Socrates Intensive Programme

Finite Geometries and Their Automorphisms

Potenza, 8 - 18 June, 1999

Classical Groups

O.H. King

Chapter 1

Forms and Groups

1.1 Introduction

We start with linear algebra (on vector spaces) and use it to obtain results in geometry (on projective spaces). The main references for Classical Groups are Dieudonne ([6], [7]), Taylor ([15]) and Dickson ([5]), though I have used Taylor more than others.

We begin with a vector space $V = V(n, K)$ of dimension n over a field K (usually $n \geq 2$). We shall often write $V(n, q)$ when K is the field $GF(q)$ (q is a power of a prime number p). It is appropriate to comment on the fields we use. It is often as easy to present the theory over an arbitrary commutative field as it is over a finite field. Moreover certain developments of the subject use information about groups over extension fields (particularly algebraic closures) to gain insight into groups over finite fields. Thus we shall develop ideas over arbitrary fields unless it becomes expensive to do so. Much of the theory can be developed over division rings, but we shall consider only (commutative) fields.

Perhaps the most fundamental classical group is the group of all invertible linear transformations on V. This group is called the General Linear Group of V and is denoted by $GL(V)$. Given a fixed basis for V, the elements of $GL(V)$ can be represented as the set of all invertible $n \times n$ matrices over K and, as such, the group is denoted $GL(n, K)$ (or $GL(n, q)$).

There are two important groups associated with $GL(n, K)$. One is the Special Linear Group $SL(V)$ or $SL(n, K)$, consisting of all the matrices of determinant 1; the notion of the determinant of a linear transformation is independent of the choice of basis so this subgroup is properly defined. Clearly $SL(n, K)$ is a normal subgroup of $GL(n, K)$. The second group is the group of all invertible semi-linear transformations on V, i.e., invertible transformations ϕ such that for any $u, v \in V$ and any $\lambda, \mu \in K$ we have $\phi(\lambda u + \mu v) = \lambda^\sigma \phi(u) + \mu^\sigma \phi(v)$ for some automorphism σ of K dependent on ϕ. This group is denoted by

$\Gamma L(V)$ or $\Gamma L(n,q)$; however, one should be a little careful to note that the elements of $\Gamma L(n,q)$ are not necessarily matrices, but rather pairs (M,σ), where $M \in GL(n,K)$ and $\sigma \in Aut(K)$. It is not difficult to show that $GL(V)$ is a normal subgroup of $\Gamma L(V)$. As we shall see shortly $\Gamma L(V)$ can be a more natural group to study from the geometer's point of view. $GL(V)$ acts transitively on non-zero vectors, and so does $SL(V)$ (provided that $n \geq 2$).

The classical groups that we shall be studying all arise as subgroups of $GL(V)$ or $\Gamma L(V)$, usually preserving a sesquilinear form.

A sesquilinear form on V is a mapping $(,) : V \times V \to K$ such that $(u+w,v) = (u,v)+(w,v), (u,v+w) = (u,v)+(u,w), (\lambda u,v) = \lambda^\sigma(u,v), (u,\mu v) = \mu(u,v)$ for some $\sigma \in Aut(K)$ (which is fixed for a given form); such a form is reflexive if $(u,v) = 0$ always implies that $(v,u) = 0$. Although set up in a rather general way, it turns out that there are essentially three different reflexive non-degenerate sesquilinear forms (we discuss non-degeneracy below): symmetric bilinear forms, where σ is the identity automorphism and $(v,u) = (u,v)$; alternating (bilinear) forms, where again σ is the identity automorphism and this time $(v,v) = 0$ for all $v \in V$ and as a consequence $(v,u) = -(u,v)$ for all $u, v \in V$; and unitary (or hermitian) forms, where σ is an involutory automorphism and $(v,u) = (u,v)^\sigma$ for all $u,v \in V$. It is often useful to think of $GL(V)$ as stabilizing the null (trivial) form: $(u,v) = 0$ for all $u,v \in V$.

It is worth making a few comments here. Some authors would take hermitian forms to be linear in the first vector and anti-linear in the second. Also there is the notion of a skew-hermitian form, where $(v,u) = -(u,v)^\sigma$. However neither consideration yields anything new to group theorists or geometers.

We soon find it easier to concentrate on well-behaved forms. A form is non-degenerate if for any $0 \neq u \in V$ there exists $v \in V$ such that $(u,v) \neq 0$. Thus degenerate forms have a non-trivial nucleus $\{u \in V : (u,v) = 0 \text{ for all } v \in V\}$. We shall assume here that our forms are non-degenerate.

The projective space $PG(n-1,K)$ (which we sometimes write as $PG(V)$) has as its points the set of 1-dimensional subspaces of V. Any invertible linear transformation on V permutes 1-dimensional subspaces so $GL(n,K)$ clearly acts on $PG(n-1,K)$. However there is a kernel to this representation: the invertible linear transformations which fix every 1-dimensional subspace of V are precisely the scalar transformations. The projective linear group, $PLG(n,K)$, on V is defined as the quotient $GL(n,K)/Z$ where Z is the set of non-zero scalar transformations of V. Whilst $GL(n,K)$ is (arguably) the most natural starting point for algebraists, it is reasonable to ask whether $PGL(n,K)$ is the most natural for geometers. Certainly $PLG(n,K)$ preserves lines , planes etc., but is it the full automorphism group of the geometric structure? The answer is no, because the full automorphism group is $P\Gamma L(n,K) = \Gamma L(n,K)/Z$. Thus geometric arguments may start from $P\Gamma L(n, K)$. The image of $SL(n, K)$ in $PGL(n, K)$ is denoted by $PSL(n, K)$; however notice that this group is isomorphic to $SL(n, K)/(Z \cap SL(n, K))$ and in practice either may represent $PSL(n, K)$. In most cases $PSL(n, K)$ is simple and is thus an alternative starting point for algebraists. As we have noted above, $GL(n, K)$ acts transitively on non-zero vectors. It follows that $PGL(n, K)$ acts transitively on the points of $PG(n-1, K)$. In fact we can make a much stronger statement: for $n \geq 2$, $PSL(n, K)$ acts 2-transitively on the points of $PG(n-1, K)$.

There are essentially two types of fundamental element of $GL(n, K)$. The first type is a transvection: broadly speaking, a transvection τ fixes every vector in an $n-1$-dimensional subspace U of V and every subspace containing a non-zero vector $u \in U$; to be precise, associated to τ is a linear form σ such that $\sigma(u) = 0$ and $\tau(v) = v + \sigma(v).u$ for every $v \in V$. These two descriptions are equivalent if $n \geq 3$; they are not quite equivalent if $n \leq 2$, and it is the more precise description which is appropriate. If we choose a basis $u_1, u_2, .., u_{n-1}$ for U, with $u_1 = u$ and extend to a basis for V, then with respect to this basis, τ is given by the identity matrix except in the $(1, n)$ position where the entry is some $\lambda \in K$; we usually think of transvections as non-trivial, so $\lambda \neq 0$. An immediate consequence is that every
transvection has determinant 1, so lies in $SL(n, K)$. Moreover the conjugate of a transvection is again a transvection, which implies that the subgroup of $SL(n, K)$ generated by transvections is a normal subgroup. It is possible to show directly that $SL(n, K)$ is generated by transvections. The images of transvections in $PGL(n, K)$ are called elations.

The second fundamental element type is a (quasi-) reflection; a (quasi-) reflection ρ fixes every vector of a $(n-1)$-dimensional subspace U and a 1-dimensional subspace W not contained in U; if we take bases $u_1, u_2, .., u_{n-1}$ for U and w for W to give a basis for V, then with respect to this basis ρ is given by a diagonal matrix with entries $1, 1, .., 1, \mu$ for some $0 \neq \mu \in K$; a reflection corresponds to $\mu = -1$. If σ is the linear form such that $\sigma(u_i) = 0, \sigma(w) = \mu - 1$, then for any $v \in V$, $\rho(v) = v + \sigma(v).w$. Clearly a non-trivial (quasi-) reflection doesn't have determinant 1 so cannot lie in $SL(n, K)$, but the corresponding element of $PGL(n, K)$ is called a homology and $PSL(n, K)$ can contain homologies: if there is an element $\nu \in K$ such that $\nu^n = \mu$, then $\nu^{-1}I.\rho \in SL(n, K)$ and this element
corresponds to a homology. The most obvious example is when n is odd: here $PSL(n, K)$ contains reflections and indeed is generated by them (except when $K = GF(3)$).

1.2 Symplectic Groups

In terms of groups, the alternating form is a good starting point. The Symplectic Group $Sp(n,K)$ of the alternating form $(,)$ is the set of all elements $g \in GL(n,K)$ such that $(g(u),g(v)) = (u,v)$ for all $u,v \in V$. Suppose that $u_1, u_2, ..., u_n$ is a basis for V and that $a_{ij} = (u_i, u_j)$ for each i,j. Then with respect to this basis $(u,v) = u^T Av$, where A is the $n \times n$ matrix with coefficients a_{ij}. We see that A is anti-symmetric. Moreover a matrix $M \in Sp(n,K)$ satisfies $M^T AM = A$. One immediate conclusion is that elements of $Sp(n,K)$ have determinant ± 1.

For any subspace U of V, define the orthogonal complement (sometimes called the conjugate subspace, or polar space) $U^\perp$ of U in V by $U^\perp = \{v \in V : (u,v) = 0 \text{ for all } u \in U\}$ (clearly $U^\perp$ is a subspace). One can show that $(U^\perp)^\perp = U$ and that $dimU + dimU^\perp = n$. In general the intersection of U and $U^\perp$ can have any dimension from 0 to $min\{dimU, dimU^\perp\}$. Two situations are particularly interesting. If $dim(U \cap U^\perp) = 0$, then we say that U is non-isotropic; the restriction of $(,)$ to U is non-degenerate, and $V = U \oplus U^\perp$; at the same time $U^\perp$ is non-isotropic. The other is when $U \subseteq U^\perp$, in which case U is termed totally isotropic; clearly in this case $dimU \leq$ n/2.$Observethata1-dimensionalsubspaceisalwaystotallyisotropic.Moreover, ifwelookata2-dimensionalsubspace$,U$say, withbasis$u,v,$theneither$(u,v)=0$inwhichcase$(\alpha u + \beta v, \lambda u + \mu v) = 0$ for all $\alpha, \beta, \lambda, \mu \in K$, or $(u,v) = \gamma \neq 0$ in which case for any $0 \neq \alpha u + \beta v$ either $(u, \alpha u + \beta v)$ or $(v, \alpha u + \beta v)$ is non-zero. Thus U is either totally isotropic or non-isotropic. The terminology clearly translates to $PG(V)$ so a line of $PG(V)$ is either totally isotropic or non-isotropic. One more useful observation: if U is totally isotopic, then any complement of U in $U^\perp$ is non-isotropic (for if we write $U^\perp = U \oplus Y$ and let $y \in Y \cap Y^\perp$, then $y \in U^\perp$ so $y \in (U \oplus Y)^\perp = U$, i.e., $y \in Y \cap U = \{0\}$).

It is often possible to work with particularly nice bases for V. Suppose that we take any non-zero vector $u_1 \in V$ and choose for v_1 any vector in V such that $(u_1, v_1) = 1$. Then the subspace U of V generated by u_1, v_1 is non-isotropic, so $V = U \oplus U^\perp$ with $(,)$ non-degenerate on $U^\perp$. The same procedure can be applied to $U^\perp$, selecting appropriate u_2, v_2 which generate a subspace W of $U^\perp$. As we continue in this way, we build a basis $u_1, v_1, u_2, v_2, ...$ for V; at each stage we leave a non-isotropic subspace of diminishing dimension, so the process cannot terminate leaving a 1-dimensional subspace and therefore n must be even. In fact any non-isotropic subspace must have even dimension. If we take the basis in the order given above, then the matrix A has the block-diagonal form $diag(J,J,J,...,J)$ where $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

However, if we order the basis $u_1, u_2, ..., v_1, v_2, ...$, then A has the form $A = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$.

