$

The more elaborate notation is chosen for the simpler structure because in most contexts the Y-axis needs to be included.

Theorem 5.2.8 *Let τ be a spreadset on a vector space W. Then the collection of subspaces defined on $W \oplus W$ by:*

$$\pi_\tau = \{[y = xT] \mid T \in \tau\} \cup \{\mathbf{0} \oplus W\}$$

is a spread, called the spread associated with τ. Moreover, for each $e \in W^*$ the spread $\pi(Q_e) = \pi_\tau$, where Q_e is the [pre]quasifield, coordinatizing τ at e.

Proof: Consider any $y = xT$ that lies in π_τ. Putting $\theta = eT$ we have

$$x \circ \theta := x^{t(e \mapsto \theta)} = xT,$$

so $y = x \circ \theta$ is the same subspace of $W \oplus W$ as $y = xT$. Conversely any $y = x \circ \theta$ may, by definition, be expressed as $y = xT$ where $T \in \tau$ maps e to θ. Thus π_τ is the same set of subspaces of $W \oplus W$ as in $\pi(Q_e)$. However, the latter is a spread because, by remark 5.2.4, Q_e is always a quasifield. Hence π_τ is also a spread and the desired result follows. ∎

Theorem 5.2.9 *Let $\pi(Q)$ be a spread coordinatized by a [pre]quasifield $Q = (W, +, \circ)$, and suppose K is the [external] kern of K. Then the standard action of K on $\pi(Q)$ coincides with the action of kern of $\pi(Q)$, that is, the standard action of K^* on $W \oplus W$ is the same the action as that of the full group of kern homologies of $\pi(Q)$.*

Proof: The non-vertical components of $\pi(Q)$ are of form $y = x \circ m$, or equivalently, yxM, where M is in the spreadset determined by Q. Now the kern of Q are the members $k \in End(W, +)$ that centralize all such M, so the standard action of k on $W \oplus W$ yields:

$$(x, xT) \mapsto (xk, xTk) = (xk, xkT) \in [y = xT],$$

and hence every $y = xT$ is left invarant by k. Hence K may be identified with a subfield of the [skew]field of kern endomorphisms of the spread $\pi(Q)$.
Now consider the converse.
Let τ be the slopeset of Q. So the non-vertical components of the spread $\pi(Q)$ are all of form $y = xT$, $T \in \tau$. Moreover, we may regard Q as being Q_e for some e. Consider any homology leaving every member of $\pi(Q)$ invariant. Since this fixes Y and X it must be of from $\alpha \oplus \beta \in GL(W, +) \oplus GL(W, +)$ and satisfy the condition:

$$\forall x \in W : (x, xT) \mapsto (x\alpha, xT\beta) \in [y = xT],$$

so $\alpha^{-1}T\beta = T$ so:

$$\forall T \in \tau : \alpha T = T\beta.$$

Now apply Schur's lemma above. ∎
We now consider the problem of deciding when a spreadset is a quasifield and when it is a pre-quasifield without an identity.

Corollary 5.2.10 *Let τ be a spreadset. Then the following are equivalent:*

1. *τ contains the identity map.*
2. *Some prequasifield Q_e coordinatizing τ is a quasifield.*
3. *All prequasifield Q_e coordinatizing τ are quasifields.*
4. *The spread π_τ includes the unit line $y = x$.*

Thus it becomes desirable to 'reduce' a spreadset τ to an equivalent spread containing the identity; we regard two spreadsets as being *equivalent* if the corresponding spreads are isomorphic. So, when are two spreadsets equivalent? A simple sufficiency condition is the following:

Remark 5.2.11 *If τ is a spreadset on W then so is $A^{-1}\tau B$, whenever $A, B \in GL(W, +)$ and the map $\theta : (x, y) \mapsto (xA, yB)$, of $W \oplus W$, is an isomorphism from the spread π_τ onto the spread $\pi_{A^{-1}\tau B}$. Moreover θ leaves invariant the common components $X = W \oplus \mathbf{0}$ and $Y = \mathbf{0} \oplus W$.*

Thus we may simplify a spreadset to an equivalent one such that the unit line belongs to it, and hence the coordinatizing prequasifields are all quasifields:

Corollary 5.2.12 *Let τ be a K-linear spreadset on a K-space W, K any field: so the components of the spread π_τ are K-subspaces of the ambient space $W \oplus W$, and the subspaces $X = W \oplus \mathbf{0}$ and $Y = \mathbf{0} \oplus W$ are among the components of π_τ. Then the spreadset τ is equivalent to a K-linear spreadset θ such that its associated spread π_θ has the same ambient space $W \oplus W$ as π_τ, and the components of π_θ are K-subspaces of $W \oplus W$ that include not only X and Y, but also the unit line $I = \{(w, w) \mid w \in W\}$.*

Thus, all spreads that are coordinatized by spreadsets, i.e. are of form π_τ for some spreadset τ, may be [re]-coordinatized by a spreadset σ such that σ includes the identity.

We have seen that every prequasifield $(Q, +.\circ)$ may be 'converted' to a quasifield $(Q, +, *)$ by choosing $e \in Q^*$ and defining $*$:

$$(x \circ e) * (e \circ y) = x \circ y,$$

and now $e \circ e$ becomes the identity. We now demonstrate that the associated spreads are isomorphic and hence both sytems have the same [outer] kern.

Let $S_x : x \mapsto x \circ a$, $a \in Q$, and $T_a : x \mapsto x * a$, $a \in Q$ denote respectively the slopemap of a in the prequasifield $(Q, +, \circ)$ and the quasifield $(Q, +, *)$ respectively. Thus the identity above yields $S_e T_{(eoy)} = S_y$, for all $y \in Q$ and so the slopeset τ_Q of the quasifield $(Q, +, *)$ is given by $\tau_Q = {S_e}^{-1}\sigma_Q$, where σ_Q is the slopeset of the prequasifield $(Q, +, \circ)$. We shall state this result in terms of:

Definition 5.2.13 *Let $(Q, +, \circ)$ be a prequasifield. Define $Q_e := (Q, +, *)$ by*

$$\forall x, y \in Q : (x \circ e) * (e \circ y) = x \circ y.$$

Then Q_e is the quasifield that normalizes *the prequasifield $(Q, +, \circ)$ at e.*

Thus we have established:

Proposition 5.2.14 *Let Q be a prequasifield normalized by a quasifield R at $e \in Q^*$. Let τ_Q and τ_R be respectively the slopeset of two systems. Then $\tau_R = E^{-1}\tau_Q$, where E is the slopemap of e regarded as member of Q. In particular, the spreads defined by a prequasifield is isomorphic to the spreads obtained by any of its normalized quasifields, and the external kernel of the two systems are the same.*

It is worth stressing that normalising a prequasifield to a quasifield is equivalent to introducing a multiplicative identity in its spreadset τ by replacing τ by $T^{-1}\tau$, where T is any non-zero element in τ.

5.3 Substructures of Quasifields.

In this lecture, we introduce certain additive and multiplicative substructures associated with quasifields and prequasifields and consider their connection with the associated spreadsets.

Note that we have already considered the most important case, viz., the kern: all the quasifields coordinatizing a translation plane, and, a fortiori, those associated with a given spreadset, have isomorphic kerns since they may be identified with the group of homologies with the ideal line as axis.

The aim here is to consider several other substructures of prequasifields that extend the notion of the kern in various ways, and thus have some geometric significance. Our main concern here is the extent to which these structure are invariant, as the quasifields from which they arise range over all the quasifields associated with a fixed spreadset.

There are basically two types of substructures that we consider here: the extreme case of each type being nearfields (associative quasifields) and semifields (distributive quasifields).

In nearly every case, our goal is to show that each type of substructure is an invariant for all the prequasifields coordinatizing a fixed spreadset $\mathcal{S}$. This reflects the fact, as we shall see in the next chapter, that the substructures we consider are nearly always associated with certain maximal groups of central collineations of the spread coordinatized by $\mathcal{S}$.

We deal first with the multiplicative substructures associated with a (pre)quasifield Q, and then turn to an additive analogue. In the multiplicative cases, the structures we refer to are just the seminuclei of the multiplicative quasigroup structure of Q^*, and we have already met these in the context of loops (rather than just quasigroups).

Although our definitions are formulated to hold for the general case, to maintain clarity, all the results in this section are established only for the finite case. We begin by repeating the definition of the nuclei of a loop in the context of prequasifields.

Definition 5.3.1 *Let $\mathcal{Q} = (Q, +, \circ)$ be a finite prequasifield. Then the middle, left and right nucleus are respectively defined as follows:*

1.
$$N_m = \{f \in Q \mid (x \circ f) \circ y = x \circ (f \circ y) \forall x, y \in Q\}$$

2.
$$N_r = \{f \in Q \mid (x \circ y) \circ f = x \circ (y \circ f) \forall x, y \in Q\}$$

3.
$$N_\ell = \{f \in Q \mid f \circ (x \circ y) = (f \circ x) \circ y \forall x, y \in Q\}$$

Each of the above are called semi-nuclei of of Q_e, and their intersection N is the nucleus of Q_e.

We consider here the nuclei of the [pre]quasifields Q_e associated with a fixed spreadset $\mathcal{S}$. Since the choice of Q_e depends on the choice of the left identity e, it is reasonable to ask to what extent the nuclei depend on the choice of e, for a fixed spreadset $\mathcal{S}$. Our aim is to show that, in the finite case, the right and middle nuclei are essentially independent of the choice of e.

As far as the left nucleus N_ℓ is concerned, there is no general coherent theory, probably because this is the only type of nucleus that turns out not

to have a geometric interpretation in the general case. However, the kern of a quasifield is contained in its left nucleus and this certainly has a geometric meaning, and is arguably fully understood. Hence we shall not consider further the left nucleus in this section, apart from noting that in the case of finite quasifelds its non-zero elements, as well as those of the other seminuclei, form a multiplicative group.

Remark 5.3.2 *Let Q be a finite quasifield with multiplicative identity e. Then $N_m^*(Q)$, $N_r^*(Q)$ and $N_\ell^*(Q)$ are multiplicative groups, with identity element e.*

Proof: Trivial. ∎
We now show the invariance of the middle nucleus of all the quasifields coordinatizing a given finite spreadset.

Theorem 5.3.3 *Let τ be a finite spreadset. Let $\alpha \subset \tau$ be the largest non-zero subset of τ^* satisfying the condition $\alpha\tau^* \subseteq \tau$; note that this is equivalent to $\alpha\tau^* = \tau$ and α is a group [under map composition] iff the identity is in τ. Let Q_e be the (pre)quasifield coordinatizing τ relative to some chosen left identity $e \in Q^*$. Then the (semi)group*

$$\alpha \cong \left\{\hat{f} : x \mapsto x \circ f \mid f \in N_m^*(Q_e)\right\} \cong N_m^*(Q_e),$$

where $N_m^*(Q_e)$ is viewed as a multiplicative (semi)group.

Proof: The element $f \in Q^*$ lies in $N_m^*(Q_e)$ iff for $x, y \in Q$:

$$\begin{aligned} (x \circ f) \circ y &= x \circ (f \circ y) \\ \iff (xT_f)T_y &= xT_{f \circ y} \\ \iff T_f T_y &= T_{f \circ y} \end{aligned}$$

and this is equivalent to $T_f \in \alpha$, and also shows that that $f \mapsto T_f$ defines a semigroup isomorphism from $N_m^*(Q_e)$ onto α of the required type. The result follows. ∎
Now we consider the analogue of the above with the middle nucleus replaced by the right nucleus.

Theorem 5.3.4 *Let τ be a finite spreadset. Let $\alpha \subset \tau$ be the largest non-zero subset of τ^* satisfying the condition $\tau^*\alpha \subseteq \tau$ note that this is equivalent to $\tau^*\alpha = \tau$ and α is a group [under map composition] iff the identity is in*

τ. Let Q_e be the (pre)quasifield coordinatizing τ relative to some chosen left identity $e \in Q^*$. Then the (semi)group

$$\alpha \cong \left\{ \hat{f} : x \mapsto x \circ f \mid f \in N_r^*(Q_e) \right\} \cong N_r^*(Q_e),$$

where $N_r^*(Q_e)$ is viewed as a multiplicative (semi)group..

Proof: The element $f \in Q^*$ lies in $N_r^*(Q_e)$ iff for $x, y \in Q$:

$$\begin{aligned} (x \circ y) \circ f &= x \circ (y \circ f) \\ \iff (xT_y)T_f &= xT_{y \circ f} \\ \iff T_y T_f &= T_{y \circ f} \end{aligned}$$

and this is equivalent to $T_f \in \alpha$, and also shows that that $f \mapsto T_f$ defines a semigroup isomorphism from $N_r^*(Q_e)$ onto α of the required type. The result follows. ∎

We now specialize to nearfields.

Definition 5.3.5 *A quasifield with associative product is called a nearfield.*

A classical theorem of Zassenhaus gives a complete classification of all finite nearfields: apart from fields they are either the Dickson nearfields, introduced ahead, or they are among a finite list of sporadic nearfields called *irregular nearfields*. The results above imply that

Corollary 5.3.6 *Let $\mathcal{S}$ be a finite spreadset containing the identity. Then the following are equivalent:*

1. *$\mathcal{S}^*$ is a group of non-singular linear maps.*
2. *Some quasifield Q_e coordinatizing $\mathcal{S}$ is a nearfield.*
3. *All quasifields Q_e coordinatizing $\mathcal{S}$ are nearfields.*

Moreover, if $\mathcal{S}^*$ is a group, then all the nearfields coordinatizing $\mathcal{S}^*$ have isomorphic multiplicative groups.

In fact, inspecting the isomorphism from α to its nuclei, developed above shows:

Corollary 5.3.7 *All the nearfields coordinatizing a given spreadset are isomorphic as spreadsets.*

So far we have considered multiplicatively closed subsets α of spreadset $\mathcal{S}$. We now turn to the additive version of this theory. To emphasize the analogy with the multiplicative case we introduce a non-standard definition.

Definition 5.3.8 *Let Q be any prequasifield. Then its distributor is the additive semigroup:*

$$\delta(Q) = \{c \in Q \mid x \circ (c + y) = (x \circ c) + (x \circ y) \forall x, y \in Q\}$$

So, at least in the finite case, $\delta(Q)$ is an additive subgroup of Q.

Theorem 5.3.9 *Let τ be a finite spreadset over a finite field K, and $\alpha \subset \tau$ be the largest non-zero subset of τ^* satisfying the condition $\tau^* + \alpha \subseteq \tau$, or equivalently, the condition $\tau^* + \alpha = \tau$; thus α is an additive group of linear maps over K. Let Q_e be the (pre)quasifield coordinatizing τ relative to some chosen left identity $e \in Q^*$. Then there is an additive group isomorphism:*

$$\alpha \cong \left\{\hat{f} : x \mapsto x \circ f \mid f \in \delta(Q_e)\right\} \cong \delta(Q_e)$$

Proof: The element $c \in Q_e$ lies in $\delta(Q_e)$ iff for $x, y \in Q_e$:

$$\begin{aligned} x \circ c + x \circ y &= x \circ (c + y) \\ \iff xT_c + xT_y &= x(T_{c+y} \\ \iff T_c + T_y &= T_{c+y} \end{aligned}$$

and this is equivalent to $T_c \in \alpha$, and also shows that that $c \mapsto T_c$ defines an additive group isomorphism from $\delta(Q_e)$ onto α of the required type. The result follows. ∎

A distributive (pre)quasifield Q is called a pre(semifield). We state this definition in terms of $\delta(Q)$:

Definition 5.3.10 *A (pre)quasifield $(Q, +, \circ)$ is a (pre)semifield if $\delta(Q) = Q$. A semifield is said to be* proper *if its multiplictaion is not associative.*

Theorem 5.3.9 above immediately yields the following characterization of the spreadsets whose associated (pre)quasifields are semifields.

Theorem 5.3.11 *Let τ be a finite spreadset. Then the following are equivalent.*

1. *Some quasifield Q coordinatizing τ is a (pre)semifield.*
2. *τ is additively closed iff every (pre)quasifield Q coordinatizing τ is a (pre)semifield.*

5.4 Hall Systems

Let K be any field. Choose an indeterminate t and consider the rank two left K vector space defined on $Q_t = K + Kt$, where $x + yt \in Q$ is identified with $(x, y) \in K^2$: so addition and scalar multiplication on Q_t are done componentwise:

$$\begin{aligned} \forall x, x', y, y' \in K : (x + yt) + (x' + y't) &= (x + x') + (y + y')t \\ \text{and } \forall k, x, y \in K : k(x + yt) &= kx + (ky)t. \end{aligned}$$

Any quasifield that has rank two over its kernel K may thus be regarded as being of form $(Q_t, +, \circ)$, where addition is standard and the multiplication $\circ$ is an extension of left multiplication by the scalars in $K \subset Q$ with the general elements of Q. Morover, for each $a \in Q_t$ the map

$$\begin{aligned} R_a \quad : \quad & Q \to Q \\ & x \mapsto x \circ a \end{aligned}$$

is required to be a K-linear bijection of Q_t, and the quasifield $(Q_t, +, \circ)$ is completely specified when all the *slope-maps* R_a, for $a \in Q$ are specified. To specify the R_a's it is now sufficient to write the 2×2 matrix over K for the linear maps R_a relative to the basis $(1, t)$ of Q_t; so R_0 is assigned the zero matrix, and the quasifield identity is assigned the identity matrix.

We now seek to classify all the quasifield $(Q_t, +, \circ)$ associated with the K-vector space Q_t, such that the following conditions hold:

Condition 5.4.1 (Hall Conditions.)

1. $(Aut(Q_t, +, \circ))_K$ *is transitive on* $Q - K$; *and*
2. K *is central In* Q.

This classification here is the first step towards classification of all the *finite* quasifields that admit maximally transitive automorphism groups, i.e. acting transitively on the non-kern elements.

Since K centralizes Q it centralizes the standard basis $(1, t)$, so the matrices [always relative to the standard basis] of its elements are just the scalars:

$$\forall k \in K : R_k := \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}.$$

That the above definition is expressed using different notation in definition 6.3.1 ahead.

Partial spreads *all* whose components lie across some subspread are called rational partial spreads.

Definition 5.7.2 *Let (V,Γ) be a partial spread and let A be a non-zero additive subspace of V such that A is a subspread of (V,Γ) and additionally:*

$$\gamma \in \Gamma \Longrightarrow \gamma \cap V \neq \mathbf{O};$$

thus A is a subspread (or a 'subplane') across Γ. *The partial spread (V,Γ) is called a* **rational** *partial spread if Γ has at least one subspread across it. If, additionally, (V,Δ) is a Desarguesian spread such that $\Delta \supset \Gamma$ then (V,Γ) is called a rational Desarguesian partial spread.*

Note that essentially the same definition, but in different terminolgy is covered by definitions 6.3.3 and 6.3.1 ahead.

If Q is a quasifield and R is a subquasifield then the spread $\pi(Q)$, coordinatized by Q, has a subspread that may be identified with $\pi(R)$ and, by definition, the partial spread Γ determined by $\pi(R)$ is rational, with $\pi(R)$ across it. The converse is also true: any rational spread $\Gamma \subset \mathcal{S}$, contained in a spread $(V,\mathcal{S})$, may be 'coordinatized' by a subquasifield R of a quasifield Q coordinatizing $(V,\mathcal{S})$. We now verify this elementary, but fundamental, property of rational partial spreads; it reflects the fact that *subplanes $\mathcal{A}_0$, of any affine plane $\mathcal{A}$, are coordinatized in the classical sense by some subternary ring T_0 of a ternary ring coordinatizing $\mathcal{A}$.*

Remark 5.7.3 *Let $\mathcal{S}$ be a spreadset defined on a vector space T. Suppose that $\pi_{\mathcal{S}} := (T \oplus T, \Sigma)$, the spread coordinatized by $\mathcal{S}$, contains a rational partial spread $\Gamma \subseteq \Sigma$ such that Γ contains the standard components $X = T \oplus \mathbf{O}$, $Y = \mathbf{O} \oplus T$ and $I = \{(t,t) \mid t \in T\}$. Let $U \leq T \oplus T$ be any subspread of $\pi_{\mathcal{S}}$ that lies across Γ. Then*

$$R := \{r \in T \mid r \oplus r \in I \cap U\},$$

is a subspace of T such that $U = R \oplus R$, and for each $e \in R^*$, the quasifield $Q_e = (T,+,\circ)$, coordinatizing the spreadset $\mathcal{S}$, contains the system $G_e = (R,+,\circ)$ as a subquasifield and the standard isomorphism from $\pi(Q_e)$ onto $\pi_{\mathcal{S}}$:

$$\Psi : \pi(Q_e) \to \pi(T \oplus T, \mathcal{S}),$$

and hence, since R_k is the scalar map $k\mathbf{1}_2$, Q_t is not a quasifield unless

$$a \in Q_t - K \Longrightarrow R_a \text{ has no eigenvalues in K.}$$

But the eigenvalues of R_t are just the roots of $f(x)$ so we have established:

Lemma 5.4.2 *Q_t cannot be a quasifield satisfying the Hall conditions 5.4.1 unless the common quadratic $f(x) = -x^2 + \alpha x + \beta$ is irreducible over K.*

Hence we shall assume that $f(x)$ is irreducible from here on: so $\beta \neq 0$. But since the determinant of R_{a+bt} is just β it follows that every non-zero R_{a+bt} is non-singular and the quasigroup condition on multiplication $(x, y) \circ (a, b) = (c, d)$ is met. To meet the remaining condition for quasigroup multiplication $(a, b) \circ (x, y) = (c, d)$, where (x, y) is the 'unkown', we first note that if $(c, d) = k(a, b)$ then $(x, y) = (k, 0)$ is a solution. Thus our main task, to show that quasigroup multiplication works, requires us to show that a solution for (x, y) exists in the following matrix equation:

$$(a, b)\begin{pmatrix} x & y \\ \frac{1}{y}f(x) & \alpha - x \end{pmatrix} = (c, d), \quad ad - bc \neq 0, \tag{5.4}$$

and, tacitly assuming $ad - bc \neq 0$, the equation may be written

$$\begin{aligned} ax + \frac{b}{y}f(x) &= c \\ ay + b(\alpha - x) &= d \end{aligned}$$

which obviously has a solution if $b = 0$. So assuming from now on that $b \neq 0$, we obtain from the above:

$$\begin{aligned} axy + b(\beta + \alpha x - x^2) &= cy \\ axy + b(\alpha x - x^2) &= dx \end{aligned}$$

yielding on recalling equation (5.5):

$$\begin{aligned} cy - dx &= \beta \\ ay - bx &= d - b\alpha \end{aligned}$$

and now our assumption $ad - bc \neq 0$ shows that this equation has a unique solution for (x, y), and this back-traces to establish a unique solution for

the equation (5.4). Thus the multiplication specified is a loop, and as a consequence $(Q_t, +, \circ)$ is a quasifield: the reader is invited to check the minor details that have not been explicitly discussed.

To verify that the group $G = (Aut(Q_t, +, \circ))_K$ does act on the quasifield $(Q_t, +, \circ)$ we note that G, as a matrix group relative to $(1, t)$, is clearly the group:

$$\left\{ \begin{pmatrix} 1 & 0 \\ u & v \end{pmatrix} \mid u \in K, v \in K^* \right\},$$

and it can be directly verifed that this group preserves the multiplication. Thus we have established:

Theorem 5.4.3 *Suppose K is a field and $f(x) = -x^2 + \alpha x + \beta$ is an irreducible quadratic over K. Let $Q = K \oplus \mathbf{O}$ and define $Q_f := (Q, +, \circ)$, where $+$ is the standard addition on $K \oplus K$, by*

$$\forall a \in K : (a, b) \circ (x, 0) = (ax, bx),$$

and

$$\forall x \in K, y \in K^* : (a, b) \circ (x, y) = \begin{pmatrix} x & y \\ \frac{1}{y} f(x) & \alpha - x \end{pmatrix}.$$

Then Q_f is a quasified iff $f(x)$ is irreducible in K, and when this is the case $\overline{K} = K \oplus K$ is in the kern of Q_f and centralizes the quasifield multiplicatively.

Let $G = Aut(Q_f)_{\overline{K}}$ be the elementwise stabliser of the kern field $\overline{K}$ in the automorphism group of the quasifield. Then G is regular on the set of all non-kern elements $K \oplus K - K \oplus 0$ of Q_f. Such Q_f are called Hall systems.

Conversely if a quasifield Q is rank two over its kern K such that K centralizes Q and $(AutQ)_K$ has $Q - K$ as an orbit then Q is a Hall sytem.

Exercise 5.4.4

1. *Show that $GF(4)$ may be regarded as a Hall system and all other Hall systems are of dimension exactly two over K.*

2. *Show that $GF(4)$ is the only Hall sytem which is also a field.*

3. *Show that no Hall system can have an algebraic-closed field as its kern.*

5.5 Coordinatizing Spreads by Spreadsets.

Let $\pi = (V, \Gamma)$ be a spread over a skewfield K; so all its components are isomorphic as vector spaces to a common vector space W. We seek to identify π with τ_W, the spread on $W \oplus W$ coordinatized by some spreadset τ; we shall regard a K-linear isomorphism ψ from π to τ_W as being a coordinatization of π by τ.

Our goal here is to show that every spread is coordinatized by at least one spreadset τ, and that τ can be chosen so that it contains the identity. It is also possible to ensure that τ and the coordinatizing isomorphism ψ may be chosen so that any ordered triple of distinct components (X_V, Y_V, Z_V) are mapped under ψ to the ordered triple $(y = 0, x = 0, y = x)$, in $W \oplus W$. However, it is desirable to consider the more general situation, where X_V and Y_V are mapped respectively to $W \oplus \mathbf{0}$ and $\mathbf{0} \oplus W$, but where no component is necessarily required to be mapped to the unit line $x = y$; for example, it is often useful to have ψ send a Baer subplane of (V, Γ) onto the unit line of $W \oplus W$.

Theorem 5.5.1 (Coordinatizing Spreads By Spreadsets.) *Let $\pi = (V, \Gamma)$ be a spread over a skewfield K, such that all the components in Γ are isomorphic as K-vector spaces to a K vector space W. Let $\alpha : X \to W$, $\beta : Y \to W$ be arbitrary vector space isomorphisms from two distinct $X, Y \in \Gamma$ onto W. Then*

1. *There is a unique linear bijection:*

$$\alpha \oplus \beta : V \to W \oplus W,$$

whose restrictions to X and Y are respectively α and β.

2. *Each $T \in \Gamma - \{X, Y\}$ is associated with a unique pair of linear bijections*

$$(X_T : T \to X, Y_T : T \to Y),$$

such that:

$$T = \{(t)X_T + (t)Y_T : t \in T\}.$$

3. *The set of linear maps on W specified by:*

$$\tau = \left\{\alpha^{-1} X_T{}^{-1} Y_T \beta \mid T \in \Gamma\right\} \cup \{\mathbf{0}_W\},$$

is a spreadset on W, and $\alpha \oplus \beta : V \to W \oplus W$ is a K-linear isomorphism from the spread (V, Γ) onto the spread π_τ coordinatized by τ, see definition 5.2.7.

4. *τ contains the identity, or equivalently the unique line lies in W_τ if and only if $\alpha = \beta$.*

Proof: We give a sketch; it is left to the reader to make the proof more precise. The components of V, regarded as $X \oplus Y$, are of form $((t)X_T, (t)Y_T$, and may be rewritten $(x, (x){X_T}^{-1}Y_T)$, or $(x, M_T(x))$, where $M_T := {X_T}^{-1}Y_T$ is essentially the slope of T. Now τ is essentially the set of images of the M_T's, together with the zero-map of W, induced on W when V is identified iwth $W \oplus W$ using $\alpha \oplus \beta$. ∎

Thus all spreads are coordinatized by some spreadset. Hence we may assume that any spread is of type W_τ and three selected components are $x = 0$, $y = 0$ and $z = 0$ respectively.

5.6 Inventory of Quasifields Coordinatizing a Fixed Spread.

From now on, *a prequasifield will always be assumed to have at least left identity.* We are here concerned with the description of all the non-isomorphic prequasifields Q such that the associated spread is is isomorphic to a given spread π. If ϕ is an isomorphism from π to $\pi(Q)$ then ϕ will be called a *coordinatization* of π by Q. Thus we are concerned with the description of all the non-isomorphic prequasifields that coordinatize π.

We now describe a concrete procedure that yields a Q coordinatizing the given π uniquely once certain geometric choices are made, and also leads to a unique isomorphism Ψ from π onto $\pi(Q)$, in terms of certain 'geometric' options: the choice of the x-axis, the y-axis, etc. We shall see that the isomorphism types of all (pre)quasifelds Q such that $\pi(Q) \cong \pi$ may be obtained as an image of some Ψ determined by fixing the geometric options.

5.6.1 Coordinatization Algorithm.

There are two basic situations to consider: determine all the isomorphism types for the prequasifields coordinatizing a spread, and also all the quasifields, with a two-sided multiplicative identity, coordinatizing the spread. We

first describe all the prequasifield coordinatizing a given spread, and then specialize to describe all the quasifields coordinatizing it.

Let $\pi = (V, \Gamma)$ be a spread on a K-space V, K a skew-field, such that the components are all K-subspaces of V.

1. Choose distinct components $X_V, Y_V \in \Gamma$; these are called the x and y-axis of the coordinatization scheme.

2. Choose a *unit point* $u \in V - (X_V \cup Y_V)$, and hence: $u = u_x \oplus u_y$; so u_x and u_y are the projections of u on X and y.

3. Let W be a K-space isomorphic to the members of Γ, and choose an *identity* $e \in W - \{0\}$.

4. Select linear bijections $\alpha : X_V \to W$, and $\beta : Y_V \to W$ such that $\alpha(u_x) = \beta(u_y) = e$.

5. The linear bijection $\alpha \oplus \beta : V \to W \oplus W$ defines a spread on $W \oplus W$ whose component-set is given by:

$$\Delta = \{\alpha \oplus \beta(\gamma) \mid \gamma \in \Gamma\} \cup \{0 \oplus W\}.$$

   Thus $\alpha \oplus \beta$ is a K-linear isomorphism from V onto $W \oplus W$ that is also an isomorphism from the spread (V, Γ) onto the W-labelled spread $(W \oplus W, \Delta)$, and this isomorphism sends u to (e, e).

6. Let Q_e be the standard prequasifield coordinatizing $(W \oplus W, \Delta)$, and let σ be the associated K-linear isomorphism from $(W \oplus W, \Delta)$ onto $\pi(Q_e)$.

The K-linear bijection

$$\sigma(\alpha \oplus \beta) : V \to W \oplus W$$

is a K-linear spread isomorphism from (V, Γ) onto $\pi(Q_e)$ such that u is mapped onto e. The prequasifield Q_e is said to coordinatize (V, Γ) relative to the axes X_V, Y_V, the unit point u and identifiers α and β; the kern of Q_e contains K.

Let υ denote the component in Γ that passes through u. Choose any K-linear bijection $\Xi : \upsilon \to W$ such that $\Xi(u) = e$, and define

$$\forall z \in \upsilon \alpha(\pi_X(z)) = \Xi(z) = \beta(\pi_Y(z)),$$

where π_X and π_Y denote the projection of V onto V_X and V_Y respectively. Such α and β are completely determined Ξ and satisfy all the requirements of α and β as defined earlier. In this case the resulting prequasifield is a quasifield, and we call it the quasifield obtained when (V, Γ) is assigned a labelling with v as unit line relative to the coordinate axes V_X and V_Y.

Every coordinatization of π by a quasifield is obtainable by a labelling relative to some unit line and point, and a pair of X and Y axis. (N.B. The statement is intended to imply that the isomorphism onto W is immaterial, once the unit point and all three axes are fixed: it is pointless to make other variations in the choice of Ξ as this will not yield coordinatizations by any new quasifields.)

5.6.2 Properties Of Coordinatization.

Theorem 5.6.1 *Let $\pi = (V, \Gamma)$ be a spread, coordinatized by a quasifield $Q_e = (W, +, \circ)$, $e \in W^*$ is the identity. Thus there is a linear bijection*

$$\Psi : V \to W \oplus W$$

such that Ψ is also an isomorphism from the spread π onto $\pi(Q)$. Let $\mathbf{u} = (u_1, u_2)$ denote the unit point, so $\Psi(\mathbf{u}) = (e, e)$. Then

1. *If A is a subspread of V[1], that contains the coordinate frame $\mathbf{e}$, the x-axis and the y-axis then $\Psi(A)$ is a subquasifield A_Q of Q_e; thus A is coordinatized by the A_Q relative to the 'same frame', as used on π to yield $\pi(Q)$; the labelling map for A is the restriction of $\Xi : U \to W$ to $A \cap U$.*
   Conversely, if R is a subquasifield of Q then $R = A_Q$, where A is a subspread of type just described.

2. *Suppose $\alpha \in GL(W, +)$. Then α is an automorphism of $(Q, +, \circ)$ iff the map $\tilde{\alpha} : (x, y) \mapsto (x^\alpha, y^\alpha)$ of $\pi(Q)$ is a collineation of the plane $\pi(Q)$ that fixes (e, e). Now $Fix(\alpha)$ is a subquasifield A of Q, and $Fix(\tilde{\alpha})$ is the subplane $\pi(A)$ of $\pi(Q)$.*

3. *If a group $G \leq GL(W, +)$ is in $Aut(Q, +, \circ)$, and A denotes the subquasifield $Fix(G)$, then G is permutation isomorphic to the (clearly*

[1] In the sense that it is an additive subgroup and the components meeting it non-trivially define a spread on it.

faithful) action of the collineation group $\tilde{G}$ retricted to any line that it fixes. Conversely, any collineation group acting on $\pi(Q)$ and fixing the unit point and the axes must be of type $\tilde{G}$, and such groups are planar, in fact, their fixed points define the subplane $\pi(A)$, where $A = Fix(G)$.

Thus, subquasifields of a quasifield Q, and subplanes of $\pi(Q)$ containing the unit point, are linked by a natural one-one correspondence. Similarly, there is a natural correspondence between subgroups of $Aut(Q)$ and planar collineation groups of $\pi(Q)$ that fix the two axis and the unit point, and the correspondence is such that the action of the collineation on any fixed component is isomorphic as an additive group to the action of the corresponding subgroup of $Aut(Q)$ on Q.

Of course, using the coordinatizing isomorphism, we can extend these links in the obvious way to encompass subgroups and subplanes of any spread coordinatized Q. These connections are freely used in the literature, without explicit reference, and we shall normally follow this practice. However, even at the cost of being repetitive, we shall consider all this explictly in the following section, without referring to the above analysis, for the very important case associated with rational partial spreads.

5.7 Coordinatizing Rational Partial Spreads.

Given a spread $(V, \mathcal{S})$, we regard a subspace $A \leq V$ as being a *subspread* of $(V, \mathcal{S})$ if the components $\sigma \in \mathcal{S}$ that meet A non-trivially induce a spread on A. More generally:

Definition 5.7.1 *Let $(V, \mathcal{S})$ be a [partial] spread and suppose A is a non-zero additive subspace of $(V, +)$. Thus*

$$\mathcal{S}(A) := \{s \in \mathcal{S} \mid s \cap A \neq 0\}$$

denotes the set of components in $\mathcal{S}$ that meet A non-trivially. The subspace A is called a subspread *of the [partial] spread $(V, \mathcal{S})$ if*

$$\mathcal{S}_A = \{s \cap A \mid s \in \mathcal{S}(A)\}$$

is the set of components of a spread on A.

In general, if A is a subspread, of a partial spread $(V, \mathcal{S})$, then $\mathcal{S}(A)$ is the partial spread determined *by the subspace A, and A is said to be a subspace* across *the partial spread $\mathcal{S}(A)$.*

That the above definition is expressed using different notation in definition 6.3.1 ahead.

Partial spreads *all* whose components lie across some subspread are called rational partial spreads.

Definition 5.7.2 *Let (V,Γ) be a partial spread and let A be a non-zero additive subspace of V such that A is a subspread of (V,Γ) and additionally:*

$$\gamma \in \Gamma \Longrightarrow \gamma \cap V \neq \mathbf{O};$$

thus A is a subspread (or a 'subplane') across Γ. The partial spread (V,Γ) is called a **rational** *partial spread if Γ has at least one subspread across it. If, additionally, (V,Δ) is a Desarguesian spread such that $\Delta \supset \Gamma$ then (V,Γ) is called a rational Desarguesian partial spread.*

Note that essentially the same definition, but in different terminolgy is covered by definitions 6.3.3 and 6.3.1 ahead.

If Q is a quasifield and R is a subquasifield then the spread $\pi(Q)$, coordinatized by Q, has a subspread that may be identified with $\pi(R)$ and, by definition, the partial spread Γ determined by $\pi(R)$ is rational, with $\pi(R)$ across it. The converse is also true: any rational spread $\Gamma \subset \mathcal{S}$, contained in a spread $(V,\mathcal{S})$, may be 'coordinatized' by a subquasifield R of a quasifield Q coordinatizing $(V,\mathcal{S})$. We now verify this elementary, but fundamental, property of rational partial spreads; it reflects the fact that *subplanes $\mathcal{A}_0$, of any affine plane $\mathcal{A}$, are coordinatized in the classical sense by some subternary ring T_0 of a ternary ring coordinatizing $\mathcal{A}$.*

Remark 5.7.3 *Let $\mathcal{S}$ be a spreadset defined on a vector space T. Suppose that $\pi_{\mathcal{S}} := (T \oplus T, \Sigma)$, the spread coordinatized by $\mathcal{S}$, contains a rational partial spread $\Gamma \subseteq \Sigma$ such that Γ contains the standard components $X = T \oplus \mathbf{O}$, $Y = \mathbf{O} \oplus T$ and $I = \{(t,t) \mid t \in T\}$. Let $U \leq T \oplus T$ be any subspread of $\pi_{\mathcal{S}}$ that lies across Γ. Then*

$$R := \{r \in T \mid r \oplus r \in I \cap U\},$$

is a subspace of T such that $U = R \oplus R$, and for each $e \in R^*$, the quasifield $Q_e = (T, +, \circ)$, coordinatizing the spreadset $\mathcal{S}$, contains the system $G_e = (R, +, \circ)$ as a subquasifield and the standard isomorphism from $\pi(Q_e)$ onto $\pi_{\mathcal{S}}$:

$$\Psi : \pi(Q_e) \to \pi(T \oplus T, \mathcal{S}),$$

identifies $\pi(G_e)$ *with the subspread* $\pi(R \oplus R, \Gamma)$ *of* $\pi(T \oplus T, \mathcal{S})$*; thus* $\pi(G_e)$ *represents a standard coordinatization of* (U, Γ)*, relative to* $e \in R^*$*, by the quasifield* G_e*.*

Conversely, given a spread (V, Σ) *coordinatized by a subquasifield* $Q = (T, +, \circ)$*, such that* $Q_0 := (R, +, \circ)$ *is a subquasifield (so they share the multiplicative identity), then the components* $y = x \circ r$*,* $r \in R$*, along with* $Y := \mathbf{O} \oplus T$*, defines a rational partial subspread of* (V, Σ)*, across* $\pi(Q_0)$*.*

Proof: The converse part is a matter of unravelling the terminology, so we only consider '$\Rightarrow$'. Since U meets the three standard components, it is evident that R is a subspace of the vector space T, and $\{r \oplus r \mid r \in R\}$ is a component of U. Thus, any line $x = r$, for $r \in R$, is a line of the translation plane associated with U and hence $x = r$ meets X in U, and this clearly implies that $X_R := R \oplus \mathbf{O}$ is a component of the spread U. Similarly, $Y_R := \mathbf{O} \oplus R$ is also a component of of U and this means $U = X_R \oplus Y_R = R \oplus R$, in particular $R \oplus R$ is an additive subspace of $T \oplus T$.
We now show that the elments of Γ, other than Y are of form $y = x \circ r$, for some $r \in R$. First observe that any member $\gamma \neq Y$, of the spread $\pi_{\mathcal{S}}$, has form $y = x \circ g$ for some $g \in T$. Now choosing $x = e$ shows $(e, g) \in \gamma)$. Hence, since Γ is the partial spread determined by $U = R \oplus R$, it follows that all members of $\Gamma \setminus \{Y\}$ are of form $y = x \circ r$, for some $r \in R$, and conversely that all such components $y = x \circ r$, $r \in R$, lie Γ.
But for $r, c \in R$, $y = x \circ r$ and $x = \circ c$ are two non-parallel lines of the affine plane associated with U, so their intersection point $(c, c \circ g) \in R \oplus R$, hence R is closed under the binary operation $\circ$. But since Q_e has no zero divisors, it follows that R^* is a subloop of $(T, \circ)$,both with the same identity e. Thus we have established that $(R, +, \circ)$ is such that $(R, +)$ is an additive group with a zero, $(R^*, \circ)$ is a loop and left or right multiplication by zero always yields zero, since $(T, +, \circ)$ is a quasifield. Thus we clearly have a zero-linked system $(R, +, \circ)$, see definition 4.2.1 satisfying the right distributive law and hence, by proposition 4.2.3, $(R, +, \circ)$ is a translation algebra. But the associated incidence structure $\pi(R, +, \circ)$ is, by hypothesis, an affine translation plane, and now, by proposition 4.2.4, $(R, +, \circ)$ is a quasifield. ∎

Chapter 6

Central Collineations and Desarguesian Nets.