In this setting, a matrix $M \in Sp(n,K)$ has the form
$$M = \begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix}$$
with $M^TAM = A$, i.e.,
$$\begin{pmatrix} M_1^T & M_3^T \\ M_2^T & M_4^T \end{pmatrix}\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix} = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$
from which $M_1^TM_3 - M_3^TM_1 = 0$, i.e., $M_1^TM_3$ is symmetric. Also $M_1^TM_4 - M_3^TM_2 = I$.
A particular application is when $n = 2$. Here $A = J$ and we find that
$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
with $ad - bc = 1$. In other words $Sp(2,K)$ is nothing other than $SL(2,K)$.

We pause to look at the geometry associated with the symplectic group. The Projective Symplectic Group $PSp(n,K)$ is the image of $Sp(n,K)$ in $PGL(n,K)$ and is isomorphic to $Sp(n,K)/(Z \cap Sp(n,K))$. We have seen that for $n \geq 2$, $PSL(n,K)$ acts 2-transitively on the points of $PG(n-1,K)$. The question naturally arises as to whether the same, or something similar, is true for $PSp(n,K)$. The immediate answer is no for $n \geq 4$, because a transformation taking u_1 to λu_1 and v_1 to μu_2 (some $\lambda, \mu \in K - \{0\}$) does not preserve $(,)$. The follow-up question then concerns transitivity and here it is appropriate to state a stronger theorem:

Theorem 1 *(Witt)*

Suppose that U, W are subspaces of V such that there is an invertible linear transformation $\phi : U \to W$ preserving $(,)$. Then there exists $\psi \in Sp(n,K)$ such that $\psi(u) = \phi(u)$ for every $u \in U$.

It is now clear that, since $(,)$ vanishes on any 1-dimensional subspace, $Sp(n,K)$ acts transitively on the non-zero vectors of V and so $PSp(n,K)$ acts transitively on the points of $PG(V)$. In showing that $PSp(n,K)$ is not 2-transitive on the points we have also shown that it is not transitive on lines. However Witt's Theorem shows us that $PSp(n,K)$ is transitive on totally isotropic lines and also on non-isotropic lines. The question arises: can we characterize $PSp(n,K)$ $(n \geq 4)$ as the stabilizer of the totally isotropic lines?

Suppose that $g \in GL(n,K)$ stabilizes the set of totally isotropic 2-dimensional subspaces. Then g also stabilizes the set of non-isotropic 2-dimensional subspaces. Let $u_1, v_1, u_2, v_2, \ldots$ be the canonical basis for V described above. Then for any $i \neq j$, $(g(u_i), g(u_j)) = (g(v_i), g(v_j)) = (g(u_i), g(v_j)) = 0$ and $(g(u_i), g(v_i)) = \gamma_i \neq 0$. The 2-dimensional subspace spanned by $u_i + u_j, v_i - v_j$ is totally isotropic so $0 = (g(u_i+u_j), g(v_i-v_j)) = \gamma_i-\gamma_j$. Hence $(g(u_i), g(v_i)) = \gamma$ for each i and for some $0 \neq \gamma \in K$. It is straightforward to show that $(g(u), g(v)) = \gamma(u, v)$ for all $u, v \in V$. Let us define the General Symplectic Group $GSp(n, K)$ by $\{g \in GL(n, K) : (g(u), g(v)) = \lambda_g(u, v)$ for all $u, v \in V\}$, where the "multiplier" λ_g is a non-zero scalar determined by g. Then any $g \in GSp(n, K)$ stabilizes the set of totally isotropic 2-dimensional subspaces of V. It follows that we have identified the full stabilizer and that the image $PGSp(n, K)$ of $GSp(n, K)$ in $PGL(n, K)$ is the stabilizer there of the set of totally isotropic lines. It is quite possible to take the argument further, whether one looks at the geometry of points and totally isotropic lines or more broadly at the geometry of totally isotropic subspaces, $PGSp(n, K)$ is the automorphism group inside $PGL(n, K)$.

The proceeding discussion indicates the possibilities for the scalar λ_g, namely all possible non-zero values. We can thus calculate how much bigger $GSp(n, q)$ is compared to $Sp(n, q)$:

$$|GSp(n, q)| = (q-1)|Sp(n, q)|.$$

Moreover the scalar transformation λI lies in $GSp(n, q)$ with multiplier λ^2, and the squares in $GF(q)^*$ form a subgroup of index $(q-1, 2)$, so $|PGSp(n, q)| = 2|PSp(n, q)|$ (q odd) or $|PSp(n, q)|$ (q even).

Recall that $SL(n, K)$ contains transvections and, indeed, is generated by them. We can ask whether $Sp(n, K)$ contains transvections. Suppose that the transvection τ given by $\tau(v) = v + \sigma(v).u$ (with $\sigma(u) = 0$) lies in $Sp(n, K)$ and choose a $w \in V$ such that $(u, w) \neq 0$. Then for any $v \in \langle u\rangle^\perp$ we have

$$(v, w) = (\tau(v), \tau(w)) = (v + \sigma(v).u, w + \sigma(w).u)$$

$$= (v, w) + \sigma(v)\sigma(w)(u, u) + \sigma(v)(u, w) + \sigma(w)(v, u) = (v, w) + \sigma(v)(u, w)$$

which implies that $\sigma(v) = 0$ for every $v \in \langle u\rangle^\perp$; in other words, for $v \in V$, $\sigma(v) = \lambda(v, u)$ where $\lambda \in K$ depends on the transvection. It is not difficult to show that every such transvection lies in $Sp(n, K)$. Moreover we show below that $Sp(n, K)$ is generated by its transvections. This implies that, in fact, every element of $Sp(n, K)$ has determinant 1. A non-trivial (quasi-) reflection doesn't have determinant 1, so doesn't lie in $Sp(n, K)$. More fundamentally, however, such a (quasi-) reflection cannot preserve an alternating form, even up to a scalar multiple, so doesn't correspond to an element of $PGSp(n, K)$.

Theorem 2 *$Sp(n, K)$ is generated by symplectic transvections.*

Proof.

It useful to denote by $\tau_{u,\lambda}$ the transvection $v \to v+\lambda(v,u).u$ and to observe that $\tau_{u,\lambda}^{-1} = \tau_{u,-\lambda}$ (also a transvection). We take an element $g \in Sp(n,K)$ and show that it is a product of symplectic transvections; to achieve that aim we can replace g by g.(a product of transvections) at any time. Suppose, first of all, that $0 \neq w \in V$ with $g(w) \neq w$. We show that we can multiply g by transvections to get an element $g_1 \in Sp(n,K)$ such that $g_1(w) = w$. If $(w, g(w)) = 0$, then choose any vector $u \in V$ such that $(w,u) \neq 0$ and $(g(w),u) \neq 0$. Then $\tau_{u,1}g(w) = g(w) + \mu u$ for some $0 \neq \mu \in K$ and $(\tau_{u,1}g(w), w) \neq 0$, so we may assume that $(g(w),w) \neq 0$. Let $u = g(w) - w$ and let $\lambda = (g(w),w)^{-1}$. Then

$$\tau_{u,\lambda}(g(w)) = g(w) + \lambda(g(w),u).u$$

$$= g(w) + \lambda(g(w), g(w) - w).(g(w) - w) = g(w) - (g(w) - w) = w.$$

Now suppose that $u_1, v_1, u_2, v_2, ..$ is a canonical basis for V as developed above. As we have just seen, we may assume that $g(u_1) = u_1$; that means that $g(v_1) = \lambda u_1 + v_1 + z$ for some $\lambda \in K$ and some $z \in \langle u_1, v_1\rangle^{\perp}$. If $\lambda = 0$, then $\tau_{u_1,1}g(u_1) = u_1$, $\tau_{u_1,1}g(v_1) = u_1 + v_1 + z$, so we may replace g by $\tau_{u_1,1}g$ if necessary and then assume that $\lambda \neq 0$. Let $y = \lambda u_1 + z$ and $\mu = \lambda^{-1}$. Then $\tau_{y,\mu}(u_1) = u_1$ and

$$\tau_{y,\mu}(g(v_1)) = g(v_1) + \mu(\lambda u_1 + v_1 + z, y).y$$

$$= \lambda u_1 + v_1 + z + \mu(\lambda u_1 + v_1 + z, \lambda u_1 + z).(\lambda u_1 + z)$$

$$= \lambda u_1 + v_1 + z + \mu(v_1, \lambda u_1).(\lambda u_1 + z)$$

$$= \lambda u_1 + v_1 + z - \mu\lambda(\lambda u_1 + z) = v_1.$$

Hence we may assume that g fixes each vector in $\langle u_1, v_1\rangle$. Recall that $V = \langle u_1, v_1\rangle \oplus \langle u_1, v_1\rangle^{\perp}$. We find that g may be regarded as an element of the symplectic group on $\langle u_1, v_1\rangle^{\perp}$ and an induction argument now shows that g is a product of transvections. Of course we need an initial case for the induction argument (i.e., $n = 2$). We leave this as an exercise.

$\square$

Next we prove the simplicity of $PSp(n,K)$. We use a simplicity criterion of Iwasawa, as stated in [15].

Theorem 3 *(Iwasawa)*

Suppose that a group G acts primitively on a set Ω and that G is generated by $g^{-1}Hg$ $(g \in G)$, where H is an abelian normal subgroup of G_α for some $\alpha \in \Omega$

(G_α being the stabilizer in G of α). Then

(i) if N is a normal subgroup of G, either N fixes each point of Ω or $G' \leq N$;

(ii) if $G = G'$, then $G/G(\Omega)$ is simple, where $G(\Omega)$ represents the subgroup of G fixing every element of Ω.

We shall take G to be $Sp(n, K)$ and Ω to be the set of points in $PG(n-1, K)$, so $G(\Omega) = Z(G)$ and $G/G(\Omega) = PSp(n, K)$. Any G_α is the stabilizer of a 1-dimensional subspace of V: we take H to be the set of transvections (including the trivial one) centred on that 1-dimensional subspace; it isn't difficult to show that $H \trianglelefteq G_\alpha$; the G-conjugates of H give all the transvections in G so generate G. Here G' is the derived subgroup of G, i.e., the subgroup generated by all commutators $a^{-1}b^{-1}ab$, where $a, b \in$
G.

Theorem 4 *$PSp(n, K)$ is simple, except when $n = 2$ and $K = GF(2)$ or $GF(3)$, and when $n = 4$ and $K = GF(2)$.*

Proof.
We need to show two things. The first is that $G' = G$. The second is that G is primitive on Ω. Both are true (the first requires the three given cases excluded), but we leave a proof as an exercise.

□

1.3 Orthogonal Groups

Orthogonal groups are similar in a number of respects to Symplectic groups, but with notable differences.

Having stressed the role of sesquilinear forms, we now define something a little different. A quadratic form on V is a mapping $Q : V \to K$ such that $Q(\lambda v) = \lambda^2 Q(v)$ for all $v \in V$ and such that the mapping $(,) : V \times V \to K$ given by $(u, v) = Q(u+v) - Q(u) - Q(v)$ is a bilinear form on V. We see that $(v, u) = (u, v)$ so $(,)$ is symmetric; we shall normally assume that $(,)$ is non-degenerate. If the characteristic of K is not 2, then for any $v \in V$, $(v, v) = 2Q(v)$, so we may recover Q from $(,)$ and vice-versa; moreover there is no requirement that $(v, v) = 0$, so there may be vectors for which $(v, v) \neq 0$. If $char K = 2$, however, then $(v, v) = 0$ for all $v \in V$ and so $(,)$ is an alternating form; nevertheless this doesn't imply that $Q(v) = 0$ and there may be vectors

for which $Q(v) \neq 0$. We have said that, in the main, we shall assume that our sesquilinear
forms are non-degenerate and that applies here: the bilinear form is non-degenerate. In consequence, when $charK = 2$ we must have n even.

For any subspace U of V, the orthogonal complement is defined (as for alternating forms) by $U^\perp = \{v \in V : (u, v) = 0 \text{ for all } u \in U\}$. The notions of totally isotropic subspaces and non-isotropic subspaces are the same as for alternating forms.

A vector $v \in V$ is said to be singular if $Q(v) = 0$ and a subspace U of V is totally singular if all of its vectors are singular. If U is totally singular, then for any $u, v \in U$, $(u, v) = Q(u + v) - Q(u) - Q(v) = 0$, so a totally singular subspace is totally isotropic. In characteristic 2, the converse fails because, for example, every 1-dimensional subspace is totally isotropic but many are not totally singular.

The Witt index, ν, of Q on V is slightly different here compared to the alternating case: here the Witt index is the dimension of a maximal totally singular subspace. Of course, this amounts to the same thing as a maximal totally isotropic subspace when $charK \neq 2$, but can be different when $charK = 2$. For finite fields $\nu \geq n/2 - 1$, i.e., $n = 2\nu, 2\nu - 1$ or $2\nu - 2$, the middle possibility cannot occur when $charK = 2$ but otherwise all possibilities can occur. There are canonical bases in each case: (i) $x_1, x_2, .., x_\nu, x_{\nu+1}, .., x_{2\nu}$, (ii) $x_1, x_2, .., x_\nu, x_{\nu+1}, .., x_{2\nu}, x_n$, and (iii) $x_1, x_2, .., x_\nu, x_{\nu+1}, .., x_{2\nu}, x_{n-1}, x_n$ with respect to which $Q(\sum_{i=1}^n \lambda_i x_i)$ is given by (i) $\sum_{i=1}^\nu \lambda_i\lambda_{\nu+i}$, (ii) $\sum_{i=1}^\nu \lambda_i\lambda_{\nu+i} + \lambda_n^2$, and (iii) $\sum_{i=1}^\nu \lambda_i\lambda_{\nu+i} + (\lambda_{n-1}^2 + \lambda_n^2 + \alpha\lambda_{n-1}\lambda_n)$ (where the polynomial $t^2 + \alpha t + 1$ is irreducible over $GF(q)$). The first case is known as the hyperbolic case and the third as the elliptic case. In $PG(n, K)$, the set of (totally) singular points is called a quadric. Thus over $GF(q)$ there are essentially two types of quadric for even n: elliptic and
hyperbolic, and for n odd essentially one type of quadric, known as a parabolic quadric.

The elements of $g \in GL(n, K)$ such that $Q(g(v)) = Q(v)$ for all $v \in V$ form the orthogonal group $O(n, K)$. When $charK \neq 2$, this is precisely the set of $g \in GL(n, K)$ such that $(g(u), g(v)) = (u, v)$ for all $u, v \in V$. There is a special notation when $K = GF(q)$ to indicate the nature of the quadratic form which $O(n, q)$ preserves: the groups of hyperbolic forms are denoted $O^+(n, q)$ and the groups of elliptic quadrics are denoted by $O^-(n, q)$; the notation carries over into various subgroups. Assuming that there are singular points (i.e., the quadric is non-empty), the subspace of $GL(n, K)$ preserving the quadric is $GO(n, K)$, i.e., the set of elements of $GL(n, K)$ preserving Q up to a scalar. The same applies to larger dimension totally singular subspaces. When $charK = 2$ it

still follows that if $g \in O(n,K)$, then $(g(u),g(v)) = (u,v)$ for all $u,v \in V$, but the converse is not
necessarily true; we have noted that, in this case, $(,)$ is an alternating form, so actually $O(n,K) \leq SP(n,K)$. Given any basis $x_1, x_2, .., x_n$ for V a quadratic form is given by an expression $Q(\sum_{i=1}^n \lambda_i x_i) = \sum_{i=1}^n b_{ii}\lambda_i^2 + \sum_{j>i} b_{ij}\lambda_i\lambda_j$ for some numbers b_{ii}, b_{ij}. Alternatively, writing $x = (\lambda_1, .., \lambda_n)$, $Q(x) = x^T Bx$, where $B = (b_{ij})$ is an upper triangular matrix. Then write $A = B + B^T$ to give a symmetric matrix A with $(x,y) = x^T Ay$ for any $x, y \in V$. A necessary condition on M is that $M^T AM = A$ (also sufficient when $charK \neq 2$) and so $detM = \pm 1$.

Let us investigate the possibility of $O(n,K)$ containing transvections. Suppose that the transformation τ given by $\tau(v) = v + \sigma(v).u$ (with σ a linear form) lies in $O(n,K)$. For any $v \in V$ such that $\sigma(v) \neq 0, (v,u) \neq 0$ we see that

$$Q(\tau(v)) = Q(v + \sigma(v).u) = Q(v) + Q(\sigma(v).u) + (v, \sigma(v).u)$$

$$= Q(v) + \sigma(v)[\sigma(v)Q(u) + (v,u)]$$

and we deduce that $Q(u) \neq 0$ and $\sigma(v) = -(v,u)/Q(u)$. Such vectors v span V and therefore $\sigma(v) = -(v,u)/Q(u)$ for all $v \in V$. Thus $\tau(v) = v - [(v,u)/Q(u)].u$ for all $v \in V$. If $charK \neq 2$, then $\sigma(u) \neq 0$ so τ cannot be a transvection; we conclude that there are no transvections in $O(n,K)$, but there are reflections. If, on the other hand, $charK = 2$, then $\sigma(u) = 0$ and τ is a transvection; thus $O(n,K)$ contains some of the transvections in $Sp(n,K)$; we have already seen that the Symplectic group contains no (quasi-) reflections, so $O(n,K)$ cannot contain any either. Although the transformation $\tau(v) = v - [(v,u)/Q(u)].u$ is in one case a reflection and in the other a transvection, it is sometimes useful to be able to refer to both cases at the same time: we refer to such a map as a symmetry; we say that the map τ above is the symmetry centred on u. It so happens that $O(n,K)$ is generated by its symmetries, except in the case of $O^+(4,2)$.

Assume that $charK \neq 2$. Then a symmetry (reflection) has determinant -1 and so not all elements of $O(n,K)$ have determinant 1. This means that $O(n,K)$ has a normal subgroup of index 2 consisting of the elements having determinant 1: it is called the Special Orthogonal Group and is denoted by $SO(n,K)$. Unfortunately not even the projective group $PSO(n,q)$ is always simple and we are lead towards the commutator subgroup of $O(n,K)$. The commutator subgroup is denoted by $\Omega(n,K)$ and turns out to be a little smaller than $SO(n,K)$.

We have seen that a conjugate of a transvection is a transvection. Similarly a conjugate of a symmetry is a symmetry: let us denote by ρ_u the symmetry taking v to $v - [(v,u)/Q(u)].u$ for each $v \in V$, then for any $g \in O(n,K)$,

$g\rho_u g^{-1} = \rho_{g(u)}$. We can also calculate that $\rho_{\lambda u} = \rho_u$ for any $0 \neq \lambda \in K$, so a symmetry is uniquely determined by a non-isotropic 1-dimensional subspace. On such a subspace, the values taken by Q on non-zero vectors are all square or all non-square. The group we are edging towards is generated by pairs of symmetries of the same type, i.e., $\rho_u\rho_w$, where $Q(u), Q(w)$ are either both square or both non-square. However it is useful to approach the problem from a slightly different perspective.

We have seen that $O(n, K)$ doesn't contain transvections (we still assume that $charK \neq 2$). However we can ask the whether there might be transformations that act as transvections on some subspace $\langle u\rangle^{\perp}$. The vector u would have to be singular (for otherwise $\langle u\rangle^{\perp}$ would be non-isotropic and therefore entertain no transvections) and The Witt index of Q is thus ≥ 1. A linear form σ on $\langle u\rangle^{\perp}$ is given by $\sigma(v) = (v, w)$ for some $w \in \langle u\rangle^{\perp}$. It turns out that a transvection on $\langle u\rangle^{\perp}$ would have to have the form $\tau(v) = v + (v, w).u$ and there is a unique element of $O(n, K)$ having this restriction to $\langle u\rangle^{\perp}$, given by

$$\rho_{u,w}(v) = v + (v, w).u - (v, u).w - Q(w)(v, u).u.$$

Such elements are called Siegel transformations, or sometimes Eichler transformations. They have the following properties (which we do not prove): if u is singular, $w, w_1, w_2 \in \langle u\rangle^{\perp}$ and $g \in O(n, K)$, then

(i) $\rho_{\lambda u,w} = \rho_{u,\lambda w}$;

(ii) $\rho_{u,w_1+w_2} = \rho_{u,w_1}\rho_{u,w_2}$;

(iii) $g\rho_{u,w}g^{-1} = \rho_{g(u),g(w)}$.

It is known that $\Omega(n, K)$ is generated by Siegel transformations, so long as $n \geq 3$ and the Witt index is ≥ 1. If the Witt index is ≥ 2, then every vector in $\langle u\rangle^{\perp}$ is a sum of two singular vectors in $\langle u\rangle^{\perp}$, so by property (ii) every Siegel transformation is a product of Siegel transformations based on two singular vectors (i.e., a product of elements of the type $\rho_{u,w}$ with u, w both singular).

A similar theory can be expounded for even q. The proof that $P\Omega(n, q)$ is simple is approached in a similar way to the simplicity of $PSp(n, K)$ and was given (essentially) by Tamagawa ([15]).

Theorem 1 *(Tamagawa)*

If $n \geq 3$, then $P\Omega(n, q)$ is simple except for the cases $P\Omega^+(4, q)$ and $P\Omega(3, 3)$.

We should mention that there is a subgroup of $O(n, K)$ called the Special Orthogonal Group, even when $charK = 2$. In all cases $SO(n, K)$ has index 2 in

$O(n, K)$. For $char K \neq 2$ any product of an even number of symmetries has determinant 1 and so lies in $SO(n, K)$. This turns out to be a useful characterisation of $SO(n, K)$ in general: an element of $O(n, K)$ lies in $SO(n, K)$ precisely when it is a product of an even number of symmetries. A Siegel transformation can be written as a product of two symmetries, so every Siegel transformation lies in $SO(n, K)$ and therefore $\Omega(n, K) \leq SO(n, K)$. In fact the two groups are the same for $K = GF(q)$ with q even (except when $n = 4$ and $q = 2$), while the index is 2 for q odd.

1.4 Unitary Groups

We shall not say very much about Unitary Groups. The development is similar to the Symplectic Group and the Orthogonal Group. On this occasion we have a hermitian form: the Unitary Group $U(n, K)$ is the subgroup of $GL(n, K)$ consisting of elements which preserve the hermitian form, $SU(n, K)$ consists of those elements of $U(n, K)$ having determinant 1, and $GU(n, K)$ consists of elements of $GL(n, K)$ which preserve the hermitian form up to a scalar multiple.

It turns out that $(v, v) = 0$ may occur, but doesn't always. The Witt index ν is given by the dimension of a maximal totally isotropic subspace of V. For finite fields $GF(q)$, the Witt index is such that $n = 2\nu$ or $2\nu + 1$. Recall that for a hermitian form, $GF(q)$ has an involutory automorphism; this can only happen if q is square. The group $PSU(n, q)$ is simple except when $(n, q) = (3, 4), (2, 4)$ or $(2, 9)$. The group $PGU(n, q)$ is the group preserving the set of isotropic points of $PG(n-1, q)$ and can, in fact, be thought of as the group preserving totally isotropic subspaces of any given dimension.

Exercises

1. Prove that $GL(n, K)$ is a normal subgroup of $\Gamma L(n, K)$.

2. Suppose that $(,)$ is an alternating bilinear form and that U is a subspace of V. Show that

   $(U^\perp)^\perp \subseteq U$ and using the fact that $dimU^\perp = n - dimU$ show that $(U^\perp)^\perp = U$.

3. Suppose that $(,)$ is an alternating bilinear form. Show that the transvection τ given by

   $\tau(v) = v + \lambda(v, u).u$ lies in $Sp(n, K)$ for every $0 \neq u \in V$ and every $0 \neq \lambda \in K$.

4. Prove that $Sp(2, K)$ is generated by transvections. Do not use the result that says $SL(2, K)$ is generated by transvections. Use as starting points the fact that if $g \in Sp(2, K)$, then g has determinant 1 and we may reduce to the case where $g(u_1) = u_1$.