Central collineations have a strong bearing on the planes upon which they act. In this section we study central collineations using two parallel but distinct approaches: the quasifield approach and the spreadset approach.

The machinery developed provides useful characterizations of *rational* Desarguesian net, those nets that are isomorphic to the nets defined by the parallel classes of subplanes of a Desarguesian plane. Note that rational partial spreads were introduced in defintion 5.7.2 and the associated nets, particularly the associated rational Desarguesian nets will be further considered in 6.3.

6.1 Central Collineations in Standard Form.

In this section, $\pi(Q)$ is a translation plane coordinatized by a quasifield $(Q, +, \circ)$. So the associated spread on $Q \oplus Q$ has as its components $X = Q \oplus \mathbf{0}$ and $Y = \mathbf{0} \oplus Q$ and all subspaces $y = x \circ m$, $m \in Q$; thus, $m = 0$ corresponds to X.

We shall investigate affine affine central collineations when their axes and coaxes are chosen canonically. Specifically, when dealing with homologies, we assume that the axis and coaxis have been chosen from the two standard components, X and Y, and when dealing with affine elations we take Y as the axis.

Since all such collineations g are among the additive bijections of $Q \oplus Q$

that leave X and Y invariant, the action of g on the affine pointset $Q \oplus Q$ is specified by:

$$\boxed{\begin{array}{rrcl} & g:(x,0) & \mapsto & (A(x),B(x)) \\ \text{For all } x,m \in Q: & g:(0,x) & \mapsto & (C(x),D(x)) \\ & g:(m) & \mapsto & (m^S) \end{array}}, \tag{6.1}$$

where A, B, C and D are all additive maps of $(Q,+)$.

6.1.1 When g is a Y-elation of $\pi(Q)$.

We consider the case when g is an elation with axis Y. So g fixes Y identically, and since (∞) is the center, g leaves the x-coordinate of all points unchanged. So the eqns (6.1) become:

$$\boxed{\begin{array}{rrcl} & g:(x,0) & \mapsto & (x,B(x)) \\ \text{For all } x,y,m \in Q: & g:(0,y) & \mapsto & (0,y) \\ & g:(m) & \mapsto & (m^S), \end{array}}$$

and now the point $(x, x \circ m)$, on the component $y = x \circ m$, gets mapped onto the point of $(x, B(x) + x \circ m)$ and this must lie on $y = x \circ m^S$, thus:

$$\forall x,m \in Q : B(x) + x \circ m = x \circ m^S,$$

and putting $0^S := a$, yields B:

$$\forall x \in Q : B(x) = x \circ a.$$

Hence:

$$\forall x,m \in Q : x \circ a + x \circ m = x \circ m^S,$$

and choosing $x = e$, a left identity, yields $a + m = m^S$, so:

$$\forall x,m \in Q : x \circ a + x \circ m = x \circ (a+m).$$

Thus, we may summarize our conclusions as follows.

Theorem 6.1.1 *Suppose Q is a quasifield such that in the associated translation plane $\pi(Q)$ the full shears group with axis Y is G. Then $g \in G$ maps the axis X onto a component $y = x \circ a$, $a \in Q$, iff:*

$$\forall x,m \in Q : x \circ (a+m) = x \circ a + x \circ m,$$

and when this condition holds the shear g is the collineation:

$$\begin{aligned}(x,y) &\mapsto (x, x\circ a + y)\\ (m) &\mapsto (m+a)\end{aligned}$$

In particular, g maps the component $y = x\circ m$, for $m \in Q$, onto the component $y = x\circ(a+m)$.

6.1.2 When g is a Y-axis homology of $\pi(Q)$.

We consider the case when g is a homology of $\pi(Q)$ with axis Y and coaxis X. So g fixes Y elementwise and, since (0) is the center, g leaves the y-coordinate of all points unchanged. So the eqns (6.1) yield:

$$\boxed{\begin{array}{lrcl} & g:(x,y) & \mapsto & (A(x),y)\\ \text{For all } x,y,m\in Q: & g:(m) & \mapsto & (m^S)\\ & g:(0) & \mapsto & (0^S)=(0)\end{array}},$$

and now the point $(x, x\circ m)$ on the component $y = x\circ m$ gets mapped to the point $(A(x), x\circ m)$, and since this must lie on the component $y = x\circ m^S$, we have:

$$\forall x,m\in Q : A(x)\circ m^S = x\circ m$$

and writing $c^S := f$, where e is a right identity for $\circ$, yields $A = T_f^{-1}$, so the above equation becomes

$$\forall x,m\in Q : (x)T_f^{-1}\circ m^S = x\circ m$$

hence:

$$\forall x,m\in Q : (x)\circ m^S = xT_f\circ m$$

so

$$(x)T_{m^S} = xT_fT_m$$

and $x = e$ yields

$$\forall m\in Q : m^S = f\circ m,$$

so both A and S have been determined in terms of f, where $y = x\circ f$ is the g-image of the unit line $y = x\circ e$. Thus g is the map:

$$\begin{aligned}g:(x,y) &\mapsto ((x)T_f^{-1}, y)\\ g:(m) &\mapsto (f\circ m)\end{aligned}$$

and so

$$(x, x \circ m) \mapsto (xT_f{}^{-1}, x \circ m),$$

and the image can lies on the component $y = x \circ (f \circ m)$ only if

$$\begin{aligned} xT_f{}^{-1} \circ (f \circ m) &= x \circ m, \\ \Rightarrow x \circ (f \circ m) = (xT_f) \circ m &= (x \circ f) \circ m, \end{aligned}$$

yielding:

Theorem 6.1.2 *Let $\pi(Q)$ be the translation plane associated with a quasi-field $(Q, +, \circ)$, with multiplicative identity e. Let G be the group of affine homologies of $\pi(Q)$ with axis Y and coaxis X. Then the G-orbit of the unit line $y = x \circ e$ consists of all components of type $y = x \circ f$, where $f \in N_m(Q)^*$, and now the unique $g \in G$ that maps the unit line onto $y = x \circ f$, for $f \in N_m(Q)^*$, is the collineation:*

$$\begin{aligned} g : (x, y) &\mapsto ((x)T_f^{-1}, y) \\ g : (m) &\mapsto (f \circ m), \end{aligned}$$

where $T_f : x \mapsto x \circ f$ is the slope of f. Moreover, the component $y = x \circ m$, $m \in Q^*$, is mapped by g onto the component $y = x \circ (f \circ m)$.

6.1.3 When g is an X-axis homology of $\pi(Q)$.

We consider the case when g is a homology of $\pi(Q)$ with axis X and coaxis Y. So g fixes X elementwise and, since (∞) is the center, g leaves the x-coordinate of all points unchanged. So the eqns (6.1) yield:

$$\boxed{\begin{array}{rrcl} & g : (x, y) & \mapsto & (x, B(y)) \\ \forall x, y, m \in Q : & g : (m) & \mapsto & (m^S) \\ & g : (0) & \mapsto & (0^S) = (0) \end{array}},$$

and now the point $(x, x \circ m)$ on the component $y = x \circ m$ gets mapped onto the point of $(x, B(x \circ m))$ and this must lie on the component $y = x \circ m^S$, thus:

$$\forall x, m \in Q : x \circ m^S = B(x \circ m)$$

and writing $e^S := f$, where e is the identity for $\circ$, yields $B = S$ and so the above equation becomes:

$$\forall x, m \in Q : x \circ m^S = (x \circ m)^S$$

and $m = e$ gives $x \circ f = (x)^S$ so

$$\forall x, m \in Q : x \circ (m \circ f) = (x \circ m) \circ f$$

and $f \in N_r^*$, yielding:

Theorem 6.1.3 *Let $\pi(Q)$ be the translation plane associated with a quasifield $(Q, +, \circ)$, with multiplicative identity e. Let G be the group of affine homologies of $\pi(Q)$ with axis X and coaxis Y. Then the G-orbit of the unit line $y = x \circ e$ consists of all components of type $y = x \circ f$, where $f \in N_r(Q)^*$, and now the unique $g \in G$ that maps the unit line onto $y = x \circ f$, for $f \in N_r(Q)^*$, is the collineation:*

$$\begin{aligned} g : (x, y) &\mapsto (x, y \circ f) \\ g : (m) &\mapsto (m \circ f), \end{aligned}$$

where $T_f : x \mapsto x \circ f$ is the slope of f. Moreover, g maps the component $y = x \circ m$, $m \in Q^*$,onto the component $y = x \circ (m \circ f)$.

6.2 Central Collineations In Matrix Form.

We have just seen how the properties of a quasifield Q are related to certain 'standard' affine central collineation groups of $\pi(Q)$. We now repeat the analysis for *spreadsets* coordinatizing a spread π. One way to proceed would be to express the results of the last section in spread-theoretic terms. But we prefer to directly establish these results so as to introduce the reader to matrix-based techniques that are indispensible in translation plane theory. For example, transposing the matrices of a spreadset, sometimes leads to a new translation plane with distinct geometric properties: this method of getting new-planes-from-old is not available without stepping back from quasifields, and even translation planes, to spreadsets.

However, working with spreadsets of matrices becomes very messy when dealing with translation planes that are infinite-dimensional over their kerns. Thus, we shall only consider spreads that are finite dimensional over a field K, and leave it to the determined reader to consider more general situations. Hence, by *the basis decomposition theorem* we are entitled to focus on the concrete case, when the spreads are constructed on the ambient space $K^n \oplus K^n$, and all K-linear automorphism and spreadset elements are K-matrices.

Throughout the section, τ denotes a spreadset of $n \times n$ matrices, that includes zero, over a field K, and $\pi_\tau = (W \oplus W, \Gamma_\tau)$ is an associated spread, where $W = K^n$, and the members of Γ_τ are $y = xT$, $T \in \tau$, along with $x = 0$: so the subspaces $X = W \oplus \mathbf{O}$ and $Y = \mathbf{O} \oplus W$ are among the components. Now any K-linear automorphism g of the spread π_τ may will be regarded as a 2×2 block matrix, where each block is an $n \times n$ matrix over K.

Exercise 6.2.1 *Any central collineation of the K-spread π_τ (so the origin is fixed by convention) is a K-linear map and hence may be represented by a 2×2 block matrix.*

Suppose E is the elation group of π_τ with axis Y. We shall describe E in terms of the matrices in τ.

Lemma 6.2.2 *Supppose A is a matrix such that $A + \tau \subseteq \tau$ (or equivalently $A + \tau = \tau$); so the matrix $A \in \tau$, and the additive matrix group $< A >$ partitions the set of matrices τ into a union of cosets of $< A >$.*

Now the block matrix

$$g_A := \begin{pmatrix} \mathbf{1} & A \\ \mathbf{O} & \mathbf{1} \end{pmatrix}$$

is a an elation with axis Y that maps $y = xT$, $T \in \tau$, to $y = x(T + A)$. Hence the orbit under g_A, of any component $y = xT$, $T \in \tau$, consists of the the components $y = xC$ where C ranges over the additive coset $T + < A >$.

Proof: For $T \in \tau$, we have:

$$(x, xT)g_A = (x, xT)\begin{pmatrix} \mathbf{1} & A \\ \mathbf{O} & \mathbf{1} \end{pmatrix} = (x, x(A + T)).$$

But since by hypothesis $A + T \in \tau$, the mapping g_A is an automorphism of the spread τ that leaves Y elementwise fixed, and cannot be a homology as it is semiregular on the other components. The lemma follows easily. ∎

We now verify the converse of the lemma: all elations with axis Y have form g_A. Assume g is any elation with axis Y. Thus g fixes Y identically so its matrix on the standard basis has form

$$\begin{pmatrix} * & * \\ \mathbf{O} & \mathbf{1} \end{pmatrix},$$

and to determine the two upper blocks we note that g leaves the X-component of any $x \oplus y \in W \oplus W$ unchanged because the lines of form $x = C$ pass through

the center of g. Thus g fixes identically the first n elements of the canonical basis of $K^n \oplus K^n$:

$$e_i \ominus \mathbf{0}, \quad i = 1, \ldots n,$$

so g can now be written as

$$g_A = \begin{pmatrix} \mathbf{1} & A \\ \mathbf{O} & \mathbf{1} \end{pmatrix},$$

and this matrix maps the component $y = xM$ onto $y = x(M + A)$, so $M + A$ must be in τ, in order that g preserves the spread. Thus τ is closed under addition by A, and, by lemma 6.2.2 above, this is sufficient for π_τ to admit g_A as an elation. Thus all the Y-axis elations are of form g_A, where A runs over the largest subset $\alpha \subseteq \tau$ such that $\alpha + \tau \subseteq \tau$. Now α is clearly an additive group of matrices and the map $E \in \alpha \mapsto g_E$ is an isomorphism from α onto the group of all Y-axis elations of τ. Hence we have obtained the following description of the group of Y-axis elations in matrix terms.

Theorem 6.2.3 *Let τ be a spreadset of matrices, that incudes zero, and let π_τ be the associated standard spread. Let*

$$E = \{A \in \tau \mid A + \tau \subseteq \tau\},$$

and define for each $A \in E$ the block matrix (all blocks with same order):

$$g_A := \begin{pmatrix} \mathbf{1} & A \\ \mathbf{O} & \mathbf{1} \end{pmatrix}.$$

Then

1. *E is an additive group and τ is the union of a set of additive E-cosets, including E.*

2. *A collineation g of π_τ is an elation with axis Y if and only if $g = g_A$, for some A in E; g_A maps X onto the component $y = xA$.*

3. *The map $A \mapsto g_A$ defines an isomorphism from the additive group of matrices E onto the full group of Y-elations of π_τ.*

4. *Let $S \leq E$ be an additive subgroup of E and g_S be the corresponding elation group, defined by $A \mapsto g_A$. Then the component orbits of g_S,*

other than Y, are in natural one-one correspondence with the additive cosets of S in τ, that union to τ: thus if $t \in \tau$ then the coset $t + S$ defines the components of the g_S-orbit of the component $y = xt$ to be the set of all components $y = xu$, $u \in t + S$.

Corollary 6.2.4 *A translation plane admits a transitive group of affine elations iff it is isomorphic to the translation plane associated with a spread π_τ, where τ is a matrix spreadset closed under addition.*

The following exercise considers the extension of the above to the infinite-dimensional case.

Exercise 6.2.5 *Let V be a finite-dimensional vector space over any [skew] field K. Define a spreadset to be a sharply one-transitive set Suppose $\tau \in GL(V, K)$ be a sharply one-transitive set of linear bijections of V: this means that for any $x, y \in V^*$ there is a unique $t \in \tau$ such that $x^t = y$. Determine the elation subgroup of the associated π_τ, in terms of τ, by generalising the above. Hence prove corollary 6.2.4for this case. Are there any problems in proving this corollary when the finite-dimensional restriction is removed? What happens if K is commutative but the vector space V is infinite-dimensional over K?*

Now we turn to the full group of *homologies* of π_τ with axis Y and with coaxis X. We follow the procedure for the elation case, but we shall insist that τ contains the multiplicative identity (to substitute for the additive identity in the elation case).

Lemma 6.2.6 *Assume the spread-set τ contins the identity matrix. Suppose A is a non-zero matrix such that $A\tau \subseteq \tau$; thus $A \in \tau$, A is non-singular and hence $A\tau = \tau$.*

Now the block matrix

$$h_A := \begin{pmatrix} A^{-1} & \mathbf{O} \\ \mathbf{O} & \mathbf{1} \end{pmatrix}$$

is a homology with axis Y and coaxis X. Hence the orbit under h_A, of any non-zero component $y = xT$, $T \in \tau^*$, consists of the components $y = xC$ where C ranges over the multiplicative coset $T < A >$, of the multiplicative group $< A >$.

Proof: The map h_A sends the component $y = xT$ onto the subspace $y = xAT$, so $AT \in \tau$. Now continue arguing as in lemma 6.2.2, to get the desired result. ∎

Conversely suppose that h is any homology with axis Y and coaxis X. Thus h has matrix $Diag(H, \mathbf{1})$, for some non-singular H corresponding to $h|X$. Now the component $y = xM$ maps to the subspace $y = xH^{-1}M$, so $H = A^{-1}M$. Now, *if τ contains the matrix* $\mathbf{1}$, then $H \in \tau^{-1}$. Now repeating the argument used in the elation case we get an analogue of the theorem above.

Theorem 6.2.7 *Let τ be a spreadset of matrices, that includes zero and the identity matrix. Let π_τ be the associated standard spread; so $Z = \{(w, w) \mid w \in K^n\}$, the unit line is in π_τ. Let:*

$$M^* = \{A \in \tau^* \mid A\tau^* \subseteq \tau^*\},$$

and define for each $A \in M^*$ the block matrix (all blocks with same order):

$$h_A := \begin{pmatrix} A^{-1} & \mathbf{O} \\ \mathbf{O} & \mathbf{1} \end{pmatrix}.$$

Then

1. *M^* is a multiplicative group of matrices such that τ is the union of a set of right multiplicative M^*-cosets, including M^*.*

2. *A collineation h of π_τ is a homology with axis Y and coaxis X if and only if $h = h_A$, for some A in M; h_A maps X onto the component $y = xA$.*

3. *The map $A \mapsto h_A$ defines an isomorphism from the multiplicative group of matrices M^* onto the full group of homologies, of π_τ, with axis Y and coaxis X.*

4. *Let $S \leq M^*$ be a multiplicative subgroup of M^* and h_S the corresponding homology group, defined by $A \mapsto h_A$. Then the component orbits of h_S, other than X and Y, are in natural one-one correspondence with the left multiplicative cosets of S in τ, that union to τ: thus if $t\tau$ then the left coset tS defines the components of the h_S-orbit of the component $y = xt$ to be the set of all components $y = xu$, $u \in tS$.*

Corollary 6.2.8 *A translation plane admits a transitive group of affine homologies sharing the same axis and coaxis iff it is isomorphic to the translation plane associated with a spread π_τ, where τ is a matrix spreadset such that τ^* is a multiplicative group.*

Next consider the situation when X is the axis and Y the coaxis of the homology group. Using a slightly 'dualised' version of the above analysis we get results similar to the above. For example, the general form the homologies being considered are matrices of type $Diag(\mathbf{1}, A)$ and this maps a component $y = xT$ onto $y = xTA$, so τ is closed under multiplication by A from the right. Continuing in this way we obtain:

Theorem 6.2.9 *Let τ be a spreadset of matrices, that includes zero and the identity matrix. Let π_τ be the associated standard spread; so $Z = \{(w, w) \mid w \in K^n\}$, the unit line is in π_τ. Let:*

$$L^* = \{A \in \tau^* \mid \tau^* * A \subseteq \tau^*\},$$

and define for each $A \in L^*$ the block matrix (all blocks with same order):

$$h_A := \begin{pmatrix} \mathbf{1} & \mathbf{O} \\ \mathbf{O} & A \end{pmatrix}.$$

Then

1. *L^* is a multiplicative group of matrices such that τ is the union of a set of right multiplicative L^*-cosets, including L^*.*
2. *A collineation h of π_τ is a homology with axis X and coaxis Y if and only if $h = h_A$, for some A in M; h_A maps I onto the component $y = xA$.*
3. *The map $A \mapsto h_A$ defines an isomorphism from the multiplicative group of matrices L^* onto the full group of homologies, of π_τ, with axis Y and coaxis X.*
4. *Let $S \leq L^*$ be a multiplicative subgroup of L^* and h_S the corresponding homology group, defined by $A \mapsto h_A$. Then the component orbits of h_S, other than X and Y, are in natural one-one correspondence with the multiplicative right cosets of S in τ, that union to τ: thus if $t\tau$ then the right coset tS defines the components of the h_S-orbit of the component $y = xt$ to be the set of all components $y = xu$, $u \in St$.*

Corollary 6.2.10 *A translation plane admits a transitive group of affine homologies sharing the same axis and coaxis iff it is isomorphic to the translation plane associated with a spread π_τ, where τ is a matrix spreadset such that τ^* is a multiplicative group.*

Corollaries 6.2.8 and 6.2.10 are each equivalent to asserting that the non-zero elements of a spreadset form a multiplicative group. Hence the spread π_τ admits a Y-axis-X-coaxis transitive homology group iff it admits an X-axis-Y-coaxis transitive homology group. So if a translation plane of order n admits an affine homology group of order $n-1$ then it admits another with axis and coaxis reversed! Thus we have:

Corollary 6.2.11 *A translation plane admits a transitive group M of affine homologies with axis Y and coaxis X iff it admits another transitive homology group L with with axis X and coaxis Y.*

6.3 Rational Desarguesian Partial Spreads.

We have already encountered rational partial spreads in section 5.7. The point being made there was that rational partial subspreads (and hence their nets) are just those arising from a subquasifield of a coordinatising quasifield. In this section we focus on rational *Desarguesian* partial spreads, and the point we make is that partial spreads defined by a Desarguesian subplane need not be Desarguesian: that is, a partial spread with a Desarguesian plane across it need not be embedable in a *Desarguesian* spread.

In view of the importance of this fact, we have kept this section independent of our earlier treatment in section 5.7. The notation here also differs slightly from our earlier notation: there is as yet no standard notation in this area.

Definition 6.3.1 *Let $\pi_\Delta := (V, \Delta)$ be a partial spread, or a spread, on $(V, +)$, the additive group of a vector space. Suppose W is any non-trivial additive subgroup of V, such that $W \neq V$. Then the components of π_Δ* DETERMINED BY *W, or the components* ACROSS *W is the subset of the component set Δ given by*

$$W^\Delta := \{D \in \Delta \mid D \cap W \neq \mathbf{O}\},$$

and the corresponding INDUCED STRUCTURE *on W is $\pi_W := (W, W_\Delta)$ where W^Δ consists of the non-trivial intersections of the components of π_Δ with W:*

$$W_\Delta := \left\{ d \cap W \mid d \in W^\Delta \right\}.$$

The subspace W is called a SUBSPREAD *of π_Δ if the structure π_W induced on it, is a spread in the usual sense, that is, every pair of distinct members of W_Δ direct-sum to W.*

To get used to this terminology we observe:

Remark 6.3.2 *A subspace W of a spread $\pi = (V, \Delta)$ is a subspread of π_Δ iff the components W^Δ across W induce a spread on it.*

Note that the spread induced on W depends only on the set of components across it, viz. W^Δ, and not on any larger [partial] spread $\delta \supset \Delta$. Such partial spreads, defined by the components of a subspread of a [partial] spread are called rational partial spreads.

Definition 6.3.3 *A partial spread (V, Λ) of a [partial] spread $\pi_\Theta = (V, \Theta)$ is a* RATIONAL *partial spread if an additive subspace W, of $(V, +)$, is such that: (1) W is a subspread of π_Θ; and (2) the components of π_Θ meeting W non-trivially are precisely the members of the partial spread Λ.*

A rational partial spread (V, Λ) is said to be a rational DESARGUESIAN *partial spread if Λ is a subset of a Desarguesian spread Δ on V.*

Thus a rational Desarguesian partial spread is a partial spread obtained from a Desarguesian spread π by taking as its components all the components of some subsplane π_0 of π. We shall usually follow the common practice of calling a Desarguesian partial spread a *Desarguesian net*; thus rational Desarguesian nets will mean the partial spread determined by a rational Desarguesian partial spread, according to our convention, and will also mean the net, in the strict sense of the word, determined by this partial spread.

If a subspace W of a partial spread defines a rational Desarguesian net of a partial spread or a spread (V, Δ), then W is Desarguesian as it lies in a Desarguesian plane. However, the converse is false: this will emerge from the following exercise.

Exercise 6.3.4 *In the following exercise assume all spreads etc. are finite.*

1. *Let $\pi_\Delta := (V, \Delta)$ be a finite spread, two-dimensional over a kern field K. Then a K-subspace W, of V, is either a component Δ or a Desarguesian Baer subplane of π_Δ.*

2. *Let $\mathcal{F}$ be a subspreadset of a spreadset $\mathcal{T}$, such that $\mathbf{O}, vecI \in \mathcal{F}$. Then the partial spread defined by $\mathcal{F}$ is a rational Desarguesian spread iff $\mathcal{F}$ is a field under matrix operations.*

3. *If Q is a right quasifield then $\pi(F)$ is a rational Desarguesian net iff Q is a right vector space over F.*

4. *Let Q be a quasifield and K a kern field. Show that $\pi(K)$ need not define a rational Desarguesian net.*

5. *Show that a spread (V, Γ) can contain a Desarguesian subplane W such that the partial spread defined by W, viz., W^Γ, need not be Desarguesian.*

Chapter 7

Simple T-extensions of Desarguesian Nets.

The aim of this chapter is to construct three methods for generating finite spreads π, and hence also translation planes. The distinguishing feature of these methods is that they each involve a partial spreadset $\mathcal{F}$ associated with a rational Desarguesian partial spread and another slope matrix 'T': the spread π is then 'generated', in some case-dependent sense, by $\{T\} \cup \mathcal{F}$.

The exact conditions for T to succeed depends on the individual case, but in each instance a wide range of planes can be constructed, in the sense that the dimensions over the kern can be almost arbitrary. Before describing the methods we need to take a closer look at spreadsets containing fields.

7.1 Spreadsets Containing Fields.

Let $\mathcal{S}$ be a finite spreadset, and suppose $\mathcal{F} \subset \mathcal{S}$, $|\mathcal{F}| > 1$. Hence, $\mathcal{F}$ is a field of linear maps iff it is additively and multiplicatively closed. We examine separately the meaning of additive and multiplicative closure of $\mathcal{F}$ using:

Hypothesis $(*)$ *Let $\mathcal{S}$ is a spreadset associated with the additive group of a* finite *vector space V. Assume $\mathcal{S}$ is coordinatized by any one of the prequasi-fields $Q_e = (V, +, \circ)$, with $\circ$ specified by choosing the left identity $e \in V^*$. Let $\mathcal{F} \neq \{\mathbf{O}\}$ be any non-empty subset of $\mathcal{S}$, and let $F \subset V$ be the set of all elements in V whose slope maps lie in $\mathcal{F}$ relative to the choice of e as the identity, thus:*

$$F := \{f \in V \mid f = (e)\phi \exists \phi \in \mathcal{F}\}.$$

and

$$\mathcal{F} = \{T_f \mid f \in F\},$$

where $T_x \in \mathcal{S}$ *denotes the slope map of* $x \in V$, *relative to* e *as the left identity, i.e.,* $T_x : y \mapsto y \circ x$, $y \in V$.

First we consider the additive closure of $\mathcal{F}$.

Proposition 7.1.1 *Assume hypothesis (*), in particular,* $F = (e)\mathcal{F} \subseteq V$. *Then the following are equivalent.*

1. $\forall x \in V, f, g \in F : x \circ (f + g) = x \circ f + x \circ g$.
2. $\mathcal{F}$ *is an additive group.*
3. $\mathcal{F}$ *is additively closed.*

Proof: The condition

$$\begin{aligned} &\forall x \in V,\ f, g \in F : x \circ (f + g) = x \circ f + x \circ g \\ \iff\ &\forall x \in V,\ f, g \in F : x \circ T_{f+g} = xT_f + xT_g \\ \iff\ &T_{f+g} = T_f + T_g, \end{aligned}$$

and this cannot hold unless the slopeset of F is additively closed and, conversely, if the slopeset of F is additively closed then the element $M = T_f + T_g \in \mathcal{F}$ agrees with T_{f+g} at the non-zero element e. Hence $T_{f+g} = T_f + T_g$ is equivalent to $\mathcal{F}$ being additively closed. Finally, the additive closure of $\mathcal{F}$ is equivalent to it being an additive group by our finiteness hypothesis. ∎

Now we consider the multiplicative closure of $\mathcal{F}$.

Proposition 7.1.2 *Assume hypothesis (*), in particular,* $F = (e)\mathcal{F} \subseteq V$. *Then the following are equivalent.*

1. $\forall x \in V, f, g \in F : x \circ (f \circ g) = (x \circ f) \circ g$.
2. $\mathcal{F}$ *is a multipicative group.*
3. $\mathcal{F}$ *is multiplicatively closed.*

Proof: The the condition

$$\begin{aligned} &\forall x \in V,\ f,g \in F : x \circ (f \circ g) = (x \circ f) \circ g \\ \iff &\forall x \in V,\ f,g \in F : xT_{f\circ g} = xT_fT_g \\ \iff &T_{f\circ g} = T_fT_g, \end{aligned}$$

and this cannot hold unless the slopeset of F is multiplicatively closed and, conversely, if the slopeset of F is multiplicatively closed then $T_{f\circ g} = T_fT_g$ since they have the same value at the non-zero point e. Hence $T_{f\circ g} = T_fT_g$ is equivalent to $\mathcal{F}$ being multiplicatively closed. Finally, the multiplicative closure of $\mathcal{F}$ is equivalent to it being a multiplicative group since this hold for any finite multiplicative closed set of linear bijections. ∎

Now consider any quasifield $Q = (V;+,\circ)$ such that a subset $F \subset V$ is a field relative to the quasifield operations and that for $x \in Q$ the following identities hold:

$$\begin{aligned} x \circ (f+g) &= x \circ f + x \circ g \\ (x \circ f) \circ g &= x \circ (f \circ g) \end{aligned}$$

It is clear from the axioms of a quasifield that $(V,+)$ is a vector space relative to the field F operating from the right via quasifield multiplication iff the above pair of conditions hold. Thus, when these conditions hold, we shall say *the quasifield Q is a* **right** *vector space over F*; it will be tacitly assumed that the vector space is defined relative to the quasifield operations. On comparing these conditions with propositions 7.1.1 and 7.1.2, we immediately deduce:

Proposition 7.1.3 *Let $\mathcal{S}$ be any finite spreadset, containing the identity map, associated with the additive group $(V,+)$ of some vector space; so $Q_e = (V,+,\circ)$ denotes the quasifield determined by $\mathcal{S}$ and $e \in V^*$. Assign to any $\{\mathbf{O}\} \subset \mathcal{F} \subseteq \mathcal{S}$ the set of images F of e under $\mathcal{F}$, thus:*

$$F := \{f \in V \mid f = (e)\phi, \phi \in \mathcal{F}\}.$$

Then the following are equivalent:

1. *$\mathcal{F}$ is a field of linear maps.*
2. *$\mathcal{F}$ is closed under addition and composition.*
3. *For some non-zero e: F is a field and Q_e is a right vector space over F.*

4. For all non-zero e: F is a field and Q_e is a right vector space over F.

Suppose $Q_e = (V, +, \circ)$ is a finite quasifield, with identity e, such that Q_e is a right vector space over a subfield $F = (U, +, \circ)$, for some additive group $(U, +) \leq (V, +)$. Now $(V, +)$ may be assigned the structure of a field $K = (V, +, \bullet)$, such that:

$$\forall v \in V, f \in F : v \circ f = v \bullet f$$

The proof is an exercise in linear-algebra/field-extensions: if V is a k-dimensiona right vector space over a field $F = GF(q)$, then V can be given an F-linear identification with a right vector space K, where K is a k-dimensional field extension of the field F: for example, view F as the field of scalar $k \times k$ matrices in $Hom(k, q)$, and then choose as K a field of matrices of order $|F|^n$; this field exists in $Hom(k, q)$ by Galois theory.

Hence $y = x \circ f$ and $y = x \bullet f$ define the same subspace of $V \oplus V$, for all $f \in F$. Hence all these subspaces are components shared by the spreads $\pi(Q_e)$ and $\pi(K)$, and this clearly means that the rational partial spread associated with $\pi(F)$ is a subpartial spreads of both, $\pi(Q_e)$ and $\pi(K)$, and since the latter is Desarguesian, we conclude that $\pi(F)$ determines a *rational Desarguesian* partial spread.

We now consider the converse of this assertion. Hence, our goal is to demonstrate that if $\pi(Q_e)$, the spread associated with a finite quasifield $Q_e = (V, +, \circ)$, contains a rational Desarguesian partial spread δ whose components include X, Y and I, then Q_e contains a subfield F such that $(V, +)$ is a right vector space over F and the components of δ is the partial spread determined by $\pi(F)$, or equivalently, the $\pi(F)$ is a spread across δ).

Since δ is Desarguesian and rational, there is a Desarguesian spread $\Delta = \pi(K)$, where $K = (V, +, \bullet)$ is a field that may be chosen so that it contains a subfield F such that $\pi(F)$ is across δ, and contains (e, e). It is possible to insist further that e, the identity of $Q_e = (V, +, \circ)$, is also the identity of K, and hence of F: use the spreadset associated with K — it clearly contains the spreadset associated with δ — to define $\bullet$ in terms of e.

Since δ is the rational partial spread determined by $\pi(F)$, and lies in both $\pi(K)$ and $\pi(Q_e)$, we have the subspace $y = x \circ f$, for $f \in F$, may be expressed as $y = x \bullet f'$ for some $f' \in F$, and vice versa. Choosing $x = e$ shows that in every case $f = f'$, since K and Q_e both have the same multiplicative identity e. Thus, we have the identity:

$$\forall x \in V, f \in F : x \circ f = x \bullet f.$$

Hence Q_e is a right vector space over F, because K has this property. So we have established that δ is the rational partial spread determined by $\pi(F)$, where F is a field in Q_e such that the latter is a vector space over F.

Hence we have shown that if a finite quasifield Q is a right vector space over a field F then $\pi(Q)$ the rational spread determined by $\pi(F)$ is a rational *Desarguesian* partial spread whose components include the standard components X, Y and I of $\pi(Q)$, and, conversely, a rational Desarguesian partial spread δ in $\pi(Q)$ that includes the standard components among its members must be determined by some $\pi(F)$, where F is a subfield of Q over which the latter is a right F-vector space. Thus the above theorem extends to include another equivalence: $\pi(F)$ determines a rational Desarguesian spread is equivalent to all the other parts of the theorem.

In the context of finite spreadsets $\mathcal{S} \supset \mathbf{1}$, associated with a vector space on $(V,+)$, the above has the following interpretation:
$\mathcal{F} \subset \mathcal{S}$ is a field of matrices iff the components associated with $\mathcal{F}$ in $\pi(Q_e)$ defines a rational Desarguesian partial spread that contains the three standard components X, Y and I of $\pi(Q_e)$.

Thus proposition 7.1.3 may be restated in more detail as follows:

Theorem 7.1.4 *Assume the hypothesis of proposition 7.1.3. Let $\mathcal{S}$ be any finite spreadset, containing the identity map, associated with the additive group $(V,+)$ of some vector space; so $Q_e = (V,+,\circ)$ denotes the quasifield determined by $\mathcal{S}$ and $e \in V^*$. Suppose $\mathcal{F} \subseteq \mathcal{S}$ and let*

$$F = \{f \in V : f = (e)\phi, \phi \in \mathcal{F}\}.$$

Then the following are equivalent:

1. *$\mathcal{F}$ is closed under addition and composition.*
2. *$\mathcal{F}$ is a field of linear maps.*
3. *$(F,+,\circ)$ is field and V is a right vector space over F, for some choice of $e \in V^*$.*
4. *$(F,+,\circ)$ is field and V is a right vector space over F, for all choice of $e \in V^*$.*
5. *The partial spread $\pi(F)$ in $\pi(\mathcal{S})$, that is $\pi(Q_e)$, determines a rational Desarguesian partial spread in $\pi(\mathcal{S})$ that includes its three standard components, X, Y and I.*

Note that in attempting to state the infinite analogue of the theorem above, care must be taken regarding two points: (1) multiplicative and additive closure will no longer force $\mathcal{F}$ to be a field, and (2) the field F may not be embeddable in a larger field of dimension k, where $k := dim_F V$.

7.2 T-extensions of Fields.

If $\mathcal{S}$ is a finite spreadset, in some $\overline{GL(V,+)}$, that contains a field $\mathcal{F}$, then the associated spread $\pi_{\mathcal{S}}$ contains the rational Desarguesian partial spread $\pi_{\mathcal{F}}$. In this section, we consider some ways of extending a field of matrices $\mathcal{F}$ to a spread $\mathcal{S}$ so that the latter is in some sense 'generated' by $\mathcal{F} \cup \{T\}$, where T is a suitably chosen in $GL(V,+) \setminus \{\mathcal{F}\}$. These procedures will yield classes of semifields, and also spreads of order q^3 admitting $GL(2,q)$.

The first method is based on having available a quasifield $Q = (V,+,\circ)$, of suqare order, that contains a subfield F, such that Q is a two-dimensional vector space over F. Since such situations arise iff the spread $\pi(Q)$ is derivable relative to the slopes of $\pi(F)$, we shall refer to the corresponding spreads as being obtained by T-derivation. This method yields a range of semifields that are two dimensional over at least one of their seminuclei, and, in a somewhat vaccuous sense yields them 'all': every such semifield 'yields itself' by the procedure to be described. However, the method is also effective in genuinely constructing long chains of two-dimensional semifields when used sensibly.

The next method is concerned with 'cyclic T-extensions' of a field $\mathcal{F}$ that also yields semifields of non-square order, but this time the field $\mathcal{F}$ lies in at least two semi-nuclei: N_m and N_r, but these can be changed by dualising and/or transposing. Thus neither of the two constructions indicated so far entirely replace the other.

The final construction we discuss is a modification of the above indicated method in the three dimensional case. This yields semifields spreads (*not* semifield spreads) of order q^3 that admit $GL(2,q)$, acting as it does on the Desarguesian spread of order q^3. The dimension of the spread over its kern can be made arbitrarily large, demonstrating that non-solvable groups can act on spreads of arbitrarily large dimensions: so far this phenomenon is known in suprisingly few cases.