5. Prove that $PSp(n, K)$ is primitive on the set of points of $PG(n-1, K)$. (Consider the cases $n = 2$ and $n \geq 4$ separately).

6. Let g_λ and τ be the elements of $G = Sp(2, K)$ given by

   $$g_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix},$$

   $$\tau = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

   Show that $g\tau g^{-1}\tau^{-1} = \begin{pmatrix} 1 & \lambda^2 - 1 \\ 0 & 1 \end{pmatrix}$

   and hence show that G' contains $\begin{pmatrix} 1 & \lambda^2 - \mu^2 \\ 0 & 1 \end{pmatrix}$

   for each $\lambda, \mu \in K$. Show that, except for $K = GF(2)$ or $GF(3)$, every element of K can be expressed as a difference of squares, and hence show that G' contains every transvection centred on the first basis vector. Show that G' must be transitive on the 1-dimensional subspaces of V and hence prove that $G' = G$.

7. Prove the following properties of Siegel transformations:

   If u is singular, $w, w_1, w_2 \in \langle u \rangle^\perp$ and $g \in O(n, K)$, then

(i) $\rho_{\lambda u,w} = \rho_{u,\lambda w}$;

(ii) $\rho_{u,w_1+w_2} = \rho_{u,w_1}\rho_{u,w_2}$;

(iii) $g\rho_{u,w}g^{-1} = \rho_{g(u),g(w)}$.

Chapter 2

Isomorphisms between Classical Groups

2.1 Orthogonal and Symplectic Groups in Characteristic 2

Recall that in defining classical groups and associated forms we commented that the forms would normally be non-degenerate. One consequence of this is that for $Sp(n, K)$, n has to be even, and in characteristic 2 the same is true of $O(n, K)$. Let us relax a little for a moment and allow the possibility of degenerate bilinear forms. Remember that we referred to the nucleus of a sesquilinear form, i.e., $X = \{u \in V : (u, v) = 0 \text{ for all } v \in V\}$. If n is odd and K has characteristic 2, then this nucleus must be non-trivial; moreover on any complement to X in V, $(,)$ must be non-degenerate.

Let us assume that $K = GF(q)$ with q even. For any quadratic form Q the associated bilinear form $(,)$ is also an alternating form. Thus $O(n, q) \leq Sp(n, q)$. The situation we look at is where the nucleus is non-singular and 1-dimensional. A slight digression is in order here so that we may set the discussion in an appropriate context. Suppose that n is even and that $(,)$ is non-degenerate, associated with a quadratic form Q, and let U be a non-singular 1-dimensional subspace. Then $W = U^\perp$ contains U and has dimension $m = n - 1$, from which we see that $W^\perp = U$, in other words the nucleus of $(,)$ on W is precisely U. Let us now concentrate on the vector space W, of odd dimension m, together with the (inherited) quadratic form Q and associated bilinear form $(,)$ with nucleus U.

We have seen that any complement of U in W will be non-isotropic. Let Y be any such complement, let $0 \neq u \in U$ and let ϕ be the projection map $: W \to Y$ given by $\phi(\lambda u + y) = y$ (any element of W may be expressed uniquely as $\lambda u + y$ for some $y \in Y$ and some $\lambda \in K$). If $w = \lambda u + y \in W$ is singular, then $0 = Q(w) = \lambda^2 Q(u) + Q(y)$, so $\lambda^2 = Q(y)/Q(u)$. The restriction of ϕ to singular vectors of W gives rise to a bijection ψ from the singular vectors of W to Y, with $\psi^{-1}(y) = y + \sqrt{(Q(y)/Q(u))}.u$. (Note that every element of $GF(q)$ is square when q is even.) We can calculate that if $w_1 = \lambda_1 u + y_1$ and $w_2 = \lambda_2 u + y_2$, then $(w_1, w_2) = (y_1, y_2)$, so ϕ preserves $(,)$ and maps totally singular 2-dimensional subspaces of W to totally isotropic 2-dimensional subspaces of Y. We appear to have a correspondence between the group on W preserving the set of totally singular 2-dimensional subspaces and the group on Y preserving the set of totally isotropic 2-dimensional subspaces; we can see that we appear to have an isomorphism between $O(m,q)$ and $Sp(m-1,q)$, or at least between $GO(m,q)$ and $GSp(m-1,q)$.

We can demonstrate an isomorphism in a more concrete fashion. When we choose the vector $u \in U$ we may assume that $Q(u) = 1$ (given an arbitrary non-zero vector $u \in U$ we may replace it by $u/(Q(u)^{1/2})$). Suppose that $g \in O(W)$, then g fixes U (which actually means that $g(u) = u$). For any $y \in Y$, we have $g(y) = \hat{y} + \lambda u$ for some $\hat{y} \in Y$ and some $\lambda \in K$. Let $\hat{g}$ be the linear transformation on Y which takes y to $\hat{y}$ for all $y \in Y$. If $y, z \in Y$ with $g(y) = \hat{y} + \lambda u, g(z) = \hat{z} + \mu u$, then

$$(y,z) = (g(y), g(z)) = (\hat{y}, \hat{z}) = (\hat{g}(y), \hat{g}(z))$$

so $\hat{g}$ preserves $(,)$ on Y. It isn't difficult to show that $\hat{g}$ must be invertible, so $\hat{g} \in Sp(Y)$. We thus have a homomorphism from $O(W)$ to $Sp(Y)$. Conversely, suppose that $\hat{g} \in Sp(Y)$ and suppose that for any $y \in Y$, $\hat{g}(y) = \hat{y}$. Define a linear transformation g on W by $g(u) = u$ and $g(y) = \hat{y} + (Q(y) + Q(\hat{y}))^{1/2}.u$ (one should check that this transformation is indeed linear). Then it is not difficult to show that g is invertible and preserves Q, so lies in $O(W)$. Hence we have a homomorphism from $Sp(Y)$ to $O(W)$ which is inverse to our homomorphism from $O(W)$ to $Sp(Y)$. It now follows that $O(m,q)$ and $Sp(m-1,q)$ are isomorphic.

2.2 The Klein Quadric

In this section we discuss briefly an isomorphism between $PSL(4,q)$ and $P\Omega^+(6,q)$ and see how it leads to an isomorphism between $PSp(4,q)$ and $P\Omega(5,q)$. A bijection is constructed between the lines of $PG(3,q)$ and the points of the Klein Quadric, $\mathcal{Q}$ in $PG(5,q)$. An automorphism of $PG(3,q)$ then leads to an automorphism of $\mathcal{Q}$.

Given a line l in $PG(3,q)$ let (x_0, x_1, x_2, x_3), (y_0, y_1, y_2, y_3) be the coordinates of two points on the line; for each $i \neq j$, let $p_{ij} = x_i y_j - x_j y_i$. Then $(p_{01}, p_{02}, p_{03}, p_{23}, p_{31}, p_{12})$ gives the coordinates of a point in $PG(5,q)$. A calculation shows that any other pair of points on l gives the same point in $PG(5,q)$.

Moreover each such point in $PG(5,q)$ lies on the quadric $\mathcal{Q}$ arising from the quadratic form:
$Q(\lambda_1,..,\lambda_6) = \lambda_1\lambda_4+\lambda_2\lambda_5+\lambda_3\lambda_6$. This quadric is known as the *Klein Quadric.* One can show that there is actually a bijection between the lines of $PG(3,q)$ and the points of $\mathcal{Q}$ and this leads to an isomorphism between $PSL(4,q)$ and $P\Omega^+(6,q)$. There is a great deal of geometry associated with the Klein Quadric, far too much to be summarised here. However it is possible to give a starting point: two lines meet in $PG(3,q)$ precisely when the corresponding points on $\mathcal{Q}$ are orthogonal.

Consider a point $u = (0,0,1,0,0,-1) \in PG(5,q)$. The points orthogonal to u are precisely the points
$(\lambda_1,..,\lambda_6)$ with $\lambda_3 = \lambda_6$. Let G be the subgroup of $P\Omega^+(6,q)$ fixing u. Then G fixes all the points with $p_{03} = p_{12}$,i.e., $x_0y_3 - x_3y_0 + x_2y_1 - x_1y_2 = 0$. This is precisely the condition that two points of $PG(3,q)$ are orthogonal with respect to a (non-degenerate) alternating bilinear form. It follows that the stabilizer in $P\Omega^+(6,q)$ of $U = \langle u\rangle$ is isomorphic to the subgroup of $PSL(4,q)$ fixing a general linear complex. One can show further that an element of G actually corresponds to an
element of $PSp(4,q)$ so giving an automorphism from $P\Omega(5,q)$ to $PSp(4,q)$.

2.3 Other Isomorphisms

In this section we summarise isomorphisms that exist between various classical groups. The first section in this chapter describes an isomorphism between $O(n,q)$ and $Sp(n-1,q)$ which works for any odd n and q any power of 2. However $O(n,q)$ doesn't belong to a non-degenerate form. In the second section we saw isomorphisms that work for any q but with the dimensions fixed: $P\Omega^+(6,q) \approxeq PSL(4,q)$ and $P\Omega(5,q) \approxeq PSp(4,q)$. Other isomorphisms similarly occur for fixed dimensions and a number occur only for certain fields. We have already seen the following:
(i) $SL(2,q) \approxeq Sp(2,q)$, in fact both are isomorphic to $SU(2,q^2)$;

The other isomorphisms listed are for simple or closely related groups:

(ii) For q odd, $PSL(2,q) \approxeq P\Omega(3,q)$;

(iii) $P\Omega^+(4,q) \approxeq (q-1,2).(PSL(2,q) \times PSL(2,q))$;

(iv) $P\Omega^-(4,q) \approxeq PSL(2,q^2)$;

(v) $P\Omega^-(6,q) \approxeq PSU(4,q)$;

(vi) $PSL(2,7) \approxeq PSL(3,2)$;

(vii) $PSU(4,2) \approxeq PSp(4,3)$;

2.4 Suzuki Groups

Previous sections have dealt with a general isomorphism between $O(n,q)$ and $Sp(n-1,q)$ for q even and n odd, and a particular isomorphism between $P\Omega(5,q)$ and $PSp(4,q)$. It is natural to ask whether these give essentially the same isomorphism: the answer is no and the reason is that if we combine the two isomorphisms to give an automorphism of $Sp(4,q)$ (q even), then the image of a transvection is not a transvection, so that the automorphism is outer (remember that the conjugate of a transvection is a transvection).

Let us approach essentially the same question from a very different perspective. The isomorphisms we have just looked at correspond to bijections between lines and points in projective space. First, in the Klein correspondence, we have a bijection between the totally isotropic lines of $PG(3,q)$ and the points on a parabolic quadric $\mathcal{P}$ in $PG(4,q)$. Secondly, the projection onto a complement of the nucleus of $\mathcal{P}$ gives a bijection from the points of $\mathcal{P}$ to the points of $PG(3,q)$. Putting these together gives a bijection from totally isotropic lines to points of $PG(3,q)$. There are many such bijections (just compose with elements of $Sp(4,q)$), but it reasonable to ask whether there is such a bijection having order 2. Such a bijection would be a sort of polarity (in fact it would be a polarity of a generalized quadrangle). It is known that a polarity exists if and only if q is an odd power of 2. Suppose that q is an odd power of 2 and let θ be such a polarity. The points P for which P lies on $\theta(P)$ are called absolute points of θ and they happen to lie on an ovoid $\mathcal{O}$ called the Suzuki-Tits ovoid. The elements of $Sp(4,q)$ which fix this ovoid form a simple group called a Suzuki group, $Sz(q)$.

For q an odd power of 2, the automorphism of $Sp(4,q)$ we have referred to can be described essentially in terms of the polarity θ: if $g \in Sp(4,q)$, then its image g' is determined by its action on the points of $PG(3,q)$, for any $X \in PG(3,q)$, $g'(X) = \theta(g(\theta(X))$. The fixed elements of the automorphism are precisely the elements of $Sp(4,q)$ which commute with θ. For $q > 2$ these turn out to be exactly the elements of $Sz(q)$.

There are various accounts of this material. For example, Todd gives a brief description in [16], and there is more detailed discussion in [15].