We now describe each of the above indicated constructions.

7.2.1 T-Derivations.

We describe here a method of constructing semifields of order q^2 that have $GF(q)$ over their middle nucleus. By transposing and/or dualising the resultant semifield plane, the $GF(q)$ can be can be taken to be any of the three seminuclei. Hence, we focus on the middle or right nucleus case (as the treatment is almost identical) and we shall generally ignore the right nucleus (which involves dualising the left nucleus).

Basically, the method begins with a quasifield $Q = (V, +, \circ)$, of arbitrary order q^2, that contains a subfield $(F, +, \circ) \cong GF(q)$ such that $(V, +)$ is a right vector space over F. Such quasifields, as we saw earlier, are essentially those obtainable from spreadsets $\mathcal{S}$ on $(V, +)$ that contain a subfield $\mathcal{F}$, or equivalently, from spreads of order q^2 that contain rational Desarguesian partial spreads of degree $q + 1$.

The key idea is that for any choice of $T \in \mathcal{S} \setminus \mathcal{F}$, regardless of the Q yielding $\mathcal{S}$, the additive group $\mathcal{F} + \mathcal{F}T$ is an additive spreadset. We shall refer to spreads constructed in this manner, as arising by applying a *T-extensions* to $\mathcal{S}$:

Proposition 7.2.1 (T-Derivations.) *Let $\mathcal{S}$ be a spreadset (or even a partial spreadset!) on a finite additive group $(V, +)$ such that $\mathcal{S} \supset \mathcal{F}$, where $\mathcal{F}$ is a field $\cong GF(q)$, and V has order q^2. Then for any $T \in \mathcal{S} - \mathcal{F}$, the additive set of matrices*

$$\Theta := \tau(T, \mathcal{F}) = \{a + Tb \mid a, b \in \mathcal{F}\}$$

is a spreadset, and hence so is the transpose:

$$\Theta^T = \{a + bT^T \mid a, b \in \mathcal{F}^T\}.$$

In particular, $\Theta\mathcal{F} = \Theta$ and $\mathcal{F}^T\Theta^T = \Theta^T$.

Proof: If $x\alpha + xT\beta = \mathbf{O}$, for $\beta \neq \mathbf{O}$, then $x\alpha\beta^{-1} - = xT$ so $F - T$ is singular for some $F \in \mathcal{F}$, contradicting the hypothesis that $\{T\} \cup \mathcal{F}$ is a subset of the (partial!) spreadset $\mathcal{S}$. Thus $\Theta = \Theta\mathcal{F}$. The rest follows easily. ∎

Note that by allowing $\mathcal{S}$ to be a partial spread, the method can be extended even to cartesian groups $Q = (V, +, \circ)$ of order q^2 that are right vector spaces over a subfield $F = GF(q)$, provided that some $t \in Q - F$ defines an additive map $x \mapsto x \circ t$ on $(V, +)$.

Recall, theorem5.3.3, that for additive spreadsets $\mathcal{S}$ the middle nucleus corresponds to the largest subset $\mathcal{F}$ such that $\mathcal{F}\mathcal{S} = \mathcal{S}$, and the right nucleus

corresponds to the transpose situation, viz., the largest $\mathcal{F} \subset \mathcal{F}$ such that $\mathcal{S} = \mathcal{S}\mathcal{F}$, theorem 5.3.4. Hence, for convenience and for its future role, we shall usually only comment on the middle nucleus situation. We note that any semifield spreadset of order q^2 is obtained by applying a T-extension to itself.

Remark 7.2.2 *If $\mathcal{T}$ is a spreadset of order q^2 containing a field $\mathcal{F} \cong GF(q)$ such that $\mathcal{F}\mathcal{T} \subset \mathcal{T}$ then*

$$\mathcal{T} = \mathcal{F} + \mathcal{F}T,$$

whenever $T \in \mathcal{T} \setminus \mathcal{F}$; in particular, $\mathcal{T}$ coincides with $\tau(T, \mathcal{F})^T$, using the notation of proposition 7.2.1.

Thus all semifields that are two-dimensional over their middle (or left) nucleus are T-extensions — of themselves! However, the process of T-extensions can be effectively used to yield a variety of examples of semifields that are two dimensional over the middle nucleus, and indeed, by transposing and dualising, over any semifield. To generate such examples, using T-extensions, one can arbitrarily repeat arbitrary long chains of steps, each step involving one of dualising-transposing-T-deriving-recordinatising and collecting the required spreadsets at each stage, for example by adopting using a loop such as the following:

Generating Two Dimensional Semifields.

a Choose spread with derivable partial spread δ.

b Coordinatise by a quasifield Q so that δ is coordinatized by a field F.

c Now either form Q' containing field F' such that Q' coordinatizes the transpose spread and Q' is a right vector space over F' a field isomorphic to F, or simply choose $Q' = Q$ and $F' = F$.

d Obtain two-dimensional semifield associated with any $t \in Q' - F'$, with middle nucleus F'.

e Dualise and/ or transpose the semifield and/or derive relative to F'-slopes.

f Return to step [a] or stop.

Certainly many non-isomorphic spreads arise thus, and as indicated above, 'all' finite semifields that are two dimensional over a seminucleus are of this form, albiet in a somewhat vaccuous sense; although T-extensions provide a useful method for generating examples of two-dimensional semifields it is not meaningful to ask if their are 'other' semifields of order q^2, with $GF(q)$ in seminucelus.

7.2.2 Cyclic Semifields.

Let W be a finite n-dimensional vector space, $n > 1$ over a field F and suppose $T \in \Gamma L(W,F) \setminus GL(W,F)$ is a strictly semi-linear bijection of W, regarded as an F-space; also let K be a subfield of F such that $T \in GL(W,K)$, for example K might be chosen to be the prime subfield of F.

We are interested here in the case when T is F-irreducible, that is, when T does not leave invariant any non-trivial proper F-subspace of W. Examples of such T are easily constructed, for instance on choosing $S \in GL(W,F)$ to correspond to a Singer cycle of $PG(n-1,F)$, $\sigma \in Gal(F)^*$, we might define $T = S\hat{\sigma}$; it is also not hard to see that S^k, for many values of k, work as well as S itself.

We now observe that the F-subspace of $Hom(W,F)$, generated by the powers of T, form an additive spreadset and thus yields a semifield; the strict F-semiinearity of T ensures that these semifields will not be a field. We shall call these semifields *cyclic.*

Proposition 7.2.3 *Suppose W is a finite n-dimensional vector space, $n > 1$, over a field F and that $T \in GL(W,K)$, where K is a proper subfield of F. If $T \in \Gamma L(W,F) \setminus GL(W,F)$ is F-irreducible, then viewing T and $f \in F$ as elements of $GL(W,K)$, the set:*

$$\Delta(T,F) := \{\mathbf{1}a_0 + Ta_1 + \ldots + T^{n-1}a_{n-1} \mid a_0, a_1, \ldots a_{n-1} \in F\}$$

is an additive spreadset over the field K. Such spreadsets will be called **cyclic semifield** *spreadsets.*

Proof: If some $\mathbf{1}a_0 + Ta_1 + \ldots T^i a_i + \ldots + T^k a_k$, for $0 \leq i \leq k \leq n-1$, where $a_k \neq 0$, is singular then there is an $x \in W^*$ such that:

$$\begin{aligned} \mathbf{0} &= (x)\mathbf{1}a_0 + Ta_1 + \ldots + T^k a_k \\ \text{so } (x)T^k &= (x)\left(\mathbf{1}a_0 + Ta_1 + \ldots + T^{k-1}a_{k-1}\right)\frac{1}{a_k} \end{aligned}$$

and hence the F-subspace of W generated by $\{x, xT, xT^2 \ldots, xT^{k-1}\}$ is T-invariant contradicting the F-irreducibilty of T. Thus all elements of type $\mathbf{1}a_0 + Ta_1 + \ldots + T^{n-1}a_{n-1}$, other than when $a_0 = a_1 = \ldots = a_{n-1}$, are non-singular, and hence $\Delta(T, F)$ is an additive group of linear non-singular K-linear maps that has the correct size to be a spreadset. The result follows. ∎

Remark 7.2.4 *The kern of $\Delta(T, F)$ is isomorphic to the centralizer of $\{T\} \cup \mathcal{F}$ in $Hom(W, +)$.*

Proof: The kern is the centralizer of the slope set of $\Delta(T, F)$ and this lies in the subalgebra, over the prime field, of $Hom(W, +)$ generated by $\{T\} \cup \mathcal{F}$. ∎

The Sandler semifields and the finite Hughes-Kleinfeld semifields are cyclic semifields, and as pointed out by Kallaher [29], almost all cyclic semifields are of these types. Thus cyclic semifields may be regarded as providing a uniform characterization of the finite Hughes-Kleinfeld and Sandler semifields, in slightly generalized form.

7.2.3 T-Cyclic $GL(2, q)$-spreads

We now define spreads that are *never* semifield-spreads, but still based on a field $\mathcal{F}$ of K-linear maps of an n-dimensional K-vector space W, K any finite field.

The construction is best described directly, as a spread on $V = W \oplus W$, rather than via a spreadset, so it becomes convenient to work with matrices, relative to a chosen K-basis of W, and we make the identifications $W = K^n$, $V = K^n \oplus K^n$. Now the field of linear maps associated with the scalar action of F on W, viz., $\hat{f} : x \mapsto xf$, becomes identified with a field $\mathcal{F}$ of $n \times n$ matrices over K, acting on K^n, and $T \in GL(n, K)$ is still required to be strictly $\mathcal{F}$-semilinear on K^n, or equivalently:

$$T \in N_{(GL(n,K)}(\mathcal{F}) - C_{(GL(n,K)}(\mathcal{F}),$$

and we shall insist that T does not leave invariant any non-trivial $\mathcal{F}$-subspace of rank ≤ 2, rather than insisting that T acts irreducibly, as in the previous case.

We shall demonstrate that the orbit τ of the subspace $y = xT$ of V, under the standard action of $\mathcal{G} = GL(2, \mathcal{F})$ on V, forms a partial spread that extends to a larger $\mathcal{G}$-invariant partial spread $\pi(T, \mathcal{F}) := \pi_{\mathcal{F}} \cup \tau$, where $\pi_{\mathcal{F}}$ is the [rational Desarguesian] partial spread associated with $\mathcal{F}$. On specialising to the case $dim_F W = 3$, the partial spread $\pi(T, \mathcal{F})$ becomes a non-Desarguesian spread of order q^3 admitting $GL(2, q)$, where $\mathcal{F} \cong GF(q)$.

Proposition 7.2.5 *Let $W = K^n$ be the standard n-dimensional vector space over a finite field $K = GF(q)$, for $n > 3$. Suppose $\mathcal{F} \subset GL(n, K)$ is a field, containing the scalar field K, and*

$$T \in N_{(GL(n,K)}(\mathcal{F}) - C_{(GL(n,K)}(\mathcal{F}),$$

so there is a non-trivial field automorphism $\sigma \in Gal(\mathcal{F}/K)^*$ such that

$$\forall X \in \mathcal{F} : X^\sigma = T^{-1}XT.$$

Let $\pi_{\mathcal{F}}$ be the rational Desarguesian partial spread determined on $V := W \ominus W$ by the spreadset $\mathcal{F}$, and let τ be the orbit of the K-subspace $y = xT$, of V, under the group:

$$\mathcal{G} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathcal{F}, ad - bc \neq 0 \right\} \cong GL(2, \mathcal{F}),$$

in its standard action on V.
Put:

$$\pi(T, \mathcal{F}) := \tau \cup \pi_{\mathcal{F}}.$$

Suppose T does not leave invariant any non-zero $\mathcal{F}$-subspace of W that has rank ≤ 2. Then the following hold.

1. *τ is a partial spread containing $q(q^2 - 1)$ components and the global stabilizer of $y = xT$ in $\mathcal{G}$ is the diagonal group*

$$\{Diag[A, A^\sigma] \mid A \in \mathcal{F}^*\}.$$

2. *The rational Desarguesian partial spread $\pi_{\mathcal{F}}$ is a $\mathcal{G}$-orbit, and $\mathcal{G}$ acts triply transtively on its components.*

3. *The $\mathcal{G}$-orbits, τ and $\pi_{\mathcal{F}}$, do not share any components and $\pi(T, \mathcal{F})$ is also a partial spread.*

4. *$\pi(T,\mathcal{F})$ is a spread iff $dim_{\mathcal{F}}W = 3$. In this case, the spread admits $\mathcal{G} = GL(2,\mathcal{F})$ so that this group partitions the components of $\pi(T,\mathcal{F})$ into two orbits, viz., τ and $\pi_{\mathcal{F}}$, and $\mathcal{G}$ acts triply transitively on the orbit $\pi_{\mathcal{F}}$ and transitively on the orbit τ.*
The kern of $\pi(T,\mathcal{F})$ is isomorphic to the centralizer of $\{T\} \cup \mathcal{F}$ in $Hom(W,+)$; hence $K = GF(q)$ is always in the kern, and $\mathcal{F}$ is not: so the spread is non-Desarguesian.

Proof: The image of (x, xT), $x \in K^n$, $x \neq \mathbf{0}$, under an element of $\mathcal{G}$:

$$g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

is $(xA + xTC, xB + xTD)$, and this meets the component $y = xT$ iff the conditions $u = xA + xTC$ and $uT = xB + xTD$ hold simultaneously for some $u \in W^*$, and this is equivalent to

$$(xA + xTC)T = xB + xTD,$$

and since T normalizes $\mathcal{F}$, and induces σ on it the above is equivalent to:

$$xT^2C^\sigma = xB + xT(D - A^\sigma),$$

and this means that the $\mathcal{F}$-subspace generated by $\{x, xT\}$ is T-invariant, contradicting the hypothesis that T cannot leave invariant non-trivial $\mathcal{F}$-subpace of dimension ≤ 2, unless $B = C = \mathbf{O}$ and $D = A^\sigma$. Now the image of (x, xT) is (xA, xAT), for all x.
Thus, the orbit τ of the component $y = xT$ under $\mathcal{G}$ contains, in addition to $y = xT$, only subspaces that are disjoint from $y = xT$ and, additionally, the global stabilizer of $y = xT$ is given by

$$\mathcal{G}_{\{y=xT\}} = \{Diag(A, A^\sigma) \mid A \in \mathcal{F}^*\},$$

so

$$|\tau| = |GL(2,q)|/(q-1) = q(q^2-1).$$

Thus we have established that the $\mathcal{G}$-orbit of $y = xT$, viz., τ, is a collection of $q(q^2-1)$ subspaces that have the same size as $y = xT$ and all members of $\tau \setminus \{y = xT\}$ are disjoint from $y = xT$. It follows that if R and S are *any* two distinct members of τ, then they are disjoint because if $R \cap S \neq \mathbf{O}$ then we may choose $g \in \mathcal{G}$ such that $(R)g = (y = xT)$ and now $y = xT$ meets the element $(S)g \in \tau$.

Instructive Diversion. *This is a case of a simple but useful principle: (a) if a rank r subspace A of a vector space V of rank $2r$ has an orbit $\mathcal{A}$ under a subgroup $G \leq GL(V,+)$ such that $A - A^g$ is non-singular or zero for all g then $\mathcal{A}$ is a partial spread that is G-invariant; (b) if the subspace A is disjoint from all the members of a G-invariant partial spread $\mathcal{B}$ then $\mathcal{A} \cup \mathcal{B}$ is also a partial spread.*

Next, to apply the second part of the above principle, consider the possibility that $y = xT$ meets $\pi_{\mathcal{F}}$, the rational Desarguesian spread coordinatized by $\mathcal{F}$. If $T - A$ is singular for $A \in \mathcal{F}^*$, then $xT = xA$, for some $A \in \mathcal{F}^*$, $x \in W^*$. Thus $y = xT$ and $y = xA$ are disjoint subspaces of V, for $A \in \mathcal{F}^*$: otherwise T leaves invariant the rank-space $x\mathcal{F}$, contrary to hypothesis. Moreover, $y = xT$ is certainly disjoint from $\mathbf{O} \oplus W$. Hence $y = xT$ is disjoint from the rational Desarguesian partial spread coordinatized by the spreadset $\mathcal{F}$. But this partial spread, viz.,

$$\pi_{\mathcal{F}} := \{y = xA \mid A \in \mathcal{F}\} \cup \{Y\}$$

is also invariant under $\mathcal{G}$ because

$$(\mathbf{0}, u)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (uc, ud)$$

shows that Y is left invariant when $c = \mathbf{0}$, and otherwise, when $cu \neq \mathbf{0}$, Y maps to $y = x(uc)^{-1}ud$, which is a component of type $y = xf$, $f \in \mathcal{F}$. Similarly, we can determine that $y = xf$, $f \in \mathcal{F}$, maps under $\mathcal{G}$ into the rational Desarguesian partial spread $\pi_{\mathcal{F}}$:

$$(y = xf)\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{cases} (y = x(a + fc)^{-1}(b + fd)) & \text{if } a + fc \neq \mathbf{O}; \\ (x = \mathbf{0}) & \text{otherwise.} \end{cases}$$

In particular, Y is not $\mathcal{G}$ invariant, and the global stabilizer $\mathcal{G}_{\{Y\}}$ of Y is doubly transitive on all the other components of $\pi_{\mathcal{F}}$: for example, note that $\mathcal{G}_{\{Y\}}$ does not leave X invariant and the global stabilizer of X in $\mathcal{G}_{\{Y\}}$ is transitive on the components in $\pi_{\mathcal{F}} \setminus \{X, Y\}$. Hence $\mathcal{G}$ leaves $\pi_{\mathcal{F}}$ invariant and acts 3-transitively on its components.

Thus, recalling that the members of $\pi_{\mathcal{F}}$ are disjoint from $y = xT$, we see that the orbit $(y = xT)\mathcal{G}$ is a partial spread such that its members all have trivial intersection with the members of $\pi_{\mathcal{F}}$.

Now specialize to the case $\mathcal{F} = GF(q)$ and $dim_{\mathcal{F}}W = 3$. Now the partial

spreads $\pi_{\mathcal{F}}$ and τ together contribute $q+1+q(q^2-1)=q^3+1$ components of the partial spread $\pi(T,\mathcal{F})$, and this is the size needed to make it into a spread. Since the $\mathcal{G}$-orbit τ now has the size of $\pi(T,\mathcal{F}) \setminus \pi_{\mathcal{F}}$, we conclude that $\mathcal{G}$ is transitive on the components of the spread outside $\pi_{\mathcal{F}}$.
This spread is coordinatized by a spreadset $\mathcal{S} \supset \mathcal{F} \cup \{T\}$, that includes the identity and yet $\mathcal{S}$ is not a field because T does not centralize $\mathcal{F}$. The slope-set of $\pi(T,\mathcal{F})$ is clearly in $Hom(W,+)$ so its kern is as claimed. ∎
By varying T, for a fixed choice of $\mathcal{F}$, it is possible to ensure that the dimension of the spread $\pi(T,\mathcal{F})$, over its kern, can be made arbitrarily large; in partciular this means that non-Desarguesian translation planes of order q^3 that admit $SL(2,q)$ can be chosen to have arbitrarily large dimension. We leave this verification as an exercise for the reader.

Chapter 8

Semifields.

Recall that a distributive quasifield is called a *semifield.* Equivalently, a semifield is a 'non-associative [skew]field' as seen in the following characterization. The aim of this chapter is to address the following question: what are the possible sizes of finite *non-associative* semifelds? We shall see that semifields that are of order p^2 are always fields. Also all translation planes of order 8 are known to be Desarguesian. But the twisted fields of A. A. Albert and the even order commutative semifelds of D. E. Knuth, taken together, demonstrate that *for all other prime-powers orders* n at least one non-associative semifield plane of order n exists. The main goal of this chapter is to introduce these planes and demonstrate that they are non-associative. This is preceeded by some after some basic results have been established.

8.1 General Remarks On Semifelds.

The following theorem is an analogue of the elementary result: finite [associative] integral domains are fields. Here we prove that finite 'non-associative' integral domains are semifields. Many important constructions of finite [pre]semifelds are based on this principle.

Remark 8.1.1 *A system* $(D, +, \circ)$ *is a semifield iff the following axioms hold:*

1. $(D, +)$ *is an abelian group;*
2. *The distributive laws are valid for* $x, y, z \in D$*:*

(a) $x \circ (y+z) = x \circ y + x \circ z$;

(b) $(y+z) \circ x = y \circ x + z \circ x$.

3. $(D^*, \circ)$ *is a loop.*

A semifield that is not a [skew]field is called a proper semifield. We shall be concerned with *finite* semifields from now on. Thus the basic question is what are the possible orders of proper non-associative semifields? This question has a complete answer, but first we draw attention to some elementary facts.

Remark 8.1.2 *Let $(D, +, \circ)$ be a finite semifield. Then its three seminuclei $N\ell$, N_m and N_r are all fields, in particular its kern coincides with N_ℓ and $(D, +)$ is a vector space over each of these nuclei, as well as over its nucleus and center (both of which are also fields).*

Proof: Exercise. ∎

Remark 8.1.3 *A semifield two dimensional over a field in its center is a field. Hence all semifields of order p^2 are known.*

Proof: Exercise. ∎

Thus all semifield planes of order p^2 are known. A spectacular extension of this result follows form a theorem of Menichetti: all semifield planes of order p^3 are known. They are forced to be coordinatized by the generalized twisted fields of Albert, see 147.

8.2 The Knuth Commutative Semifields.

Finite commutative semifields (that are not associative) appear to be quite hard to find. The following construction due to Knuth, [30], established the existence of commutative semifields of *even* order N, where $N > 8$ is not a power of 2.

Theorem 8.2.1 (The Binary Knuth Semifields.) *Let $K = GF(2^{nm}) \supset GF(2^m) = K_0$, where $n > 1$ is odd. Let $f : K \to K_0$ be any nonzero linear functional of K as a K_0 vector space. Define a new multiplication as follows:*

$$a \circ b = ab + (f(a)b + f(b)a)^2.$$

The algebraic system $(K, +, \circ)$ is a pre-semifield.

Proof: The fact that $x \mapsto x^2$ is additive in the characteristic 2 case, yields the distributive laws. So it remains to verify $a \circ b = 0$ is impossible if a and b are non-zero. Denying this, we have non-zero a and b such that

$$ab + (f(a)^2b^2 + f(b)^2a^2) = 0,$$

so

$$\frac{a}{b} + f(a)^2 + f(b)^2\left(\frac{a}{b}\right)^2 = 0,$$

which may be written as a quadratic in $x = a/b$:

$$f(b)^2x^2 + x + f(a)^2 = 0,$$

and this quadratic in x, with coefficients in K_0, is reducible in K because $x = a/b$ is a solution. But since K is odd dimension over K_0, the quadratic must be reducible even in K_0, so $x = a/b \in K_0$. Hence by the definition of $\circ$:

$$\begin{aligned} a \circ b &= ab + (f(a)b + f(b)a)^2 \\ &= ab + (f(bx)b + f(b)a)^2 \\ &= ab + (f(b)bx + f(b)bx)^2, \text{ by linearity of f} \\ &= ab, \text{ in charactersitic 2.} \end{aligned}$$

so $a \circ b = ab \neq 0$, a contradiction. ∎

Exercise 8.2.2 *Show how to obtain a commutative semifeld of the same order as the above pre-semifield.*

The usual procedure for converting a pre-quasifield to a quasifield '$(a \circ b) = (a \circ e) * (e \circ b)$', where e is an arbitrary non-zero element, of course solves exercise 8.2.2 above. However, to ensure that the resulting comutative semifield is not a field f needs to be chosen with some care. Such an f is introduced in the following theorem.

The theorem also demonstrates that in converting a presemifield to a semifield it is desirable to choose the identity 'e' with care, to avoid creating a semifield with a more opaque structure than the presemifield used to construct it.

Theorem 8.2.3 (The Binary Knuth Semifields.) *Let $K = GF(2^{nm}) \supset GF(2^m) = K_0$, where $n > 3$ is odd. Fix a K_0-basis of K of type $(1, \alpha, \alpha^2, \ldots \alpha^{n-1}$ and choose the K_0-valued functional $f : K \to K_0$ such that $f(\alpha^i) = 0$ for $0 \leq i \leq n-2$, and $f(\alpha^{n-1}) = 1$. Define new multiplications $\circ$ and $\odot$ on K as follows for all $a, b \in K$:*

$$\begin{aligned} a \circ b &= ab + (f(a)b + f(b)a)^2 \\ a \circ b &= (a \circ 1) \odot (1 \circ b) \end{aligned}$$

The algebraic system $(K, +, \circ)$ is a commutative presemifield and $(K, +, \odot)$ is a commutative semifield (but not a field) such that they both coordinatize the same semifield plane.

Proof: In view of theorem 8.2.1, it follows easily that $(K, +, \odot)$ is a commutative semifield, with identity $1 \circ 1$, and that the two systems coordinatize the same plane. It remains to check that $\odot$ is not associative. The main step is to obtain a direct representation of $\odot$, viz.:

$$a \odot b = (a \circ 1) \circ (1 \circ b) \tag{8.1}$$

Since K_0 is in the null space of f, and also its image, we obtain $1 \circ a = a + f(a)^2$, $f(a)^2 \in K_0$, and hence $f(1 \circ a) = f(a)$. Thus we have

$$1 \circ (1 \circ a) = a + f(a)^2 + (f(a) + 0)^2,$$

yielding the identity in $a \in K$:

$$1 \circ (1 \circ a) = a. \tag{8.2}$$

Now replacing a and b resp. by $1 \circ a$ and $1 \circ b$ in the defining identity for $\odot$ we have:

$$\begin{aligned} (a \circ 1) \circ (1 \circ b) &= ((a \circ 1) \circ 1) \odot (1 \circ (1 \circ b)) \\ &= a \odot b \text{by (8.2)}, \end{aligned}$$

thus (8.1) has been established.
We can now verify that $\odot$ is not associative by demonstrating that a multiplication involving α^k, $k = n - 1/2$, fails to be associative; exponents here and throughout the proof are assumed relative to *field* multplication. Note that

$k = n - 1/2$, and $n > 3$ means that $k < n - 2$, so, by definition, $f(\alpha^k) = 0$. Hence the formula for $\odot$ given in (8.1) above yields

$$\alpha^k \odot \alpha^k = (\alpha^k \circ 1) \circ (\alpha^k \circ 1) = \alpha^k \circ \alpha^k = \alpha^{n-1},$$

since $z \circ z = z^2$ in characteristic 2. Similarly,

$$\alpha^k \odot \alpha = (\alpha^k \circ 1) \circ (\alpha \circ 1) = \alpha^{k+1},$$

as by definition α^k, α and 1 are all in the kernel of f. We now show that $\odot$ is not associative, by deducing a cntradiction from the following power associativity identity:

$$\alpha \odot (\alpha^k \odot \alpha^k) = (\alpha \odot \alpha^k) \odot \alpha^k, \tag{8.3}$$

which implies that

$$\alpha \odot \alpha^{n-1} = \alpha^{k+1} \odot \alpha^k.$$

But remembering that $f(\alpha^{n-1} = 1$, the LHS becomes

$$(\alpha \circ 1) \circ (\alpha^{n-1} \circ 1) = \alpha \circ (\alpha^{n-1} + 1) = \alpha \circ \alpha^{n-1} + \alpha = \alpha^n + (0 + \alpha 1)^2 + \alpha = \alpha^n + \alpha^2 + \alpha,$$

and the RHS becomes

$$\alpha^{k+1} \odot \alpha^k = (\alpha^{k+1} \circ 1) \circ (1 \circ \alpha^k) = \alpha^{k+1} \circ \alpha^k = \alpha^n + (0^2) = \alpha^n,$$

so the associativity fails unless $\alpha^n + \alpha^2 + \alpha = \alpha^n$ and this means $\alpha = 1$ or $\alpha = 0$, contradicting: $\alpha \in K - K_0$. Thus the power associativity claimed in (8.3) fails and the desired result follows. ∎

Exercise 8.2.4 *Show that the theorem is valid even for* $n = 3$ *provided* $K_0 = GF(2^m)$, *and* $m > 1$.

Perhaps the most important feature of the theorem above is that it ensures the existence of non-Desarguesian projective planes of order 2^p, p any *prime* > 3.

8.3 Twisted Fields.

Let $c \in K = GF(q^n)$ such that $c \notin K^{q-1}$. Then $GF(q)$-linear maps of $K = GF(q^n)$ defined by:

$$\begin{aligned} P^{-1} &: K \to K \\ &\quad x \mapsto x - cx^q \end{aligned} \tag{8.4}$$

$$\begin{aligned} Q^{-1} &: K \to K \\ &\quad x \mapsto x^q - cx \end{aligned} \tag{8.5}$$

are bijective (thus justifying the inverse notation) because $x = xc^q$ or $x^q = cx$ both contradict the assumption $c \notin K^{q-1}$.

Since P^{-1} and Q^{-1} both map 1 to $1 - c = f$, we also have

$$P(f) = Q(f) = 1, \tag{8.6}$$

We now define the semifield associated with (P, Q); the above equation will establish the multiplicative identity.

Theorem 8.3.1 *Define $\odot$ by:*

$$x \odot y = xP(yQ)^q - (xP)^q(yQ)c,$$

and let $f = 1-c$. Then $(K, +, \odot)$ is a division algebra with identity $f = 1-c$ and center $F \odot f$ where $F = GF(q) \subset GF(q^n)$.

Proof: Since P and Q are inverses of F-linear bijections they too must be F-linear bijections. Now since P, Q and the field automorphism $x \mapsto x^q$ are all additive, the distributive laws hold. Zero divisors exist only if for some non-zero x and y:

$$xP(yQ)^q = (xP)^q(yQ)c \Longrightarrow (xP/yQ)/(xP/yQ)^q = c,$$

contradicting the hypothesis that c is not a $q-1$-th power. Hence the system is a presemifield.
To verify that f is the multiplicative identity, apply eq (8.6) to

$$x \odot f = xP - (xP)^q c = (xP)P^{-1} = x$$

and similarly:

$$f \odot x = xQ^q - xQc = (xQ)Q^{-1} = x.$$

Thus f is the multiplicative identity. Now we establish that $F \odot f$ may be identified with F, by remembering that S, P and Q are all members of $GL(K,+)$ that *are linear over* F, and that $fP = fQ = 1$; for all $x \in K$ and $\alpha \in F$:

$$\begin{aligned} x \odot (f\alpha) &= xP(f\alpha)Q^q - (xP)^q(f\alpha)Qc \\ &= (xP(f)Q^q - (xP)^q(f)Qc)\,\alpha \\ &= (xP - (xP)^q c)\,\alpha \\ &= (xP)P^{-1}\alpha = x\alpha \end{aligned}$$

and similarly

$$(f\alpha) \odot x = (xQ^q - xQc)\alpha = (xQ)Q^{-1}\alpha = x\alpha.$$

Thus we have shown:

$$(f\alpha) \odot x = x\alpha = x \odot (f\alpha) \forall x \in K \alpha \in F. \tag{8.7}$$

Now it is straightforward to check that $F \odot f$ is in the middle and left nuclei; for example $(x \odot f\alpha) \odot y$ and also $x \odot (f\alpha \odot y)$ may be written, by eq 8.7, as $(x\alpha) \odot y$ and $x \odot (\alpha y)$ respectively and these are equal because all the three maps defining $\odot$ are linear over $\alpha \in F$. The result follows. ∎

It appears to be surprisingly hard to determine whether or not $F \odot f$ is the *full* center of the semifield. In fact, it appears hard to verify even that the semifield is not a field. To verify this we shall determine when the semifield is non-commutative. This requires an explicit form for the Vaughan polynomial for P: our definition of P is specified *indirectly*, in terms of the Vaughan Polynomial of P^{-1}.

As indicated by Albert, the product $\odot$ cannot be regarded as explicitly known until the Vaughan polynomials for P *and* Q are explicitly known. However, in view fo the close connection between the definitions of P^{-1} and Q^{-1}, cf (8.4) and (8.5), it is possible to deduce the Vaughan polynomial of Q from that of P, so we only compute P explicitly.

8.3.1 Polynomial for P; Non-Commutivity of Semifield.

In this section we adopt the following:

Notation 8.3.2 *Regarding $K = GF(q^n) \supset F = GF(q)$ as a rank n vector space over F, and define the F-linear maps of K:*

1. $S : x \mapsto x^q$;

2. $R_a : x \mapsto xa$, *for* $a \in K$;

We regard members of $Hom_F(K,+)$ as acting on K from the right. The associative ring $\sum_{i=0}^{n-1} S^i R_{a_i}$, for $a_i \in K$, forms an F-algebra; F may be identified with the central field $\{R_f \mid f \in F\}$. By Vaughan polynomials the S^i's in the expression are linearly independent over F and hence the expressions account for $|K|^n$ K-linear maps in $Hom_F(K,+)$, but since this set has size $|F|^{n^2}$, we have a fundamental fact concerning Vaughan polynomials.

Result 8.3.3 (Fundamental Theorem of Vaughan Polynomials.) *The K-algebra $Hom_F(K,+)$ is the K-algebra:*

$$\left\{ \sum_{i=0}^{n-1} S^i R_{a_i} \mid a_i \in F, \forall i \in [0, n-1) \right\}.$$

We now compute P using eq(8.4), which may be written as $P^{-1} = x - xSR_c$, and the elementary ring identity

$$(1-\theta)(1+\theta+\theta^2+\ldots+\theta^{n-1}) = 1-\theta^n,$$

by noticing that $\theta := SR_c$ implies:

$$1-\theta = P^{-1}.$$

Thus we have:

$$P^{-1}\left(1+SR_c+(SR_c)^2+\ldots+(SR_c)^{n-1}\right) = 1-(SR_c)^n \qquad (8.8)$$

and now $(SR_c)^i$ may be expressed in the following notation,

$$(SR_c)^i = S^i R_{c_i}, \qquad (8.9)$$

where $c_i \in F^*$ is uniquely defined by the above requirement. In particular, we need to record:

Remark 8.3.4 *Define $c_i \in F$ in terms of c by:*

$$\forall i \in [1,n] : (SR_c)^i = S^i R_{c_i}. \qquad (8.10)$$

Then

1. P^{-1} *commutes with all terms of type* $S^i R_{c_i}$

2. $c_n \in GF(q)$. $c_{i+1} = (c_i)Sc$.

3. $c_n \in GF(q)^*$, *but* $c_n \neq 1$.

Proof: The first part holds because, by definition, $P^{-1} = 1 - (SR_c)$ and terms $S^i R_{c_i}$ are all powers of a single term SR_c. In particular, eq (8.10) means that

$$S^{i+1}R_{c_{i+1}} := (SR_c)^{i+1} = (SR_c)^i SR_c = S^{i+1}R_{(c_i)Sc}.$$

The next case follows from eq (8.10) by putting $i = n$ and noting:

$$c_n = S^n c_n = (SR_c)^n = S^n c(cS)(cS^2)\dots(cS^{n-1}) = \nu(c),$$

where the norm $\nu(c)$ relative to S must lie in its fixed field, so $c \in GF(q)$ Now if $1 = \nu(C) = c^{q^n-1/q-1}$ then we claim c is a $q-1$-th power. Now writing $c = \omega^{k(q-1)+r}$, ω a primitive element of $GF(q^n)^*$ and $0 \leq r < (q-1)$, implies $\omega^{r(q^n-1)/q-1} = 1$, so $r = 0$. ∎

Now the commutivity condition for P^{-1}, the fact that $(SR_c)^n = S^n R_{c_n} = R_{c_n}$, and by the final case above, $1 - R_{c_n} \in GF(q)^*$, means that the identity (8.8) may be restated as follows:

$$P = (1 + SR_{c_1} + S^2 R_{c_2} + \dots + S^{n-1}R_{c_{n-1}})(1 - R_{c_n})^{-1}. \tag{8.11}$$

The above identity is the Vaughan polynomial for P. If desired, a similar identity for Q may be obtained, or deduced from the expression for P.

We now use the above Vaughan polynomial for P to determine when the divison algebra $(D, +, \odot)$ is commutative. The definition of $\odot$ means that it is commutative iff:

$$xP(yQ)^q - (xP)^q yQc = yP(xQ)^q - (yP)^q(xQ)c$$

so putting $y \mapsto yQ^{-1}$ shows commutivity is equivalent to the identity:

$$xPy^q - (xP)^q yc = yQ^{-1}P(xQ)^q - (yQ^{-1}P)^q(xQ)c$$

and viewing both sides as functions of y, implies that the commutivity is equivalent to:

$$SR_{xP} - R_{(xP)Sc} = Q^{-1}P(R_{xQS} - SR_{(xQ)c}),$$

and using the Vaughan expansion for P in eq (8.11) above, and recalling the definition of Q^{-1}, eq (8.5), we see that commutivity of the semifield is equivalent to the following identity after the $GF(q)^*$ element $(1-R_{c_n})^{-1}$ is shifted to the LHS.

$$\begin{aligned}(SR_{xP}-R_{(xP)Sc})(1-R_{c_n}) &= (S-R_c)(1+SR_{c_1}+S^2R_{c_2}+\ldots S^iR_{c_i}\ldots \\ &\quad \ldots S^{n-1}R_{c_{n-1}})(R_{xQS}-SR_{(xQ)c}),\end{aligned}$$

and on making the substitution $xQ \leftarrow t$ we have:

$$\begin{aligned}(SR_{xP}-R_{(xP)Sc})(1-R_{c_n}) &= (S-R_c)(1+SR_{c_1}+S^2R_{c_2}+\ldots S^iR_{c_i}\ldots \\ &\quad \ldots S^{n-1}R_{c_{n-1}})(R_{tS}-SR_{tc}),\end{aligned}$$

We now compute the coefficient of the powers of $S^i > S^2$ on the RHS when this is expressed in standard S-polynomial form:

$$\begin{aligned}((S+S^2R_{c_1}+S^3R_{c_2}+\ldots S^{i+1}R_{c_i}\ldots) &- R_c(1+SR_{c_1}+S^2R_{c_2}+\ldots+S^iR_{c_i}\ldots \\ &\ldots +S^{i+1}R_{c_{i+1}}\ldots))\times(R_{tS}-SR_{tc}) = \\ ((S+S^2R_{c_1}+S^3R_{c_2}+\ldots+S^{i+1}R_{c_i})\ldots &- (R_c+SR_{cSRc_1}+S^2R_{cS^2c_2}+\ldots+S^iR_{cS^ic_i}\cdot \\ &\ldots +S^{i+1}R_{cS^{i+1}c_{i+1}}\ldots))\times(R_{tS}-SR_{tc}),\end{aligned}$$

and the terms in S^i above, after expansion, have form

$$\begin{aligned}&= S^iR_{c_{i-1}}R_{tS}-S^iR_{cS^ic_i}R_{tS}-S^{i-1}R_{c_{i-2}}SR_{tc}+S^{i-1}R_{cS^{i-1}c_{i-1}}SR_{tc} \\ &= S^iR_{c_{i-1}(tS)}-S^iR_{cS^ic_i(tS)}-S^iR_{c_{i-2}Stc}+S^iR_{(cS^i)(c_{i-1}S)(tc)} \\ &= S^i[R_{c_{i-1}(tS)}-R_{cS^ic_i(tS)}-R_{c_{i-2}Stc}+R_{(cS^i)(c_{i-1}S)(tc)}],\end{aligned}$$

and this coefficient for $i \in [2, n-1]$ must vanish for all t, which means

$$(c_{i-1}-(cS^i)c_i)t^q+(cS^ic_{i-1}S-c_{i-2}S)tc \equiv 0$$

and this is equivalent, for $i > 1$, to

$$\begin{aligned}c_{i-1}-(cS^i)c_i &= 0 \\ \text{and } cS^ic_{i-1}S-c_{i-2}S &= 0,\end{aligned}$$

and the case $i = 2$, remembering $c_1 := c$, yields: $c_1 = cS^2c_2$, but now by $c_2 = cSc$ we have $c^{-1} = cS$, hence also $c_2 = 1$. Now lemma 8.3.4(2), page 144, above shows that the c_i for $i \geq 1$ alternates:

$$c_1 = c, c_2 = 1, c_3 = c, c_4 = 1, c_5 = c, \ldots c_n = 1,$$

where $c_n = 1$ is forced because, by lemma 8.3.4 again, c_n is in $GF(q)$, unless c itself is in $GF(q)$. But recall that $1 - c_n \neq 0$ means that only the latter case can occur. But also remember that $c^q = c^{-1}$ means that $c^2 = 1$ as S fixes $GF(q)$ elementwise. So $c = \pm 1$ and $c = 1$ means it is a $q - 1$-th power. Hence $c = -1$ is the only possibility, and this actually works: now $P = Q$ is automatic and the above constraints are all met easily.