Chapter 3

Aschbacher's Theorem

3.1 Introduction

The idea of Aschbacher's Theorem is that a number of classes of subgroup are identified and every subgroup belongs to at least one class. The theorem doesn't state directly which subgroups are maximal within each class. We don't attempt a complete proof of Aschbacher's Theorem. Rather we consider the substantive ideas (and in consequence leave a number of details unaddressed). The treatment here arises from work on analogous theorems for classical groups over arbitrary fields, carried out jointly with Shangzhi Li and Roger Dye. We shall frequently assume that $G = Sp(n, q)$ (because it gives us something to focus on), but the treatment is designed for a more general setting.
It is also convenient to assume that any subgroups we consider do not lie in the centre of G, and often we assume that they contain the centre.

3.2 Reducible subgroups

Given $G = Sp(n, q)$ (with the understanding of the previous paragraph), assume that M is a subgroup of G. We say that M is reducible if every member of M fixes a proper non-trivial subspace U of V. Observe that if $g \in M$ and $gU = U$, then also $gU^\perp = U^\perp$. Moreover we also find that $g(U \cap U^\perp) = U \cap U^\perp$. Observe that for any $u, v \in U \cap U^\perp$ we have $u \in U, v \in U^\perp$ so that $(u, v) = 0$. Thus $U \cap U^\perp$ is totally isotropic. One possibility is that $U \cap U^\perp = \{0\}$, in which case U is non-isotropic. Otherwise $U \cap U^\perp$ is a non-trivial totally isotropic subspace fixed by every member of M. Thus there are only two types of reducible subgroups that we need consider.
There is an occasional twist when the fixed subspace is non-isotropic: if U is isometric to $U^\perp$ (i.e., there is an invertible linear map from U to $U^\perp$ preserving the form), then G contains elements interchanging U and $U^\perp$; this gives rise to an imprimitive subgroup of a type we shall see shortly, but all we need to observe here is that reducible subgroups need not be maximal.

3.3 Irreducible Subgroups that are not Absolutely Irreducible

Suppose that N is an irreducible subgroup of G. Then Schur's Lemma says that $End_{KN}(V)$ is a division ring. Put another way, the $n \times n$ matrices over K that commute with all matrices in N form a division ring. A theorem of Wedderburn states that a finite division ring is a field, so $F = End_{KN}(V)$ is a field; moreover all the scalar matrices commute with N so K is embedded in F via the scalar matrices. If $F = K$, then N is said to be absolutely irreducible. If N is not absolutely irreducible, then N preserves a vector space structure over F: if $[F : K] = r$, then r divides n and elements of N can be expressed as $m \times m$ block matrices (where $m = n/r$) with blocks representing F over K. If M is the normalizer of N in G, then a standard group theory argument tells us that M normalizes F^* (the non-zero elements of F) and so normalizes F. This tells us that conjugation by M induces a field automorphism on F and M consists of semi-linear transformations over F, in other words M preserves the F-structure on V.

We have here a second class of subgroups of G: those that preserve an extension field. Such subgroups fix the set of 1-dimensional F-subspaces of V and so correspond to subgroups fixing a spread of $PG(n-1, q)$. Two further considerations are the size of the extension field (in fact the degree may be assumed prime) and the question of what happens if V is 1-dimensional over F. The only thing we have to note is that there is not very much F-space structure if V is 1-dimensional over F. In that case we say that M normalizes F, in other words induces an automorphism of F, and N is a Singer cyclic subgroup of G.

3.4 Irreducible subgroups with normal reducible subgroups (non-homogeneous)

Now assume that M is an irreducible subgroup of G, but that M has a reducible normal subgroup N (not lying in the centre of G). Let W be an irreducible subspace of V under N. Then by the arguments in the previous section, W is either non-isotropic or totally isotropic.

Consider the subspace $U = \langle gW : g \in M \rangle$ of V. This subspace is fixed by M and M is irreducible on V, so $U = V$. The following is a standard type of argument: suppose that $g_1W, g_2W, .., g_kW$ is any finite collection of subspaces with $g_1, g_2, ..., g_k \in M$ and for $g \in M$ consider the intersection $Y = gW \cap (g_1W + g_2W + .. + g_kW)$. For any $h \in N$, $hg = gh'$ for some $h' \in N$, so that $hgW = gh'W = gW$; similarly $hg_iW = g_iW$ and therefore h fixes Y. By the minimality of W it follows that $Y = \{0\}$ or $Y \subseteq g_1W + g_2W + .. + g_kW$. This means that, starting from $g_1 = I$, we can construct subspaces $g_1W, g_2W, .., g_kW$ such that $V = g_1W \oplus g_2W \oplus .. \oplus g_kW$.

What does this tell us about M? For one thing, we can choose a basis for V such that N is block-diagonal. However this does not tell us quite enough about the action of N. Further information is revealed by the following theorem.

Theorem 1 *(Clifford, [4])*

Suppose that M is an irreducible group acting on a vector space V and suppose that N is a reducible normal subgroup of M. Then V is the direct sum of N-invariant subspaces V_i $(1 \leq i \leq k)$ which satisfy the following conditions:

(i) $V_i = X_{i1} \oplus X_{i2} \oplus .. \oplus X_{it}$, where each X_{ij} is an irreducible N-subspace of V, t is independent of i, and X_{ij} and X_{kl} are isomorphic as N-spaces if and only if $i = k$;

(ii) For any N-subspace U of V we have $U = U_1 \oplus U_2 \oplus .. \oplus U_k$, where $U_i = U \cap V_i$ for each i, in particular any irreducible N-subspace of V lies in one of the V_i's;

(iii) M permutes the set $\{V_1, V_2, .., V_k\}$ transitively.

A subspace U of V fixed by N is said to be KN- isomorphic to W if there is an invertible linear transformation $\phi : W \rightarrow U$ such that $\phi(h(w)) = h(\phi(w))$ for every $w \in W$ and every $h \in N$. The concept of homogeneity gives information on the action of M on V. To begin with, let Y be the sum of all subspaces of V that are KN-isomorphic to W. Then Y is a subspace of V fixed by N; it is called the homogeneous component of V containing W and V is homogeneous if $Y = V$. In the next section we shall consider the homogeneous case further.

For the rest of this section, we assume that V is not homogeneous under N. Clifford's Theorem says that V can be decomposed uniquely into the direct sum $V = V_1 \oplus \cdots \oplus V_k$ of its homogeneous components (with $V_1 = Y$ and $k \geq 2$) and M acts transitively on the set $\Sigma = \{V_i : 1 \leq i \leq k\}$ of all these components. Each irreducible subspace lies in one of the V_i. For any $1 \leq i \leq k$, let $M_i = \{g \in M : gV_i = V_i\}$. If V_i is reducible as an M_i- space, say M_i fixes a subspace U_i, then the images of U_i under M form a direct sum, a proper subspace of V, invariant under M, but this contradicts M irreducible and so V_i is
irreducible under M_i. It follows that each V_i is either non-isotropic or totally isotropic. We also know that M is transitive on Σ, so the V_i's all have the same dimension and are either all non-isotropic or all totally isotropic.

Suppose that V_1 is non-isotropic, and consider the action of M_1 on $V_1^{\perp}$. Observe that $V_1^{\perp}$ is fixed by N and each irreducible subspace of $V_1^{\perp}$ must lie in some V_i, but $V_1 \cap V_1^{\perp} = \{0\}$ so $i \neq 1$. By Clifford's Theorem, $V_1^{\perp}$ can be expressed as the direct sum of its intersections with the V_i's, but the intersection with V_1 is $\{0\}$ so $V_1^{\perp} \subseteq \sum_{i\neq 1} V_i$, and thus $V_1^{\perp} = \sum_{i\neq 1} V_i$. The same argument applies to other V_i and so the V_i's are mutually orthogonal. Hence one possibility is that M permutes transitively a number of mutually orthogonal non-isotropic subspaces whose direct sum is V. Such a group acts irreducibly and imprimitively on V.

Suppose now that the V_i's are all totally isotropic. One possibility is that $k = 2$ and this would give another imprimitive subgroup. We show that $k \geq 3$ leads to an imprimitive group as described in the previous paragraph.

We first use Clifford's Theorem to express $V_1^{\perp}$ as $V_1 \oplus W_2 \oplus W_3 \oplus .. \oplus W_k$ where $W_i = V_1^{\perp} \cap V_i$ for each $i \geq 2$. Then $W = W_2 \oplus W_3 \oplus .. \oplus W_k$ is a complement to V_1 in $V_1^{\perp}$ and thus non-isotropic. Hence $W^{\perp}$ is non-isotropic and contains V_1. Applying Clifford's Theorem to $W^{\perp}$ we see that $W^{\perp} = V_1 \oplus T_2 \oplus T_3 \oplus .. \oplus T_k$ where $T_k = W^{\perp} \cap V_i$; thus if we take $U_1 = T_2 \oplus T_3 \oplus .. \oplus T_k$ then we have $dim U_1 = dim V_1$, $W^{\perp} = V_1 \oplus$
U$_1$ and U_1 is invariant under N. Notice that if the V_i's are irreducible under N, then each T_i is either V_i or $\{0\}$, from which we deduce that $U_1 = V_i$ for some $i \geq 2$; however, in general we cannot assume that the V_i's are irreducible under N.

By Clifford's Theorem, V_1 can be expressed as a sum $X_1 \oplus X_2 \oplus ... \oplus X_t$ of isomorphic irreducible N-invariant subspaces. Let $Y_1 = (X_2 \oplus ... \oplus X_t)^{\perp} \cap U_1$. Then Y_1 is invariant under N and its dimension is the same as X_1, from which we deduce that Y_1 is irreducible and so also totally isotropic. An alternative way of reaching the same point is to write out $X_1^{\perp}$ as we did $V_1^{\perp}$ in the previous paragraph and construct an N-invariant complement to X_1 in $X_1^{\perp}$, whose conjugate subspace is $X_1 \oplus Y_1$. Applying the same technique to each of $X_2, X_3, .., X_t$ we arrive at irreducible N-invariant
subspaces $Y_1, Y_2, .., Y_t$ whose direct sum is U_1. For each j the subspace $X_j \oplus Y_j$ is non-isotropic, and the t non-isotropic subspaces so constructed are mutually orthogonal. When we say that $X_1, .., X_t$ are KN-isomorphic it means that they have bases with respect to which any element h of N is represented by the same matrix P for each X_j. Given a basis $x_{j1}, ..$ for X_j there is a complementary basis $y_{j1}, ..$ for Y_j such that $(x_{jr}, y_{js}) = \delta_{rs}$. If $h \in N$ is represented on X_j by P, then h is represented on Y_j by $(P^T)^{-1}$. It follows that h is represented by the same matrix on each Y_j and this means that $Y_1, .., Y_t$ are KN-isomorphic. We conclude that U_1 is a homogeneous component of V, i.e., U_1 is one of
$V_2, .., V_k$; without loss of generality $U_1 = V_2$. Recall that $V_1^{\perp} = V_1 \oplus W_2 \oplus W_3 \oplus .. \oplus W_k$ where $W_i = V_1^{\perp} \cap V_i$ for each $i \geq 2$, but now $W_2 = \{0\}$ so by consideration of dimension $W_i = V_i$ for each $i \geq 3$. Continuing in this way gives

us a direct sum of pairwise orthogonal non-isotropic subspaces preserved by M.

3.5 Irreducible subgroups with normal reducible subgroups (homogeneous)

The situation we now have is that N is a reducible normal subgroup of M such that N is homogeneous on V, i.e., all irreducible KN- subspaces of V are KN- isomorphic and span V. We have already seen that V can be expressed as a direct sum of irreducible subspaces. These are now KN-isomorphic, so if we choose bases appropriately, elements of N can be represented by block diagonal matrices $diag(P, P, .., P)$ where P represents an element of N acting on W. Suppose that an element A of M is given in block-diagonal form by (A_{ij}).
Then $A.diag(P, P, .., P).A^{-1} = diag(P', P', .., P')$ for a suitable matrix $P' \in N|_W$ depending on P, i.e., $A.diag(P, P, .., P) = diag(P', P', .., P').A$, from which we deduce that $A_{ij}P = P'A_{ij}$ for each i, j.

For any given i, j, the matrix A_{ij} represents a linear transformation of W. Let T be the kernel of this transformation (i.e., the set of vectors $w \in W$ such that $A_{ij}w = 0$). Then for any $w \in T$ and any $P \in N|_W$ we have $A_{ij}Pw = P'A_{ij}w = P'0 = 0$ so that $Pw \in T$. Hence T is an N-invariant subspace of W. However W is irreducible, so $T = W$ or $\{0\}$. If $T = W$, then $A_{ij} = 0$; clearly not every A_{ij} can be 0, so for some particular i, j, $T = \{0\}$ and A_{ij} is invertible. We fix B as an invertible A_{ij} so that $BP = P'B$ and therefore $P' = BPB^{-1}$; note that the same B applies to every P and thus B normalizes N. Now for any i, j, $A_{ij}P = P'A_{ij} = BPB^{-1}A_{ij}$ so $B^{-1}A_{ij}P = PB^{-1}A_{ij}$ and hence $B^{-1}A_{ij}$ centralizes P, in fact centralizes N on W. We write $C_{ij} = B^{-1}A_{ij}$ and $C = (C_{ij})$ so that $A = diag(B, B, .., B)C$.

Let us think a bit further about the matrices that centralize N on W. We have selected W as an irreducible N-subspace, so $F = End_{KN}(W)$ is a field containing K. Another way of saying the same thing is that F is the centralizer of N on W; if B normalizes N then it also normalizes F. If $[F : K] = s$, then F can be represented as $s \times s$ matrices over K and s divides the K-dimension r of W. From this, subject to an appropriate basis for W, F may be represented as block diagonal matrices $diag(R, R, .., R)$ where R is $s \times s$ and there are $m = r/s$ copies of R; moreover N can be regarded as a subgroup of $GL(m, F)$. We shall see that
M preserves the F-structure on V. Suppose that $v \in V$ and that $D \in F$ is represented by
$diag(E, E, .., E)$, where E is the matrix for D on W and in turn $E = diag(R, R, .., R)$ with R $s \times s$. Then

$$ADv = diag(B, B, ..B)Cdiag(E, E, .., E)v = diag(B, B, ..B)diag(E, E, .., E).Cv$$

$$= diag(BEB^{-1}, BEB^{-1}, ..BEB^{-1})diag(B, B, ..B)Cv = D'Av,$$

where D' is conjugate to D in F. This conjugation amounts to a field automorphism, so A is a semilinear transformation of V over F. There are two possibilities here. If $s > 1$, then M stabilizes a field extension and we get a class of subgroups that we already know about.

Suppose $s = 1$, then A is a tensor product $B \otimes C$ where $B \in GL(r, K), C \in GL(d, K)$. Here M preserves a tensor product decomposition $U \otimes W$. The geometry is not easy to describe. However, in essence, there are a number of subspaces of the form $u \otimes W$ and M permutes the subspaces in this set.

3.6 Irreducible subgroups with no reducible normal subgroups

In the previous sections we have seen that if M contains a reducible normal subgroup (properly containing the centre of G), then M is either imprimitive or stabilizes a tensor product decomposition (or stabilizes an extension field). Suppose now that every normal subgroup of M is absolutely irreducible and let N be a normal subgroup, minimal amongst the normal subgroups not contained in the centre. Take $\bar{M}, \bar{N}$ to be the images of M, N in $PGL(n, q)$. Then $\bar{N}$ is a minimal normal subgroup of $\bar{M}$. A fundamental property of such subgroups is that they can be expressed as a direct product of isomorphic simple subgroups (c.f., [2], p25). There are essentially three possibilities: (i) $\bar{N}$ is simple; (ii) $\bar{N}$ is a direct product of abelian simple groups; (iii) $\bar{N}$ is a direct product of non-abelian simple groups. It is the third possibility that we concentrate on in this section.

We assume that $\bar{N} = \bar{N}_1 \times \bar{N}_2 \times .. \times \bar{N}_k$ with the $\bar{N}_i$ isomorphic, non-abelian and simple and we denote by N_i the pre-image in N of $\bar{N}_i$ for each i. Thus $N = N_1 N_2 ... N_k$ and each of the factors centralizes each of the others, modulo the centre of N, i.e., for any $i \neq j$ we have $[N_i, N_j] \leq Z(N)$. The first thing we need to show is that, in fact, each element of N_i commutes with each element of N_j when $i \neq j$ (this makes the product $N = N_1 N_2 ... N_k$ a central product). Let $f \in N_i$, $g \in N_j$ $(i \neq j)$ and suppose that $\bar{f}$ has order r in $\bar{N}_i$. Then $g^{-1} f g = \lambda f$ for some $0 \neq \lambda \in K$, so $f^r = g^{-1} f^r g = \lambda^r f^r$ and therefore $\lambda^r = 1$. Now $\bar{N}_i$ is non-abelian simple, so is generated by involutions (elements of order 2) and for any involution $\bar{f}$, $g^{-1} f g = \pm f$. Also $g^{-1} f g = f$ for any $f \in Z(N_i)$. This means that $g^{-1} f g = \pm f$ for any $f \in N_i$. However we can choose r to be an odd prime divisor of $|\bar{N}_i|$; Sylow's Theorem ensures that $\bar{N}_i$ has elements of order r, for such elements f we must have $g^{-1}fg = f$, and the simplicity of $\bar{N}_i$ means that it is generated by elements of order r. Hence $g^{-1}fg = f$ for all $f \in N_i, g \in N_j$. The N_i's commute as claimed. The other important structural property is that in acting by conjugation, M permutes the N_i's (and in particular, if $g \in M$, then for each i, $g^{-1}N_ig$ is an N_j).

The main argument now centres on the observation that N_1 is a normal subgroup of N and we attempt to apply the techniques developed to deal with $N \trianglelefteq M$. First suppose that N_1 is irreducible and let $F = End_{N_1}(V)$. Then F is a field containing K. However, $N_2 \leq End_{N_1}(V)$, so $N_2 \leq F$, a contradiction to N_2 non-abelian. Therefore N_1 is reducible on V.

Let W be an irreducible N_1-subspace of V. For any $g \in N_2N_3..N_k$, the subspace gW is N_1-isomorphic to W, but V is irreducible under N so the N-images of W span V and hence V is homogeneous under N_1. Given this, our techniques from earlier sections tell us that N preserves a tensor space decomposition $U \otimes W$. On this occasion, however, the N_j's ($j \geq 2$) commute with N_1 and in consequence they fix U. We can show that $N_2N_3..N_k$ must be absolutely irreducible on U (using the absolute irreducibility of N on V) and then apply exactly the same arguments to U. We find that N preserves a tensor product decomposition $V_1 \otimes V_2 \otimes .. \otimes V_k$ (with $V_k = W$), fixing each component. In permuting the N_i's when acting by conjugation, M permutes transitively the components of the tensor product decomposition. It follows that these components are isometric. For each j, N preserves a set of subspaces of V:

$$S_j = \{v_1 \otimes v_2 \otimes ... \otimes v_{j-1} \otimes V_j \otimes v_{j+1} \otimes ... \otimes v_k : 0 \neq v_i \in V_i, i \neq j\}$$

and M permutes $S_1, S_2, ..., S_k$.

3.7 Subgroups of Symplectic Type

In this section we consider the possibility that M has an irreducible normal subgroup N (minimal subject to not lying in the centre of M) such that $\bar{N}$ is a direct product of (at least two) isomorphic abelian simple groups, in other words $\bar{N}$ is an elementary abelian r-group, for some prime r.

Clearly $\bar{N}$ is abelian, but what about N itself? Well since N is irreducible, $End_{KN}(V)$ is a field F containing $GF(q)$. Moreover Wedderburn's Density Theorem (c.f., [13], p649) tells us that the ring generated by N is precisely $End_F(V)$; if V is m-dimensional over F, then $End_F(V)$ is just the set of all $m \times m$ matrices over F with respect to an appropriate basis. Given that N is abelian the same must be true for $End_F(V)$, but this can only be true if $m = 1$. It follows from this that $End_F(V) = F$ and N is a subgroup of F^*. However F^* is cyclic, so N is cyclic and therefore $\bar{N}$ is too. But this contradicts the notion of N as elementary abelian with at least two factors. Hence N is not abelian.

Suppose that $a, b \in N$ such that $ab \neq ba$. Then the images $\bar{a}, \bar{b}$ of a, b in $\bar{N}$ commute and have order r. Thus $b^{-1}ab = \mu a$ for some $0, 1 \neq \mu \in K$ and $b^r \in Z$ so $b^{-r}ab^r = a$ and therefore $\mu^r = 1$. We know that r is prime and that $\mu \neq 1$, so r must divide $q-1$; in particular r is different from p. At the same time a and $b^{-1}ab$ have the same determinant, so $\mu^n = 1$ and, since r is prime, r divides n. Denote by R the subgroup of $GF(q)^*$ of order r and let λ be a generator for
R, then for any $a, b \in N$, we have $a^{-1}b^{-1}ab = \lambda^i$ for some $0 \leq i < r$.

Let N_C be the centre of N. Then the minimality of N means that $N_C = N \cap Z$, where Z is the centre of G. If a is any non-central element of N, then the M-conjugates of a generate N. Let $b = g^{-1}ag$ such that b doesn't commute with a, so $b^r = a^r$ and $a^{-1}b^{-1}ab = \mu = \lambda^i$ for some $0 < i < r$, and consider the element $c = b^{-1}a$. We use the fact that $b^{-1}a = \mu ab^{-1}$ to deduce that $c^r = a^r b^{-r} \mu^{r(r-1)/2}$. Two situations unfold, depending on whether or not $r = 2$.

Suppose that $r > 2$. Then $c^r = 1$ and c is non-central in N (for example, c does not commute with a). Now the subgroup of N generated by the M-conjugates of c must be the whole of N. Let $c_1, c_2, .., c_m$ be a minimal set of such generators. Then $c_i^r = 1$ for each i and $[c_i, c_j] \in R$, and $a^r = 1$ for all $a \in N$. Hence N has order r^{m+1} and N/N_C is an elementary abelian r-group.

If $r = 2$, then the situation is similar, but a little more complicated. Recall that r does not divide q, so here q is odd, and $\lambda = -1$. Thus $c^2 = -1$. This time we get a minimal set, $c_1, c_2, .., c_m$, of generators among M-conjugates of c for N, satisfying $c_i^4 = 1, c_i^2 = -1$. We still find that N has order r^{m+1} and N/N_C is an elementary abelian r-group.

In both cases N is an extra-special r-group.

We have said that the group $\bar{N} = N/N_C$ is an elementary abelian r-group. That means that we can think of $\bar{N}$ as a vector space L over $GF(r)$, and in this context we regard the binary operation on L as addition. To emphasize this point, let us represent the mapping from N to L by ϕ. Given two elements $\phi(x), \phi(y) \in L$, define $f(\phi(x), \phi(y)) = k$, where $x^{-1}y^{-1}xy = \lambda^k$. Then f is an alternating form on L (notice that $f(\phi(x), \phi(y))$ does not depend on the choice of pre-images x, y), and must be non-degenerate (given any $x \in N - N_C$ there is a $y \in N$ not commuting with x). It isn't difficult to see that conjugacy of N by M preserves f, so M can be embedded in $Sp(m, r)$. Moreover, when $r = 2$ we can define a
quadratic form Ψ on L by $\Psi(x) = 0$ or 1, depending on whether $x^2 = 1$ or -1, in which case conjugacy by M preserves Ψ.