Thus we have established

Theorem 8.3.5 *Assume $n > 2$. $(D, +, \odot)$ is commutative iff $c = -1 \neq 1$ and $P = Q = (1 + S)$.*

8.4 Generalised Twisted Fields.

The twisted fields of Albert, discussed in the previous section, are important partly because they help to demonstrate that non-associative semifields of odd order p^r exist, for p prime, iff $r > 2$. The generalized twisted fields, introduced in this section, have proven to be of importance because they arise in several major classification theorems: Menichetti's classification of the semifields of order p^3 and in the Cordero-Figueroa-Liebler classification of semifield planes admitting large autotopism groups of various types. In all these cases the associated planes are shown to be among th class of generalized twisted fields of Albert, rather than in the class of planes coordinatized by just the ordinary twisted fields of the previous section.

We begin with an elementary result from arithmetic that has wide applications in the exploitation of finite fields.

Result 8.4.1 *Let q be a prime power. Then*

$$\gcd\left(q^a - 1, q^b - 1\right) = q^{\gcd(a,b)} - 1.$$

Proof: The RHS divides the LHS because, in general, $q^m - 1$ divides $q^n - 1$ if m divides n. Let u be any maximal prime power dividing LHS. Then $q^a \equiv 1 \pmod{u}$ and $q^b \equiv 1 \pmod{u}$ and also q is invertible $\pmod{u}$. So a and b are divisible by the order A of $q \pmod{u}$. So A divides $\gcd(a, b)$, hence u divides $q^{\gcd(a,b)} - 1$, so u divides the RHS. ∎

Throughout the section we adopt the following hypothesis:

Notation 8.4.2 *The integer $q = p^s > 1$ is a power of the prime p. $K = GF(q^n)$ and $AutK$ denotes the associated Galois group generated by $\rho : x \mapsto x^q$. Assume $S, T \in AutK$ such that*

1. $1 \neq S \neq T \neq 1$; *and*

2. $Fix(S,T) = GF(q)$.

Note that any finite field with two distinct non-trivial automorphisms, S and T, can be viewed as satisfying all the above conditions if we define $GF(q)$ to be the fixed field of the group $< S,T >$.

Write $N = K^{S-1}K^{T-1}$, so N^* is a multiplicative subgroup of K^*. Fix an element $c \in N - K$.

Exercise 8.4.3 Take $K = GF(q^n)$, $S : x \mapsto x^q$, and $T = S^{-1}$. Show that c can be chosen provided $n > 2$ and $q > 2$. What goes wrong when $n = 2$?

The *Albert product* on K, written $< x,y >_c$ and abbreviated to $x \circ y$ is defined by:

$$\forall x,y \in K : x \circ y :=< x,y >_c := xy - x^T y^S c. \tag{8.12}$$

Remark 8.4.4 $< x,y >_c = 0 \iff x = 0 \vee y = 0$.

Since S and T are additive, $(K,+,\circ)$ must also satisfy both distributive laws: so we have a finite 'non-associative integral domain' and, as in the associative case, this means that multiplication defines a quasigroup on the non-zero elements. Thus we have:

Lemma 8.4.5 *Suppose the triple $(D,+,\circ)$ is such that $(D,+)$ is a FINITE abelian group such that both the distributive laws hold. Then $(D^*,\circ)$ is a quasigroup, or equivalently, $(D,+,\circ)$ is a presemifield if and only if:*

$$x \circ y = 0 \iff x = 0 \vee y = 0.$$

Proof: The distributive laws imply that the maps $x \mapsto x \circ a$ and $x \mapsto b \circ x$ are additive and so the no-zero-divisor hypothesis holds iff both maps are injective and hence bijective. The lemma follows. ∎

In view of eqn 8.12, lemma 8.4.5 above, applied to the Albert product, immediately yields:

Theorem 8.4.6 *Let $\mathcal{A}_c := (K,+,\circ)$, where $\circ =<,>_c$ is an Albert product on $K = GF(q^n)$ and $(K,+)$ is the additive group of of the field. Then $\mathcal{A}_c$ is a pre-semifield.*

The planes coordinatized by the presemifields $\mathcal{A}_c$ will be called the *Albert planes*. The presemifields $\mathcal{A}_c$ will be called *generalized twisted fields*.

The following proposition yields the list of orders that Albert plane have.

Proposition 8.4.7 *Let $K = GF(q^n)$, $Fix(< S,T >) = GF(q)$, where $S \neq T$ are distinct nontrivial $GF(q)$-linear field automorphisms in $AutK$ such that $Fix(< S,T >) = GF(q)$. Let $N = K^{S-1}K^{T-1}$, then $K - N \neq \emptyset$ iff*

1. *$q > 2$ and $n > 2$; now any pair of distinct non-trivial S and T will yield $K - N \neq \emptyset$;*

2. *If $q = 2$ and n is not a prime; now, wlog $1 \leq a < b < n$, the pair*

$$\left(S : x \mapsto x^{p^a}, T : x \mapsto x^{p^b}\right)$$

yields $K - N \neq \emptyset$ iff and $\gcd(a,b) > 1$ shares a non-trivial factor with n.

Proof: We may write $S - 1 = q^s - 1$ and $T - 1 = q^t - 1$. So N^* only contains powers of ω^{q-1} where ω is a primitive generator of $GF(q^n)$. So if $q > 2$ then an Albert sytem exists so long distinct S and T exist such that $Fix(< S,T >) = GF(q)$. This can be arranged by taking $S : x \mapsto x^q$ and T to be a power of S but distinct from it: unless S^2 is the identity, i.e., $n = 2$. If $n = 2$ then obviously no T satisfying are requirements exist.
So it remains to consider the case when $q = 2$, again $n > 2$ is forced. Now putting $S : x \mapsto x^{2^a}$ and $T : x \mapsto x^{2^b}$, we clearly have $1 < a, b < n$, where

$$gcd(a,n) \neq 1 \neq \gcd(b,n)$$

since for integer $x > 1$:

$$N^* \supseteq K^* 2^x - 1 =< \omega^{2^x-1} >=< \omega >,$$

holds unless $1 \neq \gcd(2^n - 1, 2^x - 1) = \gcd(n,x)$, by result 8.4.1, 147. Thus n cannot be prime, and furthermore a and b must share a proper prime factor with n. Now

$$\begin{aligned} N^* &= < \omega^{2^a-1}\omega^{2^b-1} > \\ &= \left\{\omega^{x(2^a-1)+y\left(2^b-1\right)} \mid x, y \in \mathcal{Z}\right\} \\ &= < \omega^{\gcd\left(2^a-1,2^b-1\right)} > \\ &= < \omega^{\left(2^{\gcd(a,b)}-1\right)} >, \end{aligned}$$

and so $N^* < K^*$ iff

$$K^* \neq < \omega^{\left(2^{\gcd(a,b)}-1\right)} >$$

and this holds iff

$$\left(2^{\gcd(a,b)} - 1, 2^n - 1\right) \neq 1,$$

and this is equivalent to $\gcd(a, b)$ and n sharing a non-trivial factor. ■

Exercise 8.4.8

1. There are no generalized twisted fields of order < 64 and there do exist gtt of order 64.
2. There exists generalized twisted fields of order 2^n, provided n is not a prime *and* $n > 4$.
3. Using Albert's approach for twisted fields, determine when generalized twisted fields coordinatize non-Desarguesian translation planes.

8.5 Some Two-Dimensional Semifields.

In this section we mention two classes of semifields whose planes admit geometric characterizations. They are also associated with tangentially transitive planes. We use the following notation.

Let F be a finite field of odd order and $a \in F^*$ a non-square in F. Let λ be an indeterminate over F, and θ a non-trivial field automorphism of F. Let $D = F \oplus \lambda F$.

Theorem 8.5.1 (Dickson's Commutative Semifields.) *Suppose $a \in F^*$ is non-square, so F is odd. Then*

$$(x + \lambda y) \circ (z + \lambda t = (xz + a(yt)^\theta) + \lambda(yz + xt)$$

is a commutative semifield such that:

1. *F is the middle nucelus of $(D, +, \circ)$;*
2. *$K = Fix(\theta) \cap F$ is the rightnucleus, the left nucelus and hence also the center of D.*

Theorem 8.5.2 (Hughes-Kleinfeld Semifelds.) *Suppose* $a = x^{1+\theta} + xb$ *has no solution for* x *in* F. *Then*

$$(x + \lambda y) \circ (z + \lambda t = (xz + aty^{\theta}) + \lambda(yz + (x^{\theta} + y^{\theta}b)t$$

is a semifield and F *is its right and middle nucleus. Conversely, if* D *is a semifield that is a finite two dimensional over a field* F *such that the middle and right nucelus of* D *coincide then* D *is a Hughes-Kleinfeld semifield.*

Chapter 9

Generalised André Systems and Nearfields.

In this section we introduce important classes of quasifields that do not coordinatize semifeld planes.

9.1 Construction Of Generalised André Systems.

Let F be an extension field of a field K, $\Lambda = Gal(F/K)$, and let $\lambda : F^* \to \Lambda$ be any map such that the $\lambda(1) = 1$. Then $Q_\lambda = (F, +, \circ)$ is defined by taking $(F, +)$ as the additive group of the field F and $\circ$ is defined, in terms of field multiplication, so that for $x, f \in F$:

$$\begin{aligned} x \circ f &= x^{\lambda_f} f \quad f \neq 0 \\ x \circ 0 &= 0. \end{aligned}$$

So Q_λ obeys the right distributive law, has a multiplicative identity, has a unique solution for $\square \circ f = g$, whenever $f \neq 0$, and multiplying by zero yields zero. Hence, in the finite case, Q_λ is a quasifield iff the equation $f \circ \square = g$ has a unique solution for $\square$ when $f, g \in F^*$. For a treatment of the general case, including when K is a skewfield, see Lüneburg [31]. The system Q_λ is called a λ-system, or a generalized André system, *if turns out to be a quasifield*; the corresponding translation plane is called a generalized André plane.

We shall only consider finite generalized André planes here. An effective way to study them is to describe them in number-theoretic terms. We denote the set of the first k natural numbers $0, 1, \ldots, k-1$ by I_k.

Definition 9.1.1 *Let $F = GF(q^d) \supset K = GF(q)$, $n = q^d > q$, and let $\rho : x \mapsto x^q$ be the generator of $Gal(F/K)$. Choose a primitive generator ω of the multiplicative group F^*. Let $\lambda : i \mapsto \lambda_i$ be any map from I_{n-1} into I_d such that $\lambda_0 = 0$. Define $Q_\lambda := (F, +, \circ)$, where $+$ is field addition, and $\circ$ is given by:*

$$\omega^i \circ \omega^j := (\omega^i)^{q^{\lambda_j}} \omega^j = \omega^{iq^{\lambda_j}+j},$$

and $x \circ 0 = 0 = 0 \circ x$ for all $x \in F$. We regard Q_λ as the λ-structure associated with (λ, q, q^d).

We now consider which choices of λ make Q_λ a quasifield. As indicated above, Q_λ will be a quasifield provided the equation $f \circ \square = g$ has, for $f, g \in F^*$, a unique solution for $\square$, and by our finiteness hypothesis, this is equivalent to the the injectivity of all the maps $z \mapsto \phi \circ z$, for $\phi \in F^*$. However, this condition *fails* iff there exists $x, y \in I_n$, $x \not\equiv y \pmod{n}$, so wlog $\lambda_x \geq \lambda_y$, such that

$$\begin{aligned} & \exists f \in I_n : \omega^f \circ \omega^x = \omega^f \circ \omega^y \\ \iff & \exists f \in I_n : fq^{\lambda_x} + x \equiv fq^{\lambda_y} + y \pmod{n-1} \\ \iff & \exists f \in I_n : x - y \equiv f\left(q^{\lambda_x} - q^{\lambda_y}\right) \pmod{n-1}, \end{aligned}$$

so Q_λ fails to be a quasifield is equivalent, for $\lambda_x \geq \lambda_y$, to the following condition:

$$\iff \exists f \in I_n : x - y \equiv fq^{\lambda_y}\left(q^{\lambda_x - \lambda_y} - 1\right) \pmod{n-1}. \qquad (9.1)$$

But choosing $t = t_{(x,y)} = \gcd(\lambda_x - \lambda_y, d-1)$ in the above condition (9.1) above means that

$$\frac{x-y}{q^t-1} \equiv fq^{\lambda_y}\frac{q^{\lambda_x-\lambda_y}-1}{q^t-1} \pmod{\frac{q^d-1}{q^t-1}},$$

and now, since by an elementary result 8.4.1, page 147, we have

$$\gcd\left(q^{\lambda_y}\frac{q^{\lambda_x-\lambda_y}-1}{q^t-1}, \frac{q^d-1}{q^t-1}\right) = 1,$$

a solution for f in equation (9.1) exists iff $\frac{x-y}{q^t-1}$ is an integer, that is $x \equiv y \pmod{q^t-1}$. Thus, the condition that $z \mapsto \phi \circ z$ is injective for for all non-zero f, is equivalent to ensuring that $x \equiv y \pmod{q^t-1}$ cannot hold, unless $x \equiv y \pmod{n}$. Thus we have

Theorem 9.1.2 (Fundamental λ-Law.) *[12, Lemma 2.1] Let Q_λ be a λ-structure on $GF(q^d)$, defined in terms of the field automorphism $\rho : x \mapsto x^q$ of $GF(q^d)$, and the primitive element ω of order $n-1$, $n := q^d$. Assign to every two distinct integers $x, y \in I_n$:*

$$t_{x,y} := \gcd(\lambda_x - \lambda_y, d)$$

Then Q_λ is a quasifield iff:

$$x \equiv y \pmod{q^{t_{x,y}}-1} \Longrightarrow x \equiv y \pmod{n-1}.$$

In particular, if λ yields a quasifield for some choice of the primitive ω then it works for all choices of ω. However, changing ω, while holding λ fixed, will in general yield non-isomorphic quasifields.

The following exercise will be used in normalising λ-systems.

Exercise 9.1.3 *Suppose*

$$GF(q^d) \supset GF(q^s) \supset GF(q)$$

and let $\rho : x \mapsto x^q$ denote the primitive automorphism in $Gal(q^d/q)$. Then:

(1) s divides d;

(2) If $\rho^k \in Gal(q^d/q^s)$ then s divides k.

Proof: Part (1): the larger field is a vector space over the smaller field. Part (2): By Euclid algoritm $k = sx + y$, $0 \leq y < s$, so $\rho^k \in Gal(q^d/q^s)$ implies that ρ^y also lies in the same field, so y is a multiple of s, since the Frobenius automorphism for the field is ρ^s. Hence $y = 0$. ∎

Proposition 9.1.4 *Let $\lambda : I_{q^d-1} \to I_d$, q a prime-power, define the generalsied André system $Q_\lambda = (F, +, \circ)$ on $F = GF(q^d)$, based on the Frobenius automorphism $\rho : x \mapsto x^{q^d}$ and the primitive element $< \omega >$. Then:*

(1) $\Phi_\lambda := Fix\{\rho^{\lambda_i} \mid i \in I_{q^d-1}\}$, *is a subfield* $GF(q^s)$ *of* F *such that* s *divides* d *and also divides* λ_i, *for all* $i \in I_{q^d-1}$; *and*

(2) The function $\mu : I_{q^d-1} \to I_{\frac{d}{s}}$ *defined by* $\mu : i \mapsto \frac{\lambda_i}{s}$ *yields a* λ*-system* $Q_\mu = (F, +, *)$ *by:*

$$\omega^i * \omega^j = (\omega^i)^{R^\mu_j}\omega^j,$$

relative to ω *and* $R = \rho^S$, *the Frobenius automorphism of* $Gal(q^d/q^S)$.

Moreover, $\Phi_\mu := Fix\{\rho^{\mu_i} \mid i \in I_{q^d-1}\}$, *is the fixed field of the Frobenius automorphism* $R : x \mapsto x^{q^S}$ *defining* Q_μ *and* $(F, +, *) = (F, +, \circ)$.

Proof: In view of the previous exercise, it essentially remains to verify that the two products coincide:

$$\begin{aligned} \omega^i * \omega^j &= (\omega^i)^{R^\mu_j}\omega^j \\ &= (\omega^i)^{(\rho^S)^{(\lambda_j/S)}}\omega^j \\ &= (\omega^i)^{(\rho)^{(\lambda_j)}}\omega^j \\ &= \omega^i \circ \omega^j, \end{aligned}$$

as required. ■

Hence, any finite generalized André system may be expressed in the form $Q_\lambda = (F, +, \circ)$ where $\circ$ is determined by a λ-function $\lambda : I_{q^d-1} \to I_d$, associated with $GF(q^d)$, such that

$$\Phi_\lambda := Fix\{\rho^{\lambda_i} \mid i \in I_{q^d-1}\} = GF(q),$$

the fixed field of the Frobenius automorphism $\rho : x \mapsto x^q$ used in defining $\circ$ from λ.

Thus without loss of generality we assume that if $\lambda : I_{q^d-1} \to I_d$ defines a generalized Adré sysytem then the λ is chosen so that the fixed field of the group generted by $\left\{\rho^{\lambda_i} \mid : i \in I_{q^d-1}\right\}$ is just $GF(q)$, the fixed field of the Frobenius automorphism $x \mapsto x^d$.

9.2 No Shears In λ-Systems.

Proposition 9.2.1 *In the* λ*-system* Q_λ *suppose* $a, b, a+b \in Q^*_\lambda$ *and that for all* $c \in Q_\lambda$:

$$c \circ (a + b) = c \circ a + c \circ b.$$

Then $\lambda_a = \lambda_b$.

Proof: Solving for $\lambda_{(a+b)}$:

$$c\lambda_{(a+b)} = \frac{(c)\lambda_a a + (c)\lambda_b b}{(a+b)},$$

and writing $c = xy$ we get:

$$(xy)\lambda_{(a+b)} = \frac{(xy)\lambda_a a + (xy)\lambda_b b}{(a+b)},$$

and noting that all λ's are multiplicative bijections:

$$(x)\lambda_{(a+b)}(y)\lambda_{(a+b)} = \frac{(x)\lambda_a(y)\lambda_a a + (x)\lambda_b(y)\lambda_b b}{(a+b)},$$

and by the formula for $c\lambda(a+b)$:

$$\frac{(x)\lambda_a a + (x)\lambda_b b}{(a+b)}\frac{(y)\lambda_a a + (y)\lambda_b b}{(a+b)} = \frac{(x)\lambda_a(y)\lambda_a a + (x)\lambda_b(y)\lambda_b b}{(a+b)},$$

yielding:

$$(x)\lambda_{(a+b)}(y)\lambda_{(a+b)} = \frac{(x)\lambda_a(y)\lambda_a a + (x)\lambda_b(y)\lambda_b b}{(a+b)},$$

and by the formula for $c\lambda_{(a+b)}$:

$$\begin{aligned} ((x)\lambda_a a + (x)\lambda_b b)\,((y)\lambda_a a + (y)\lambda_b b) &= \\ (x)\lambda_a(y)\lambda_a a + (x)\lambda_b(y)\lambda_b b(a+b), & \\ \text{and expanding yields:} & \\ (x)\lambda_a(y)\lambda_a a^2 + (x)\lambda_b(y)\lambda_b b^2 + (x)\lambda_a(y)\lambda_b ab + (x)\lambda_b(y)\lambda_a ab &= \\ (x)\lambda_a(y)\lambda_a a(a+b) \;+\; (x)\lambda_b(y)\lambda_b b(a+b & \end{aligned}$$

yielding the field automorphism identity in x and y (zero values permitted):

$$(x)\lambda_a(y)\lambda_a + (x)\lambda_b(y)\lambda_b = (x)\lambda_a(y)\lambda_b + (x)\lambda_b(y)\lambda_a$$

and by Vaughan polynomials in two variables these additive identities cannot be equal unless $\lambda_a = \lambda_b$. ■

Corollary 9.2.2 *A finite generalized André system cannot be a semifield unless λ is identically zero, in which case it is just a field.*

Exercise 9.2.3 *Let $n = q^d$, q a prime power, and suppose $\lambda : I_{n-1} \to I_d$ be a map such that $\lambda_0 = 0$. Put $t_{xy} = \gcd(\lambda_x - \lambda_y, d)$, for $x, y \in I_n$. Assume λ is a λ-system in the sense that:*

$$x \equiv y \pmod{q^{t_{xy}} - 1} \Longrightarrow x \equiv y \pmod{q^d - 1}.$$

1. *The zero map is a λ-function, and the corresponding quasifield Q_λ is a field.*
2. *Find all the λ-systems when $d = 2$.*
3. *$t_{xy} = 1$ for all distinct $x, y \in I_n$ iff d is prime.*
4. *If d is prime then λ is constant on the additive cosets of the ideal of I_n generated by $q - 1$. Conversely, any function constant on the additive cosets of the principal ideal $I_{n-1}(q-1)$ is a λ function.*
5. *Show that, apart from fields, no quasifields Q_λ of order $n = 2^p$ can exist if p is prime.*
6. *If $i \equiv j \pmod{q^{t_{ij}} - 1}$ for distinct $i, j \in I_{n-1}$ then $\lambda_i = \lambda_j$.*

9.3 Cyclic Groups In λ-Sytems.

Proposition 9.3.1 (Period v_λ of a λ-system.) *Call the integer $k \in I_{n-1}$ a* scale *for a λ function iff:*

$$x \equiv y \pmod{k} \Longrightarrow \lambda_x = \lambda_y.$$

Then the set of scales may be expressed as an ideal $v_\lambda I_{n-1}$ of I_{n-1}, where the integer $v_\lambda | n - 1$. The integer $v := v_\lambda$ is called the **period** *of λ.*

Proof: If k is a scale then ka is a scale because $x \equiv y \pmod{ka}$ implies $x \equiv y \pmod{k}$. If m and k are scales we must show $m - k$, where $m \geq k$ wlog, is also a scale. Suppose $|x - y| = m - k$, and wlog $x = y + m - k$. Now $\lambda_y = \lambda_{y+m}$ because m is a scale, and $\lambda_{y+m} = \lambda_x$ because k is a scale. So $\lambda_x = \lambda_y$. Thus the scales form an additive subgroup of I_{n-1} and the rest follows because the integers form a principal ideal domain with I_{n-1} as an image. ∎

The $v_\lambda := v$ shows that Q_λ has a cyclic subgroup.

Corollary 9.3.2 *$< \omega^{v_\lambda} >$ is a cyclic subgroup of Q_λ with the same multiplication when the field multiplication on $< \omega >$ is restricted to $< \omega^{v_\lambda} >$.*

Proof: By scaling law:

$$\lambda_{va} = \lambda_v = \lambda_0 = 0.$$

■

The following implies a lower bound for the cyclic group associated with v, as defined above.

Proposition 9.3.3 *Let $u = \text{lcm}\{q^m - 1 \mid m|d, 0 < m < d\}$. Then v_λ divides u.*

Proof: We must show u is a scale: $x \equiv y \pmod{u}$ implies $\lambda_x = \lambda_y$. So assume $\lambda_x - \lambda_y \neq 0$, thus $t_{xy} = \gcd(\lambda_x - \lambda_y, d)$ is a non-zero divisor of d. If $x \equiv y \pmod{u}$, then every *non-zero* $q^{t_{ab}} - 1$, for distinct $a, b \in I_{n-1}$, divides u and hence also $x - y$. But for $a = x$, $b = y$ we now have $x \equiv y \pmod{q^{t_{xy}} - 1}$. Now by the definition of a λ-system, we have, see theorem 9.1.2, $\lambda_x = \lambda_y$. The contradiction yields the result.■

9.4 André Systems.

The following proposition introduces the original André systems in terms of generalized André systems.

Theorem 9.4.1 *Define the map*

$$\nu : I_{n-1} \to I_{q-1}$$
$$\nu(i) \equiv i \pmod{(q-1)}$$

and let $\mu : I_{q-1} \to I_d$ be an arbitrary map such that $\mu(0) = 0$. Then

1. *$\lambda = \mu\nu()$ is a λ-function defining a quasifield Q_λ called an André system. The v for an André system divides $q - 1$*

2. *Conversely, if a λ-system has v dividing $q - 1$ then it must be a generalized André system.*

3. *In any André system* $\lambda(x \circ y) = \lambda(xy)$. *Hence the system is nearfield iff* λ *is a homomorphism from* I_{n-1} *to* I_d.

Proof: If $i \equiv j \pmod{q^{t_{ij}} - 1}$ then certainly $i \equiv j \pmod{q-1}$ and this implies $\lambda_i = \lambda_j$, by the definition of ν and μ, and now $t_{ij} = d$ so $i \equiv j \pmod{q^d - 1}$, and hence $i = j$. Thus an André system is a quasifield. Also if $i \equiv j \pmod{q-1}$ then the defintion of an Andr'e system implies that $\lambda_i = \lambda_j$; but v is the least integer for which this holds. Thus v divides $q-1$. The converse follows because v dividing $q-1$ means that λ is constant on points differing by multiples of $q-1$: so choose μ to be the common value of such additive cosets of $< q-1 >$.
To check $\lambda(x \circ y) = \lambda(xy)$ in additive form we write $x = \omega^X$, $y = \omega^Y$ and now we need to show

$$\lambda(Xq^{\lambda_Y} + Y) \equiv \lambda(X + Y).$$

But $Xq^{\lambda_Y} + Y \equiv X + Y \pmod{q-1}$ certainly holds, because $q \equiv 1 \pmod{q-1}$, so the identity holds because the 'scale' v for λ divides $q-1$. ∎

9.5 Highest Prime-Power Divisors of $a-1$ Dividing $a^d - 1$.

Let u be a prime dividing $a-1$. The aim of this section is to consider the highest power of u that divides $a^n - 1$, where $n > 1$ is an integer. A lower bound follows by a simple induction:

Lemma 9.5.1 *If* u^A *divides* $a-1$ *and* u^B *divides* n *then* u^{A+B} *divides* $a^n - 1$.

Proof: Write $n = u^B\delta$, where $\gcd(u, \delta) = 1$. Apply induction on B. Since $(a-1)$ is a factor of $a^n - 1$ the desired result holds for $B = 0$. Assume $u^{A+B} \| a^n - 1$, when $B = b$. Then consider the next case $B = b+1$ using:

$$a^{u^{b+1}\delta} - 1 = (a^{u^b\delta} - 1) \sum_{i=0}^{u-1} a^{u^b\delta i},$$

and now by the inductive hypothesis the term $(a^{u^b\delta} - 1)$ is divisible by u^{A+B} and the summation is $\equiv u \pmod{u}$ since each of the u terms involved in it

are $\equiv 1 \pmod{u}$. Thus the lhs is divisible by u^{A+B}, when $B = b+1$. The desired conclusion follows. ∎
In the somewhat vacuous case, when $\gcd(n,u) = 1$, the lower bound above implies an exact value for the highest power of u dividing $a^n - 1$:

Corollary 9.5.2 *Suppose u is a prime divisor of $a-1$ such that $u^\alpha \| a-1$ and $u^\beta \| n$. Then: $u^{\alpha+\beta} | a^n - 1$, and if $\beta = 0$ then $u^{\alpha+\beta} \| a^n - 1$.*

We adopt the hypothesis of the corollary for the rest of the section; $u^r \| R$ means u^r is the highest power of the prime u dividing the integer R.

Our principal aim is to show that the corollary 9.5.2 holds in the general case when $u^\alpha > 2$ and β is arbitrary: thus the exact value of the highest power of u dividing $a^n - 1$ is the lower bound given in the corollary, unless $2 \| a-1$, in which case the lower bound $u^{\alpha+\beta}$ is *not* sharp for $\beta > 0$. We verify this first.

Remark 9.5.3 *Suppose $2 \| a-1$, and write $n = 2^\beta \delta$, so δ is odd. Then, for $\beta \geq 1$:*

$$a^n - 1 \equiv 0 \pmod{2^{\beta+2}}.$$

Proof: If $\beta = 1$ then

$$a^n - 1 = (a^{d/2} - 1)(a^{n/2} + 1) \equiv 0 \pmod{8},$$

as required. The general case follows by induction on β: assume the result holds when $2^\beta \| n$, and consider the next case where $n = 2^{2^{\beta+1}\delta}$, δ odd.

$$a^{2^{\beta+1}\delta} - 1 = \left(a^{2^\beta \delta} - 1\right)\left(a^{2^\beta \delta} + 1\right) \equiv 0 \pmod{2^{\beta+2}2},$$

by the inductive hypothesis, so the desired result follows. ∎
Thus, the remark asserts that if $u = 2$ and $\alpha = 1$ then $u^{\alpha+\beta+1}$ divides $a^n - 1$, where $u^\beta \| n$. The rest of the section is concerned with showing that this does not happen in any other case, that is, we shall establish that:

$$u^{\alpha+\beta} \| a^n - 1 \Rightarrow u^\alpha = 2,$$

and this situation has been considered in remark 9.5.3 above.

We begin by noting that in all cases it is justifiable to assume $n = u^\beta$ whenever convenient:

Remark 9.5.4 *When $u^\beta \| n$ then $u^A \| a^n - 1$ iff $u^A \| a^{u^\beta} - 1$.*

Proof: Defining m so that $n = u^\beta m$, we have $\gcd(u, m) = 1$, and hence also

$$a^n - 1 = (a^{u^\beta} - 1) \sum_{i=0}^{m-1} a^{u^\beta i},$$

and since $a \equiv 1 \pmod{u}$ we now have

$$a^n - 1 = (a^{u^\beta} - 1)m,$$

yielding the desired result, since $\gcd(u, m) = 1$. ∎
So to determine when $u^{\alpha+\beta} \| a^n - 1$, we need to consider its negation, the following condition:

$$u^{\alpha+\beta+1} | a^{u^\beta} - 1. \tag{9.2}$$

As mentioned earlier, the condition cannot hold when $\beta = 0$. Thus if the condition (9.2) ever holds, for some u^α, then there is a maximum integer $b \geq 1$ such that condition (9.2) fails for $\beta := b$ but holds for $\beta = b + 1$. We have seen already, in remark 9.5.3, that if $u^\alpha = 2$ then $b = 1$ can be chosen, and condition (9.2) holds for $\beta \geq 1$. In order to show that condition (9.2) does not hold in any other circumstance we essentially need to establish if it fails for a given β (which it always does when $\beta = 0$) then it cannot hold for the next β, unless, as we have seen, $u^\alpha = 2$.

Lemma 9.5.5 *Suppose that there is an integer $\beta \geq 0$ such that:*

$$a^{u^\beta} - 1 \not\equiv 0 \pmod{u^{\alpha+\beta+1}}. \tag{9.3}$$

$$a^{u^{\beta+1}} - 1 \equiv 0 \pmod{u^{\alpha+\beta+2}} \tag{9.4}$$

Then $\beta = 0$ and $u^\alpha = 2$.

Proof: Writing

$$a^{u^{\beta+1}} - 1 = \left(a^{u^\beta} - 1\right) \left(\sum_{i=0}^{u-1} a^{u^\beta i} \right),$$

we have by condition (9.4):

$$\left(a^{u^\beta} - 1\right) \left(\sum_{i=0}^{u-1} a^{u^\beta i} \right) \equiv 0 \pmod{u^{\alpha+\beta+2}}$$

and since by lemma 9.5.1 and condition (9.3)

$$u^{\alpha+\beta} \| a^{u^\beta} - 1,$$

we now have

$$\sum_{i=0}^{u-1} a^{u^\beta i} \equiv 0 \pmod{u^2} \tag{9.5}$$

and we also have from lemma 9.5.1 that for each i:

$$a^{u^\beta i} \equiv 1 \pmod{u^{\alpha+\beta}}, \tag{9.6}$$

and in particular:

$$\text{If } \alpha+\beta \geq 2 \text{ then: } a^{u^\beta i} \equiv 1 \pmod{u^2} \tag{9.7}$$

which combines with (9.5) to yield:

$$\text{If } \alpha+\beta \geq 2 \text{ then: } u \equiv 0 \pmod{u^2}, \tag{9.8}$$

which is a contradiction, unless $\alpha+\beta \leq 1$.
But since hypothesis $u|a-1$, we must now have $\alpha = 1$ and $\beta = 0$, and condition (9.3) holds, as remarked earlier. In view of our hypothesis that $u^\alpha > 2$ we now also have:

$$u^\alpha = u \text{ is an odd prime divisor of } a-1 \tag{9.9}$$

Moreover, the condition (9.4) reduces to

$$a^u - 1 \equiv 0 \pmod{u^3}. \tag{9.10}$$

and on applying (9.9) this yields

$$\sum_{i=0}^{u-1} a^i \equiv 0 \pmod{u^2}. \tag{9.11}$$

Moreover,

$$\begin{aligned} \sum_{i=0}^{u-1} a^i &= u + \sum_{i=1}^{u-1} (a^i - 1) \\ &= u + (a-1) \sum_{i=1}^{u-1} \sum_{j=1}^{i-1} a^j, \end{aligned}$$

and since $a-1 \equiv 0 \pmod{u}$ and $a^j \equiv 1 \pmod{u}$ we also have $(a-1)a^j \equiv (a-1)1 \pmod{u^2}$. Thus

$$\begin{aligned}\sum_{i=0}^{u-1} a^i &\equiv u + \sum_{i=1}^{u-1} i \pmod{u^2}, \\ &\equiv u + (a-1)\frac{u(u-1)}{2} \pmod{u^2}\end{aligned}$$

and since the LHS $\equiv 0 \pmod{u^2}$, by eqn (9.11), we now have:

$$1 + \frac{(a-1)(u-1)}{2} \pmod{u},$$

but since the prime u is an odd divisor $a-1$ we have a contradiction. ∎
Combining lemma 9.5.5 with remark 9.5.3 yields, for $u^\alpha > 2$, $u^{\alpha+\beta}$ is the highest power of u dividing $a^n - 1$

Theorem 9.5.6 *Suppose $a > 1$ and $n \geq 1$ are integers and u is a prime divisor of $a-1$ such that $u^\alpha \| a-1$ and $u^\beta \| n$.*

1. *If $u^\alpha > 2$ or $\beta = 0$ then*
$$u^{\alpha+\beta} \| a^n - 1.$$

2. *If $u^\alpha = 2$ and $\beta \geq 1$ then*
$$u^{\alpha+\beta+1} | a^n - 1.$$

Our next objective is to apply the theorem above to show that under its hypothesis $a^k - 1/a - 1$ ranges over all residues mod$N$, as k varies. This is crucial in defining the Dickson nearfields.

Lemma 9.5.7 *Let $a > 1$ and $N > 1$ be integers such that:*

1. *every prime divisor of N divides $a-1$; and*

2. *if $a \equiv 3 \pmod 4$ then $N \not\equiv 0 \pmod 4$.*

Then $a^N - 1 \not\equiv 0 \pmod{N(a-1)}$ for $1 \leq n < N$.

Proof: To obtain a contradiction assume that for some $n \in [1, N-1]$:

$$a^n - 1 \equiv 0 \pmod{N(a-1)}. \tag{9.1}$$

Since $n < N$, there is at least one prime divisor u of N such that for some integer $b \geq 0$, $u^b \| n$ and $u^{b+1} | N$. By theorem 9.5.6, $a^n - 1$ is divisible by $u^{\alpha+\beta}$, and this is the highest power of u dividing $a^n - 1$, unless $u^\alpha = 2$. So for $u^\alpha > 2$, $u^{\alpha+b} \| a^n - 1$, contrary to eqn (9.1). Thus we may further assume that $u^\alpha = 2$, So 2^{b+1} divides N, and this contradicts our hypothesis that $N \not\equiv 0 \pmod 4$, when $2 \| a - 1$, unless $b = 0$. But in this case theorem 9.5.6 still implies $u^{\alpha+b} \| a^n - 1$, again contradicting eqn (9.1). ∎
We now obtain the desired result, that $a^k - 1/a - 1$ ranges over the residues mod$n$ as k ranges over $1 \ldots n$.

Proposition 9.5.8 *Let $a > 1$ and $n > 1$ be integers such that:*

1. *every prime divisor of n divides $a - 1$; and*
2. *if $a \equiv 3 \pmod 4$ then $n \not\equiv 0 \pmod 4$.*

Then the n distinct integers:

$$1, \frac{a^2-1}{a-1}, \frac{a^3-1}{a-1}, \ldots, \frac{a^n-1}{a-1},$$

constitute a complete set of n residues mod$n$. *In particular, $a^n - 1/a - 1 \equiv 0 \pmod n$.*

Proof: The difference of two distinct terms of the above list, associated with $i > j$, yields:

$$\begin{aligned} \frac{a^i-1}{a-1} &\equiv \frac{a^j-1}{a-1} \pmod n \\ \Rightarrow a^j \frac{a^{i-j}-1}{a-1} &\equiv 0 \pmod n \\ \Rightarrow \frac{a^{i-j}-1}{a-1} &\equiv 0 \pmod n, \end{aligned}$$

contradicting lemma 9.5.7. Thus each of the n listed terms is a distinct residue mod$n$. Moreover, $a^n - 1/a - 1 \equiv 0 \pmod n$ follows directly from theorem 9.5.6. ∎

9.6 Dickson Nearfields.

Let $F = GF(q^n)$, and assume (q, n) is a Dickson pair: so the prime divisors of n divide $q-1$, and if $q \equiv 3 \pmod 4$ then $n \not\equiv 0 \pmod 4$.

Hence $(q^n-1)/n$ is an integer because the maximum prime-power divisors of n divide $q^n - 1$. So the cyclic group F^* has a unique subgroup N of order $q^n - 1/n$, and on applying proposition 9.5.8, to the cyclic group F^*/N^* of order n, we may write F^* as a union of cosets of N in the form:

$$F^* = \theta N \bigcup \theta^{\frac{q^2-1}{q-1}} N \bigcup \theta^{\frac{q^3-1}{q-1}} N \bigcup \ldots \bigcup \theta^{\frac{q^n-1}{q-1}} N,$$

where $\theta \in F^* - N$ is such that θN generates the cyclic group F^*/N.