We saw earlier that r divides n. In fact n is a power of r, as we now show (in outline). First observe that m must be even and that we can choose a $GF(r)$-basis for L, $\phi(x_1), \phi(x_2), .., \phi(x_m)$ such that
$f(\phi(x_{2k-1}), \phi(x_{2k})) = 1$ if $1 \leq k \leq m/2$ and $f(\phi(x_i), \phi(x_j)) = 0$ for any other $i \leq j$. Given that $x_1^r = 1$, the minimum polynomial of x_1 on V is $x^r - 1$ and V can be decomposed into a direct sum $V_0 \oplus V_1 \oplus .. \oplus V_{r-1}$, where $x_1(v) = \lambda^i v$ for each $v \in V_i$ and each $0 \leq i < r$. Now $x_1^{-1}x_2^{-1}x_1x_2 = \lambda$ so for any $v \in V_i$, $x_1(x_2(v)) = \lambda x_2(x_1(v)) = \lambda^{i+1}x_2(v)$ and so $x_2(v) \in V_{i+1}$. Thus $\langle x_2 \rangle$ permutes $V_0, V_1, .., V_{r-1}$ transitively and the V_i's all have the same dimension. Suppose that $m = 2$. Then we can take a non-zero vector $v_0 \in V_0$ and find that the subspace spanned by $v_0, x_2(v_0), .., x_2^{r-1}(v_0)$ is invariant under x_1 and x_2 and hence invariant under N, but N is irreducible on V so these vectors must span V and therefore $n = r$. Now suppose that $m \geq 4$ and let $\hat{N} = \langle x_3, x_4, .., x_m \rangle$. Then $\hat{N}$ fixes V_0 so there is an irreducible subspace $\widehat{V_0}$ of V_0 under $\hat{N}$. We now construct the subspace $\hat{V} = \oplus_{i=0}^{r-1} x_2^i \hat{V_0}$ of V. This is invariant under $\hat{N}$ but also under x_1 and x_2 so is invariant under N. However N is irreducible on V, so $\hat{V} = V$ and therefore $\hat{V_0} = V_0$. This shows that $\hat{N}$ is irreducible on V_0.
An induction argument now applies: $dimV_0 = r^{(m-2)/2}$. Hence $dimV = r^{m/2}$.

3.8 Normalizers of Simple Groups

The groups we are left with are subgroups M of G such that any minimal normal subgroup of $\bar{M}$ is irreducible and simple. Let N be a pre-image of such a minimal normal subgroup and suppose that $\bar{N}$ is abelian. We may assume that N is absolutely irreducible, so $End_{KN}(V) = K$. Wedderburn's Density Theorem tells us that the ring generated by N is the set of all $n \times n$ matrices over K, but the only way in which this can happen with $\bar{N}$ abelian is if $n = 1$. This trivial case is generally omitted. Hence we may assume that $\bar{N}$ is non-abelian.

If we try and think of examples of such simple groups $\bar{N}$ we arrive at possibilities $PSL(n, q'), PSp(n, q'), P\Omega(n, q'), PSU(n, q')$ for various q' dividing q. There are two types of subgroup like this that we need to consider, exemplified by $PSL(n, q') \leq PSL(n, q)$ (with $GF(q')$ a subfield of $GF(q)$ of prime degree) and $PSp(n, q) \leq PSL(n, q)$. Thus M normalizes such a subgroup.

The remaining subgroups M have absolutely irreducible normal subgroups N such that $\bar{N}$ is non-abelian and simple and doesn't arise as in the previous paragraph.

3.9 Aschbacher's Theorem

We now have a formal statement of Aschbacher's Theorem ([1]). We begin with the definition of eight classes of subgroups. In the cases of alternating and hermitian forms, totally singular is often used to mean totally isotropic. The notation is similar to that used by Aschbacher. In particular O represents a standard classical group ($GL(n,q)$, $Sp(n,q)$, $O(n,q)$ or $U(n,q)$), and Γ represents the full semilinear group (preserving a form up to scalar multiples in the symplectic, orthogonal and unitary cases).

C_1 consists of the stabilizers of non-trivial proper subspaces U of V such that U is non-isotropic or totally singular, or U is a non-singular point of V in the case of the Orthogonal Group with q even. If U is non-isotropic, then U is not isometric to $U^{\perp}$.

C_2 consists of stabilizers of sets $\{U_1, U_2, .., U_k\}$ of subspaces of V such that $V = \oplus_{i=1}^{k} U_i$ and one of the following holds: (i) the sum is orthogonal and the U_i's are isometric; (ii) in the orthogonal case (with q odd) $k = 2$, $U_2 = U_1^{\perp}$, and U_1, U_2 are similar; (iii) $k = 2$, U_1, U_2 are totally singular of dimension $n/2$ and in the symplectic case q is odd when $n = 4$.

C_3 consists of the groups $N_\Gamma(F)$ where F varies over extension fields of K of prime index dividing n such that the K-space structure on V extends to an F-space structure and such that $C_0(F)$ is irreducible on V.

C_4 consists of the stabilizers of tensor product decompositions $U \otimes W$ where U, W are non-isometric K-spaces. In the symplectic case q is odd.

C_5 consists of the groups $N_\Gamma(U)K$ as F varies over the subfields of K of prime index r and U varies over the n-dimensional F-subspaces of V such that U is an absolutely irreducible $FN_O(U)$-module.

C_6 consists of the groups $N_\Gamma(R)$, where $n = r^m$ is a power of a prime $r \neq p$ and R varies over the groups of symplectic type such that $|R : Z(R)| = r^{2m}$, R is of exponent r if r is odd and of exponent 4 if $r = 2$, R acts irreducibly on V, and one of :(i) $|Z(R)| > 2$, $|K| = p^e$ where e is the order of p in the group of units of the integers modulo $|Z(R)|$, there is no form if e is odd, and the form is hermitian if e is even; (ii) the form is alternating, $|Z(R)| = 2$, $|K| = p$, and $R \approxeq (D_8)^{m-1}Q_8$; (iii) in the hyperbolic orthogonal case, $|Z(R)| = 2$, $|K| = p$, and $R \approxeq (D_8)^m$.

C_7 consists of the stabilizers of tensor product decompositions $V_1 \otimes V_2 \otimes .. \otimes V_k$ where the V_i's are similar. In the alternating case, q is odd. Also the group on each V_i must be quasi-simple.

C_8 consists of the stabilizers of forms $f(,)$ or Ψ on V with either: (i) (,) is the null form, and
$f(,)$ is alternating or hermitian, or q is odd and $f(,)$ is symmetric; (ii) $(,)$ is alternating, q is even, and Ψ is a quadratic form.

Theorem 1 *(Aschbacher)*

Let G be a finite group such that $G_0 \leq G \leq Aut(G_0)$ with G_0 a simple classical group. If $G_0 \approxeq P\Omega^+(8, q)$ assume that G contains no triality automorphism. Let H be a proper subgroup of G such that $G = HG_0$. Then either H is contained in one of $C_1 - C_8$ or the following hold:

(i) $H_0 \leq H \leq Aut(H_0)$ for some non-abelian simple group H_0;

(ii) Let L be the full covering group of H_0 and let V be the natural vector space on which L acts (such that the projective image of L is precisely H_0), then L is absolutely irreducible on V;

(iii) The representation of L on V is defined over no proper subfield of K;

(iv) If L fixes a form on V, then G_0 is the group $PSL(n, K), PSp(n, K), P\Omega(n, K)$ or $PSU(n, K)$ corresponding to the form.

3.10 Class C_1

The subgroups in this class are reducible, i.e., they fix a subspace. In this section we address a different aspect of the maximal subgroup problem. Aschbacher's Theorem tells us that a maximal subgroup lies in one of a number of classes, but it doesn't tell us directly which members of each class are maximal. One approach is to use Aschbacher's Theorem itself: if a member of one class is not maximal, then it lies in one of the eight classes or is almost simple. We can look at various properties of the eight classes (for example orders of subgroups) in an attempt to show that our group is not properly contained in a member of these classes, and then attempt to show that it cannot lie in an almost simple subgroup. We can attempt the latter with or without recourse to the Classification of
Finite Simple Groups (according to taste). We use this type of approach in the next Chapter. The object of this section is to see a geometric argument.

We assume here that $G = Sp(n, q)$ and M is a reducible subgroup. As we have already seen, if M stabilizes a subspace W of V, then M also stabilizes $W \cap W^\perp$. This leads us to conclude that we need only consider non-isotropic or totally isotropic subspaces. We consider a totally isotropic subspace W of dimension r and show that the full stabilizer M is indeed a maximal subgroup of G. The approach comes from [11].

The first thing to recollect is that G is generated by transvections. The approach we adopt is to show that any subgroup of G properly containing M

contains all the transvections in G. Suppose that $M < H \leq G$.

Given a vector $0 \neq v \in V$, a transvection ρ centred on v is given $\rho(x) = x + \lambda(v, x)v$ for some $0 \neq \lambda \in GF(q)$. We see immediately that if $v \in W^{\perp}$, then $\rho(w) = w$ for every $w \in W$. Therefore M contains any transvection centred on a vector in $W^{\perp}$.

M is given as the stabilizer of W and thus stabilizes $W^{\perp}$ (which contains W), so there appear to be at least three orbits of M on $V - \{0\}$, for M separates: non-zero vectors in W; vectors in $W^{\perp} - W$; and vectors in $V - W^{\perp}$. The appearance is only misleading if $W^{\perp} = W$, in which case $dimW = n/2$ (remember that $dimW^{\perp} = n - dimW$) and the second set is empty. We show that each of these sets is, in fact, an orbit. We make substantial use of Witt's Theorem.

Suppose that u_1, w_1 are non-zero vectors in W. Then we can extend to bases $u_1, u_2, .., u_r$ and $w_1, w_2, .., w_r$ for W and the map $\phi : W \to W$ given by $\phi(u_i) = w_i$ for each i is an invertible linear transformation from W to itself preserving $(,)$ $((u_i, u_j) = (w_i, w_j)$ for any $i, j)$. By Witt's Theorem ϕ extends to an element of G which, by its nature, stabilizes W, so lies in M. This shows that any two non-zero vectors of W lie in the same orbit of M. If $x, y \in W^{\perp} - W$ and $w_1, w_2, .., w_r$ is a basis for W, then the map $\theta : \langle w_1, w_2, .., w_r, x\rangle \to \langle w_1, w_2, .., w_r, y\rangle$ given by $\theta(w_i) = w_i, \theta(x) = y$ is an invertible linear transformation preserving $(,)$ and Witt's Theorem leads to an element of M taking x to y. If $x, y \in V - W^{\perp}$, then things are a touch more complicated: $\langle x\rangle^{\perp} \cap W$ has dimension $r - 1$ and we can construct a basis $u_1, u_2, .., u_{r-1}$; any extension to a
basis for W gives a vector u_r which is not orthogonal to x; we can choose a scalar multiple such that $(x, u_r) = 1$. In the same way we can find a basis $w_1, w_2, .., w_r$ for W such that $(y, w_i) = 0$ for $i < r$ and $(y, w_r) = 1$. Now the map $\psi : \langle u_1, u_2, .., u_r, x\rangle \to \langle w_1, w_2, .., w_r, y\rangle$ given by $\psi(u_i) = w_i, \psi(x) = y$ is an invertible linear transformation and Witt's Theorem leads to an element of M taking x to y. Hence there are exactly three orbits of M except when $r = n/2$ when there are two.

The first observation we make on these orbits is that H cannot stabilize W so cannot fix the first orbit. If there are just two orbits, then H is already transitive on non-zero vectors. If there are three orbits of M, then H cannot fix the union of the first two orbits, because they form the non-zero vectors in $W^{\perp}$ and the stabilizer of $W^{\perp}$ is the stabilizer of W. It is not difficult to find vectors in the second orbit which span $W^{\perp}$ and hence H cannot fix the second orbit. Hence in all case H is transitive on the non-zero vectors of V.

If v is any non-zero vector in V, $h \in H$ such that $h(v) \in W$ and ρ is a transvection centred on v (as given above) , then

$h\rho h^{-1}(x) = h(h^{-1}(x) + \lambda(h^{-1}(x), v).v) = x + \lambda(x, h(v)).h(v)$, a transvection centred on $h(v)$ and thus contained in M. Hence $h\rho h^{-1}, h \in H$ and it follows that H contains every transvection in G. Therefore $H = G$.

We have proved that M is a maximal subgroup of G. Notice that the proof applies without modification to arbitrary fields.

3.11 Application of Aschbacher's Theorem to Subgroups of $PSp(4, q)$, q even

Let us see what information we can derive about subgroups of $PSp(4, q)$ when q is even. The motivation for the question comes from two closely related ideas. The first was posed by Antonio Cossidente: a Singer cyclic group in $Sp(4, q)$ has order $q^2 + 1$ and there are such groups that intersect the Suzuki group in subgroups of size $q + \sqrt{2q} + 1$ and $q - \sqrt{2q} + 1$; these subgroups have orbit sizes $q + \sqrt{2q} + 1$ and $q - \sqrt{2q} + 1$, respectively, on the Suzuki ovoid; to what extent does something like this characterize the Suzuki ovoid? (Note that q is an odd power of 2, so $\sqrt{2q}$ exists.) If M preserves an ovoid and has subgroups having these orbit lengths, then $q^2 + 1$ divides the order of M. The second idea is that a group M acting transitively on an ovoid must also have order divisible by $q^2 + 1$. Thus we seek to identify subgroups of $Sp(4, q)$ whose order is divisible by $q^2 + 1$. We note at this point that $Sp(4, q)$ has order $q^4(q^2 - 1)^2(q^2 + 1)$.

The following are the classes of maximal subgroups of $Sp(4, q)$ with q even. This list comes, in the main, from ([12]).
Class C_1: A non-isotropic subspace would have dimension 2 and so be isometric to its conjugate; stabilizers of such subspaces lie inside subgroups in class C_2. This leaves totally isotropic subspaces of dimensions $1, 2$ (order $q^4(q-1)(q^2-1)$ in each case).

Class C_2: We have the stabilizer of a pair of 2-dimensional orthogonal non-isotropic subspaces (order $2q^2(q^2 - 1)^2$)

Class C_3: $Sp(2, q^2).2$ (order $2q^2(q^2 - 1)(q^2 + 1)$)

Class C_5: $Sp(4, q')$ where q' divides q (order $q'^4(q'^2 - 1)^2(q'^2 + 1)$).

Class C_8: The only possibilities here are orthogonal groups, one is the group of a hyperbolic quadratic form (order $2q^2(q^2 - 1)^2$) and the other is the group of an elliptic quadratic form (order $2q^2(q^2 - 1)(q^2 + 1)$).

$\mathcal{S}$: Almost simple subgroups (satisfying a number of further restrictions).

The classes C_4, C_6, C_7 don't occur here.

It is useful to have the following lemma.

Lemma 1 *Suppose that a, b are positive integers with $c = hcf(a, b)$. Then*

$$(2^a+1, 2^b+1) = 2^c+1 \text{ if } a/s, b/s \text{ are both odd, and } 1 \text{ otherwise;}$$
$$(2^a+1, 2^b-1) = 2^c+1 \text{ if } a/s \text{ is odd and } b/s \text{ is even, and } 1 \text{ otherwise;}$$
$$(2^a-1, 2^b-1) = 2^c-1.$$

Proof.
Exercise.

Theorem 2 *If M is a subgroup of $Sp(4, q)$ with q even such that q^2+1 divides the order of M, then either M stabilizes a spread of lines in $PG(3, q)$ or an elliptic ovoid in $PG(3, q)$, or M is almost simple.*

Proof.
The orders of the groups in classes C_1, C_2 and C_5, and the order of $O^+(4, q)$ are not divisible by $q^2 + 1$, so only C_3, one group in C_8, and $\mathcal{S}$ remain.

□

We now turn attention to papers by David Flesner ([8],[9],[10]). Here he addresses the question of maximal subgroups of $PSp(4, 2^a)$, in the main concentrating on subgroups containing central elations or non-centred skew elations. The first thing to note is that $PSp(4, 2^a)$ is isomorphic to $Sp(4, 2^a)$ so the theorems give us information about $Sp(4, 2^a)$; the second thing is that central elations are just the images of transvections in $PSp(4, 2^a)$ while non-centred skew elations are dual to elations, i.e., they are the images of elations under the outer automorphism of $PSp(4, 2^a)$ that we have met before. We need to note the first theorem, but for us it is the second which is more significant. Both theorems appear in the third paper but refer to ideas developed in the earlier papers.

Theorem 3 *(Flesner)*

The conjugacy classes of those maximal subgroups of $PSp(4, 2^a)$ which contain central elations or non-centred skew elations are as follows:

(a) *stabilizer of a point;*

(a^*) *stabilizer of a totally isotropic line;*

(b) *maximal index orthogonal group;*

(b^*) *stabilizer of a pair of hyperbolic lines;*

(c) non-maximal index orthogonal group;

(c^*) dual of non-maximal index orthogonal group;

(d_r) (for each prime r dividing a) stabilizer of subgeometry over the maximal subfield $GF(2^{a/r})$.

The second theorem comes at the end of [10] and it is only proper to note that Flesner gives an outline proof, because he feels that the theorem is not as complete as the previous one. However I have no reason to doubt the validity of the theorem.

Theorem 4 *(Flesner)*

If M is a maximal subgroup of $PSp(4, 2^a)$ which contains no central elations or non-centred skew elations, then either $q = 2$ and M is isomorphic to A_6, or M contains normal subgroups M_1 and M_2 such that $M \geq M_1 \geq M_2 \geq 1$, where M/M_1 and M_2 are of odd order, and M_1/M_2 is isomorphic to either $PSL(2, q')$ or $Sz(q')$ for some power q' of 2.

Flesner's first theorem gives subgroups in the main Aschbacher classes. It is the second theorem which addresses the question of almost simple subgroups.

Theorem 5 *If M is a maximal subgroup of $Sp(4, q)$ with $q > 2$ even such that q^2+1 divides the order of M, then one of the following occurs: (i) M stabilizes a spread of lines in $PG(3, q)$, (ii) M stabilizes an elliptic ovoid in $PG(3, q)$; (iii) $M_0 \leq M \leq Aut(M_0)$ for some subgroup $M_0 \approxeq PSL(2, q^2)$ or $Sz(q)$.*

Proof.
Suppose that M is a maximal subgroup of $Sp(4, q)$ (q even and greater than 2), with order divisible by $q^2 + 1$, not stabilizing a spread of lines in $PG(3, q)$ or an elliptic ovoid in $PG(3, q)$. Then M is almost simple and doesn't appear amongst the subgroups listed in Flesner's first theorem. Thus M contains normal subgroups M_1 and M_2 such that $M \geq M_1 \geq M_2 \geq 1$, where M/M_1 and M_2 are of odd order, and M_1/M_2 is isomorphic to either $PSL(2, q')$ or $Sz(q')$ for some power q' of 2. The term "almost simple" means that there is a non-abelian simple group M_0 such that $M_0 \leq M \leq Aut(M_0)$; in consequence M_0 is the unique minimal normal subgroup of M and any non-trivial normal subgroup of M contains M_0. The subgroup M_2 has odd order so cannot contain M_0 (any non-abelian simple group has even order) and therefore $M_2 = 1$ and $M_0 \leq M_1$. Now M_1/M_2 is simple so $M_1 = M_0 = PSL(2, q')$ or $Sz(q')$ for some power q' of 2 and $M \leq Aut(M_0)$. We write $q = 2^e$ and $q' = 2^f$.

Consider first the case where $M_0 \approxeq PSL(2, q')$. The order of M is $q'(q'^2 - 1)g$ for some divisor g of f. Let $s = (2e, 2f)$. One possibility is that $2e/s$ is even or $2f/s$ is odd, in which case $(2^{2e} + 1, 2^{2f} - 1) = 1$. Here $q'^2 - 1$ divides $(q^2 - 1)^2$

and so $q' < q^2$, but also $q^2 + 1$ divides $g < q' - 1$ so $q^2 < q'$ giving a contradiction. Therefore $2e/s$ is odd and $2f/s$ is even, so $(2^{2e} + 1, 2^{2f} - 1) = 2^s + 1$, $(2^{2e} - 1, 2^{2f} - 1) = 2^s - 1$. We have $q'^2 - 1$ divides $(q^2 - 1)^2(q^2 + 1)$ so $q'^2 - 1 \leq (2^s - 1)^2(2^s + 1) < 2^{3s} - 1$ and therefore $2f < 3s$. Given that $2f/s$ is even, we can only have $f = s$ and then $2e/f$ is odd. If $2e \geq 3f$, then $q^2 + 1 > q'^3 > (q'^2 - 1)g$, a contradiction. Thus we are left with just one possibility: $2e/f = 1$, i.e., $q' = q^2$ and $M_0 \approxeq PSL(2, q^2)$.

Now suppose that $M_0 \approxeq Sz(q')$. The automorphism group of $Sz(q')$ is $Sz(q').f$ so the order of M is $q'^2(q'^2+1)(q'-1)g$ for some divisor g of f. The significant facts are that q^2+1 divides $q'^2(q'^2+1)(q'-1)f$ and $q'^2(q'^2+1)(q'-1)$ divides $q^4(q^2-1)^2(q^2+1)$; we immediately deduce that q'^2 divides q^4, so that $f \leq 2e$, and that $q'^2 + 1$ divides either $q^2 + 1$ or $(q^2 - 1)^2$. Let $t = (2e, f)$. Then $(2e, 2f) = t$ or $2t$. If $(2e, 2f) = t$, then $2f/t$ is even, so $(2^{2e} + 1, 2^{2f} + 1) = 1$ and $(2^{2e} - 1, 2^{2f} + 1) = 1$, but then $q'^2 + 1$ cannot divide $q^2 + 1$ or $(q^2 - 1)^2$, a contradiction. On the other hand if $(2e, 2f) = 2t$, then $2e/t$ is even and therefore $(2^{2e} + 1, 2^f - 1) = 1$ and so $q^2 + 1$ divides $(q'^2 + 1)g$. However, $q > e$ so $q^2 + 1 > f \geq g$ and therefore $(2^{2e} + 1, 2^{2f} + 1) \neq 1$. It follows that $(2^{2e} - 1, 2^{2f} + 1) = 1$ and so $q'^2 + 1$ divides $q^2 + 1$. Hence $f = t$ and e/f is odd. Finally $q' > g$ so $q^2 + 1 < (q'^2 + 1)^{3/2}$ and therefore $e/f = 1$, i.e., $q' = q$. We have shown that $M_0 \approxeq Sz(q)$.

$\square$

Bibliography

[1] M.Aschbacher, On the maximal subgroups of the finite classical groups, Invent. Math., 76, 469-514, 1984.

[2] M.Aschbacher, Finite Group Theory, CUP, 1986.

[3] P.J.Cameron, Projective and polar spaces, QMW Maths Notes 13 (Queen Mary and Westfield College, University of London).

[4] A.H.Clifford, Representations induced on an invariant subgroup, Ann. Math. 38, 533-550, 1937.

[5] L.E. Dickson, Linear groups with an exposition of the Galois field theory, Teubner, 1901.

[6] J.Dieudonne, La geometrie des groupes classiques, (3rd ed.), Springer, 1971.

[7] J.Dieudonne, Sur les groupes classiques, Hermann, 1948.

[8] D.E.Flesner, Finite symplectic geometry in dimension four and characteristic two, Illinois J. Math. 19, 41- 47, 1975.

[9] D.E.Flesner, The geometry of subgroups of $PSp_4(2^n)$, Illinois J. Math. 19, 48- 70, 1975.

[10] D.E.Flesner, Maximal subgroups of $PSp_4(2^n)$ containing central elations or noncentered skew elations, Illinois J. Math. 19, 247- 268, 1975.

[11] O.H.King, Some maximal subgroups of the classical groups, J. Alg. 109-120, 1981.

[12] P.B. Kleidman, M.W. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Notes Series 129, Cambridge University Press, Cambridge 1990.

[13] S.Lang, Algebra, (3rd ed.), Addison-Wesley, 1993.

[14] T.Tamagawa, On the structure of orthogonal groups, Amer. J. Math. 80, 191-197, 1958.

[15] D.E.Taylor, The geometry of the classical groups, Heldermann (Berlin), 1992.

[16] J.A.Todd, As it might have been, Bull. London Math. Soc. 2, 1-4, 1969.