Lemma 9.6.1 *Suppose $b, c \in F^*$ are given by:*

$$\begin{aligned} b &= \theta^{\frac{q^\beta-1}{q-1}} y, \exists y \in N; \\ c &= \theta^{\frac{q^\gamma-1}{q-1}} z, \exists z \in N. \end{aligned}$$

Then

$$b^{q^\gamma} c \in \theta^{\frac{q^{(\beta+\gamma) \bmod n}-1}{q-1}} N.$$

Proof:

$$\begin{aligned} b^{q^\gamma} c &= (\theta^{\frac{q^\beta-1}{q-1}} y)^{q^\gamma} \theta^{\frac{q^\gamma-1}{q-1}} z \\ &= \theta^{\frac{q^{\beta+\gamma}-q^\gamma}{q-1}} y^{q^\gamma} \theta^{\frac{q^\gamma-1}{q-1}} z \\ &= \theta^{\frac{q^{\beta+\gamma}-q^\gamma+q^\gamma-1}{q-1}} y^{q^\gamma} z, \\ &\in \theta^{\frac{q^{\beta+\gamma}-1}{q-1}} N, \text{ by invariance of } N \text{ under group homomorphisms,} \\ &= \theta^{\frac{q^{(\beta+\gamma) \bmod n}-1}{q-1}} N, \end{aligned}$$

the desired result. ∎

Definition 9.6.2 (Dickson Nearfields.) *Let (q, n) be a Dickson pair. Then for $m \in \theta^{\frac{q^i-1}{q-1}} N$, define the field automorphism $\lambda(x) \in \mathrm{Gal}(GF(q^n)/GF(q)$ by:*

$$\lambda(m) : x \mapsto x^{q^i},\ i \in \{1, 2 \ldots, n\},$$

and the product $(F, \circ)$, $f = GF(q^n)$, *by* $x \circ 0 = 0$, *for* $x \in F$ *and:*

$$x \circ m = \begin{cases} x^{\lambda(m)}m & \text{if } m \in F^* \\ 0 & \text{if } m = 0 \end{cases}$$

We call all any such $(F, +, \circ)$ *a Dickson nearfield, associated with* λ *and* θ.

It is a tautology to claim that any Dickson nearfield is a generalized André plane. However, we have yet to establish that $(F, +, \circ)$ is always a nearfield. This is our goal for the rest of the section, so we assume the notation of definition 9.6.2. To establish that the product $\circ$ yields a quasifield essentially involves showing that 'slopemaps' of the non-identity elements of F^*, relative to $\circ$, are semiregular on F^*.

Lemma 9.6.3 *Suppose:* $x \circ m = x$ *for some* $x, m \in F^*$. *Then* $m = 1$.

Proof: Suppose $x \circ m = x$. Writing $x = \theta^{\frac{q^j-1}{q-1}}$ and $y = \theta^{\frac{q^i-1}{q-1}}$, where $i, j \in [1, n]$, we have

$$\begin{aligned} \left(\theta^{\frac{q^j-1}{q-1}}\right)^{q^i} \theta^{\frac{q^i-1}{q-1}} &\equiv \theta^{\frac{q^j-1}{q-1}} \pmod N, \\ \text{so } \theta^{\frac{q^{j+i}-1}{q-1}} &\equiv \theta^{\frac{q^j-1}{q-1}} \pmod N, \\ \text{so } \theta^{\frac{q^{j+i}-q^j}{q-1}} &\in N, \\ \text{so } \left(\theta^{\frac{q^i-1}{q-1}}\right)^{q^j} &\in N, \\ \text{so } \theta^{\frac{q^i-1}{q-1}} &\in N, \end{aligned}$$

yielding $i = n$. So $1 = x \circ m = xm$, and we have $m = 1$ as required. ∎

To show that $(F^*, \circ)$ is a group we first note that it is an associative binary system with identity. The proof depends on extensive tacit use of the 'product' computed in lemma 9.6.1.

Lemma 9.6.4 $(F^*, \circ)$ *is an associative binary system with identity* $1 \in F$.

Proof: Since $a \circ b \in F^*$ whenever $a, b \in F^*$ we have a binary system, and the multiplicative identity of F^* is the identity for $(F^*, \circ)$ by the definition of $\circ$. To show $\circ$ is associative, we represent $x, y, z \in F^*$ in the form:

$$\begin{aligned} x &= \theta^{\frac{q^a-1}{q-1}} n_y, \exists n_x \in N; \\ y &= \theta^{\frac{q^b-1}{q-1}} n_y, \exists n_y \in N; \\ z &= \theta^{\frac{q^c-1}{q-1}} n_z, \exists n_z \in N, \end{aligned}$$

where $a, b, c \in \{1 \ldots, n\}$. Applying lemma 9.6.1 repeatedly to the definition of $\circ$, we have

$$\begin{aligned} x \circ (y \circ z) &= \left(\theta^{\frac{q^a-1}{q-1}} n_x\right) \circ (y \circ z) \\ &= \left(\theta^{\frac{q^a-1}{q-1}} n_x\right)^{q^{(b+c) \bmod n}} \theta^{\frac{q^{(b+c) \bmod n}-1}{q-1}} n_y^{q^c} n_z \\ &= \theta^{\frac{q^{(a+b+c) \bmod n}-q^{(b+c) \bmod n}}{q-1}} \theta^{\frac{q^{(b+c) \bmod n}-1}{q-1}} n_x^{q^{(b+c) \bmod n}} n_y^{q^c} n_z \\ &= \frac{\theta^{q^{(a+b+c) \bmod n}-1}}{q-1} n_x^{q^{(b+c) \bmod n}} n_y^{q^c} n_z, \end{aligned}$$

and similarly:

$$\begin{aligned} (x \circ y) \circ z &= \left(\theta^{\frac{q^{(a+b) \bmod n}-1}{q-1}} n_x^{q^b} n_y\right) \circ z \\ &= \left(\theta^{\frac{q^{(a+b) \bmod n}-1}{q-1}} n_x^{q^b} n_y\right) \circ \theta^{\frac{q^c-1}{q-1}} n_z \\ &= \left(\theta^{\frac{q^{(a+b) \bmod n}-1}{q-1}} n_x^{q^b} n_y\right)^{q^c} \theta^{\frac{q^c-1}{q-1}} n_z \\ &= \left(\theta^{\frac{q^{(a+b+c) \bmod n}-q^c}{q-1}} n_x^{q^{(b+c) \bmod n}} n_y^{q^c}\right) \theta^{\frac{q^c-1}{q-1}} n_z \\ &= \theta^{\frac{q^{(a+b+c) \bmod n}-1}{q-1}} n_x^{q^b+q^c} n_y^{q^c} n_z, \end{aligned}$$

and the associativity of $\circ$ follows on comparing the values of $(x \circ y) \circ z$ and $x \circ (y \circ z)$ obtained above. ∎

The maps $T_m : x \mapsto x \circ m$, for $m \in F^*$, are obviously in $GL(F, +)$ and lemma 9.6.4 above implies that such maps are closed under composition, thus:

$$\tau = \{T_m : x \mapsto x \circ m \in GL(F, +) \mid m \in F^*\}$$

is a subgroup of $GL(F, +)$, and by lemma 9.6.3 every T_m, $m \in F^* - \{1\}$, is semiregular on F^*. This forces the difference between any two distinct members of τ to be a non-singular map of $(F, +)$, since otherwise a non-identity element of τ would fix some element of F^*. Thus τ together with the zeromap forms a spreadset that is multiplicatively closed. Now by this alone (or alternatively by lemma 9.6.4 above) $(F, +, \circ)$ is a nearfield. Thus we have established:

Theorem 9.6.5 *Given a Dickson pair (q, n) and $(F, +, \circ)$ be as in definition 9.6.2. Then $(F, +, \circ)$ is a generalized André system relative to the given λ that is associative. Such generalized André systems are called Dickson nearfields.*

Chapter 10

Large Planar Groups.

The aim of this chapter is to consider large planar groups acting on translation planes, or what amounts to the same thing, to consider quasifields that admit large automorphism groups, in one sense or another. The emphasis here is strongly on the finite case. We shall describe all the finite quasifields amitting maximal automorphism groups: those admitting automorphism groups that act transitively on their non-fixed points. We also treat comprehensively the structure of a Baer group and obtain a sharp upper bound for the size of a planar p-group of a finite translation plane of characteristic p.

10.1 Planar and Automorphism Groups.

In this section we make some general remarks concerning planar collineation groups of arbitrary [affine or projective] planes, and their identification with the automorphism groups of planar ternary rings coordinatizing the planes. Our interest is in the case where the planes are translation planes, but the arguments in the general case is exactly the same. The material covered here will be taken for granted in the sequel.

Let G be a planar group acting on a plane π, and let π_G be the fixed plane of G. Now G may be identified with an automorphism group $\hat{P}$ of any planar ternary ring Q obtained when π is coordinatized with the axis chosen in π_G. Thus π_G is coordinatized by a subplanar ternary ring R of Q, and the elements $g \in G$ are of form

$$g : (x, y) \mapsto \left(x^{\hat{g}}, x^{\hat{g}}\right),$$

for some $\hat{g} \in (AutQ)_R$. So the map $g \mapsto \hat{g}$ is a faithful permutation representation of G into $(AutQ)_R$, and this representation is permutation-isomorphic to the G-representation $G \to G^\ell$ obtained by restricting G to its action on any line ℓ that it leaves invariant. Conversely any subgroup $J \leq (AutQ)_R$ is of form $J = \hat{G}$ for some subgroup $G \leq Aut\pi$, obviously

$$G = \left\{ g : (x,y) \mapsto \left(x^{\hat{g}}, x^{\hat{g}}\right) \mid \hat{g} \in J \right\},$$

and the fixed plane of G is just $\pi(J)$.

Hence any planar group G of a plane π, with fixed plane π_G, has a faithful representation ρ in $(AutQ)_R$, where Q is a planar ternary ring obtained when π is coordinatized by choosing axes in π_0, and R is the subternary ring coordinatizing π_G. The representation ρ may be chosen so that if H is a subgroup of G then $Fix(\rho(H)) = Q_H$ is the subternary of Q such that π_H is coordinatized by Q_H and $\rho(H) = (AutQ)_{Q_H}$.

Our interest is the case *when π is an affine translation plane and G is a planar group*, fixing the line at infinity. So π_G is a subaffine translation plane of π, and π may be coordinatized by a quasifield Q such that π_G is coordinatized by a subquasifield R, and the restriction representation of G on any component that it fixes is permutation isomorphic to the standard representation of G in $(AutQ)_R$, indicated above.

However, an additional tool is available in the case of translation planes: G and all its subgroups are linear over the kern field $F = R \cap K$, where $K = kern(Q)$. For example F may always be chosen to be the prime subfield in Q. Note that the choice of F may sometimes be more general than any type of kern field. The main examples arise when Q is a left or right vector space over a subfield F, relative to the quasifield operations. Such F can occur, for example, when Q is a semifield and F is some subfield not contained in the kern, or whenever $\pi(F)$ defines a rational Desarguesian partial spread of a translation plane $\pi(Q)$. In all these cases, not only G is F-linear, but the Baer condition provides a useful constraint:
If $(Q \geq A > B$ form a chain of quasifields that are also F-spaces then $2a \leq b$, where a and b are the dimensions of A and B treated as F-spaces.
However, all this easily generalizes to arbitrary finite planar ternary rings and finite planes. But translation planes admit further constraints when G is a Baer group and π_G is any Baer subplane. Roughly, we shall show in the next section that this means that when G gets 'large' π_G is forced to be Desarguesian. This leads to a sharp upper bound for arbitrary planar p-groups acting on arbitrary finite translation planes with the same characteristic.

10.2 Baer Collineation Theory.

Let $G \leq (AutQ)_F$ be an automorphism group of a *finite* quasifield Q of order q^2 and characteristic p that fixes the Baer subquasifield F *elementwise.* We consider the structure of G, and its influence on the structure of F. Throughout the section, $B = (B_0, B_1)$ is any basis of Q relative to any *kern* field $K \subset F$ such that B_0 is a basis of F; so K can always be taken to be the prime subfield of Q. Now for each $f \in F$ its slope map T_f leaves F invariant and in fact T_f^F represents the slope map of $f \in F$, regarded as a member of the subquasifield F. Thus on any basis of type B, T_f has matrix form given by:

$$T_f = \begin{pmatrix} M_f & \mathbf{O} \\ A_f & B_f \end{pmatrix}, f \in F,$$

where M_f is the matrix of the slopemap T_f^F. Now, on the *same basis*, $g \in G$ has matrix form

$$g = \begin{pmatrix} \mathbf{1} & \mathbf{O} \\ U_g & W_g \end{pmatrix}, g \in G$$

But since for $g \in G$ and $f \in F$ we have

$$(x \circ f)g = (x)g \circ (f)g = (x)g \circ f \Longrightarrow T_f g = g T_f,$$

which in matrix form may be written:

$$\forall f \in F, g \in G : T_f = \begin{pmatrix} M_f & \mathbf{O} \\ A_f & B_f \end{pmatrix} \begin{pmatrix} \mathbf{1} & \mathbf{O} \\ U_g & W_g \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{O} \\ U_g & W_g \end{pmatrix} \begin{pmatrix} M_f & \mathbf{O} \\ A_f & B_f \end{pmatrix},$$

yielding

$$\forall f \in F, g \in G : \begin{pmatrix} M_f & \mathbf{O} \\ A_f + B_f U_g & B_f W_g \end{pmatrix} = \begin{pmatrix} M_f & \mathbf{O} \\ U_g M_f + W_g A_f & W_g B_f \end{pmatrix}. \tag{10.1}$$

Moreover, since $\{T_f \mid f \in F\}$ is a set of matrices any two distinct members of which differ by a non-singular matrix, the same applies to the B_f's and the number of these present is sufficient to form a spreadset (which clearly includes the identity), and so position $(2,2)$ in the above matrix equation shows that W_g is in the kern of a spreadset B_f with identity, In particular:

Remark 10.2.1 *$\{W_g \mid g \in G\}$ form a multiplicative group in a field of matrices. Moreover, if $|\{W_g \mid g \in G\}| > \sqrt{|F|}$, then*

$$\{B_f \mid f \in F\}$$

is a field.

Next consider the possibility of a p-element $\rho \in G$, p being the characteristic of the quasifield. So ρ has only one eigenvalue in the algebraic closure of the prime field, *viz.* 1, since $\lambda^{p^i} = 1 \Rightarrow \lambda = 1$, so ρ must act trivially on the factor space Q/F, regarding Q and F as additive groups. Thus its matrix is of form:

$$\rho = \begin{pmatrix} \mathbf{1} & \mathbf{O} \\ U_g & \mathbf{1} \end{pmatrix}$$

and by the eqn (10.1) we further have:

$$B_f U_g = U_g M_f, f \forall f \in F,$$

and since U_g intertwines two sets of irreducible matrices it must be in a field and hence non-singular. Thus we have shown:

Proposition 10.2.2 *$(AutQ)_F$ has a unique p-Sylow subgroup P, and this is elementary abelian of form:*

$$\left\{ \begin{pmatrix} \mathbf{1} & \mathbf{O} \\ U & \mathbf{1} \end{pmatrix} \mid f \in J \mid U \in J \right\} \tag{10.2}$$

where J is an additive group of matrices that is a subgroup of a field of matrices.

Moreover any $\rho \neq 1$, in the p-Sylow subgroup, can be expressed in the form where $U = \mathbf{1}$, provided the basis $B = (B_0, B_1)$ is modified to another basis $B' = (B_0', B_1)$, without altering B_1 the basis of the *complement* F, but replacing the basis B_0 of F by a possibly different basis B_0' of F. To see this, note that the matrix for ρ on the new basis is obtained by conjugating its given matrix by a matrix of type $Diag(C, \mathbf{1})$: thus we require non-singular C such that

$$Diag(C, \mathbf{1}) \begin{pmatrix} \mathbf{1} & \mathbf{O} \\ U & \mathbf{1} \end{pmatrix} Diag(C^{-1}, \mathbf{1}) = \begin{pmatrix} \mathbf{1} & \mathbf{O} \\ \mathbf{1} & \mathbf{1} \end{pmatrix}$$

and this works using $C = U^{-1}$.

Now return to the fundamental equation when B_2 is modified to ensure that the p-elements include the matrix

$$\begin{pmatrix} \mathbf{1} & \mathbf{O} \\ \mathbf{1} & \mathbf{1} \end{pmatrix}$$

Feeding this into the fundamental equation shows that $B_f = M_f$ for all $f \in F$. Thus we have shown:

Proposition 10.2.3 *Suppose $(AutQ)_F$ includes a non-trivial p-element ρ. Then relative to a basis $B = (B_0, B_1)$, with B_0 chosen to be an arbitrary basis of F, and appropriate B_1, the following holds:*

1. *ρ has the form*
$$\begin{pmatrix} \mathbf{1} & \mathbf{O} \\ \mathbf{1} & \mathbf{1} \end{pmatrix};$$
2. *$B_f = M_f$ for all $f \in F$;*
3. *The $\{U_g \mid g \in G\}$ forms an additive subgroup in the matrix field associated with the outer kern of $\{M_f \mid f \in F\}$.*
In particular, if the p-Sylow subgroup in $(AutQ)_F$ has order $> \sqrt{|F|}$ then F is a field.

Now consider the group homomorphism $\nu : g \mapsto W_g$; the kernel H of ν consists of all members in G that has $W_g = \mathbf{1}$, and this we have seen is simply the unique Sylow p-subgroup of G and so the image is a p-complement.So by Maschke's theorem a p-complement of F relative to H may be chosen and on that basis H has the form $Diag(M_f, B_f)$, with all the W_f's in the kern of the spreadset $\{B_f \mid f \in F\}$. In particular W_f's form a cyclic group so G is solvable and contains a Hall p' subgroup which is cyclic, and when this group has order $> \sqrt{|F|}$ then $\{B_f \mid f \in F\}$ is a field, and as we've seen above, this means that $\{M_f \mid f \in F\}$, and hence F also is a field provided a non-trivial p-element exists in G. We may summarize this as follows, in terms of the related translation plane.

Theorem 10.2.4 *Let π be a translation plane of order q^2, q a power of the prime p. Let G be a Baer group, so its fixed plane π_G has order q. Then G divides $q(q-1)$ and satisfies the following conditions:*

1. *G is solvable with a unique elementary abelian Sylow p-subgroup P, consisting of all the p-elements in G.*
2. *The kern of π_G has an additive subgroup isomorphic to P; so π_G is Desarguesian if $P > \sqrt{q}$.*
3. *The Hall p'-subgroups of G are cyclic and isomorphic to the multiplicative subgroups of the kern of π_G.*

Further properties are developed in the exercises below, based mainly on the discussion preceeding the theorem above. These exercises are of paramount importance in the study of translation planes!

Exercise 10.2.5 *Suppose G contains non-trivial p-elements and also a non-trivial p'-group of order $> \sqrt{|F|}$.*

1. *Relative to some basis the matrices T_f are of form:*

$$\{Diag(k, k^\sigma) \mid wherek \in K\},$$

where K is a field of matrices and σ is a field automorphism of K.

2. *Q is a vector space over F under quasifield automorphisms, F acting from the right.*

3. *The slopes of $\pi(F)$ in $\pi(Q)$ defines a derivable net.*

4. *If a Desarguesian Baer subplane ψ of a translation plane π of order q^2 is fixed elementwise by an element u such that $\gcd(u,p) = 1$, p is the characteristic, then the slopes of ψ define a derivable net in π.*

In the next lecture we shall obtain an upper bound for planar p-groups acting on translation planes. Our arguments crucially depend on a result that we establsihed in the present lecture: *large* Baer groups G have *Desarguesian* fixed plane π_G. Since no version of this result is known that applies to planes that are not translation planes (up to duality), the results of the following section are only known to hold for translation planes.

10.3 Planar p-Groups.

In this section Q is a finite quasifield with characteristic p, admitting an automorphism group P. Let $Fix(P) := F$; so F is a subquasifield of P, and $|Q| \geq |F|^2$, or P is trivial. Assume P is linear map of Q when this is viewed as a vector space over some field K, over which Q is known to be a vector space. So we may choose $K = GF(p)$, or, more generally, K may be taken to be any field contained in $F \cap Kern(Q)$, but it will prove useful to permit yet further possibilities for F: the most important case occurs when $\pi(F)$ contains a subplane that defines a rational Desarguesian partial spread in

the spread associated with Q. We shall write f to denote the dimension of F over K: thus $|F| = q^f$.

In all cases, P leaves invariant a $GF(p)$-space $A \supset P$ such that $|A| = p|F|$: regard Q as a $GF(p)$ vector space and note that the number of rank-one extensions of a subspace of any subspace of a finite characteristic p vector space is $\equiv 1 \pmod{p}$. Now the restriction representation $\rho : P \to P^A$ acts semiregularly on the $|A - P| = p|F| - |F|$ points of $A - F$, and let $\partial_A P$ denote the kernel of ρ. Thus $|\partial_A P|| \geq q^f$. For the fixed-quasifield of $\partial_A P$, we use he notation:

$$\partial_A F := Fix(\partial_A P),$$

and observe that the Baer condition for subplanes, when applied to non-trivial P, implies that

$$|\partial_A F| \geq q^{2f} \geq |F|^2.$$

Thus we have established:

Remark 10.3.1 *For all rank-one $GF(p)$-extensions A of F in Q:*

1. $|\partial_A P|| \geq q^f$;
2. $|\partial_A F| \geq q^{2f} \geq |F|^2$.

Note that $\partial_A P$ and $\partial_A F$ might vary with the choice of A, we shall only require the inequalities to hold; accordingly we simplify our notation by writing:

Notation 10.3.2 *If P is a non-trivial p-group in $AutQ$ with fixed subquasifield F then choose some P-invariant $GF(p)$-space $A \supset F$, where $|A|/|P| = p$ and define:*

1. $\partial P := \partial_A P$.
2. $\partial P := \partial_A P$.
3. $\partial^{k+1} P = \partial \partial^k P$ *and* $\partial^{k+1} F = \partial \partial^k F$ *whenever* $\partial^k P$ *is non-trivial.*

By repeatedly applying remark 10.3.1:

$$\begin{aligned} |\partial P| &\geq |P|/q^f \\ \text{and } |\partial F| &= q^{2f+d_1} \exists d_1 \geq 0 \\ \text{so} & \\ |\partial^2 P| &\geq |P|/q^f q^{2f+d_1} \end{aligned}$$

$$\begin{aligned}
\text{and } |\partial^2 F| &= q^{2^2 f+2d_1+d_2}\exists d_2 \geq 0 \\
&\text{so} \\
|\partial^3 P| &\geq |P|/q^f q^{2f+d_1} q^{2^2 f+2d_1+d_2} \\
\text{and } |\partial^3 F| &= q^{2^3 f+2^2 d_1+2d_2+d_3}\exists d_3 \geq 0 \\
&\text{so} \\
|\partial^4 P| &\geq |P|/q^f q^{2f+d_1} q^{2^2 f+2d_1+d_2} q^{2^3 f+2^2 d_1+2d_2+d_3} \\
\text{and } |\partial^4 F| &= q^{2^4 f+2^3 d_1+2^2 d_2+2d_3+d_4}\exists d_4 \geq 0,
\end{aligned}$$

and in general:

$$\begin{aligned}
|\partial^{k+1} P| &\geq |P|/q^f q^{2f+d_1} q^{2^2 f+2d_1+d_2} q^{2^3 f+2^2 d_1+2d_2+d_3} \ldots q^{2^k f+2^{k-1}d_1+2^{k-2}d_2+\ldots} \\
\text{and } |\partial^{k+1} F| &= q^{2^{k+1} f+2^k d_1+2^{k-1}d_2+\ldots+d_{k+1}}\exists d_{k+1} \geq 0,
\end{aligned}$$

provided $\partial^k P$ is non-trivial. We rewrite these as:

$$\begin{aligned}
|\partial^{k+1} P| &\geq \frac{|P|}{q^{f+(2f+d_1)+(2^2 f+2d_1+d_2)+(2^3 f+2^2 d_1+2d_2+d_3)\ldots+(2^k f+2^{(k-1)}d_1+2^{(k-2)}d_2+\ldots}} \\
\text{and } |\partial^{k+1} F| &= q^{2^{k+1} f+2^k d_1+2^{k-1}d_2+\ldots+d_{k+1}}\exists d_{k+1} \geq 0,
\end{aligned}$$

and so

$$\begin{aligned}
|\partial^{k+1} P| &\geq |P|/q^{f(2^{k+1}-1)+d_1(2^k-1)+d_2(2^{k-2}-1)+d_3(2^{k-3}-1)\ldots d_k} \\
\text{and } |\partial^{k+1} F| &= q^{2^{k+1} f+2^k d_1+2^{k-1}d_2+\ldots+d_{k+1}}\exists d_{k+1} \geq 0.
\end{aligned}$$

Now choose k so that ∂^{k+1} is the trivial (after which ∂ is no longer defined. Then we have

$$|P| = q^{f(2^{k+1}-1)+d_1(2^k-1)+d_2(2^{k-2}-1)+d_3(2^{k-3}-1)\ldots d_k},$$

and

$$|Q| = q^{2^{k+1} f+2^k d_1+2^{k-1}d_2+\ldots+d_{k+1}}.$$

So

$$|P|q^{f+d_1+d_2+d_3\ldots+d_{k+1}} = q^{2^{k+1} f+2^k d_1+2^{k-1}d_2+\ldots+d_{k+1}} = |Q|,$$

so we get our main result:

Proposition 10.3.3

$$|P| = \frac{|Q|}{q^{f+d_1+d_2+d_3\ldots+d_{k+1}}}.$$

Corollary 10.3.4 *Let quasifield Q with $Kern(Q) \supset K \cong GF(q)$, so $|Q| = q^n$ for some positive integer n. Then the Sylow p-subgroups in $(AutQ)_K$ have order $\leq q^{n-1}$.*

Consider the extremal case $|P| = q^{n-1}$: so $f = 1$ and all the d_i's vanish. This means we have a strict Baer chain of quasifields

$$GF(q) = F = Q_0 \subset Q_1 \subset Q_2 \ldots \subset Q$$

such that $(AutQ_{i+1})_{Q_i}$ is divisible by $|Q_i|$, and so all the Q_i's with the possible exception of the last one, viz. Q, are fields. But fields Q_{i+1} cannot admit $|Q_i|$ automorphisms fixing the Baer subfield $|Q_i|$ unless $|Q_i| = 2$. Thus either $|Q_1| = q$, as happens in, say, the Hall planes, or $Q \supset Q_1 \supset F$ where $F = GF(2)$, $Q_1 = GF(4)$, and Q has order 4^2. Thus we have shown

Corollary 10.3.5 *If a quasifield of order q^n admits an automorphism p-group P of order q^{n-1} that fixes a kern plane of order q elementwise then either Q is two-dimensional over its kern or $|Q| = 16$.*

Specialising to $q = p$ we obtain an absolute bound for the Sylow p-subgroup of the automorphism group of a quasifield:

Corollary 10.3.6 *A quasifield of order n cannot admit an automorphism group of order n.*

Thus a translation plane of order n does not admit planar groups of order n. Actually the above corollary may be refined to the following:

Corollary 10.3.7 *A quasifield of order p^n cannot admit an automorphism p-group of order $\geq p^{n-1}$, unless $n = 2$ or $p^n = 16$.*

As already indicated both cases do occur.

10.4 Klein Groups On Odd-Order Spreads.

Every finite p-group S, p a prime, contains maximum order elementary abelian p-subgroup A, and the rank of S is defined to be r if $|A| = p^r$; thus the rank of S is the rank of the maximum $GF(p)$-subspaces that it contains. For an arbitrary finite group G, its p-rank is defined to be the rank of its Sylow p-subgroups.

In the context of translation planes the importance of p-rank stems from the fact that in certain cases there is a tendency for the p-rank of a group G acting on a spread π of order u^n to force n to be very large, *provided* $\gcd(u,p) = 1$. For Chevalley-type groups, representation theory leads to such results but are too advanced to introduce at this stage.

However, for $p = 2$, Ostrom has proved a remarkable theorem, using only very elementary ideas, that lead to similar conclusions: and these conclusions apply to *all* groups with large 2-ranks — not just to the Lie-Chevalley type of groups. Here we prove Ostrom's theorem.

We are concerned with the action of elementary abelian 2-groups A on spreads $\pi = (V,\Gamma)$ of odd order p^r, $p > 2$ an odd prime. Ostrom's theorem implies that $|A|$ divides r, thus generalising the standard result on Baer involutions. Hence the two rank of any finite group G implies information concerning the lower bound for the size of the *odd order* spreads π on which it may act.

Theorem 10.4.1 (Ostrom's Baer Trick.) *Let A be an elementary abelian 2-group in $Aut(V,\Gamma)$, where $\pi = (V,\Gamma)$ is a spread of odd order q^n, whose kern contains the field $F = GF(q)$. Suppose all the involutions in A are Baer collineations, linear over the kern field F. Then $|A|$ divides n.*

Proof: We may write $|A| = 2^R$. For $R = 1$ the result holds because n is even if π admits a Baer involution. We use induction on the exponent R to complete the proof.
Let α and β be any two distinct involutions in A, and consider the Klein group

$$K = \{\alpha, \beta, \alpha\beta, \mathbf{1}\}.$$

Since A is abelian π_α is K-invariant. Now β cannot act trivially on π_α because this would force π_α to be elementwise fixed by a Klein group, and this cannot occur in spreads of odd order.
To establish that β induces a *Baer* involution on π_α, we need to rule out the possibility that $\beta|\pi_\alpha$ is an involutory central collineation.
First consider the case the possibility that β induces on π_α a *kern* involution $\hat{\beta} = \beta|\pi_\alpha$; now clearly $\hat{\alpha} = \alpha|\pi_\beta$ is also a kern involution. Thus $\hat{\beta}$ and $\hat{\alpha}$ are both $-\mathbf{1}$, on the spaces π_β and π_α respectively. But since $V = \pi_\alpha \oplus \pi_\beta$, because the two subspaces are disjoint and of rank $n/2$, we clearly have

$$\alpha\beta = \hat{\alpha} \oplus \hat{beta} = -\mathbf{1} \oplus -\mathbf{1} = -\mathbf{1}.$$

Now the group K contains a *kern* involution of π, contrary to our hypothesis that the non-trivial elements in A are all Baer collineations.
It remains to rule out the case when β induces an *affine* homology on π_α, with axis, say, $C \in \Gamma$. Now $C_0 = C \cap \pi_\alpha$ is the fixed subspace on C common to π_α and π_β. As α and β are both F-linear involutions of the vector space C with the same fixed space C_0 (neither fixed space can be larger because we are dealing with Baer involutions) they must coincide on C,that is,

$$\alpha|C = \mathbf{1}_{C_0} \oplus -\mathbf{1}_D = \beta|C,$$

where D is any complement of C_0 in C. But now $\alpha\beta$ is a homology with axis C, contradicting again our hypothesis that A contains only Baer involutions. Thus we see that A induces on π_α a group of *Baer* involutions A_1 of order 2^{R-1}. Now by our inductive hypothesis 2^{R-1} divides the dimension $R/2$ of π_α, and the desired result follows by induction. ∎

Corollary 10.4.2 *Let π be a spread of odd order q^n containing $GF(q)$ in its kern. If π admits an automorphism group G with two-rank r then 2^{r-1} divides n.*

Proof: Let A be an elementary abelian group of G of rank n. So A is semilinear on V, the vector space associated with π, over the kern field $K = GF(q)$. Now the K-linear part of A has order $\geq |A|/2$, and Ostrom's Baer trick can be applied to it. ∎

Corollary 10.4.3 *Let π be a spread of odd order q^n containing $GF(q)$ in its kern. If π admits an elementary abelian 2-group of order 2^r and the involutions in A form a single conjugacy class in $Aut\pi$ then 2^r divides n, provided $|A| > 2$.*

Proof: If A contains even one Baer involution then the conjugacy hypothesis allows us to apply the Ostrom Baer trick. So assume all the involutions in A are homologies, and consider a Klein subgroup $H \leq K$. Now Ostrom has observed that there are (in any projective plane) only two possibilities for such H: (1) all its elements share the same axis and center; or (2) each of the three non-trivial elements of H have as center and axis the opposite sides of a triangle: each of the three anti-flags of the triangle corresponding to one of the three non-trivial elements of H.

Possibility (1) cannot occur since then on the common coaxis W we the Klein group H acting semirgularly and faithfully: this is easily seen to be impossible: e.g. H becomes an elementary abelian non-cyclic Frobenius complement on W (in a Frobenius group whose kernel consists of all the maps $x \mapsto x+w$, $w \in W$, of W).
Possibilty (2) cannot occur, in the context of our conjugacy hypothesis, for then the homology whose axis is the ideal line, would be conjugate to a homology with an affine line as axis. ∎

10.5 Tangentially Transitive Planes.

Let π be any projective [resp. affine] plane, and π_0 be a proper subprojective [resp. subaffine] plane. Then a line is a *tangent* [line] to π_0 if it meets it at exactly one point. Similarly, a point is a *tangent* [point] if it meets exactly one line of π_0.

Now suppose G is a planar group with fixed plane π_G. Then it is clear that G permutes the tangents to π_G through any element of π_G, that is, G leaves invariant the set of non-fixed elements $\Theta(\epsilon)$ though each of its fixed elements $\epsilon \in \pi_G$. It is easy to see that all the restriction maps $\rho_\epsilon : G \to G^{\Theta(\epsilon)}$, for $\epsilon \in \pi_G$, are faithful representations of G that are permutation isomorphic, and hence G is transitive on all the tangents through some fixed element of π_G iff it is transitive on the tangents through each element of π_G. When this happens we say G is tangentially transitive.

Definition 10.5.1 *Let G be a planar collineation group of a plane π with fixed plane π_G. Then G is said to be* tangentially transitive *relative to π, and π_G is called a* tangentially transitive *subplane iff G acts transitively on the tangents through some (and hence each element of π_G). π is called tangentially transitive (tt) iff it is tt relative to some proper subplane.*

The definition may easily be characterised in algebraic terms, by noting the equivalence between planar groups and automorphisms of coordinatizing ternary rings, c.f. section 10.1.

Remark 10.5.2 *Let T be a ternary ring and suppose $G \leq AutT$ is transitive on $T - Fix(G)$; so $S = F(G)$ is the subternary ring of T consisting of the*

fixed elements of G. Then $\pi(T)$, the plane coordinatized by T, is tangentially transitive relative to $\pi(S)$, with respect to the group:

$$\hat{G} := \{(x,y) \mapsto (x^g, y^g) \mid g \in G\}.$$

Conversely, suppose π is a plane admitting a tangentially transitive group G coordinatized by a ternary ring T when the axes are chosen in the fixed plane π_G. Then π_G is coordinatized by a subternary ring S and $(AutT)_S$ contains a subgroup $\tilde{G}$ such that $\tilde{G}$ is transitive on $T - S$, with $Fix(\tilde{G}) = S$.

We saw in an earlier lecture that the Hall quasifields Q are two dimensional over their kern K, by part of their definition, and that $(AutQ)_K$ is transitive on $Q - K$, theorem 5.4.3. Hence the algebraic characterization of tt above yields

Remark 10.5.3 *A Hall plane π is tangentially transitive relative to some Baer subplanes π_0 coordinatized by the kern.*

A direct explanation of why Hall planes are tangentially transitive may be given in terms of derivation. A Hall plane H is derived from a Desarguesian plane $\Delta = \pi(F)$, the field F being a Baer extension of a field K, and Δ is derived relative to the slopes of $\pi(K)$. Part of the inherited group includes a group of central collineations with Y-axis leaving $\pi(K)$ invariant, viz:

$$G : \{(x,y) \mapsto (xa + b, y) \mid a \in K^*, b \in K\}.$$

Notice G is transitive on $\{\lambda a + b \mid a \in K^*, b \in K\}$, the set of slopes shared by the Desarguesian plane and the derived Hall plane. Thus on the derived side Y becomes a Baer subplane and G acts tangentially transitively relative to Y.

This can be generalized, by using a semifield D, two dimensional over its middle nucleus N_m, instead of a field. Now, by repeating the above argument, $\pi(D)$ when derived yields a translation plane tt relative to the Baer subplane, corresponding to the Y-axis of $\pi(D)$. Thus we have established:

Remark 10.5.4 *Let D be a semifield plane with middle nucelus M, which we assume to be a commutative field. Then π' the plane obtained by deriving relative to the slopeset of $\pi(M)$ is tangentially transitive relative to a Baer subplane. The plane π' is called a* GENERALISED HALL PLANE.

The procedure above can be repeated in more general contexts. Take any affine plane π of order n^2 admitting a group of central collineations G of order $n^2 - n$ that fixes an affine line Y elementwise and leaves invariant a derivable net Δ that includes Y and is left invariant by G. Then on the derived side G becomes a Baer group of order $n^2 - n$ and hence must act transitively on all the tangent points on any fixed line of π_G, its fixed Baer subplane.

This procedure permits the construction of tangentially transitive planes in several Lenz-Barlotti classes, apart from translation planes. The fact that duals of two dimensional translation planes are derivable and admit large groups of central collineations makes them promising candidates from this procedure. It is an exercise to verify that this procedure actually does work. Similarly verify that the derived Ostrom-Rosatti planes are tangentially transitive relative to some Desarguesian planes.

Notice, however, that in the constructions we have sketched so far, because they are based on derivation, the planes π are tangentially transitive relative to subplanes that are both Desarguesian and Baer. This invites the obvious questions:
If π is tt relative to π_0 then does π_0 have to be (1) Desarguesian (2) Baer.
In the finite case there is only one known case where π_0 can be *chosen* to be non-Baer — although a Baer choice is also possible in this case — in the remarkable Lorimer-Rahilly translation plane of order 16, see p 66. In all known cases, finite or infinite, π_0 is Desarguesian.

In this section we consider tangentially transitive *finite translation planes.* We show that in this case all tt planes are generalized Hall planes (including the Lorimer-Rahilly plane), and this essentially answers the two questions raised above in the affirmative. This leaves open the question of describing explicitly the generalized Hall planes, or rather, the finite semifield planes that are two-dimensional over their middle nucleus. We hope to provide a satisfactory answer to this question too. Note that the Hughes-Kleinfeld planes are coordinatized by semifields that are two-dimensional over their middle nucleus.

The rest of the section is devoted to showing that if a finite translation plane π is tangentially transitive relative to a subplane π_0 then it is a generalized Hall plane.

We begin by stating a special case of remark 10.5.2, relevant to the translation plane case.

Remark 10.5.5 *Let π be an affine translation plane and π_0 an affine sub-*

plane. Then π is tangentially transitive relative to π_0 iff it can be coordinatized by a quasifield Q such that π_0 is coordinatized by a subquasifield F such that $(AutQ)_F$ is transitive on $Q - F$.

We note that the case $|Q| = |F|^2$ has already been covered.

Lemma 10.5.6 *If $|Q| = |F|^2$ and $(AutQ)_F$ is transitive on $Q - F$ then F is a field and Q is a a vector space over F in the sense that for all $f, g \in F$ and $x, y \in Q$:*

1. $(x+y) \circ f = x \circ f + y \circ f$;
2. $x \circ (f+g) = x \circ f + x \circ g$;
3. $(x \circ f) \circ g = x \circ (f \circ g)$.

Proof: Recall exercise 2.(2). ∎

Now the condition that Q is a rank-two right vector space over F means that the slopes of $\pi(F)$ in $\pi(Q)$ define a rational (Baer) Desarguesian partial spread in $\pi(Q)$, and such partial spreads are [generic] derivable partial spreads. The derived spread admits a group of central collineations of order $n^2 - n$ where $|Q| = n^2$: the group is just the inherited group corresponding to the Baer group acting on $\pi(Q)$:

$$\{\hat{g} : (x, y) \mapsto (x^g, y^g) \mid g \in G\}.$$

Now it is an exercise to check that a spread of order n^2 admitting a Baer group of order $n(n-1)$ is a semifield spread with $GF(n)$ in N_m.

Thus we have shown:

Corollary 10.5.7 *If $|Q| = |F|^2$ then the plane $\pi(Q)$ is obtained by deriving a a plane coordinatized by a semifield relative to the slopeset of its middle nucleus. This by definition means that $\pi(Q)$ is a generalized Hall plane.*

Thus from now on we may assume that $|Q| > |F|^2$. Choose any $\lambda \in Q - F$. Then since G is transitive on $Q - F$ we see that $N_G(G_\lambda)$ induces a regular group on $Fix(G_\lambda) \cap Q - F$. However, $Fix(G_\lambda)$ is a quasifield Q_λ containing F, so we now have a quasifield $Q_\lambda \supset F$ such that $(AutQ_\lambda)_F \supset N_\lambda$ such that N_λ is regular on $(Q_\lambda)_F$. However N_λ must contain a Baer involution so the regularity is contradicted unless Q_λ is a Baer extension of F, in which case lemma 10.5.6 so F is a field and additionally the following identities apply, for $f, g \in F$:

1. $\lambda \circ (f+g) = \lambda \circ f + \lambda \circ g$;
2. $(\lambda \circ f) \circ g = \lambda(\circ f \circ g)$.

However, since λ was chosen arbitrarily, and the above identities obviously apply even when λ is replaced by members of F, we conclude from the above (plus the quasifield distributive law):

Lemma 10.5.8 *F is a field and Q is a vector space over F [acting from the left] of dimension $N > 2$. Moreover G is a linear group of this vector space.*

Now view Q as the projective space $PG(N-1,q)$ and observe that the projective group G has two point orbits. Hence by an important result, G also has two hyperplane orbits, one of which must be all the hyperplanes through the 'point' F. The other hyperplane orbit must therefore include all the hyperplanes 'off' a point: this is the same number as the number of points off a hyperplane, viz., q^{N-1}. Thus we have shown

Lemma 10.5.9 *If $N > 2$ then G contains a p-group of order q^{N-1}, p being the characteristic of F.*

But now we have seen that this is impossible, unless $q = 2$ and $N = 4$, corresponding to the case when $F = GF(2)$. It can be shown however, that even in this case $AutQ$ contains *another* subgroup H that H fixes a Baer subfield K elementwise and acts transitively on $Q - K$, so in a technical sense we still have a generalized Hall plane. However, the first choice of F is also possible: corresponding to the Lorimer-Rahilly plane of order 16, and this is the only known finite plane which is tangentially transitive relative to a non-Baer subplane. Let us summarize our conclusions:

Theorem 10.5.10 *A finite translation plane π is tangentially transitive relative to a subplane π_0 iff π is a generalized Hall plane and π_0 is a Desarguesian Baer subplane (defining a derivable net) unless the order of the plane is 16 in which case π_0 may taken as a plane of order to when π is the Lorimer-Rahilly plane of order 16: and this is the only case where the non-Baer possibility can occur.*

Note that we have not verified here the claimed uniqueness of the Lorimer-Rahilly plane, although this has been established in the literature, see Walker [40]

Chapter 11

Infinite Baer Nets.

In this chapter, we analyze the structure of a net embedded in a translation plane which contains at least one Baer subplane. Actually, it is not necessary that the translation plane be finite. In fact, we may analyze any vector space net containing a weaker version of subplane than Baer.

If a net contains a Baer subplane, it may contain exactly one. Or there may be exactly two Baer subplanes in the given net such that the subplanes share all of their parallel classes. In these lectures, we concentrate mainly on the case where there are at least three Baer subplanes sharing an affine point (the zero vector) and all of their infinite points (parallel classes).

11.1 Point-Baer And Line Baer Subplanes.

In any finite projective plane π of order n, a Baer subplane π_0 is just a subplane of order $\sqrt{n}$. Hence, to extend the notion of a Baer subplane usefully to the infinite case, it becomes necessary to replace the order-property of a Baer subplane by a characterization that can be used to define this concept in the infinite case. This lecture reviews some of the possible ways in which this has been attempted and also introduces a structure theorem of nets containing at least three Baer subplanes due to Johnson and Ostrom. This will be used in the next two lectures to extend the comprhensive characterization of such nets in the finite case, due to Foulser, to the infinite case.

A point-Baer subplane of a projective plane is a subplane such that every point of the plane is incident with a line of the subplane. Similarly, a line-Baer subplane is a subplane such that every line is incident with a point of

1. $\lambda \circ (f+g) = \lambda \circ f + \lambda \circ g$;
2. $(\lambda \circ f) \circ g = \lambda(\circ f \circ g)$.

However, since λ was chosen arbitrarily, and the above identities obviously apply even when λ is replaced by members of F, we conclude from the above (plus the quasifield distributive law):

Lemma 10.5.8 *F is a field and Q is a vector space over F [acting from the left] of dimension $N > 2$. Moreover G is a linear group of this vector space.*

Now view Q as the projective space $PG(N-1,q)$ and observe that the projective group G has two point orbits. Hence by an important result, G also has two hyperplane orbits, one of which must be all the hyperplanes through the 'point' F. The other hyperplane orbit must therefore include all the hyperplanes 'off' a point: this is the same number as the number of points off a hyperplane, viz., q^{N-1}. Thus we have shown

Lemma 10.5.9 *If $N > 2$ then G contains a p-group of order q^{N-1}, p being the characteristic of F.*

But now we have seen that this is impossible, unless $q = 2$ and $N = 4$, corresponding to the case when $F = GF(2)$. It can be shown however, that even in this case $AutQ$ contains *another* subgroup H that H fixes a Baer subfield K elementwise and acts transitively on $Q - K$, so in a technical sense we still have a generalized Hall plane. However, the first choice of F is also possible: corresponding to the Lorimer-Rahilly plane of order 16, and this is the only known finite plane which is tangentially transitive relative to a non-Baer subplane. Let us summarize our conclusions:

Theorem 10.5.10 *A finite translation plane π is tangentially transitive relative to a subplane π_0 iff π is a generalized Hall plane and π_0 is a Desarguesian Baer subplane (defining a derivable net) unless the order of the plane is 16 in which case π_0 may taken as a plane of order to when π is the Lorimer-Rahilly plane of order 16: and this is the only case where the non-Baer possibility can occur.*

Note that we have not verified here the claimed uniqueness of the Lorimer-Rahilly plane, although this has been established in the literature, see Walker [40]

Chapter 11

Infinite Baer Nets.

In this chapter, we analyze the structure of a net embedded in a translation plane which contains at least one Baer subplane. Actually, it is not necessary that the translation plane be finite. In fact, we may analyze any vector space net containing a weaker version of subplane than Baer.

If a net contains a Baer subplane, it may contain exactly one. Or there may be exactly two Baer subplanes in the given net such that the subplanes share all of their parallel classes. In these lectures, we concentrate mainly on the case where there are at least three Baer subplanes sharing an affine point (the zero vector) and all of their infinite points (parallel classes).

11.1 Point-Baer And Line Baer Subplanes.

In any finite projective plane π of order n, a Baer subplane π_0 is just a subplane of order $\sqrt{n}$. Hence, to extend the notion of a Baer subplane usefully to the infinite case, it becomes necessary to replace the order-property of a Baer subplane by a characterization that can be used to define this concept in the infinite case. This lecture reviews some of the possible ways in which this has been attempted and also introduces a structure theorem of nets containing at least three Baer subplanes due to Johnson and Ostrom. This will be used in the next two lectures to extend the comprhensive characterization of such nets in the finite case, due to Foulser, to the infinite case.

A point-Baer subplane of a projective plane is a subplane such that every point of the plane is incident with a line of the subplane. Similarly, a line-Baer subplane is a subplane such that every line is incident with a point of

the subplane. Every finite point-Baer subplane is line-Baer and conversely. However, in the infinite case, the concepts of point-Baer and line-Baer are independent (Barlotti [3]). So, a subplane is Baer if and only if it is both point-Baer and line-Baer. An affine point-Baer subplane is an affine plane which is point-Baer when the plane is considered projectively. A collineation σ of an affine plane which fixes a point-Baer subplane pointwise is said to be a point-Baer perspectivity if and only if the collineation fixes each subplane of a set C of point-Baer subplanes which form a cover of the points of the affine plane. The collineation σ is a point-Baer elation if and only if $Fix\sigma$ is in C. Otherwise, σ is a point-Baer homology. C is called the center of the collineation, the elements of C are called the central planes and $Fix\sigma$ is the axis.

If a collineation fixes a point-Baer subplane pointwise then, conceivably, it is not a point-Baer perspectivity. However, the structure of point-Baer collineations is essentially completely determined for translation planes. An axial-Baer perspectivity σ is a point-Baer perspectivity such that $Fix\sigma$ projectively nontrivially intersects each point-Baer subplane of the center.

The authors have recently provided a general structure theory for point-Baer and line-Baer perspectivities. In particular, the following result is fundamental.

Theorem 11.1.1 (Jha, Johnson [22].) *Let π be a translation plane and let σ be a collineation which fixes a point-Baer subplane pointwise.*

Then σ is either a point-Baer homology (and hence an axial-Baer homology) or σ is an axial-Baer elation and in this case all the planes of the center are proper Baer subplanes. In particular, in all cases, the axis $Fix\sigma$ is a proper Baer subplane of π and σ has a unique center.

Let N be a vector space net which admits at least three distinct point-Baer subplanes that share the same infinite points and mutually share an affine point. Assume that N has exactly these same infinite points.

In [10], Foulser completely determined the structure of N, when the planes are finite. In the section following this preliminary part, we show that this theory can also be determined in the more general situation when N is possibly infinite. When we can, we follow the general outlines of Foulser's argument. However, there are some situations which require different approaches so we will require a slightly different method paying particular attention to commutativity properties.

We have mentioned the notation of a direct product of affine planes. We shall require the following results of Johnson and Ostrom [28].

Theorem 11.1.2 *(Johnson-Ostrom [28, (4.20) and (5.1)].) Let M be an Abelian translation net. If M contains three distinct point-Baer subplanes incident with a point whose infinite points are the infinite points of M then M is a regular direct product net and each pair of the planes are isomorphic.*

Furthermore, M is then a vector space net over a field L and the point-Baer subplanes may be considered L-subspaces.

If one of the subplanes π_o has kernel K_o and M is isomorphic to $\pi_o \times \pi_o$ then M is a K_o-vector space net.

At least three of the point-Baer subplanes of the net which share an affine point and all of their parallel classes are K_o-subspaces but not all point-Baer subplanes are necessarily K- subspaces.

We point out that in (4.20) of [28], it is proved that L may be taken as the prime field of any of the affine planes.

In the following result, we specialize to the situation we are discussing.

Theorem 11.1.3 (Johnson-Ostrom (5.2) [28].) *Let M be a vector space net over a skewfield K where M is a regular direct product net of two isomorphic point-Baer subplanes with kernel K_o.*

Then M admits $\Gamma \cong GL(2, K_o)$ as a collineation group that fixes an affine point and fixes each parallel class.

Furthermore, Γ is generated by the groups which fix point-Baer subplanes pointwise.

If $M = \pi_o \times \pi_o$ and K_o is the kernel of π_o as a left K_o-subspace then the action of an invertible element

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

on M is $(p_o, p_1) \to (ap_o + cp_1, bp_o + dp)$ for a, b, c, d in K_o and p_o, p_1 points of π_o.

Exercise 11.1.4 *Suppose M is a regular direct product net of two Desarguesian affine planes of order $q = p^r$. Using the above theorem, show there is a group isomorphic to $GL(2, q)$ acting on the net M.*

11.2 Regular Direct Products.

In this lecture, we consider a coordinate set for a regular direct product. However, before doing this we need to consider in some detail the meaning of the linear group $GL(2, K)$ when K is a non-commutative skewfield.

When K_o is a skewfield which is not a field, there are some important differences between the commutative and noncommutative case with the consideration of the group $GL(2, K_o)$. Actually, the use of the notation is a bit problematic as the elements are not necessarily K-linear mappings in the traditional sense.

Consider a Desarguesian affine plane (x, y) considered as a 2-dimensional left vector space over a skewfield $(K, +, \cdot)$. Since we may also consider the affine plane as a 2-dimensional right space over K, we take components to have the form $y = x\alpha$ for α in K and $x = 0$ and note that $y = x\alpha$ and $x = 0$ are 1-dimensional left K-subspaces. We may consider the mappings called the kernel mappings

$$T_\beta : (x, y) \to (\beta x, \beta y).$$

It follows easily that $\{T_\beta \mid \beta \in K\}$, forms a field isomorphic to $K \equiv (K, +, \cdot)$ and fixes each component of the Desarguesian plane.

Now consider the mappings $(x, y) \to (xa + yb, xc + yd)$ such that the corresponding determinant $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ defined as $ac^{-1}d - b \neq 0$ if $c \neq 0$ and $ad \neq 0$ otherwise. Then it follows easily that each mapping is a $\{T_\beta\}$-linear mapping. Hence, we may justify the designation $GL(2, K)$.

Traditionally, the kernel of a translation plane is the set of endomorphisms which leave each component of the plane invariant. Hence, $\{T_\beta \mid \beta \in K\} = K^\circ$ is the kernel of the Desarguesian plane π. Furthermore, the full collineation group of π which fixes the zero vector (the translation complement) is $\Gamma L(2, K)$ or is $\Gamma L(2, K^\circ)$. Since the use of K or $K^\circ \cong K$ is merely in the distinction between K and the associated kernel mappings, we also refer to K as the kernel of the plane. So, considering the translation complement of π as $\Gamma L(2, K)$ then $K^{\circ^*} = K^\circ - \{T_o\}$ is a group of semilinear mappings and as a collineation T_β is in $\Gamma L(2, K)$ but is in $GL(2, K)$ if and only if β is in $Z(K_o)$. That is to say that the elements of $GL(2, K)$ are the elements of $\Gamma L(2, K)$ which commute with K° and T_β commutes with K° if and only if β is in $Z(K)$. The notation can be particularly tricky if one considers βx as a linear mapping over the prime field P of K. For example, βx is normally

written $x\beta$, when considering β as a P-linear endomorphism. Then considering an element u in K as a P-linear endomorphism, it follows then that $\beta u = u\beta$ when considering the elements as linear endomorphisms whereas it is not necessarily the case that $\beta u = u\beta$ when the operation juxtaposition is considered as skewfield multiplication.

Note that elements of $GL(2, K)$ act on the elements (x, y) on the right whereas T_β acts on the elements (x, y) on the left.

In the statement of the above theorem, and we have π_o with kernel K_o, we have $GL(2, K_o)$ acting on the left side on a subnet instead of the right. If it occurs that a subgroup R of this group acts as a collineation of a translation plane Σ with kernel K containing π_o , then R is a subgroup of $\Gamma L(\Sigma, K)$. We now consider this situation.

We shall consider an affine translation plane with kernel K as follows: Let X be a left K-subspace and form $V = X \oplus X$. We denote points by (x, y) for x, y in X.

When we have an affine translation plane Σ with kernel K, we similarly consider the lines through $(0, 0)$ (components) in the form $x = 0, y = xM$ where M is a K-linear transformation. The kernel K then gives rise to a set of kernel mappings

$$\{T_\beta : (x, y) \to (\beta x, \beta y) \mid \beta \in K\} = K^\circ.$$

In the finite dimensional case, we may take M as a matrix with entries in K_o say as $[a_{ij}]$ and define $xM = (x_1, x_2, ...x_n)M$ as $(\Sigma x_i a_{i1}, ..., \Sigma x_i a_{in})$. It follows that M becomes a left K-linear mapping with scalar multiplication defined by $\beta x = (\beta x_1, \beta x_2, ..., \beta x_n)$ and furthermore, $\{(x, xM)\}$ is a left K-linear subspace. In this case K° is a skewfield isomorphic to K and as a collineation group of Σ, $K^{\circ *}$ is a semilinear K-group. Similar to the Desarguesian case, one may consider the left scalar multiplication as a linear endomorphism over the prime field P of K. When we do this, we shall use the notation $K_\circ$. Hence, the $M's$ now commute with the elements of $K_\circ$.

To be clear, we now have three different uses of the term kernel of a translation plane. We always consider the translation plane as $X \oplus X$ where X is a left vector space over a skewfield K, the kernel mappings are denoted by K° and the component kernel mappings thought of as prime field endomorphism are denoted by $K_\circ$. All three skewfields are isomorphic and each is called the kernel of the translation plane where context usually determines which skewfield we are actually employing.

We now consider a coordinate set for a regular direct product net.

We point out that in the proof of (4.20) of [28], it is noted that two point-Baer subplanes that share the same infinite points and an affine point sum to the entire vector space and furthermore their intersections on any line concurrent with the common affine sum to the line.

We may identify any point-Baer subplane as π_o within the direct product so that the points of the net have the general form (p_1, p_2) for p_1 and p_2 in π_o and the lines have the form $L_1 \times L_2$ for L_1 and L_2 parallel lines of π_o. It follows that the net M is $\pi_o \times \pi_o$ with the identity mapping defined on the set of parallel classes.

Considering the translation plane π_o with kernel K_o , we specify two lines incident with the zero vector as $x_o = 0$ and $y_o = 0$. We further decompose π_o in terms of these two subspaces and write the elements of π_o as (x_o, y_o) where x_o, y_o are in a common K_o-subspace W_o . We may take $y_o = x_o$ as the equation of a line of π_o incident with the zero vector so that the remaining lines are of the general form $y_o = x_o M$ where M is a K_o-linear transformation of W_o for M in a set Π_o.

The points of the net now have the general form (x_o, y_o, x_1, y_1) where x_o, y_o, x_1, y_1 are in W_o. The lines of the net are as follows: $(y_o = x_o M + c_o) \times (y_o = x_o M) + c_1)$ for all M in Π_o containing I and O and $(x_o = c_o) \times (x_o = c_1)$.

Note change bases by the mapping $\chi : (x_o, y_o, x_1, y_1) \longmapsto (x_o, x_1, y_o, y_1)$

Finally, we write $(x_o, x_1) = x$ and $(y_o, y_1) = y$ when (x_o, y_o, x_1, y_1) is a original point of the net or (x_o, x_1, y_o, y_1) is a point after the basis change.

Note that, before the basis change χ, the lines of the net are sets of points

$$\{(x_o, x_o M + c_o, x_1, x_1 M + c_1) \text{ for all } x_o, x_1 \text{ in } W_o\} \text{ , for fixed } c_o \text{ and } c_1 \text{ in } W_o$$

and

$$\{(c_o, y_1, c_1, y_2) \text{ for all } y_1, y_2 \text{ in } W_o\}, \text{ for fixed } c_o \text{ and } c_1 \text{ in } W_o.$$

Hence, after the basis change, the lines of the net have the basic form

$$x = (c_o, c_1) \quad \text{and } y = x \begin{bmatrix} M & 0 \\ 0 & M \end{bmatrix} + (c_o, c_1).$$

Before the basis change χ, the point-Baer subplanes incident with the zero vector which are in a $GL(2, K_o)$ orbit of π_o have the following form:

$\rho_\infty = \{(0,0,x_1,y_1)$ for all x_1, y_1 in $W_o\}$ and $\rho_\alpha = \{(x_o, x_1, \alpha x_o, \alpha x_1)$ for all x_o, x_1 in $W_o\}$ for each α in K_o. **We shall call these subplanes ρ_∞, or ρ_α the base subplanes.**

We now observe that the group $GL(2, K_o)$ acting on the right is represented by mappings of the form $(x_o, x_1, y_1, y_2) \longmapsto (ax_1 + bx_2, cx_1 + dx_2, ay_1 + by_2, cy_1 + dy_2)$.

11.3 Baer Nets: Structure Theory.

As we indicated earlier, Foulser has completely determined in the finite case the structure of vector space nets that admit at least three Baer subplanes that share the same slopeset. In this lecture, we extend Foulser's analysis to the infinite case.

We assume that we have a translation plane Σ with kernel K and there are at least three point-Baer subplanes as above with kernel K_o which are left invariant under the mappings $K^{\circ *}$ or equivalently are K-subspaces. Then there is a regular direct product net N isomorphic to $\pi_o \times \pi_o$ embedded in Σ. The translation complement of Σ is a subgroup of $\Gamma L(\Sigma, K)$ with the elements acting on the left. Furthermore, there is group of the direct product net N which is isomorphic to $GL(2, K_o)$ and naturally embedded in $GL(4, K_o)$ with the elements acting on the right. It is easy to see that if a collineation g of Σ fixes a K-subspace π_o pointwise then g is in $GL(\Sigma, K)$ and hence commutes with the mappings T_β. Now any kernel homology group $K^{\circ *}$ induces a faithful kernel group on any invariant point-Baer subplane so K may be considered a subskewfield of K_o.

We shall use the notation (∞) to denote the parallel class containing the line $x = 0$ and (0) to denote the parallel class containing the line $y = 0$. We shall use both the original direct product point notation and the notation after the basis change χ more-or-less simultaneously. After our main structure theorem, we shall use the representation after the basis change exclusively.

Lemma 11.3.1 *Let Σ be any point-Baer subplane incident with the zero vector and sharing all parallel classes with the net. Then $(0, x_o, 0, x_1)$ is in $\Sigma \cap (x = 0)$ if and only if $(x_o, 0, x_1, 0)$ is in $\Sigma \cap (y = 0)$.*

Proof: Let the infinite points of $x = 0, y = x \begin{bmatrix} M & 0 \\ 0 & M \end{bmatrix}$ be denoted by

(∞) and (M) respectively.

Let $(x_o, 0, x_1, 0)$ be a point of $\Sigma \cap (y = 0)$. Form the line $(\infty)(x_o, 0, x_1, 0)$ $\equiv (x = (x_o, x_1))$ and intersect the line $y = x$ to obtain $(x_o,\ x_o, x_1, x_1)$. Since all such lines are lines of Σ , the intersection is a point of Σ. Now form the line of Σ , $(0)(x_o, x_o, x_1, x_1)$ and intersect $x = 0$ to obtain $(0, x_o, 0, x_1)$ in $\Sigma \cap (x = 0)$.

Exercise 11.3.2 *Is there any difference between the proof of the above lemma in the infinite case and in the finite case?*

Lemma 11.3.3 *Now assume the subplane Σ is not a base subplane.*

For $(0, x_o, 0, x_1)$ in $\Sigma \cap (x = 0)$ define a mapping λ on W_o which maps x_o to x_1.

Then λ is a $1-1$ and onto additive transformation of W_o.

Furthermore, $\Sigma = \{(x_o, y_o, \lambda x_o, \lambda y_o)$ for all x_o, y_o in $W_o\}$.

Proof: It is easy to check that no two distinct point-Baer subplanes incident with a common affine point and sharing all of their parallel classes can share two distinct affine points. Hence, $x_o = 0$ if and only if $x_1 = 0$ when $(0, x_o, 0, x_1)$ is a point of Σ and Σ is not the base subplane ρ_∞ or ρ_o.

It follows that the subplane Σ is a translation affine subplane and hence a subspace of the underlying vector space taken over at least over the prime field.

Hence, it follows that λ is $1-1$ since the intersections with any of the base subplanes contain exactly the zero vector and it is also now clear that λ is additive. It remains only to show that λ is an onto mapping.

From the above remarks, any two distinct point-Baer subplanes sharing a common affine point and their infinite points sum to the vector space and their intersections with a line incident with the common point sum to the line. Hence, given any element x_1^* of W_o consider the vector $(0, 0, 0, x_1)$ there exists vectors $(0, x_o^*, 0, 0\ )$ in $\rho_o \cap (x = 0)$ and $(0, x_o, 0, x_1)$ in $\Sigma \cap (x = 0)$ such that

$$(0, 0, 0, x_1^*) = (0, x_o^*, 0, 0) + (0, x_o, 0, x_1).$$

It follows that $x_1 = x_1^*$ so there exists a vector $(0, x_o, 0, x_1^*$ in Σ. Hence, the mapping $\lambda : x_o \rightarrow x_1$ is onto.

If $(0, x_o, 0, \lambda x_o, 0)$ is in $\Sigma \cap (x = 0)$ then $(x_o, 0, \lambda x_o, 0)$ is in $\Sigma \cap (y = 0)$ so that $(x_o, y_o, \lambda x_o, \lambda y_o)$ is in Σ for all x_o, y_o in W_o as Σ is the direct sum of any two components. Let $(x_o^*, y_o^*, x_1^*, y_1^*)$ be any point of Σ then it follows that

Σ also contains $(0,0,\lambda x_o^* - x_1^*, \lambda y_o^* - y_1^*)$ and since $\Sigma \cap \rho_\infty = (0,0,0,0)$ this forms $x_1^* = \lambda x_o^*$ and $y_1^* = \lambda y_o^*$. This completes the proof of the lemma.∎

Exercise 11.3.4 *If the plane is finite, how would the above proof be able to be simplified?*

To see that it is not possible that Σ is not a base subplane, we show that, in fact, λ is in K_o.

Lemma 11.3.5 *For* $y = x \begin{bmatrix} M & 0 \\ 0 & M \end{bmatrix}$ *a line of the net and* $(x_o, 0, x_1, 0)$ *in* Σ *then* (x_o, x_oM, x_1, x_1M) *is also in* Σ.

Proof: We have seen this previously in the preliminary section. We form $(x_o,0,x_1,0)(\infty) \equiv (x = (x_o, x_1))$ and intersect $y = x \begin{bmatrix} M & 0 \\ 0 & M \end{bmatrix}$ to obtain the point (x_o, x_oM, x_1, x_1M). Since all of the points and lines are points and lines of Σ, it follows that the intersection point is also in Σ. ∎
The previous lemma shows that if $(x_o,0,x_1,0)$ is in Σ then so is (x_o, x_oM, x_1, x_1M) which, in turn, implies that $(0, x_oM, 0, x_1M)$ is in Σ. However, also we have that $x_1 = \lambda x_o$ and we know that $(0, x_oM, 0, \lambda(x_oM))$ is in Σ. Subtracting, since Σ is additive, we have that $(0,0,0,(\lambda x_o)M - \lambda(x_oM))$ is in Σ for all x_o. Since $\Sigma \cap \rho_\infty = (0,0,0,0)$, it follows that $(\lambda x_o)M) = \lambda(x_oM)$.

Let L_o be any skewfield such that $\{M$ for M in $\Pi_o\}$ is a set of L_o-linear transformations. Then it follows that L_o must be contained in the kernel K_o of $\pi_o = \rho_\infty$. Hence, λ is in $L_o \subseteq K_o$.

Hence, we have proved the following result:

Theorem 11.3.6 *Let M be any Abelian net which contains three point-Baer subplanes that share the same affine point and share all of their parallel classes.*

Then there is a skewfield K_o such that M is a K_o- vector space net and there is a K_o-space W_o such that the points of M may be identified with $W_o \oplus W_o \oplus W_o \oplus W_o$. The set of all point-Baer subplanes of M that share the zero vector is isomorphic to the set $\{\{(0,0,y_o,y_1)$ for all (y_o,y_1) in $W_o \oplus W_o\} \cup_{\alpha \in K_o} \{(x_o,y_o,\alpha x_o, \alpha y_o)$ for all (x_o,y_o) in $W_o \oplus W_o\}\}$.

Furthermore, there is a collineation group Γ *of the net isomorphic to* $GL(2, K_o)$ *which fixes* $(0,0,0,0)$ *and all parallel classes and acts triply transitively on the set of all point-Baer subplanes incident with* $(0,0,0,0)$. *Moreover, if* B *denotes the set of all point-Baer subplanes of* M *and* $\Gamma_{[\pi_o]}$ *is the pointwise stabilizer of a subplane* π_o *of* B *then*

$$\Gamma = \left\langle \Gamma_{[\pi_o]} \mid \pi_o \in B \right\rangle.$$

Exercise 11.3.7 *Restate this theorem in the finite case assuming that* M *is a net of degree* q^2 *and degree* $q+1$ *that contains three Baer subplanes. Let the kernel of any one of the subplanes be* $GF(h)$. *How many Baer subplanes are in the net?*

Corollary 11.3.8 *Let* M *be Abelian net which contains three point-Baer subplanes that share the same affine point* A *and all of their parallel classes.*

If one of the point-Baer subplanes has kernel K_o*then the set of all point-Baer subplanes of* M *incident with* A *is isomorphic to* $PGL(1, K_o)$.

Proof: We consider the above representation after the basis change χ. The group

$$\left\langle Diag \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \text{ such that } \lambda \epsilon K_o \right\rangle \cdot \left\langle Diag \begin{bmatrix} \beta & 0 \\ 0 & 1 \end{bmatrix} \text{ such that } \beta \epsilon K_o - \{0\} \right\rangle$$

fixes $\pi_o = \rho_\infty$pointwise and acts doubly transitively on the point-Baer subplanes. Note that $DiagA = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}$.

Exercise 11.3.9 *Restate the corollary in the finite case assuming that one of the subplanes has kernel* $GF(h)$.

Below, we completely determine the collineation group of a net of type in the statement of the above theorem. We first verify the following result.

Theorem 11.3.10 *Let* R *be any Abelian net which contains three point-Baer subplanes that share the same affine point* A *and all of their parallel classes. Let* π_o *be any point-Baer subplane incident with* A. *Then* π_o *is an affine translation plane with kernel* K_o. *Let* G_{π_o} *denote the full linear translation complement of* π_o.

Then there is a collineation group of R *isomorphic to* G_{π_o} *which leaves* π_o *invariant.*

Proof: We have noted that R is a regular direct-product net. The result then follows from a previous exercise.■

Theorem 11.3.11 *Let R be any Abelian net which contains three point-Baer subplanes that share the same affine point A and all of their parallel classes. Let π_o be any point-Baer subplane incident with A.*

Then π_o is an affine translation plane with kernel K_o. Let G^{π_o} denote the full linear translation complement of π_o obtained as a collineation group of R which leaves π_o invariant.

Then the full collineation group of R which fixes π_0 is isomorphic to the product of G^{π_o} by $GL(2, K_o)$. The two groups intersect in the group kernel of π_o naturally extended to a collineation group of R.

Exercise 11.3.12 *Assume that R is a finite net of order q^2 and degree $q+1$ and that the kernel of a Baer subplane is $GF(q)$. Show the net defines a regulus in $PG(3, q)$. Consider the group of the regulus net acting in $PG(3, q)$. Show there is a subgroup isomorphic to $PGL(2, q) \times PGL(2, q)$.*

Proof of the theorem: The group $GL(2, K_o)$ acts 3-transitively on the point-Baer subplanes of the net R and fixes R componentwise. Hence, we may assume that a collineation fixes the zero vector and permutes the point-Baer subplanes $\pi_\infty = \{(0, p)$ such that $p \in \pi_o\}, \pi_\lambda = \{(p, \lambda p)$ such that $p \in \pi_o$ and λ in the kernel of $\pi_o\}$ (when $\lambda = 0$ the subplane π_o is identified with $\pi_o \times 0$.

So, if a collineation g of R which fixes the zero vector then we may assume that g leaves π_∞, π_o, and π_1 invariant. Hence, g is in G_{π_o} as it acts faithfully on π_o.

Since $GL(2, K_o)$ fixes R componentwise, assume g fixes R componentwise. Then g induces the kernel mappings on π_o and on π_1 and is fixed-point-free as it also leaves π_∞ invariant. Thus, the faithful stabilizer of π_o in $GL(2, K_o)$ which fixes π_∞, π_o, and π_1 is $\left\langle \begin{bmatrix} \beta & 0 \\ 0 & \beta \end{bmatrix} \text{ such that } \beta \epsilon K_o \right\rangle$ in this representation. It then follows that the collineation group of R is the product as maintained.■

Chapter 12

Hering-Ostrom Theory: Elation-Generated Groups.

The celebrated Lenz-Barlotti theory describes maximal groups of central collineations of arbitrary projective and affine planes. Similarly, one might ask for a description of groups that are generated by groups of central collineations of a plane that share neither an axis nor a center. For example, in affine Desarguesian planes of order p^r, if E_1 and E_2 are groups of elations with distinct affine axes they generate the group $G \cong SL(2, p^s)$ whenever s divides r.

A fundamental theorem of Ostrom asserts that the same conclusion holds for arbitrary finite translation planes with characteristic $p > 3$. The case $p \leq 3$ has been completely resolved by Hering, where the conclusions are slightly more complicated: for example, in the spreads associated with the even order Lüneburg planes, elation groups might generate Suzuki groups. Taken together, the Hering-Ostrom theorem provides a complete description of groups G generated by affine elations of [partial] spreads and has proven be a powerful tool for the investigation of finite translation planes.

It is thus natural to seek to generalise this theorem. Major results on finite translation planes have been obtained by Foulser based on extending the Hering-Ostrom theorem to generalised elations. It turns out that a generalised elation, in the context of a spread, is either an affine elation or a Baer p-element, and this leads to a Baer analogue of the Ostrom's theorem. In the next chapter, we use this to establish striking incompatibilty results concerning Baer p-elements and affine elations, and also incompatibility among Baer p-elements that have different slopesets in odd characteristic. These

results are due to Foulser in the odd characteristic case. In characteristic 2, Foulser's results do not apply as there are counterexamples. However, as demonstrated by the authors via group-theoretic results of Dempwolff, there is still still a high degree incompatibility between Baers and elations, even in spreads of even order. In all cases, the incompatibilities indicated have a profound influence on the collineation group of a translation plane. For example, it implies that semifield planes of odd order cannot admit Baer p-elements.

One of the main goals of the present chapter is to prove Ostrom's result, describing the groups G generated by elations acting on finite partial spreads of characteristic $p > 3$; we refer the reader to Lüneburg's immaculate treatment [31] for the full Hering-Ostrom theorem. In addition to Ostrom's theorem, and its generalization to finite-dimensional spreads, we shall establish Foulser's analogue of Ostrom's result that applies to generalised elations: this will be applied in the next chapter to establish the incompatibility theorems indicated above.

12.1 Field Extensions and Spreads.

Let $V = F^n \oplus F^n$, and let $K \supset F$ be an extension field of the finite field F. Rather than using tensor product notation, we shall write: $V_K = K^n \oplus K^n$, $X_K = K^n \oplus \mathbf{0}$, $Y_K = \mathbf{0} \oplus K^n$; in general if W is an F-subspace of V then W_K denotes the K-subspace of V_K generated by W; so W_K consists of all the K-linear combination of any F-basis of W. This follows by noting that F-independent subsets in V are also K-independent: look at the rank of the matrix M_W of any F-linear basis of W: the rank of M_W, whether viewed as an F-matrix or as a K-matrix is always the same.

Next consider $g \in Hom(V, F)$; g_K is the unique extension g_K of g to $Hom(V, K)$ and the two maps have the same matrix relative to any F-basis of V, in particular relative to the canonical basis. So $g \in GL(V, F)$ if and only if $g_K \in GL(V_K, K)$.

We shall be particularly concerned with the action that a group $G \leq GL(V, F)$ induces on a K-subspace $U \leq V_K$ that is G_K-invariant, sometimes when $V \cap U = \mathbf{O}$. In all cases, the action of G_K on U is just the action associated with the matrix group representing G, and we write G^U to mean G_K^U, the action of G_K on U.

A spread Γ on V corresponds in the obvious way to a *partial* spread Γ_K

of V_K, and Γ includes the standard components X and Y of $F^n \oplus F^n$ iff Γ_K does: that is X_K and Y_K lie in Γ_K, and a similar comment applies to the unit line I. We always assume that we are dealing with spreads and partial spreads containing the standard components X and Y, as well as the unit line I. Let $\mathcal{M}$ be the spreadset of matrices defining Γ; so $\mathcal{M}$, viewed as a set of K-matrices is a *partial* spreadset defining the partial spread Γ_K.

Next focus on a rank two K-subspace $U \leq V_K$ that meets non-trivially the subsaces X and Y of V, and let Γ_U be the set of all components $\gamma_K \in \Gamma_K$ that meet U non-trivially. Since U has rank 2 over K, Γ_U is a Desarguesian K-spread on U, and it meets non-trivially each of X, Y and I, in three distinct components.

Next suppose $G \leq GL(V, F)$ preserves Γ and such that G_K leaves U-invariant. So G_K is a K-linear automorphism group of the partial spread Γ_K and also leaves U invariant. Thus $G_K^U \leq GL(2, K)$. Moreover, the given elation groups continue to act as elation elation groups on the Desarguesian spread Γ_U, so $G_K^U \cong SL(2, K')$ for some $K' \subseteq K$. The close connection between G_K^U and G leads to a similar conclusion for G, as required.

This suggests a strategy: take any F-spread admitting G, then seek an extension field K over which G fixes a 2-space made up of distinct eigenvectors of some normal subgroup of G and then apply the above argument.

Returning to the main theme, assume G acts transitively on the non-zero points of U. Now the components of Γ that meets U non-trivially do so in at least one non-zero point of V, so the components of Γ_K induce the standard Desarguesian spread on U. Note that the point of this claim is that the components of the standard Desarguesian spread that U carries, simply because it is a 2-dimensional space, must *extend* to components of Γ_K.

Suppose now that the p-Sylow subgroups of G are non-trivial but not planar. So if P is such a group then V_P is a component of Γ. By the conjugacy of Sylow subgroups it follows that the associated components, which we call p-axes [of G] form a G-orbit Now P certainly fixes a component of the Desarguesian spread Δ_U. Also wlog X is the axis of P. So if more than one axis is involved then the transitivity of P on the axes implies that the axes all meet U non-trivially and each corresponds to the axis of a shears group of Δ_U. The non-planarity hypothesis means that P acts faithfully on Δ_U and hence is elementary abelian. All these groups generate $SL(2, L)$ on Δ_U, where $F \leq L \leq K$.

12.2 Algebra Generated By Matrix A.

Let A be an $n \times n$ matrix over a field F, and define the F-algebra generated by A to be the smallest ring $< A >$ of matrices containing A and $F\mathbf{1}$. Since we have finite dimension, A satisfies a unique monic minimum polynomial $f(x) = \sum_{i=0}^{k-1} f_i x^i$ over F; thus

$$A^k = \sum_{i=0}^{k-1} f_i A^i = 0,$$

and we have an algebra isomorphism:

$$< A > \cong F[x]/(f(x)).$$

Thus we have:

Remark 12.2.1 *$< A >$ is a field iff its minimum polynomial $f(x)$ is irreducible and now $< A >$ is isomorphic to an extension field of F by any of the roots of $f(x) = 0$.*

Now, even in the general case, if λ is an eigenvalue of A then $f(\lambda) = 0$, so if $f(x)$ is *irreducible* then the algebra $F(\lambda) \cong F[x]/(f(x))$ is the extension field of F by λ. But the eigenvalues of A are just the roots of $f(x) = 0$, since the minimum and the characteristic polynomials have the same roots. In particular, the eigenvalues of A are all congugate in the algebraic closure of F. Hence the previous remark may be restated as:

Remark 12.2.2 *The F-algebra $< A >$ is a field iff its minimum polynomial $f(x)$ is irreducible and now $< A >$ is an extension field of F such that $< A > \cong F(\lambda)$, where λ is any eigenvalue of A; the fields $F(\lambda)$ are isomorphic as λ ranges over the eigenvalues of A.*

We can now consider the the case of interest: when the F-algebra $< A >$ does *not* contain any non-zero singular matrices. In this case, if for some non-zero $T \in < A >$ the minimum polynomial $f_T(x) = g_T(x)h_T(x)$, where $\min[\partial g, \partial h] \geq 1$, and $T \in < A >$ then $g_T(T)$ and $h_T(T)$ are both non-zero and singular matrices since ther product $f_T(T)$ is zero. This contradicts our assumption that the non-zero elements in $< A >$ are non-singular, so we have:

Proposition 12.2.3 *If the F-algebra $< A >$, i.e. the polynomial ring $F[A]$, is a partial spreadset of matrices then it is a field of matrices isomorphic to the field $F(\lambda)$, where λ may be chosen to be any eigenvalue of A: these are all conjugate over F.*

12.3 Properties of $SL(n, K)$.

In this section, we mention a couple of properties of the unimodular group $SL(2, q)$. The first property is will be tacitly assumed in several places.

Theorem 12.3.1 *Let $GL(n, K)$ be the group of non-singular maps of an n-dim-ensional vector space over a finite field K and let $SL(n, K)$ be its full unimodular subgroup.*

If H is a subgroup of $GL(n, K)$ such that $H \cong SL(n, K)$ then $H = SL(n, K)$.

Proof: Let p denote the characteristic of K. Then every $SL(n, K)$ in $GL(n, K)$ is generated by the set of all Sylow p-subgroups of $GL(n, K)$, and these are all in the 'standard' unimodular group $SL(n, K)$ since this group is normal in $GL(n, K)$ and contains at least one of the Sylow p-groups of $GL(n, K)$. ∎

In the infinite case the Sylow 'p-subgroups' may be identified with the maximal groups that have characteristic polynomial $(x-1)^n$, and these groups are generated by all the transvections, and all transvections are conjugate by a basis-change argument. Such considerations permit the extension of the above theorem to the case where K is any infinite field.

We record for convenience:

$$\rho := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}; \quad \sigma = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}. \quad \Longrightarrow \quad \tau := \sigma^{-1}\rho^{-1}\sigma^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{12.1}$$

12.4 Ostrom's Theorem.

We adopt the notation:

$$\rho = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}; \quad \rho_M = \begin{pmatrix} 1 & \mathbf{M} \\ 0 & 1 \end{pmatrix}.$$

From now on until Ostrom's theorem has been established we shall assume:

Hypothesis 12.4.1 *$\mathcal{N} \supset \{X, Y, 1\}$ is a partial spread on $V = F^n \oplus F^n$ admitting an automorphism group $G =< \rho, \rho_A >$, for some $A \neq \mathbf{0}$.*

The following elementary observations associated with the above hypothesis will be frequently used:

Remark 12.4.2 *The maps ρ and ρ_A are non-trivial elations of $\mathcal{N}$ with axis X and Y respectively. Moreover:*

1. *The map $\rho_A \in Aut\mathcal{N}$ maps X to $y = xA$; more generally an elation of $\mathcal{N}$ with axis Y mapping X onto a component $y = xM$ must be the map ρ_M, and conversely if $\rho_M \in Aut\mathcal{N}$ then it is an elation of the type just mentioned.*

2. *If $\rho_M \in Aut\mathcal{N}$ then M is non-singular; so A is non-singular.*

3. *The group G_Y of all Y-axes elations in G is isomorphic to an additive group of matrices $\mathcal{E}$ contained in the full set of slopes of $\mathcal{N}$. In fact*

$$\mathcal{E} = \{E \in F_n \mid \rho_E \in G\},$$

or equivalently

$$\mathcal{E} = \{E \mid y = xE \in Orb_{G_Y}(X)\} \cong G_Y.$$

4. *The elation ρ maps Y onto the unit line: $y = x := \mathbf{1}$.*

5. *The Y-orbit under G includes the unit line $\mathbf{1}$ among its components.*

Proof: The maps ρ and ρ_A are both elations of $\mathcal{N}$ since their fixed spaces are precisely components, viz., X and Y respectively. All the listed items are equally trivial to verify. ∎

Now suppose U is any G-invariant rank 2 K-subspace of V_K, using our standard notation, see page 197. So U cannot be part of a component since G contains non-trivial elation groups with distinct axes. Moreover, both ρ and ρ_A are elations of U, viewed as a K-spread, and this spread is Desarguesian because it has order $|K|$ and K is in the kern. So G_K induces a unimodular group $\tilde{G}$ of U. Furthermore, distinct elation axes associated with non-trivial elations in G must meet U in *distinct* components:

Lemma 12.4.3 *Suppose α and β are components of $\mathcal{N}$ such that each is the axes of a non-trivial elation in G. Then $\alpha_K \cap U$ and $\beta_K \cap U$ are distinct components of U.*

Proof: Let A and B be the groups of elations of $\mathcal{N}$ whose axes are respectively the components $\alpha, \beta \in \mathcal{N}$. Since A and B are both non-trivial p-groups and are K-linear each fixes a 1-dimensional K-subspace of U elementwise.

These spaces are disjoint since α_K and β_K are distinct components of $\mathcal{N}_K$. ∎
The following proposition shows that the group $G =< \rho, \rho_A >$ leaves invariant a rank 2 K-subspace U of V_K and induces on U the group $SL(2,K)$, *when K is taken to be $F(\lambda)$*, where λ is an eigenvalue of A. Thus establishing Ostrom's theorem will mainly involve showing that the G induces $SL(2,K)$ *faithfully* on U.

Proposition 12.4.4 *Assume $F = GF(p)$ is a prime field, $p > 3$, and fix the extension field $K = F(\lambda)$, where λ is any eigenvalue of an F-matrix A, in the algebraic closure of F. Then the group $G =< \rho, \rho_A >$ leaves invariant a rank two K-space U such that $G^U = SL(2,K)$.*

Proof: There is a K-matrix B such that

$$B^{-1}AB = \begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}, \tag{12.2}$$

now by a direct computation

$$\beta\rho\beta^{-1} = \rho, \tag{12.3}$$

where $\beta = Diag(\mathbf{B}, \mathbf{B})$.

Similarly the β-conjugate of ρ_A is given by:

$$\begin{pmatrix} \mathbf{B} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} \begin{pmatrix} \mathbf{1} & \mathbf{A} \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \begin{pmatrix} \mathbf{B^{-1}} & \mathbf{0} \\ \mathbf{0} & \mathbf{B^{-1}} \end{pmatrix} = \begin{pmatrix} \mathbf{1} & \mathbf{BAB^{-1}} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}, \tag{12.4}$$

and by eqn 12.2 the RHS above has top row of form:

$$(\underbrace{1,0,0,\ldots,0}_{n},\underbrace{\lambda,0,0,\ldots,0}_{n}),$$

so the β-conjugate of ρ_A leaves invariant the rank 2 K-space

$$\overline{U} = \left\{ (\underbrace{x,0,0,\ldots,0}_{n},\underbrace{y,0,0,\ldots,0}_{n}) \mid x,y \in K \right\},$$

and similarly ρ, which is its own β-conjugate, by eqn (12.3), also leaves $\overline{U}$ invariant. Thus the β-conjugate group $\beta G\beta^{-1}$ of G leaves invariant the 2-space W and clearly induces on it the group

$$\overline{G} =< \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} >$$

and now by Dickson's analysis, for $p > 3$[1], the subgroup of $H = SL(2,K)$ generated by $\overline{G}$ is $SL(2,L)$, where $L = Z(\lambda)$, Z the prime field of F. But as our hypothesis species that $Z = F$ and $K = F(\lambda)$, we conclude that $\overline{G} = SL(2,K)$.
Thus we have shown a β-conjugate of G induces $SL(2,K)$ on a rank 2 subspace of V_K. Hence the same must hold for G. ∎
From now we adopt the hypothesis and notation of the proposition above: $K = F(\lambda)$, where $F = GF(p)$ and λ is any eigenvalue of A; U is a G-invariant two-dimensional K-subspace of V_K, and as remarked earlier U is a rank-two K-space that is also a Desarguesian spread; so we have seen that $\tilde{G} = G^U = SL(2,K)$. It follows that $\tilde{G}$ is transitive on the non-zero points of U.

Lemma 12.4.5 *The set of axes $\mathcal{E}$ of non-trivial elations in G are in natural 1-1 correspondence with the components of U, i.e., the map*

$$\eta \in \mathcal{E} \mapsto \eta_K \cap U,$$

is a bijection from $\mathcal{E}$ onto the one-spaces of U.

Proof: Since by remark 12.4.2X is in $\mathcal{E}$, the transtivity of $\tilde{G}$ on U^* implies that every one-space of U is of form $\eta_K \cap U$, for some component $\eta \in \mathcal{E}$. The converse that every member $\mathcal{E}$ meets U in a component, has been mentioned in lemma 12.4. ∎
In order to count the conjugacy classes of p-elements in $SL(2,q)$ consider:

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix},$$

and so we have:

Remark 12.4.6 *Let P be a p-Sylow subgroup of $SL(2,q)$, q a power of the prime p. Then $N(P)$ has at most two non-trivial conjugacy classes in P and distinct classes have the same cardinality.*

Lemma 12.4.7 *There is an additive group of matrices $\mathcal{A} \cong (K,+)$ such that the identity $I \in \mathcal{A}$ and the subgroup of Y-shears in G is:*

$$\left\{ \begin{pmatrix} \mathbf{1} & M \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \mid M \in \mathcal{A} \right\}$$

[1]This explains Ostrom's constraint $p > 3$.

Proof: Let E be the elation subgroup of G associated with the Y-axis. This induces faithfully an elation group on U with axis Y, faithful, because elations of G extend to elations of G_K and hence cannot fix any points outside a component. So E may be identified with a *sub*group of η the full elation group in G^U with axis Y: it is conceivable that $G_{\{Y\}}$ contains a p-group $P > E$ such that P, although not itself an elation group, induces on U the full elation group η, of size $|K|$.
Consider the $G_{\{Y\}}$-conjugacy class of any non-trivial $a \in E$. We show that $E \cong (K,+)$ by showing that this class has $> |K|/2$ elements, and noting that any elation group in G has order $\leq |K|$, since it must faithfully induce an elation group of U.
Consider any non-trivial elation $a \in E$. Hence for any $t \in G_{\{Y\}}$, $\tilde{t}\tilde{a}\tilde{t^{-1}}$ agrees on U with the elation $tat^{-1} \in E$ and distinct $\tilde{t}\tilde{a}\tilde{t^{-1}}$ are 'induced' by distinct tat^{-1}, since they have distinct actions on U. So the number of elations $\nu \in E$ must exceed the number of elations of U fixing Y that lie in a conjugacy class of the stabilizer Y in $\tilde{G}$. So by remark 12.4.6, and the fact that E contains the identity, shows that $|E| > (q-1)/2$, so $|K| \geq |E| \geq q + 1/2 > q/2$ and this forces $E = K$, by Lagrange's theorem, and the fact that E^U may be identified with a subgroup of $(K,+)$. Since E consists of matrices of type ρ_M, where $y = xM$ is a component of $\mathcal{N}$ meeting U non-trivially, the desired result follows once we have noted $\mathbf{1} \in \mathcal{A}$. This holds because by remark 12.4.2.5 the unit line $y = x$ of $\mathcal{N}$ is in the G-orbit of Y and hence meets U non-trivially: so $\rho_1 \in G$ means that $\mathbf{1} \in \mathcal{A}$. ∎

Lemma 12.4.8 *The additive group $\mathcal{A} \cong (K,+)$ is also closed under inversion of its non-zero elements.*

Proof: Since $\mathbf{1} \in \mathcal{A}$, we have $-\mathbf{1} \in \mathcal{A}$, and the corresponding automorphism $\sigma \in G$. Hence by eqn 12.1 G contains:

$$\tau = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ -\mathbf{1} & \mathbf{0} \end{pmatrix}$$

and now any component $y = xM$ of $\mathcal{N}$ moves under τ to the component $y = x(-M^{-1}) \in \mathcal{N}$. So for, $M \in \mathcal{A}$, we must have $-M^{-1} \in \mathcal{A}$ since G, and hence τ, maps components meeting U into other components of the same type. But since τ is an additive group $M^{-1} \in \mathcal{A}$. ∎

Lemma 12.4.9 *G contains the map:*

$$\delta_A : (x, y) \mapsto (xA, yA^{-1}) >$$

Proof: Since $\mathcal{A}$ is closed under inversion we have $\rho_{A^{-1}} \in G$, since $A \in \mathcal{A}$. Hence G contains the map

$$\rho_A \tau^{-1} \rho_{A^{-1}} \tau \rho_A \tau^{-1},$$

which by a direct calculations is the matrix $Diag[A, A^{-1}]$ defining δ. ∎
The following result is essentially the theorem of Ostrom. It implies that if two elations with distinct axes fix a characteristic p partial spread $\mathcal{N}$, with $p > 3$ and $|\mathcal{N}| > 2$, then the group they generate a group $G \cong SL(2, q)$ and G leaves invariant a rational Desarguesian net contained in $\mathcal{N}$.

Theorem 12.4.10 (Ostrom's Elation Theorem.) *The spreadset $\mathcal{A}$ is a field $\cong K$, and $G = SL(2, \mathcal{A} \cong SL(2, K)$. Morover, the partial spread $\Delta_{\mathcal{A}}$ associated with $\mathcal{A}$ is a rational Desarguesian partial spread and G has the standard action on this partial spread, induced by its standard action on $\Delta_{\mathcal{F}}$, a Desarguesian spread associated with a field extension $\mathcal{F}$ of the field $\mathcal{A}$.*

Proof: We first establish that the polynomial ring $F[A]$ is a field $\cong K$. Since δ_A maps the component $y = xM$ onto $y = xA^{-1}MA^{-1}$, we have $A^{-1}MA^{-1} \in \mathcal{A}$, whenever $M \in \mathcal{A}$. Choosing M from $A, I \in \mathcal{A}$, we see that all odd and even powers of A^{-1}, and hence all powers of A lie in $\mathcal{A}$. But since $\mathcal{A}$ is an additive group it is also an F-module, over the prime field F. Thus the polynomial ring $F[A]$ is a subset of $\mathcal{A}$. But the non-zero elements of the algebra $< A >$ are invertible and, of course, closed under differences. Thus the algebra $< A >$ is also a partial spreadset of matrices, and hence, by proposition 12.2.3, the algebra is isomorphic to the field $F(\lambda) = K$.
But since, by lemma 12.4.8 $\mathcal{A} \cong (K, +)$, we now have $\mathcal{A} =< A >$ is a field of matrices $\cong K$. So, by lemma 12.4.7 we clearly obtain $< \rho, \rho_A >= SL(2, \mathcal{A}) \cong SL(2, K)$. Moreover, by lemma 12.4.7, the components of $\mathcal{N} - \{Y\}$, meeting U non-trivially are just those of form $y = xk$, $k \in \mathcal{A} \cong K$.
Next choose a matrix field $\mathcal{F} \supset \mathcal{A}$ such that $|\mathcal{F}| = |F|^n$, so the associated Desarguesian spread $\Delta_{\mathcal{F}}$ contains the partial spread associated with $\mathcal{A}$, that is the components of $\mathcal{N}$ that meet U non-trivially, or equivalently, the components of $\mathcal{N}$ that are the axis of non-trivial elations in the group G.

Thus $G \cong SL(2,K)$ leaves invariant a Desarguesian spread $\Delta_{\mathcal{F}}$ such that the components of $\mathcal{N}$ that are the non-trivial elation axes of elements in G, when G is regarded as acting on $\mathcal{N}$, form the slopeset of a subplane of $\Delta_{\mathcal{F}}$. [This may be esablished even without reference to 'U', since the only way that $SL(2,K)$ acts on a Desarguesian spread over a larger finite field $F \supset K$ is to leave invariant the subplane $K \oplus K$.] ∎

Ostrom's theorem needs to be slightly modified if we permit characteristic $p = 3$. We summarize without proof the situation when $p = 3$ is permitted in Ostrom's theorem.

Theorem 12.4.11 *Let π be a finite translation plane of odd order p^r. Let σ and τ denote two elations in the translation complement with distinct axes. Then one of the two following situations occur:*

1. *$\langle \sigma, \tau \rangle \cong SL(2, p^z)$ for some positive integer z and the elation net is a Desarguesian net which may be coordinatized by $GF(p^z)$.*

2. *$\langle \sigma, \tau \rangle \cong SL(2,5)$ and $p = 3$ and the elation net is a Desarguesian net which may be coordinatized by $GF(9)$.*

Finally, it is noted that Ostrom's theorem is actually more general than considered above and can be more generally applied to collineation groups generated by Baer p-groups. Note that what needs to be considered is whether the group generated by the set of all elations is also isomorphic to $SL(2, p^w)$ for some positive integer w and what occurs when $p = 2$ or 3.

We also may observe that this result is generally valid over finite dimensional vector spaces of characteristic p. The proof given uses the above result to deal with the exceptional case when $p = 3$, but is otherwise self-contained although it largely follows the Ostrom argument described above.

Theorem 12.4.12 *Let π be a translation plane which is finite dimensional over its kernel and let K be a subfield of the kernel of characteristic not 2.*

Let σ and τ be affine elations with distinct axes in the translation complement and let $G = \langle \sigma, \tau \rangle$. Let N denote the net each of whose components are axes of elations in G.

If G is finite then the characteristic of π is $p < \infty$ and one of the two following situations occur:

1. *$G \cong SL(2, p^s)$ for some positive integer s. Furthermore, N is a Pappian net which may be coordinatized by $GF(p^s)$.*

2. $G \cong SL(2,5)$. *In this case, N is a Pappian net which may be coordinatized by $GF(9)$.*

Proof: Assume the dimension of π over K is $2k$. Represent σ by $(x,y) \longmapsto (x, Ax+y)$ and τ by $(x,y) \longmapsto (x+y, y)$ where A is a $k \times k$ matrix with elements in K.

Note that the order of σ is finite if and only if the characteristic is finite p.

The proof of the theorem now follows from the following sequence of lemmas.

Lemma 12.4.13 *Let λ be an eigenvalue of A in some extension field $K(\lambda)$. Then A and hence λ has finite order and*

$$F = GF(p)(\lambda) \simeq GF(p^s),$$

for some positive integer s.

Proof: Consider $\sigma\tau = \begin{bmatrix} I & A \\ 0 & I \end{bmatrix}\begin{bmatrix} I & 0 \\ I & I \end{bmatrix} = \begin{bmatrix} I+A & A \\ I & I \end{bmatrix}$. Now square $\sigma\tau$ to obtain $\begin{bmatrix} (I+A)^2+A & (I+A)A+A \\ 2I+A & I+A \end{bmatrix}$. Squaring this element, we note that the entries in the $(1,1)$ -position are always nontrivial polynomial in A over $GF(p)$. If this element has finite order, it follows that eventurally the element in the $(1,1)$-entry is a polynomial in A over $GF(p)$ which is equal to $(1,1)$ -entry of a previous element in $\langle\sigma\tau\rangle$. Hence, A satisfies a polynomial over $GF(p)$. Thus, the minimal polynomial for A has coefficients in $GF(p)$ so that every eigenvalue in an extension field does as well.

Consider the field $GF(p)(\lambda)$ within $K(\lambda)$. Let the minimal polynomial for A have degree n so that every element in $GF(p)(\lambda)$ may be written in the form $\sum_{i=0}^{n} \lambda^i \alpha_i$ for $\alpha_i \in GF(p)$. Hence, $GF(p)(\lambda) = F$ is a finite field isomorphic to $GF(p^s)$ for some positive integer s.■

Lemma 12.4.14 *Let V denote the underlying vector space over K and let U be a 1-dimensional λ-eigenvector in $V \otimes_K K(\lambda) = V^*$. Then $U \oplus U$ is G-invariant.*

Proof: Realize σ and τ as linear transformations over V^* and apply the form to conclude that $U \oplus U$ is G-invariant. ■

Lemma 12.4.15 *$U \oplus U$ defines a Pappian plane which contains a G-invariant Pappian subplane π_o coordinatized by F.*

Proof: Since $F = GF(p)(\lambda)$ is a subfield of $K(\lambda)$, there is a Pappian subplane π_o of $U \oplus U$.

Since the elements in G restricted to $U \oplus U$ are all in $End_{GF(p)}\pi_o$, it follows that G leaves π_o invariant. ∎

Lemma 12.4.16 *If $G \mid \pi_o$ is G^{π_o} then either $G^{\pi_o} \simeq SL(2,p^s)$ or $p = 3$ and $G^{\pi_o} \simeq SL(2,5)$.*

Proof: Since π_o is a finite translation plane of odd order, the result follows from Ostrom's theorem ([34] and [35]). ∎

Lemma 12.4.17 *There are exactly $1 + p^s$ elation axes in N when G^{π_o} is $SL(2,p^s)$ and 10 elation axes in N when G^{π_o} is $SL(2,5)$.*

Proof: It follows exactly as in the previous section that every elation axis of N is also an axis of π_o . Since the group generated by the elations is transitive on the components of π_o(even in the case that the group is $SL(2,5)$ where $F \simeq GF(9)$ and there are 10 elations in $SL(2,5)$), we have that every component of π_o is an elation axis of N. ∎

Lemma 12.4.18 *When the group $G^{\pi_o} \simeq SL(2,p^s)$ then $(\mid A \mid, p) = 1$ and $x = 0, y = xM$ for all M in $GF(p)[A]$ is a partial spread. Hence, $GF(p)[A]$ is a field.*

Proof: The arguments of the previous section can be utilized in this case to conclude that $\left\langle \begin{bmatrix} A^{-1} & 0 \\ 0 & A \end{bmatrix} \right\rangle$ is a collineation group of the translation plane.

Hence, $y = x$ maps to $y = xA^{2i}$ under the group and $y = xA$ maps to $y = xA^{2i+1}$. It follows that $A^j - I$ is nonsingular or zero for each integer j. ∎

Lemma 12.4.19 *When the group $G^{\pi_o} \simeq SL(2,5)$ then $(\mid A \mid, p = 3) = 1$ and $x = 0, y = xM$ for all M in $GF(3)[A]$ is a partial spread so that $GF(3)[A]$ is a field.*

Proof: Hence, we may conclude that the net N is $\{x = 0, y = x(xA\alpha + \beta I)$ for all α, β in $GF(3)\}$ assuming that the Ostrom theorem is proved for finite planes in this case. Moreover, although not a collineation necessarily of the plane, the net admits the group $\left\langle \begin{bmatrix} I & A\delta + \gamma I \\ 0 & I \end{bmatrix}; \delta, \gamma \in GF(p) \right\rangle$. Now again apply the arguments of the previous section again, we may conclude again that the group $\left\langle \begin{bmatrix} A^{-1} & 0 \\ 0 & A \end{bmatrix} \right\rangle$ acts on the elation net N so that by the above argument, $(\mid A \mid, p = 3) = 1$. ∎

Lemma 12.4.20 *The elation net is a Pappian net and the group induced on $U \oplus U$ is faithful.*

Proof: Let $V = X \oplus X$. Then X is a semi-simple $K\langle A \rangle$-module $= \sum_{i=1}^{w} N_i$. Let F_i denote the restriction of $K\langle A \rangle$ to N_i. Then N_i is a 1-dimensional F_i -algebra. Moreover, $GF(p)[A]$ is a field which forms a partial spread set so that $GF(p)[A]$ acts faithfully on each N_i. Since one of these N_i's may be taken as U, it follows that $GF(p)[A]$ is isomorphic to $GF(p^s)$ or $GF(9)$ exactly when the induced group on $U \oplus U$ is $SL(2, p^s)$ or $GF(9)$. ∎
The main result theorem 12.4.12 has now been established.∎

12.5 Generalized Elations.

In this section, we present the preliminaries for the theorem of Foulser on Baer p-groups acting on translation planes of order p^r. When $p \neq 2$, Foulser showed that the Baer axes of two distinct Baer p-collineations in the translation complement are identical or share exactly the zero vector. In the previous section, Ostrom's theorem was presented. This theorem can be viewed as a theorem on partial spreads generated by certain automorphism groups called generalized elations. Once this is achieved, it is possible to show that Ostrom's Theorem may be applied to conclude that the groups generated by Baer p-elements are exactly those in the elation case. Using the extension of Ostrom's theorem, it is possible to extend Foulser's work to the finite dimensional case as well.

In this section, we follow Foulser's work in [11].

Definition 12.5.1 *Let V be a vector space of dimension n over $K \simeq GF(p^r)$. Let σ be a linear transformation of V . Let $Fix\sigma$ denote the set of vectors fixed by σ. Then σ is said to be a generalized elation of V of type t if and only if σ fixes $V/Fix\sigma$ pointwise and the dimension of $Fix\sigma = t$..*

The subspace $Fix\sigma$ is called the 'axis'of σ and $C(\sigma) = (\sigma - 1)V$ is called the 'center'of σ.

Remark 12.5.2 *We have seen that elations are generalized elations of type $n/2$. Consider a Baer collineation σ of order p. We shall show that σ a generalized elation also of type $n/2$.*

Note that σ is a generalized elation if and only if $(\sigma - 1)^2 = 0$.

Proposition 12.5.3 *Let σ be a generalized elation of V of type t. Then*

(1) The order of σ is p;

(2) $\dim C(\sigma) + \dim Fix\sigma = n$;

(3) $t \geq n/2$ and

(4) If W is a complement of $Fix\sigma$ then, with respect to $Fix\sigma \oplus W$, σ has the following matrix representation

$$\begin{bmatrix} I & A \\ 0 & I \end{bmatrix}$$

where A is a $t \times (n - t)$ matrix.

Exercise 12.5.4 *Prove (1).*

Exercise 12.5.5 *Prove (2) noting that $V/Fix\sigma \cong (\sigma - 1)V$.*

Exercise 12.5.6 *Use (2) to prove (3) noting that $C(\sigma) \subseteq Fix\sigma$.*

Exercise 12.5.7 *Prove (4).*

Corollary 12.5.8 *The group generated by a set of generalized elations with the same axis is elementary Abelian of order p^a for some positive integer a.*

We now specialize to the case when σ is a generalized elation which is a collineation of a translation plane π of order $q^{n/2}$ with associated vector space of dimension n over a field $K \simeq GF(q = p^r)$.

We recall that if π_o^+ is a projective subplane of order m of a projective plane π^+ of order w then $m \leq \sqrt{w}$. Hence, if τ is a planar collineation of a translation plane then $Fix\tau$ has dimension less than or equal to half the dimension of the underlying vector space.

Theorem 12.5.9 *A generalized elation acting as a collineation of a finite translation plane of order p^s is either an elation or a Baer p-element.*

Proof. Note that we must have that a generalized elation σ is of type s if the order of the plane is p^s since the dimension of the vector space is $2s$ over $GF(p)$. Hence, the cardinality of $Fix\sigma$ is also p^s.

Exercise 12.5.10 *Show that if a collineation σ of an affine plane of order k fixes exactly k points then $Fix\sigma$ is either a line or a Baer subplane.*

It remains to show that a Baer p-element is a generalized elation.

Choose any complement W of $Fix\sigma$ so that with respect to the decomposition $Fix\sigma \oplus W$, we have the following representation for σ

$$\begin{bmatrix} I & A \\ 0 & B \end{bmatrix}$$

It remains to show that $B = I$. Note that the order of σ is p so we must have $B^p = I$.

Suppose L and M are components intersecting $Fix\sigma$ in a $s/2$ -dimensional subspace. Choose a basis for the intersections with $Fix\sigma$ and extend to a basis for L and M and hence for the translation plane. With the decomposition $L \oplus M$, we have a basis of $4(s/2)$-vectors and letting x_i, y_i be $(s/2)$-vectors, the representation is (x_1, x_2, y_1, y_2) where M is $x_1 = x_2 = 0$, L is $y_1 = y_2 = 0$ and $Fix\sigma$ is given by the equation $x_2 = 0 = y_2$. Without loss of generality, we assume that $y = x$ is a component of $Fix\sigma$.

Now consider the $p^{s/2} + 1$-components of the translation plane that lie on $Fix\sigma$. These have matrix equations as follows $x = 0, y = 0, y = x, y = x \begin{bmatrix} B_{1i} & B_{2i} \\ 0 & B_{4i} \end{bmatrix}$ where it may be noted that the components of $Fix\sigma$ are $x_2 = 0, y_2 = 0, y_2 = x_2$ and generally $y_2 = x_2 B_{4i}$ for $i = 1, 2, ..., p^{s/2} - 1$.

Since the collineation fixes $x = 0, y = 0, y = x$ it follows that the form for σ is now

$$\begin{bmatrix} I & E & 0 & 0 \\ 0 & D & 0 & 0 \\ 0 & 0 & I & E \\ 0 & 0 & 0 & D \end{bmatrix}$$

Note that comparing the previous decomposition, we have $\begin{bmatrix} E & 0 \\ 0 & E \end{bmatrix} = A$ and $\begin{bmatrix} D & 0 \\ 0 & D \end{bmatrix} = B$.

Since σ fixes each line of $Fix\sigma$ so that $\begin{bmatrix} I & -ED^{-1} \\ 0 & D^{-1} \end{bmatrix} \begin{bmatrix} B_{1i} & B_{2i} \\ 0 & B_{4i} \end{bmatrix} \begin{bmatrix} I & E \\ 0 & D \end{bmatrix} = \begin{bmatrix} B_{1i} & B_{2i} \\ 0 & B_{4i} \end{bmatrix}$ which implies in particular that $D^{-1}B_{4i}D = B_{4i}$. Since $\{B_{4i}$ $i = 1, 2, ..., p^{s/2} - 1\}$ defines a spread set, and a spread set acts transitively on the non-zero vectors of the associated vector space $V_{s/2}$, it follows that D centralizes an irreducible set of linear transformations of $V_{s/2}$. By Schur's lemma, it follows that D belongs to a field (finite division ring) isomorphic to $GF(p^e)$. In any case, since $B^p = 1$ also $D^p = 1$ and hence $D = 1$ so that also $B = 1$.

We now may restate Ostrom's theorem for generalized elations of vector spaces provided the set of images of the fixed point subspaces is a partial spread. The previous proof may be reread to prove the following theorem.

Theorem 12.5.11 *Let V be a finite vector space of dimension $2k$ over $GF(p)$. Let σ and τ be generalized elations of V with distinct axes.*

Let $S = \{Fix\sigma \langle \sigma, \rho \rangle, Fix\tau \langle \sigma, \rho \rangle\}$.

Then the following are equivalent:

(1) $\langle \sigma, \rho \rangle \simeq SL(2, p^z)$ for some positive integer z.

(2) S is a partial spread of V.

(3) Representing $\langle \sigma, \rho \rangle = \left\langle \begin{bmatrix} I & I \\ 0 & I \end{bmatrix}, \begin{bmatrix} I & 0 \\ A & I \end{bmatrix} \right\rangle$ then $GF(p)[A]$ is a field isomorphic to $GF(p^z)$.

Furthermore, when the above conditions are satisfied then S is a Desarguesian partial spread coordinatizable by $GF(p^z)$ within the Desarguesian plane coordinatized by $GF(p^k)$ and the unique involution in $SL(2, p^z)$ is the kernel homology -1.

The questions now are whether it can be guaranteed that two Baer p -collineations always or ever have disjoint axes and if it is possible that, in the above theorem σ could be an elation while ρ is a Baer p-collineation. Both of these questions have been resolved by Foulser when $p > 3$. Recall that a Baer subplane of a finite projective plane of order n is a subplane of order $\sqrt{n}$.

Chapter 13

Foulser's Theorem: Baer-Elation Incompatibility.

In this chapter, we demonstrate the high degree of incompatibility between Baer p-elements and affine elations, acting on a translation plane π of order p^{2r}. Among the most startling of such results is Foulser's theorem, asserting that non-trivial Baer p-elements and non-trivial affine elations cannot simultaneously act on π if p is odd. The first section of this chapter establishes striking constraints of this type, all due to Foulser, that apply to translation planes of odd order. The second section is concerned with the even order versions of Foulser's theory: here affine elations and Baer 2-elements *are* compatible, but they constrain each otehr quite severely.

13.1 Baer-Elation Theory: Odd Order Case.

We begin with a theorem that allows us to use Ostrom's theorem for generalsied elations due to Foulser.

Theorem 13.1.1 *Let π be a translation plane of order p^{2k} for $p > 3$.*

If σ and τ are Baer p-collineations in the translation complement whose axes are distinct then $Fix\sigma \cap Fix\tau = 0$.

Proof: Sketch. Suppose not! Then there exist σ and τ as Baer p-collineations such that $Fix\sigma \cap Fix\tau = X$ has maximum dimension r over $GF(p)$. We note that if X is a proper subplane of $Fix\sigma$ then $r \leq k/2$ and if X is a part of a line of $Fix\sigma$ this restriction is still valid.

Note that any generalized elation leaves invariant any subspace containing the axis. Hence, both σ and τ leave $Fix\sigma + Fix\tau$ invariant and act faithfully as generalized elations of $(Fix\sigma + Fix\tau)/X = V_1$. Let $\sigma_1 = \sigma \mid V_1, \tau_1 = \tau \mid V_1$.

We consider the following three possible cases:

(1) $Fix\sigma_1 \cap Fix\tau_1 = 0$ on V_1,

(2) both σ_1 and τ_1 are non-trivial on V_1 and $Fix\sigma_1 \cap Fix\tau_1 \neq 0$ and

(3) either σ_1 or $\tau_1 = 1$.

We consider case (3) first and assume $\sigma_1 = 1$.

Exercise 13.1.2 *Show that $\sigma_1 = 1$ if and only if σ fixes $Fix\tau$.*

Since σ fixes $Fix\tau$, σ is a generalized elation on $Fix\tau$ so induces either an elation or a Baer p-element on $Fix\tau$. In either case, we may choose a decomposition for V as follows: Let $Fix\tau \cap Fix\sigma = X_0$, $Fix\sigma = X_0 \oplus X_1$, $Fix\tau = X_0 \oplus X_2$ and $V = X_0 \oplus X_1 \oplus X_2 \oplus X_3$.

The group E generated by the Baer p-collineations with axis $Fix\tau$ is an elementary Abelian group p-group and all nonidentity elements of this group have the same axis. It follows that σ normalizes E and since the order of σ is p, σ commutes with some element of E and we may assume that σ and τ commute (here we don't insist on the maximality condition on intersection dimension).

Exercise 13.1.3 *Under the assumptions that σ and τ are Baer collineations (generalized elations), and assuming the matrix acts on the right, show that*

$$\sigma = \begin{bmatrix} I & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ A_1 & A_3 & I & 0 \\ A_2 & A_4 & 0 & I \end{bmatrix}$$

and that

$$\tau = \begin{bmatrix} I & 0 & 0 & 0 \\ B_1 & I & B_2 & 0 \\ 0 & 0 & I & 0 \\ B_3 & 0 & B_4 & I \end{bmatrix}$$

Exercise 13.1.4 *Using the above exercise and the fact that σ and τ commute show that $A_3 = B_2 = 0$ and*

Exercise 13.1.5 *Change basis by* $\begin{bmatrix} A_1 & 0 & 0 & 0 \\ A_2 & A_4 & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{bmatrix}$ *and realize that the general form of* τ *does not change to obtain that, without loss of generality,* $A_1 = A_4 = I$ *and* $A_2 = 0$. *Then ,again using the fact that* σ *and* τ *commute, show that that* $B_1 = B_4$.

Exercise 13.1.6 *Show that* $\sigma\tau$ *is a generalized elation by computing* $\sigma\tau$ *and its fixed point space.*

Exercise 13.1.7 *Compute* $(\sigma\tau - 1)^2$ *and show that the following matrix is obtained:*

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2B_1 & 0 & 0 & 0 \end{bmatrix}.$$

Now since $(\sigma\tau - 1)^2 = 0$, it follows that $B_1 = 0$. From the above exercise, it turns out that the fixed point space of $\sigma\tau$ is too large to be either a line or a Baer subplane.

This proves case (3). Actually, this same proof can be adapted to show hat Baer p-elements and elations cannot coexist when $p > 2$. We shall come back to this in a later section.

Case (2) both σ_1 and τ_1 are non-trivial on V_1 and $Fix\sigma_1 \cap Fix\tau_1 \neq 0$.

Suppose that $Fix\sigma_1 = Fix\sigma/X$ and $Fix\tau_1 = Fix\tau/X$. Then $Fix\sigma/X \cap Fix\tau/X = X$ or rather $Fix\sigma_1 \cap Fix\tau_1 = 0$.

Hence, assume without loss of generality, that $y + X$ is in $Fix\sigma_1 - Fix\sigma/X$ and write $y = v + u$ where v is in $Fix\sigma$ and u is in $Fix\tau$. Since σ_1 fixes $y + X$, it follows that σ also fixes $u + X$. Since τ fixes $X = Fix\sigma \cap Fix\tau$ pointwise, it follows that $\langle u, X\rangle \subseteq Fix\tau$. Note that u is nonzero by assumption. But, $\langle u, X\rangle \subseteq \sigma(Fix\tau) = Fix\tau^{\sigma^{-1}}$. But, $Fix\tau^{\sigma^{-1}} \neq Fix\tau$ since if it were this would imply that $\sigma_1 = 1$ by an exercise above. Hence, τ and $\tau^{\sigma^{-1}}$ are generalized elations of V both of whose fixed point space properly contain X which is contrary to the maximality condition.

Hence, it remains to consider

Case (1) $Fix\sigma_1 \cap Fix\tau_1 = 0$ on V_1.

We give the proof in a series of lemmas.

Lemma 13.1.8 $(\sigma - 1)Fix\tau \oplus X = Fix\sigma$ *and* $(\tau - 1)Fix\sigma \oplus X = Fix\tau$

Proof: Consider $(\sigma-1)v$ for v in $Fix\tau$. If $(\sigma-1)v \neq 0$ then v is not in X. If $(\sigma-1)v$ is in $Fix\sigma \cap Fix\tau$ then σ fixes $v+X$ and clearly τ fixes $v+X$ so that σ_1 and τ_1 fix a common nonidentity element and hence $Fix\sigma_1 \cap Fix\tau_1 \neq 0$.

Notice that the kernel of $\sigma - 1$ in $Fix\tau$ is $Fix\tau \cap Fix\sigma$ and $Fix\tau/X \simeq (\sigma - 1)Fix\tau$. By the rank-nullity theorem, the result now follows.

Lemma 13.1.9 $\langle \sigma, \tau \rangle = G$ *leaves* $(\sigma-1)Fix\tau \oplus (\tau-1)Fix\sigma = V_2$ *invariant.*

Proof: Note that $(\sigma - 1)^2 = (\tau - 1)^2 = 0$ and apply $(\sigma - 1)$ to $(\sigma - 1)v + (\tau - 1)u$ for v in $Fix\tau$ and u in $Fix\sigma$ realizing that $(\tau - 1)w$ is in $Fix\tau$ for any w in V. Hence, $\sigma - 1$ and $\tau - 1$ and thus σ and τ leave the given subspace invariant.

Exercise 13.1.10 *Check that the sum is a direct sum.*

Lemma 13.1.11 *Let* $\rho_2 = \rho \mid V_2$. *Let* $G_2 = \langle \sigma_2, \tau_2 \rangle$. *Then* $G_2 \simeq SL(2, p^z)$ *for some positive integer* z.

Proof: The idea of the proof is to show that the set $\{Fix\sigma_2^g$, $Fix\tau_2^h$ for g,h in $G_2\}$ is a partial spread and then apply Ostrom's theorem. Note that σ_2 and τ_2 are generalized elations of V_2.

Note that $Fix\sigma_2 = Fix\sigma \cap V_2 = (\sigma - 1)Fix\tau$ and $Fix\tau_2 = Fix\tau \cap V_2 = (\tau - 1)Fix\sigma$. These subspaces are both of dimension $k - r$ and since we have a direct sum above, these particular fixed point spaces are disjoint so that V_2 has dimension $2(k - r)$ and the generalized elations are of type $k - r$.

Now assume there exist ρ and γ in G which are conjugate to σ and/or τ such that $Fix\rho_2 \neq Fix\gamma_2$ but $Fix\rho_2 \cap Fix\gamma_2 \neq 0$. Then, it follows that $Fix\rho \cap Fix\gamma \subseteq X \oplus Fix\sigma_2 \cap Fix\rho_2$ contrary to the maximality condition. Hence, $G_2 \simeq SL(2, p^z)$. In particular, -1 is in G_2 acting on V_2. This proves the lemma.

Lemma 13.1.12 *Let* θ *be in* G *such that* $\theta_2 = -1$. *Then* $\theta^2 = 1$.

Exercise 13.1.13 *Note that any nonidentity collineation can pointwise fix a subspace of dimension* $\leq k$ *(one half the dimension of the translation plane). Prove the above lemma by considering* $X \oplus V_2$ *and realizing that* G *fixes* X *pointwise and show that the dimension of* $X \oplus V_2$ *is* $2k - r > k$.

Lemma 13.1.14 $G \simeq G_2$.

Proof: Since G fixes V_2, the group induced on V_2 is isomorphic to $G/G[V_2]$ where $G[V_2]$ is the subgroup which fixes V_2 pointwise. The above exercise shows that $G[V_2] = \langle 1 \rangle$.■

Remark 13.1.15 *A result of Baer's states that in any finite affine plane, an involution either fixes pointwise a line or a Baer subplane. Thus, the dimension of a pointwise fixed subspace by an involution of a translation plane is half the dimension of the translation plane*

Note that $(-\theta)^2 = 1$ so that $-\theta$ is an involution.

Lemma 13.1.16 *The subspace fixed pointwise by $-\theta$ contains V_2. Then $r = k/2$.*
Furthermore, θ is in $Z(G)$.

Proof: From the preceding, we have $2(k - r) \leq k$ so that $k/2 \leq r$ but $r \leq k/2$ since X is either contained with a line of $Fix\sigma$ or is a subplane of it (note that the intersections of subplanes is either contained within a line or is a subplane of each containing subplane). So, $r = k/2$. Note that $(w\theta w^{-1})_2 = \theta_2^w = \theta_2 = -1$. It follows that $Fix\theta^{-1}w\theta w^{-1}$ contains $X \oplus V_2$ since G fixes X pointwise. Hence, $\theta^{-1}w\theta w^{-1} = 1$ which proves the lemma.

Thus, it follows that $Fix\theta$ is left invariant by G. Represent $Fix\theta = X \oplus W$ where both X and W are $k/2$-dimensional subspaces.

Lemma 13.1.17 $W \oplus (Fix\sigma + Fix\tau) = V$.

Proof: By the previous notes on dimension, it suffices to show that the indicated direct sum is, in fact, direct.

If $\theta(v + u) = v + u$ for v in $Fix\sigma$ and u in $Fix\tau$ then recalling that θ is in $Z(G)$, we have $\sigma\theta(v + u) = \theta(v + \sigma(u)) = v + \sigma(u)$. It then follows that $\sigma(u) - u = (\sigma - 1)u$ is fixed by θ. But, θ acts as -1 on V_2 so that $u = 0$. Similarly, $v = 0$.

Now let $\phi_3 = \phi \mid Fix\theta$. Then σ_3 and τ_3 are generalized elations of $Fix\theta$ with identical fixed point spaces X since σ does not fix a nonidentity element of W.

Hence, we obtain

Lemma 13.1.18 *$\langle \sigma_3, \tau_3 \rangle$ is an elementary Abelian p -group (of order p^2).*

Exercise 13.1.19 *Show that the commutator subgroup G' of G fixes $Fix\theta$ pointwise.*

However, $G' = G$ as $G \simeq SL(2, p^z)$. On the other hand, G leaves invariant V_2 and θ acts on V_2 as -1, $V_2 \cap Fix\theta = 0$. Hence, there exists an element g of order p which fixes a nonzero point of V_2 which implies that $Fixg$ has dimension strictly larger than k –a contradiction. Hence, this completes the proof of case (3) and consequently the proof of the theorem.

It might be pointed out that both Ostrom's and Foulser's theorems can be stated for $p = 3$ also and in this case, it is possible that $SL(2, 5)$ is generated. Furthermore, the full group generated by elations or Baer p -collineations is completely determined by the work of Ostrom, Hering and Foulser.

We mentioned above that an adaption of the proof of case (3) will show that it is not possible to have both Baer p-collineations and elations acting on a translation plane of odd order. We state this formally. We note that this case only requires that p is odd.

Theorem 13.1.20 *Let π be a finite translation plane of odd order p^r.*

Then the collineation group of π does not contain both Baer p -collineations and elations.

Furthermore, Foulser shows that all Baer axes of p-collineations share their parallel classes.

Theorem 13.1.21 *Let π be a finite translation plane of odd order p^{2k} for $p > 3$.*

If B denotes the set of axes of Baer p-collineations in the translation complement then each subplane of B lies in the same net of degree $p^k + 1$.

Proof: In this case, the group generated by any pair of Baer p -collineations is $SL(2, p^z)$ for some positive integer z. Since any two distinct axes π_0 and π_1 share exactly the zero vector, we may decompose the space as $\pi_0 \oplus \pi_1$ so that the collineation group has the form

$$\left\langle \begin{bmatrix} a & b \\ c & d \end{bmatrix}; ad - bc = 1 \text{ for all } a, b, c, d \text{ in } K \simeq SL(2, p^z) \right\rangle.$$

In particular, we have the subgroup $\left\langle \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}; a \text{ in } K - \{0\} \right\rangle$. Choose a in the prime subfield $F \simeq GF(p)$ of K and since $p > 3$, we may assume that $a \neq a^{-1}$. We note that a field of $2k \times 2k$ matrices over a field $GF(p)$ contains the scalars αI_n. Hence, $a = \lambda I_{2k}$ for λ in $GF(p) \subseteq$the kernel of the translation plane.

In other words, $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ is a kernel homology if a is in the prime subfield of K. Hence, it follows that $\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} = g_a$ acts as a scalar group on each subplane π_0 and π_1 so fixes each line of π_o and each line of π_0 incident with the zero vector. But, $\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} a^2 & 0 \\ 0 & 1 \end{bmatrix} = h \neq I$ fixes each line of π_0 and fixes π_1 pointwise. Since the fixed lines of h are exactly the lines of π_1, it follows that each line of π_0 extending to a line of π is a line of π_1. Hence, each line of π_0 incident with the zero vector is a line of π_1 and conversely. Hence, the lines of π_0 incident with the zero vector are exactly the lines of π_1 which are incident with the zero vector.

Furthermore, more can be said about the structure of the net containing the Baer axes and we shall come back to this in the next section in more generality both for even order and for infinite order.

13.2 Incompatibility Theory: Even Order Translation Planes.

We have seen in the previous section that, when p is odd, it is not possible that elations and Baer p-collineations can coexist in translation planes of order p^r. This is definitely not the case in planes which are not translation planes. For example, there exist semi-translation planes of order q^2 derived from dual translation planes for which there is a Baer group of order q and an elation group of order q as well. Furthermore, it is possible that Baer involutions and elations exist even in Desarguesian affine planes of even order. If π is Desarguesian of order q^2 coordinatized by $GF(q^2)$ then the field automorphism of order 2 which fixes $GF(q)$ pointwise induces a Baer involution.

When π is a semifield plane of even order, Ganley [14] has shown that if there is a Baer involution then the full group which fixes the Baer axis

pointwise has order 2.

Exercise 13.2.1 *Let π^+ be any projective plane and π_o^+ a projective subplane. Let σ be a central collineation. Then show that σ leaves π_o^+ invariant if and only if the center and axis of σ are in π_o^+ and for some point P of π_o^+ then σP is also a point of π_o^+.*

Exercise 13.2.2 *Let π be a semifield plane with special point (∞) on the line at infinity. Let π_o be an affine subplane of order h of π one of whose parallel classes is (∞). Show there exists an elation group of order h which leaves π_o invariant.*

Note that, in a semifield plane of even order q^2, if there exists a Baer subplane sharing the special point on the line at infinity then there exists an elation group of order q which leaves the subplane invariant.

13.2.1 Maximal Elation Groups and Baer involutions.

Here we consider this more generally. The reader is referred to Jha and Johnson [21] for more details.

Theorem 13.2.3 *Let π be a translation plane of even order q^2 for $q = 2^r$. Let π_o be a Baer subplane of π which is fixed pointwise by a Baer 2 -group B. If π admits an elation group $\mathcal{E}$ of order q which normalizes $\mathcal{B}$ then $\mid \mathcal{B} \mid \leq 2$. If $\mid \mathcal{B} \mid = 2$ then the full collineation group which fixes π_o pointwise has order 2.*

Proof: The proof will be given as a series of lemmas. In particular, we shall require a more-or-less standard representation of the translation plane and Baer subplane.

Represent π is the form $\{(x_1, x_2, y_1, y_2);\ x_i, y_i$ are r -vectors over $GF(2)$ for $i = 1, 2\}$. Represent with equation $x_1 = y_1 = 0$ and consider a spread for π is the form $lx = 0, y = 0, y = xM$ where x is a $2r$ -vector and M is a nonsingular $2r \times 2r$ matrix. We also assume, with loss of generality, that $x = 0, y = 0, y = x$ are components of π_o also and that the axis of $\mathcal{E}$ is $x = 0$.

This first lemma depends on the previous representations and should be clear by now.

Lemma 13.2.4 *Let the kernel of π_o be denoted by K_o where K_o is consider as the set of $r \times r$ matrices centralizing the slopes of π_o.*

(i) $\mathcal{B}$ may be represented in the following form:

$$\left\langle \begin{bmatrix} I & B & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & B \\ 0 & 0 & 0 & I \end{bmatrix} ; B \in \lambda \text{ and } 0, I \in \lambda \right\rangle.$$

(ii) The components of π_o may be represented in the form

$$x = 0, y = x \begin{bmatrix} C & f(C) \\ 0 & C \end{bmatrix}$$

for C in a set Ω of matrices where $f : \Omega \longmapsto Hom_{GF(2)}(V_{2r}, V_{2r})$ where V_{2r} is a $2r$-dimensional vector space over $GF(2)$ such that $f(I) = f(0) = 0$.

Exercise 13.2.5 *Prove that λ is contained in the kernel K_o of π_o.*

Note that since we are assuming that $\mathcal{E}$ normalizes $\mathcal{B}$, it follows that E acts transitively on the non-axis components of π_o . Hence, we have

Lemma 13.2.6 *$\mathcal{E}$ may be represented in the form*

$$\left\langle \begin{bmatrix} I & 0 & C & f(C) \\ 0 & I & 0 & C \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{bmatrix} ; C \in \Omega \right\rangle.$$

Exercise 13.2.7 *Prove that if $\mathcal{B}$ has order > 2 then we may take λ to include $\{0, I, B, B + I\}$ for some fixed $B \neq 0$ or I.*

Now let $\sigma_D = \begin{bmatrix} I & D & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & D \\ 0 & 0 & 0 & I \end{bmatrix} \in \mathcal{B}$ and let $\tau_E = \begin{bmatrix} I & 0 & E & f(E) \\ 0 & I & 0 & E \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{bmatrix} \in \mathcal{E}$.

Exercise 13.2.8 *Show that $\sigma_D\tau_E$ is a Baer involution and a component $y = x\begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}$ is fixed by $\sigma_D\tau_E$ if and only if $m_3 = D^{-1}E$ and $Dm_4 = f(E) + ED + m_1D$. (Hint: Write out what the conditions are for a component to be fixed by $\sigma_D\tau_E$ recalling that D is in the kernel of K_o and hence commutes with E).*

Lemma 13.2.9 *Let $S_D = \{\sigma_D\tau_C;\ C \in \Omega\}$. The components by elements of S_D cover π. Hence, this implies that, for each $C \in \Omega$, $B^{-1}C$ is also in Ω and furthermore, B^i and B^jC is in Ω for all integers i, j.*

Exercise 13.2.10 *Prove the previous lemma.*

Thus, we have:

Lemma 13.2.11 *$\langle \sigma_I\tau_{B^{-1}C}, \sigma_B\tau_C\rangle$ fixes the same Baer subplane pointwise (namely, $\{(0, y_2B^{-1}C, y_1, y_2)\}$).*

Hence, $Dm_4 = f(E) + ED + m_1D$ for $(D, E) \in \{(B, C), (I, B^{-1}C), (B + 1, (B^{-1} + 1)C\}$.

Choose $(D, E) = (I, B^{-1}C)$, we obtain $m_4 = f(B^{-1}C) + B^{-1}C + m_1$. Now reapplying (B, C), we obtain

$$Bm_4 = B(f(B^{-1}C) + B^{-1}C + m_1) = f(C) + CB + m_1B$$

which implies that

$$Bf(B^{-1}C) + (B + I)C + f(C) = Bm_1 + m_1B.$$

Let $g_0(C) = Bf(B^{-1}C) + f(C)$.

Exercise 13.2.12 *For $k \geq 1$ if*

$$g_k(C) = g_{k-1}(C)B^{2k-1} + B^{2k-1}g_{k-1}(C)$$

then

$$g_k(C) = B^{2^k}m_1 + m_1B^{2^k}.$$

(Hint: Recall that $BC = CB$.)

Since B is in the kernel of the subplane of order q , it follows that $B^q = B$.

Hence, when $q = 2^r$, it follows that $g_r(C) = Bm_1 + m_1B = g_0(C) + (B + I)C$.

Lemma 13.2.13 *Let* $J(C) = \sum_{i=1}^{q-1} B^i f(C) B^{-i}$.

Then

(i) $J(C) + BJ(B^{-1}C) = (I + B)C$ *and*

(ii) $J(B^2C) = B^2J(C)$.

Proof:

Exercise 13.2.14 *Show that* $g_k(C) = \sum_{i=o}^{2^k-1} B^i f(C) B^{(2^k-1)-i} + \sum_{i=1}^{2^k} B^i f(B^{-1}C) B^{2^k-i}$.

Then let $k = r$ *and using the fact that* $g_r(C) + g_{0(C)} = (I + B)C$ *conclude that (i) is valid.*

Exercise 13.2.15 *Since* BC *is in* Ω, *replace* C *by* BC *in (i) to conclude (ii).*

Since the above lemma is valid for all elements C of Ω, letting $C = I$, we obtain by induction that

$$J(B^{2^k}) = B^{2^k} J(I) = 0.$$

Letting $r = k$, we have that $J(B) = 0$. In (i) above, let $C = B$ to obtain $(I + B)B = 0$. Hence, $B = 0$ or I contrary to our assumptions. Hence, the Baer 2-group has order 2 or 1. If the order is 2 then since the group fixing the Baer axis normalizes the 2-group fixing it pointwise, it follows that any Baer group must commute with a given Baer involution which cannot occur unless the group has order 2 itself. This completes the proof of the theorem.

13.2.2 Large Baer groups and Elations.

Considering possible incompatibility relations, we consider the co-existence of a 'large' Baer group and an elation group of order > 2. Recall that it follows from the previous subsection that the existence of a Baer group of order $> \sqrt{q}$ shows that the Baer axis is a Desarguesian subplane. In this subsection, we consider the possible incompatibility with Baer groups of order $> \sqrt{q}$ and elation groups of order > 4.

Previously, we required that a given elation group normalizes a Baer group and hence centralizes it. A result of Dempwolff [9] shows that if a Baer group of order $> \sqrt{q}$ normalizes an elation group E then it must centralize it.

Exercise 13.2.16 *Let π be a translation plane of order 2^r that admits a Baer group $\mathcal{B}$ of order $> \sqrt{q}$. Let E be any affine elation group. Let S_2 be a Sylow 2-subgroup containing the full elation group E^* with axis E. Show that there exists a Baer group $\mathcal{B}^*$ of order $\mid \mathcal{B} \mid$ contained in S_2. Show that $\mathcal{B}^*$ normalizes the full group E^*.*

Hence, if we use the result of Dempwolff, we may assume the existence of an elation group E and a Baer group $\mathcal{B}$ of order $> \sqrt{q}$ which centralizes each other.

Theorem 13.2.17 *Let π be a translation plane of order $q^2 = 2^{2r}$ that admits a Baer group of order $\geq 2\sqrt{q}$. If E is any elation group of π then $\mid E \mid \leq 2$.*

Proof: We formulate the proof in a manner similar to the above. In particular, we take the representation exactly as in the previous subsection. However, now we know that the elements of λ belong to a field $K \simeq GF(q)$ that coordinatizes the Baer subplane so that we may assume that the elements of Ω belong to the field K. ∎

Lemma 13.2.18 *For each C of Ω, then $\mid C\lambda \cap \lambda \mid \geq 4$.*

Proof: Note that λ is a vector space over $GF(2)$ as it is additive. Similarly, $C\lambda$ is a vector space over $GF(2)$. Furthermore, $\dim\lambda > r/2$ so $\geq r/2 + 1$. Hence, $C\lambda + \lambda$ is a subspace of K so that the dimension of the intersection $C\lambda \cap \lambda$ is at least 2. Hence, the order is at least 2^2.

The impact of the previous lemma is that there are at least two Baer groups of order 4 which come from the same element τ_C.

Lemma 13.2.19 *For each C in Ω, there exist distinct nonzero elements E and F such that*

$\langle \sigma_B\tau_I, \sigma_{BC}\tau_C \rangle$ fixes a Baer subplane $\{(0, y_2B, y_1, y_2)\}$ pointwise for $B \in \{E, F\}$.

Proof: Let CE and CD be in $C\lambda \cap \lambda$. Recall that $\sigma_D\tau_E$ fixes $y = x \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}$ if and only if $m_3 = D^{-1}E$ and $Dm_4 = f(E) + ED + m_1D$. Thus, the indicated group must fix the same Baer subplane pointwise.

Noting that $f(I) = 0$, let $D = B$ and $E = I$ to obtain $Bm_4 = B + m_1B$. But, also we may let $D = BC$ and $E = C$ to obtain $BCm_4 = f(C) + BC^2 + m_1BC$.

Thus, $C(B + m_1B) = f(C) + BC^2 + m_1BC$.

Exercise 13.2.20 *Show that* $C^2m_1B + m_1BC^2 = f(C)C + Cf(C)$.

Exercise 13.2.21 *Let* $f(C) = f_0(C), f_1(C) = f(C)C + Cf(C)$ *and, in general, let*

$$f_k(C) = C^{2^{k-1}} f_{k-1}(C) + f_{k-1}(C)C^{2^{k-1}}.$$

Show that $f_k(C) = C^{2^k} m_1B + m_1BC^{2^k}$.

Now let $k = r$ where $q = 2^r$. Then, $f_r(C) = C^{2^{r-1}} f_{r-1}(C) + f_{r-1}(C)C^{2^{r-1}} = Cm_1B + m_1BC$. From $C(B + m_1B) = f(C) + BC^2 + m_1BC$, we obtain $Cm_1B + m_1BC = CB + CB^2 + f(C)$.

Hence, $(C + C^2)B = C^{2^{r-1}} f_{r-1}(C) + f_{r-1}(C)C^{2^{r-1}} + f(C)$. Since B can take on either of the nonzero elements E or F, this can only occur when $C + C^2 = 0$ and hence that $C = 0$ or I. Hence, we have shown that the only possible elations τ_C are τ_0 and τ_I. That is, the elation group has order at most 2.

Chapter 14

The Translation Planes of order q^2 that admit $SL(2,q)$.

In this final chapter, we consider the set of translation planes of order q^2 that admit $SL(2,q)$ in the translation complement and mention a classification. The theory developed from Walker's thesis who classified all such translation planes of odd order that have $GF(q)$ in their kern, and Sch—äefer dealt with the even order case. Foulser and Johnson showed that no further cases occur when the kern hypothesis is dropped.

The resulting classification, of translation planes of order q^2 admitting $SL(2,q)$, constitutes one of the most powerful tools in finite translation plane theory. As a demonstration, we show how the classification allows us to completely determine the translation planes that admit large Baer groups that generate a nonsolvable group.

We first consider the examples that arise in the classification.

14.0.3 Desarguesian Planes.

A Desarguesian plane of order q^2 may be coordinated by a field $F \simeq GF(q^2)$ and admits $\Gamma L(2,q^2)$ in the translation complement where the p-elements are elations where $p^r = q$. In particular, there is a regulus net R which is left invariant by a subgroup isomorphic to $GL(2,q)$.

14.0.4 Hall Planes.

If the net R is derived, the group $GL(2,q)$ is inherited as a collineation group of the derived plane. Hence, the Hall planes admit $GL(2,q)$ where the p-elements are Baer p-collineations.

14.0.5 Hering and Ott-Schaeffer Planes.

The reader is referred to Lüneburg [31] for details.

Definition 14.0.22 *Let $\mathcal{Q}$ be any set of $q+1$ points in $PG(3,q)$ such that no four of the points are coplanar. Then $\mathcal{Q}$ is called a $(q+1)$-arc.*

The $(q+1)$-arcs are all determined as follows:

Theorem 14.0.23 *Let $\mathcal{Q}$ be a $(q+1)$-arc then $\mathcal{Q}$ may be represented as follows:*

(1) (Segre [38]) If q is odd then the representation is $\{(s^3, s^2t, st^2, t^3); s,t$ in $GF(q), (s,t) \neq (0,0)\}$. Even if q is even, if an arc has this representation, we call this a 'twisted cubic' $\mathcal{Q}^3$.

(2) (Casse and Glynn [8]) If q is even then the representation is $\mathcal{Q}^\alpha = \{s^{\alpha+1}, s^\alpha t, st^\alpha, t^{\alpha+1}); s,t$ in $GF(q), (s,t) \neq (0,0)\}$ where α is an automorphism of $GF(q)$ which is a generator.

Theorem 14.0.24 *Let V_4 denote a 4-dimensional vector space over $K \simeq GF(q)$. Consider the following matrix group:*

$$S^\beta = \left\langle \begin{bmatrix} a^{\beta+1} & ba^\beta & ab^\beta & b^{\beta+1} \\ ca^\beta & da^\beta & cd^\beta & db^\beta \\ ac^\beta & bc^\beta & ad^\beta & bd^\beta \\ cc^\beta & dc^\beta & cd^\beta & d^{\beta+1} \end{bmatrix}; a,b,c,d \in K \text{ and } ad-bc \neq 0 \right\rangle.$$

(1) If q is not 3^r or 2 and $\beta = 2$ then $S^{\beta=2}$ is isomorphic to $GL(2,q)$ and acts triply transitive on the points of the twisted cubic $\mathcal{Q}^3$. Furthermore, S^2 acts irreducibly on V_4.

(2) If $q = 2^r$ and β is an automorphism α of K then $S^{\beta=\alpha}$ is isomorphic to $GF(2,q)$ and acts triply transitive on the points of the $(q+1)-arc$, $\mathcal{Q}^\alpha$. Furthermore, S^α acts irreducibly on V_4.

Theorem 14.0.25 *Let Σ be $PG(3,q)$ and consider the plane $x_4 = 0$ where the points are given homogeneously by (x_1, x_2, x_3, x_4) for x_i in $GF(q)$, $i = 1, 2, 3, 4$.*

(1) Then $x_1 x_3 = x_2^\beta$ for $\beta \in \{2, \alpha\}$ defines an oval cone C_β with vertex $(0,0,0,1)$ and oval $\mathcal{O}_\beta = \{(1, t, t^\beta, 0), (0,0,1,0); t \in GF(q)\}$ in $x_4 = 0$.

(2) The $(q+1)$-arc $\mathcal{Q}^\beta = \{(1, t, t^\beta, t^{\beta+1}), (0,0,0,1); t \in GF(q)\}$ is contained in C_β and the q lines $L_t = \left\langle (0,0,0,1), (1, t, t^\beta, t^{\beta+1}) \right\rangle$ intersect $\mathcal{O}_\beta$ in $(1, t, t^\beta, 0)$. Hence, there is a unique line $L_\infty = \langle (0,0,0,1), (0,0,1,0) \rangle$ of the oval cone which does not contain a point of $\mathcal{Q}_\beta$.

We shall call L_∞ the 'tangent' line to $(0,0,0,1)$. More generally, any image of L_∞ under an element of the group S^β is called the tangent line at the corresponding image point.

(3) Consider the plane $x_1 = 0$ which intersects $\mathcal{Q}^\beta$ in exactly the point $(0,0,0,1)$. We shall call $x_1 = 0$ the 'osculating' plane at $(0,0,0,1)$. Each image of $x_1 = 0$ under an element of S^β is also called an osculating plane and the corresponding image point.

Theorem 14.0.26 *If $\mathcal{Q}^\beta$ is a twisted cubic then the set of $q+1$-tangents form a partial spread $\mathcal{T}$.*

Theorem 14.0.27 *Assume q is even and $\beta = \alpha$ for some automorphism of $GF(q)$. Let S_2 denote a Sylow 2-subgroup of S^α.*

(1) Then S_2 fixes a unique point P of $\mathcal{Q}^\alpha$ and fixes the tangent plane $T(P)$.

(2) Choose any point Q of $\mathcal{Q}^\alpha - \{P\}$ and form the lines XQ and then the intersection points $I = T(P) \cap XQ$ and then the lines PI of $T(P)$ incident with P. Let $N_i(P)$ denote the two remaining lines of $T(P)$ incident with P for $i = 1, 2$.

Then $\mathcal{R}_i = N_i(P)S^\alpha$ is a regulus and $\mathcal{R}_j$ is the opposite regulus to $\mathcal{R}_i$ for $i \neq j$.

To construct the Hering and Ott-Schaeffer planes we require that $q \equiv -1 \pmod 3$.

Theorem 14.0.28 *When $q \equiv -1 \pmod 3$ any element ρ of order 3 in S^β fixes a 2-dimensional subspace M pointwise.*

(1) There is a unique Maschke complement L for ρ such that $V_4 = L \oplus M$.

(2) If $\beta = 2$ and q is odd then $\mathcal{T} \cup LS^2 \cup MS^2$ is the unique S-invariant spread of V_4.

The corresponding translation plane is called the 'Hering plane'of order q^2.

(3) If $\beta = \alpha$ *and* q *is even then* $\mathcal{R}_i \cup LS^\alpha \cup MS^\alpha$ *is a* S*-invariant spread of* V_4 *for* $i = 1$ *or* 2 *and for any automorphism* α *of* $GF(q)$.

The corresponding translation planes are called the 'Ott-Schaeffer planes'.

Remark 14.0.29 *(1) The Hering and Ott-Schaeffer planes admit affine homologies of order* 3 *with* $q(q-1)$ *distinct axes.*

(2) Schaeffer determine the planes when α *is the Frobenius automorphism and Ott generalized this to arbitrary automorphisms. (See Hering [17], Schaeffer [37] and Ott [33].)*

(3) Each Ott-Schaeffer plane is derivable. If α *is an automorphism for a given Ott-Schaeffer plane then* α^{-1} *is the automorhpism for its corresponding derived plane. (See e.g. Johnson [27]. If* $q = 2^r$ *it turns out that the number of mutually non-isomorphic planes is* $\varphi(r)$ *as the automophisms used in the construction are generators of the cyclic group of order* r.

14.0.6 The Three Walker Planes of order 25.

Let

$$\tau_s = \begin{bmatrix} 1 & 0 & 0 & 0 \\ s & 0 & 0 & 0 \\ 3s^2 & s & 1 & 0 \\ s^3 & 3s^2 & s & 1 \end{bmatrix}; s \in GF(5)$$

and

$$\rho = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$$

Then $\langle \tau_s, \rho \rangle = S \simeq SL(2,5)$.

Furthermore, let

$$H = \left\langle \begin{bmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & t & 0 \\ 0 & 0 & 0 & t^{-1} \end{bmatrix}; t \in GF(5) - \{0\}. \right\rangle$$

Then, there are exactly three mutually nonisomorphic spreads π_2, π_4, π_6 of order 25 that admit S such that H fixes exactly 6 components of each

plane and ρ fixes either 2, 4, or 6 of these components respectively. These planes are determined by Walker in [41].

14.0.7 The Translation Planes with Spreads in $PG(3, q)$ admitting $SL(2, q)$.

The translation planes or order q^2 with kernels containing $GF(q)$ and admitting $SL(2, q)$ as a collineation group are completely determined by Walker and Schaeffer.

Theorem 14.0.30 *Let π be a translation plane of order q^2 with spread in $PG(3, q)$ that admits $SL(2, q)$ as a collineation group.*

Then π is one of the following types of planes:

(1) Desarguesian,

(2) Hall,

(3) Hering and q is odd

(4) Ott-Schaeffer and q is even

(5) one of three planes of order 25 of Walker.

14.0.8 Arbitrary Dimension.

There are exactly three semifields planes of order 16 one each with kernel $GF(2), GF(4)$ and $GF(16)$ each of which is derivable. We have considered the planes derived from the semifields planes with kernel $GF(4)$ that admit $PSL(2, 7)$ as a collineation group. The semifield plane with kernel $GF(2)$ derives the Dempwolff plane of order 16 which admits $SL(2, 4)$ as a collineation group. Furthermore, the kernel of the Dempwolff plane is $GF(2)$ (see e.g. Johnson [26]).

Using methods of combinatorial group theory and linear algebra, Foulser and I were able to prove that the only translation plane of order q^2 that admits $SL(2, q)$ as a collineation group and whose spread is not in $PG(2, q)$ is, in fact, the Dempwolff planes.

Theorem 14.0.31 *(Foulser-Johnson [13]). Let π be a translation plane of order q^2 that admits a collineation group isomorphic to $SL(2, q)$ in its translation complement.*

Then either the plane has its spread in $PG(3, q)$ or is the Dempwolff plane of order 16.

Actually, the way that the proof was given, it was not necessarily to assume that $SL(2,q)$ acts faithfully on the translation plane. That is, it is possible that $PSL(2,q)$ acts on the plane. In fact, this essentially never occurs.

Corollary 14.0.32 *Let π be a translation plane of order q^2 that admits a collineation group isomorphic to $PSL(2,q)$ then π is Desarguesian.*

14.0.9 Applications.

Let π be a translation plane of odd order p^r that admits at least two Baer p-groups B_1 and B_2 in the translation complement with distinct Baer axes. Assume that $\mid B_i \mid > \sqrt{p^r} \geq 3$. Then, by Foulser's work (which works in the characteristic 3 case in this situation), it follows that the Baer axes lie in the same net of degree $p^r + 1$. The Baer groups generate a group G isomorphic to $SL(2,p^s)$ for $p^s > p^{r/2}$. From here, it follows that the group G must be $SL(2,q)$. Applying the previous theorem, we have:

Theorem 14.0.33 *(Jha and Johnson [23]) Let π be a translation plane of odd order p^r that admits at least two Baer p-groups of order $> \sqrt{p^r} \geq 3$. Then π is the Hall plane of order p^r.*

Recall, that Foulser's result is not necessarily valid in translation planes of even order but there is considerable incompatibility between elation and Baer 2-groups.

Dempwolff analyzed the groups generated by two Baer 2-groups with distinct axes and orders $\sqrt{2^r}$ if the translation plane is of order 2^{2r}.

Theorem 14.0.34 *(Dempwolff [9]) Let π be a translation plane of even order q^2 and let G be a collineation group in the translation complement which contains at least two Baer 2-groups of orders $> \sqrt{q}$ with distinct axes. Let N denote the subgroup of G generated by affine elations.*

Then one of the following situations occur:

(1) $q^2 = 16, G \simeq SL(3,2)$ and π is either the Lorimer-Rahilly or Johnson-Walker plane, or

(2) $G/N \simeq SL(2,2^z)$ where $2^z > \sqrt{q}$ and $N \subseteq Z(G)$.

Using the incompatibility results previous mentioned, we know that any elation group centralizing a Baer 2-group can have order ≤ 2. If, in fact, the

order is 1 then we argue that, in fact, we obtain $SL(2,q)$ so that the results of Foulser and myself apply. If the order of is 2 then some group representation theory shows that $G \simeq SL(2,2^z) \oplus N$ and we argue that $SL(2,2^z)$ contains a Baer group of order $> \sqrt{q}$ which again shows that $SL(2,q)$ is a collineation group. We note that the Dempwolff plane of order 16 does not occur here since there are no large Baer 2-groups in this plane.

Hence, we may show:

Theorem 14.0.35 *(Jha and Johnson [24]) Let π be a translation plane of even order q^2 that admits at least two Baer groups with distinct axes and orders $> \sqrt{q}$ in the translation complement.*

Then, either π is Lorimer-Rahilly or Johnson-Walker of order 16 *or π is a Hall plane.*

Bibliography

[1] Albert, A. A. Finite non-commutative division algebras, Proc. Amer. Math. Soc. **9** (1958), 928-932.

[2] André, J. Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. Math. Z. 60 (1954), 156-186.

[3] Barlotti, A. On the definition of Baer subplanes of infinite planes. J. Geom. 3 (1973), 87-92.

[4] Bernardi, M. Esistenza di fibrazioni in uno spazio proiettivo infinito. Ins. Lombardo Accad. Sci. Lett. Rend. A 197 (1973), 528-542.

[5] Bruck, R. H. and Bose, R.C. The construction of translation planes from projective spaces. J. Aalg. 1 (1964), 85-102.

[6] Bruen, A. and Fisher, J.C. Spreads which are non dual spreads. Cana. Math. Bull 12 (1969), 801-803.

[7] Buekenhout, F. Existence of unitals in finite translation planes of order q^2 with a kernel of order q. Geom. Ded. 5 (1976), 189-194.

[8] Casse, L.R.A. and Glynn, F. G. The solution to Beniamino Segre's problem $I_{r,q}$, $r = 3$, $q = 2^h$. Geom. Ded. 13 (1982), 157-164.

[9] Dempwolff, U. Grosse Baer-Untergruppen auf Translationsebenen gerader ordnung. J. Geom. 14 (1982), 1-1-115.

[10] Foulser, D.A. Subplanes of partial spreads in translation planes. Bull. London Math. Soc. 4 (1972), 32-38.

[11] Foulser, D.A. Baer p-elements in translation planes. J. Alg. 31 (1974), 354-366.

[12] Foulser, D.A. A generalization of André systems. Math. Z. 100 (1967), 380-395.

[13] Foulser, D.A. and Johnson, N.L. The translation planes of order q^2 that admit $SL(2,q)$ as a collineation group I. Even order and II. Odd order. J. Alg. 86 (1984), 385-406 and J. Geom. 18 (1982), 122-139 respectively.

[14] Ganley, M. J. Baer involutions in semifield planes of even order. Geom. Ded. 2 (1973), 499-508.

[15] Hall, M. Jr. Projective Plnaes. Trans. Amer. Math. Soc. 54 (1943), 229-277.

[16] Hering, Ch. On shears of translation planes. Abh. Math. Sem. Hamburg 37 (1972), 258-268.

[17] Hering, Ch. A new class of quasifields. Math. Z. 118 (1970), 56-57.

[18] Hughes, D. R. and Piper F. C., Projective Planes, Springer Verlag, New York, 1973.

[19] Jha, V. and Johnson, N.L. Quasifibrations. Bull. Belg. Math. Soc. 3 (1996), 313-324.

[20] Jha, V. and Johnson, N.L. Regular parallelisms from translation planes, Discrete J. Math. 59 (1986), 91-97.

[21] Jha, V. and Johnson, N.L. Coexistence of elations and large Baer groups in translation planes, J. London Math. Soc. (2)32 (1985), 297-304.

[22] Jha, V. and Johnson, N.L. Structure Theory for point-Baer and line-Baer collineations Groups in Affine planes. Mostly finite geometries. Lecture Notes in Pure and Applied Math., Vol. 190, Marcel Dekker. New York-Basel-Hong Kong, (l997), 235-277.

[23] Jha, V. and Johnson, N.L. The odd order analogue of Dempwolff's B-group problem, J. Geom. 28(1) (1987), 1-6.

[24] Jha, V. and Johnson, N.L. Solution to Dempwolff's nonsolvable B-group problem, European J. Comb., vol. 7, no. 3 July(1986), 227-235.

[25] Jha, V. and Johnson, N.L. Baer involutions in translation planes admitting large elation groups, Resultate *d.* Math. Vol. 11 (1987), 63-71.

[26] Johnson, N.L. The translation planes of order 16 that admit SL(2,4), Ann. Discrete Math. 14 (1982), 225-236.

[27] Johnson, N.L. Tensor product planes and generalized Ott-Schaeffer planes. Osaka J. Math. 25(1988), 441-459.

[28] Johnson, N.L. and Ostrom, T.G. Direct products of affine partial linear spaces. Journal of Combinatorial Theory (A), vol 75, no. 1 (1996), 99-140.

[29] Kallaher, M. J. Translation Planes, **Handbook of Incidence Structures**, F. Buekenhout ed., North-Holland, Amsterdam, New York, Oxford, Tokyo, 1995, 137-192.

[30] Knuth, D. E. A class of projective planes, Trans. Amer. Math. Soc., **115** (1965), 541-549.

[31] Lunebürg, H. **Translation Planes.** Springer-Verlag, Berlin, 1979.

[32] T. G. Ostrom, Finite Translation Planes, Springer-Verlag, Berlin, LNM 158, 1970.

[33] Ott, U. Eine neue Klasse endlicher translationsebenen. Math. Z. 143 (1975), 181-185.

[34] Ostrom, T.G. Linear transformations and collineations of translation planes. J. Alg. 14 (1970), 405-416.

[35] Ostrom, T.G. Elations in finite translation planes of characteristic 3. Abh. Math. Sem. Hamburg 42 (1974), 179-184.

[36] Prince, A. Private communication.

[37] Schaeffer, H.J. Translationsebenen, auf denen die Gruppe $SL(2, p^n)$ operiert. Diplomarbeit Tübingen, 1975.

[38] Segre, B. Lectures on Modern Geometry, Roma: Cremonese, 1961.

[39] Veblen, O and Young, J. W. **Projective Geometry, Volumes I and II.**Blaisdell, New York-Toronto-London, 1938.

[40] Walker, M. A note on tangentially transitive affine planes. Bull. London Math. Soc. 81 (1976), 273-277.

[41] Walker, M. On translation planes and their collineation groups. Ph. D. Thesis, University of London, 1973.

Vikram Jha
Mathematics Department
Glasgow Caledonian University
Cowcaddens Road
Glasgow G4 OBA
Scotland
email: vjha@gcal.ac.uk

Norman L. Johnson
Mathematics Department
University of Iowa
Iowa City, Iowa 52242
email: njohnson@math.uiowa.edu